



Consorci
Administració Oberta
de Catalunya

Declaración de Prácticas de Certificación
Entidad de Certificación UNIVERSITATS I RECERCA


(EC-UR)

Referencia: D1111_E0650_N-DPC EC-UR

Versión: 7.0

Fecha: 05/08/2016

Control documental

Estado formal	Elaborat per: Servei de Certificació Digital	Aprovat per: Direcció del Consorci AOC
Fecha de creación	26/09/2006	
Control de versiones	Fecha:	05/08/2016
	Descripción:	Revisión Global – Integración de CATCert en Consorci AOC
Nivel de acceso información	pública	
Título	Declaración de Prácticas de Certificación – Entidad de Certificación UNIVERSITATS I RECERCA	
Fichero	D111 E0650 N-DPC EC-URv7r0 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	 <p>Esta obra está sujeta a una licencia Reconocimiento-No Comercial-Sin obras derivadas 3.0 España de Creative Commons. Para ver una copia, visitad http://creativecommons.org/licenses/by-nc-nd/3.0/es/deed.ca o enviad una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.</p>	

Índice

Índice.....	3
1. Introducción.....	11
1.1 PRESENTACIÓN.....	11
1.1.1 Tipos y clases de certificados.....	13
1.1.2. Relación entre la Declaración de Prácticas de Certificación (DPC) y otros documentos.....	20
1.2. NOMBRE DEL DOCUMENTO E IDENTIFICACIÓN.....	20
1.2.1. Identificación de este documento	20
1.2.2. Identificación de políticas de certificación cubiertas por esta DPC.....	21
1.3. COMUNIDAD DE USUARIOS DE CERTIFICADOS	23
1.3.1 Prestadores de servicios de certificación.....	23
1.3.2 Entidad de Certificación Raíz	24
1.3.3 EC-UR.....	24
1.3.4 Entidades de Registro	24
1.3.5 Usuarios finales.....	25
1.4. USO DE LOS CERTIFICADOS	26
1.3.6 Usos típicos de los certificados	26
1.4.2. Aplicaciones prohibidas.....	36
1.5 ADMINISTRACIÓN DE LA DECLARACIÓN DE PRÁCTICAS.	38
1.5.1 Organización que administra la especificación	38
1.5.2 Datos de contacto de la organización.....	38
1.5.3 Persona que determina la conformidad de una Declaración de Prácticas de Certificación (DPC) con la política	38
1.5.4 Procedimiento de aprobación.....	39
2. Publicación de información y directorio de certificados.....	40
2.1. DIRECTORIO DE CERTIFICADOS	40
2.2. PUBLICACIÓN DE INFORMACIÓN DE LA EC-UR	40
2.3. FRECUENCIA DE PUBLICACIÓN.....	40
2.4. CONTROL DE ACCESO.....	40
3. Identificación y autenticación.....	41
3.1. GESTIÓN DE NOMBRES.....	41
3.1.1. Tipos de nombres.....	41
3.1.2. Significado de los nombres	42
3.1.3. Utilización de anónimos y pseudónimos.....	42
3.1.4. Interpretación de formatos de nombres.....	42

3.1.5.	Unicidad de los nombres	42
3.1.6.	Resolución de conflictos relativos a nombres	42
3.2.	VALIDACIÓN INICIAL DE LA IDENTIDAD	42
3.2.1.	Prueba de posesión de clave privada	42
3.2.2.	Autenticación de la identidad de una organización	42
3.2.3.	Autenticación de la identidad de una persona física	42
3.2.4.	Información no verificada	43
3.3.	IDENTIFICACIÓN Y AUTENTICACIÓN DE SOLICITUDES DE RENOVACIÓN	44
3.3.1.	Validación para la renovación de certificados	44
3.3.2.	Validación para la renovación de certificados después de la revocación	44
4.	Características de operación del ciclo de vida de los certificados.....	45
4.1.	SOLICITUD DE EMISIÓN DE CERTIFICADO	45
4.1.1.	Legitimación para solicitar certificados	45
4.1.2.	Procedimiento de alta: Responsabilidades de la ER	46
4.2.	PROCESAMIENTO DE LA SOLICITUD DE CERTIFICACIÓN	47
4.2.1.	Certificados personales	47
4.2.2.	Requisitos específicos para el CEIXSA	49
4.2.3.	Informaciones adicionales para el CDS, el CDS-1 EV, el CDSCD y el CDS-1 Sede electrónica EV	49
4.2.4.	Informaciones adicionales para el CIPISR.....	49
4.2.5.	Otros certificados	49
4.3.	EMISIÓN DE CERTIFICADO	50
4.3.1.	Acciones de la EC-UR durante el proceso de emisión.....	50
4.3.2.	Comunicación de la emisión al suscriptor.....	50
4.4.	ACEPTACIÓN DEL CERTIFICADO	51
4.4.1.	Responsabilidades de la Entidad de Registro	51
4.4.2.	Conducta que constituye aceptación del certificado	52
4.4.3.	Publicación del certificado	52
4.4.4.	Notificación de la emisión a terceros	52
4.5.	USO DEL PAR DE CLAVES Y DEL CERTIFICADO	52
4.5.1.	Uso del par de claves por los poseedores de claves y uso de los certificados por los suscriptores	52
4.5.2.	Uso por el tercero que confía en los certificados	54
4.6.	RENOVACIÓN DE CERTIFICADOS SIN RENOVACIÓN DE CLAVES	54
4.7.	RENOVACIÓN DE CERTIFICADOS CON RENOVACIÓN DE CLAVES.....	55
4.8.	MODIFICACIÓN DE CERTIFICADOS.....	55
4.9.	REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS.....	55

4.9.1.	Causas de revocación de certificados	55
4.9.2.	Legitimación para solicitar la revocación	57
4.9.3.	Procedimientos de solicitud de revocación	57
4.9.4.	Plazo temporal de solicitud de revocación.....	58
4.9.5.	Plazo máximo de procesamiento de la solicitud de revocación	58
4.9.6.	Obligación de consulta de información de revocación de certificados	58
4.9.7.	Frecuencia de emisión de listas de revocación de certificados (LRCs).....	58
4.9.8.	Periodo máximo de publicación de LRCs	59
4.9.9.	Disponibilidad de servicios de comprobación de estado de certificados	59
4.9.10.	Obligación de consulta de servicios de comprobación de estado de certificados	59
4.9.11.	Otras formas de información de revocación de certificados	59
4.9.12.	Requisitos especiales en caso de compromiso de la clave privada	60
4.9.13.	Causas de suspensión de certificados	60
4.9.14.	Legitimación para solicitar la suspensión	60
4.9.15.	Procedimientos de solicitud de suspensión.....	61
4.9.16.	Período máximo de suspensión	61
4.9.17.	Habilitación de un certificado suspendido	61
4.10.	SERVICIOS DE COMPROBACIÓN DE ESTADO DE CERTIFICADOS	62
4.10.1.	Características de operación de los servicios	62
4.10.2.	Disponibilidad de los servicios	62
4.10.3.	Otras funciones de los servicios.....	62
4.11.	FIN DE LA SUSCRIPCIÓN	62
4.12.	DEPÓSITO Y RECUPERACIÓN DE CLAVES	62
4.12.1.	Política y prácticas de depósito y recuperación de claves.....	62
4.12.2.	Política y prácticas de encapsulamiento y recuperación de claves de sesión	62
5.	Controles de seguridad física, de gestión y de operaciones	64
5.1	CONTROLES DE SEGURIDAD FÍSICA	64
5.1.1	Localización y construcción de las instalaciones	64
5.1.2	Acceso físico	64
5.1.3	Electricidad y aire acondicionado	64
5.1.4	Exposición al agua	64
5.1.5	Advertencia y protección de incendios	64
5.1.6	Almacenaje de soportes	64
5.1.7	Tratamiento de residuos.....	64

5.1.8	Copia de seguridad fuera de las instalaciones	65
5.2	CONTROLES DE PROCEDIMIENTOS.....	65
5.2.1	Funciones fiables	65
5.2.2	Número de personas por tarea.....	65
5.2.3	Identificación y autenticación para cada función.....	65
5.2.4	Roles que requieren separación de tareas	65
5.3	CONTROLES DE PERSONAL	65
5.3.1	Requisitos de historial, calificaciones, experiencia y autorización.....	67
5.3.2	Requisitos de formación	67
5.3.3	Requisitos y frecuencia de actualización formativa.....	67
5.3.4	Secuencia y frecuencia de rotación laboral	67
5.3.5	Sanciones por acciones no autorizadas	67
5.3.6	Requisitos de contratación de profesionales	67
5.3.7	Suministro de documentación al personal	67
5.4	PROCEDIMIENTOS DE AUDITORÍA DE SEGURIDAD	67
5.4.1	Tipos de acontecimientos registrados	67
5.4.2	Frecuencia de tratamiento de registros de auditoría.....	67
5.4.3	Periodo de conservación de registros de auditoría	67
5.4.4	Protección de los registros de auditoría.....	68
5.4.5	Procedimientos de generación de copias de seguridad.....	68
5.4.6	Localización del sistema de acumulación de registros de auditoría.....	68
5.4.7	Notificación del acontecimiento de auditoría al causante del acontecimiento	68
5.4.8	Análisis de vulnerabilidades	68
5.5	ARCHIVO DE INFORMACIONES.....	68
5.5.1	Tipos de acontecimientos registrados	69
5.5.2	Periodo de conservación de registros.....	69
5.5.3	Protección del archivo	69
5.5.4	Procedimientos de generación de copias de seguridad.....	69
5.5.5	Requisitos de sellado de cautela de fecha y hora.....	69
5.5.6	Localización del sistema de archivo	69
5.5.7	Procedimientos de obtención y verificación de información de archivo.....	70
5.6	RENOVACIÓN DE CLAVES	70
5.7	COMPROMISO DE CLAVES Y RECUPERACIÓN DE DESASTRE	70
5.7.1	Procedimiento de gestión de incidencias y compromisos	70
5.7.2	Corrupción de recursos, aplicaciones o datos	70
5.7.3	Compromiso de la clave privada de la Entidad	70

5.7.4	Desastre sobre las instalaciones	70
5.8	FINALIZACIÓN DEL SERVICIO	71
5.8.1	EC-UR.....	71
5.8.2	Entidad de Registro.....	71
6.	Controles de seguridad técnica	72
6.1.	GENERACIÓN E INSTALACIÓN DEL PAR DE CLAVES.....	72
6.1.1.	Generación del par de claves	72
6.1.2.	Envío de la clave privada al suscriptor	73
6.1.3.	Envío de la clave pública al emisor del certificado.....	73
6.1.4.	Distribución de la clave pública del Prestador de Servicios de Certificación ..	73
6.1.5.	Medidas de claves.....	74
6.1.6.	Generación de parámetros de clave pública.....	74
6.1.7.	Comprobación de calidad de parámetros de clave pública	74
6.1.8.	Generación de claves en aplicaciones informáticas o en bienes de equipo...74	
6.1.9.	Propósitos de uso de claves.....	74
6.2.	PROTECCIÓN DE LA CLAVE PRIVADA.....	75
6.2.1.	Módulos de protección de la clave privada	75
6.2.2.	Control por más de una persona (n de m) sobre la clave privada	75
6.2.3.	Depósito de la clave privada.....	75
6.2.4.	Copia de seguridad de la clave privada	75
6.2.5.	Archivo de la clave privada.....	76
6.2.6.	Introducción de la clave privada en el módulo criptográfico	76
6.2.7.	Almacenaje de la clave privada en el módulo criptográfico.....	76
6.2.8.	Método de activación de la clave privada	76
6.2.9.	Método de desactivación de la clave privada	76
6.2.10.	Método de destrucción de la clave privada	76
6.2.11.	Clasificación de los módulos criptográficos	76
6.3.	OTROS ASPECTOS DE GESTIÓN DEL PAR DE CLAVES.....	77
6.3.1.	Archivo de la clave pública	77
6.3.2.	Periodos de utilización de las claves pública y privada.....	77
6.4.	DATOS DE ACTIVACIÓN	77
6.4.1.	Generación e instalación de los datos de activación	77
6.4.2.	Protección de los datos de activación.....	77
6.4.3.	Otros aspectos de los datos de activación.....	78
6.5.	CONTROLES DE SEGURIDAD INFORMÁTICA.....	78

6.5.1.	Requisitos técnicos específicos de seguridad informática	78
6.5.2.	Evaluación del nivel de seguridad informática	79
6.6.	CONTROLES TÉCNICOS DEL CICLO DE VIDA	79
6.6.1.	Controles de desarrollo de sistemas.....	79
6.6.2.	Controles de gestión de seguridad	79
6.6.3.	Evaluación del nivel de seguridad del ciclo de vida	79
6.7.	CONTROLES DE SEGURIDAD DE RED.....	79
6.8.	SELLO DE TIEMPO	80
7.	Perfiles de certificados y listas de certificados revocados.....	81
7.1	PERFIL DE CERTIFICADO	81
7.2	PERFIL DE LA LISTA DE REVOCACIÓN DE CERTIFICADOS	81
8.	Auditoría de conformidad	82
8.1	FRECUENCIA DE LA AUDITORÍA DE CONFORMIDAD	82
8.2	IDENTIFICACIÓN Y CALIFICACIÓN DEL AUDITOR.....	82
8.3	RELACIÓN DEL AUDITOR CON LA ENTIDAD AUDITADA	82
8.4	RELACIÓN DE ELEMENTOS OBJETO DE AUDITORÍA	82
8.5	ACCIONES A EMPRENDER COMO RESULTADO DE UNA FALTA DE CONFORMIDAD.....	82
8.6	TRATAMIENTO DE LOS INFORMES DE AUDITORÍA	83
9.	Requisitos comerciales y legales.....	84
9.1	TARIFAS.....	84
9.1.1	Tarifa de emisión o renovación de certificados.....	84
9.1.2	Tarifa de acceso a certificados	84
9.1.3	Tarifa de acceso a información de estado de certificado	84
9.1.4	Tarifas de otros servicios.....	84
9.1.5	Política de reintegro	84
9.2	CAPACIDAD FINANCIERA.....	84
9.2.1	Seguro de responsabilidad civil	84
9.2.2	Otros activos	84
9.2.3	Cobertura de aseguramiento para suscriptores y terceros que confíen en certificados	84
9.3	CONFIDENCIALIDAD	85
9.3.1	Informaciones confidenciales	85
9.3.2	Informaciones no confidenciales	85
9.3.3	Responsabilidad para la protección de información confidencial	85
9.4	PROTECCIÓN DE DATOS PERSONALES.....	85
9.4.1	Política de Protección de Datos Personales	85
9.4.2	Datos de carácter personal no disponibles a terceros	85
9.4.3	Datos de carácter personal disponibles a terceros	85
9.4.4	Responsabilidad correspondiente a la protección de los datos personales ...	85

9.4.5	Gestión de incidencias relacionadas con los datos de carácter personal.....	86
9.4.6	Prestación del consentimiento en el uso de los datos personales	86
9.4.7	Comunicación de datos personales.....	86
9.5	DERECHOS DE PROPIEDAD INTELECTUAL.....	86
9.5.1	Propiedad de los certificados e información de revocación	86
9.5.2	Propiedad de la política de certificado y Declaración de Prácticas de Certificación.....	86
9.5.3	Propiedad de la información relativa a nombres.....	86
9.5.4	Propiedad de claves.....	86
9.6	OBLIGACIONES Y RESPONSABILIDAD CIVIL.....	87
9.6.1	Entidades de Certificación.....	87
9.6.2	Obligaciones y otros compromisos de las Entidades de Registro.....	87
9.6.3	Garantías ofrecidas a suscriptores y verificadores	87
9.6.4	Suscriptores	87
9.6.5	Verificadores	88
9.6.6	Otros participantes	88
9.7	RENUNCIAS DE GARANTÍAS	88
9.7.1	Rechazo de garantías de la EC-UR.....	88
9.8	LIMITACIONES DE RESPONSABILIDAD	88
9.8.1	Limitaciones de responsabilidad de la EC-UR.....	88
9.8.2	Caso fortuito y fuerza mayor.....	89
9.9	INDEMNIZACIONES	89
9.9.1	Cláusula de indemnidad de suscriptor.....	89
9.9.2	Cláusula de indemnidad de verificador.....	89
9.10	PLAZO Y FINALIZACIÓN.....	89
9.10.1	Plazo	89
9.10.2	Finalización	89
9.10.3	Supervivencia.....	89
9.11	NOTIFICACIONES	89
9.12	MODIFICACIONES	90
9.12.1	Procedimiento para las modificaciones	90
9.12.2	Periodo y mecanismos para notificaciones.....	90
9.12.3	Circunstancias en las que un OID tiene que ser cambiado.....	90
9.13	RESOLUCIÓN DE CONFLICTOS.....	90
9.13.1	Resolución extrajudicial de conflictos	90
9.13.2	Jurisdicción competente.....	90

9.14	LEY APLICABLE	90
9.15	CONFORMIDAD CON LA LEY APLICABLE	90
9.16	CLÁUSULAS DIVERSAS	90
9.16.1	Acuerdo íntegro.....	90
9.16.2	Subrogación	91
9.16.3	Divisibilidad	91
9.16.4	Aplicaciones	91
9.16.5	Otras cláusulas.....	91
ANEXO – Control documental		92
	CONTROL DE VERSIONES DPC EC-UR 1ER SEMESTRE 2016	92

1. Introducción

Este documento es la Declaración de Prácticas de Certificación de la Entidad de Certificación 'Universitats i Recerca' (en adelante EC-UR, Entidad de Certificación del Parlament de Catalunya).

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

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

1.1 Presentación

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

En cumplimiento de dicho pacto institucional y para desarrollar el programa Catalunya en Xarxa (Cataluña en Red), Localret y la Generalitat de Catalunya acordaron la creación del Consorci per a l'Administració Oberta Electrònica de Catalunya (Consortio 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 Electrònica 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 emitieran para 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 catalanas.

Actualmente existen nueve entidades de certificación vinculadas a la jerarquía pública de certificación de las administraciones públicas catalanas: EC-GENCAT, EC-SAFP, EC-PARLAMENT, EC-idCAT, EC-AL, EC-UR, EC-URV, EC-SectorPublic y EC-Ciudadania. El Departamento de Universidades, Investigación y Sociedad de la Información (DURSI), la Fundación Catalana para la Investigación y la Innovación (FCRI), las universidades públicas (UB, UAB, UPC, UPF, UdG, URV y UdL), la universidad no presencial (UOC), la Asociación Catalana de Entidades de Investigación (ACERO), la Administración Abierta de Cataluña (AOC), la Agencia Catalana de Certificación (CATCert) y el Centro de Supercomputación de Cataluña (CESCA), firmaron un convenio el 23 de octubre de 2003 con el objetivo que las universidades y centros de investigación incorporen la firma electrónica para incrementar la seguridad de sus comunicaciones telemáticas.

El 17 de diciembre de 2003 se creó la Entidad de Certificación Vinculada a la jerarquía de entidades de certificación de las entidades públicas de Cataluña, denominada de Universidades e Investigación (EC-UR), gestionada por el CESCA, en su consideración de Entidad de Certificación Virtual. Ésta permite a las instituciones adheridas al Anillo Científico obtener certificados digitales corporativos de clase 1, tanto para su personal, como para su hardware y para la misma Institución (certificados de entidad).

Al surgir la necesidad de dotar de firma electrónica a los estudiantes, se amplía la emisión de certificados con la inclusión de los certificados de estudiantes que son de clase 2 de colectivo.

El conjunto de funciones de colaboración y soporte del CESCA a las instituciones en la gestión de las funciones de emisión técnica, administración, suspensión, habilitación, revocación y renovación de certificados forman la Entidad de Registro, también denominada Entidad de Registro de Universidades e Investigación (ER-UR). También existe la posibilidad que las instituciones suscriptoras de los certificados de la Entidad de Certificación y, cuando sea necesario, de las Entidades de Certificación Vinculadas a la misma, puedan actuar como Entidades de Registro.

Las instituciones actúan como suscriptores de los certificados y aportan la información de registro, debidamente comprobada, con la diligencia de una Entidad de Registro Virtual de la EC-UR o como hemos indicado, realizan el registro como Entidad de Registro. También realizan la validación y la aprobación interna y previa de las solicitudes de certificados y, cuando sea necesario, solicitan la suspensión, revocación o renovación de certificados.

Además se regula la posibilidad de uso, por las entidades de certificación, de nuevas tarjetas con la consideración de dispositivo de creación de firma electrónica, con funcionalidades avanzadas, como la autenticación con biometría, y el procedimiento para su aceptación por la Entidad de Certificación.

Por otro lado, el Acuerdo de Gobierno de 16 de octubre de 2013 asigna la prestación de servicios de certificación al Consorci Administració Oberta de Catalunya (AOC), como

medida de racionalización del sector público, que se concreta en la integración de la Agència Catalana de Certificació en el Consorci AOC, en el cual revertirán todas las marcas, derechos, deberes y servicios gestionados hasta la fecha por CATCert.

La integración se hizo efectiva 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-URha definido una tipología de servicios de certificación que le permiten emitir certificados digitales para diversos usos y usuarios finales diferentes.

Los certificados de usuarios finales se dividen en:

- Certificados de infraestructura, caracterizados por el hecho de que el poseedor de la clave privada es un operador de una infraestructura, y que se utiliza para autorizar operaciones relacionadas con los servicios de certificación, como la aprobación de solicitudes de certificación.
- Certificados personales, caracterizados por el hecho de que el poseedor de la clave privada es una persona física, que en certificados de clase 1 actúa habitualmente en representación o por cuenta de una persona jurídica.
- Certificados de entidad, caracterizados por el hecho que el suscriptor del certificado y de acuerdo con la ley, el firmante, es una persona jurídica que actúa por medio de un poseedor de claves.
- Certificados de dispositivo, caracterizados por el hecho de que no hay un poseedor de la clave privada sino que son utilizados por dispositivos informáticos, que en certificados de clase 1 se encuentran bajo la responsabilidad de una persona jurídica.

Los certificados de clase 1 son, por tanto, certificados corporativos, caracterizados por el hecho de que la persona física tiene una vinculación con el suscriptor del certificado, que es una persona jurídica. Habitualmente el suscriptor actúa como entidad de registro de los certificados, aunque no es estrictamente necesario.

El resto de certificados son certificados de clase 2. El registro de los datos para la emisión de los certificados de clase 2 lo realiza siempre la Entidad de Certificación o una entidad de registro bajo la responsabilidad de la entidad de certificación, mediante la certificación administrativa previa de los datos, cuando la emisión se dirija a un público restringido, o mediante la captación directa de toda la información necesaria para la emisión de certificados.

La Entidad de Certificación podrá emitir los siguientes tipos de certificados:

1.1.1.1 Certificados de infraestructura

- Certificado de infraestructura personales de identificación y firma electrónica reconocida de operadores (CIPISR), que se usa para autorizar operaciones

relacionadas con los servicios de certificación, como la aprobación de solicitudes de certificación.

- Certificado de infraestructura de entidad de certificación vinculada (CIC), que se expide a las entidades de certificación de las instituciones, con nivel 3, ya que la Entidad que los firma es de nivel 2.
- Certificado de infraestructura de dispositivo servidor seguro (CIDS), que es utilizado por una aplicación informática servidor de SSL o de TLS de infraestructura para identificarse ante las aplicaciones cliente que se conectan y para proteger el secreto de las comunicaciones entre el cliente y el servidor, como por ejemplo los servidores de las entidades de certificación.
- Certificado de infraestructura de dispositivo de aplicación digitalmente asegurada (CIDA), que es utilizado por aplicaciones informáticas de la infraestructura que se identifican digitalmente, firman electrónicamente webservices u otros protocolos y que reciben documentos y mensajes cifrados, como por ejemplo las aplicaciones de notificación de mensajes de las entidades de certificación.
- 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.
- Certificado de infraestructura de entidad de sellos de tiempo (CIT), que es utilizado por una entidad para firmar los sellos de tiempo que emite.
- Certificado de infraestructura de entidad de validación (CIV), que es utilizado por un servidor de entidad de validación para firmar sus informes.

1.1.1.2. Certificados personales

La EC-UR emite los siguientes tipos de certificados personales:

- Certificados personales de identidad y de firma electrónica reconocida de clase 1 con cargo (CPISR-1 Cargo), que identifican a la persona que los posee, a su organización suscriptora, y su cargo en la misma, y que sirven para firmar mensajes con dispositivo seguro de creación de firma, así como mensajes de autenticación y de acceso seguro a sistemas informáticos.
- Certificados personales de identidad y de firma electrónica reconocida de clase 1 con cargo para extranjeros (CPISR-1 con Cargo Extranjero), que identifican a la persona que los posee, su organización suscriptora, y su cargo en ésta, y que sirven para firmar mensajes con dispositivo seguro de creación de firma, así como mensajes de autenticación y de acceso seguro a sistemas informáticos.
- Certificados personales de identificación y firma electrónica reconocida de clase 1 con cargo para uso concreto (CPISR-1 con Cargo uso), que identifican a la persona que los posee, la organización suscriptora, el cargo en la misma, y las limitaciones materiales de uso, y que sirven para firmar mensajes con dispositivo seguro de creación de firma, así como mensajes de autenticación y de acceso seguro a sistemas informáticos.
- Certificados personales de identificación y de firma electrónica reconocida de clase 2 con cargo (CPISR-2 Cargo), que identifican la persona que los posee, la organización suscriptora, y el cargo en la misma, y que sirven para firmar mensajes con dispositivo seguro de creación de firma, así como mensajes de autenticación y acceso seguro a sistemas informáticos.

- Certificados personales de cifrado de clase 1 con cargo (CPX-1 Cargo), que identifican a la persona que los posee, a su organización suscriptora, y su cargo en la misma, y que se utilizan para recibir o producir mensajes o documentos confidenciales, en cualquier formato. No permiten la firma electrónica de mensajes de datos .
- Certificados personales de cifrado de clase 2 con cargo (CPX-2 Cargo), que identifican a la persona que los posee, a su organización suscriptora, y su cargo en la misma, y que se utilizan para recibir o producir mensajes. o documentos confidenciales, en cualquier formato. No permiten la firma electrónica de mensajes de datos.
- Certificados personales de identidad y de firma electrónica reconocida de clase 2 para estudiantes (CPISR-2 de Estudiante), que identifican a la persona que los posee, a su organización suscriptora, y su condición de estudiante, y que sirven para firmar mensajes con dispositivo seguro de creación de firma, así como mensajes de autenticación y de acceso seguro a sistemas informáticos.
- Certificados personales de identidad y de firma electrónica reconocida de clase 2 para estudiantes extranjeros (CPISR-2 de Estudiante Extranjero), que identifican a la persona que los posee, su organización suscriptora, y su condición de estudiante, y que sirven para firmar mensajes con dispositivo seguro de creación de firma, así como mensajes de autenticación y de acceso seguro a sistemas informáticos.
- Certificados personales de cifrado de clase 2 para estudiantes (CPX-2 de Estudiante), que identifican a la persona que los posee, a su organización suscriptora, y su condición de estudiante, y que se utilizan para recibir, y producir mensajes confidenciales.
- Certificados personales de cifrado de clase 2 para estudiante extranjero (CPX-2 de Estudiante Extranjero), que identifican a la persona que los posee, su organización suscriptora, y su condición de estudiante, y que se utilizan para recibir, y producir mensajes confidenciales.
- Certificados personales de identificación, cifrado y firma avanzada con cargo de empleado público de clase 1 (CPIXSA-1Cargo EP), que identifican la persona que los posee, su organización suscriptora, y que sirven para firmar mensajes de autenticación y de acceso seguro a sistemas informáticos.

El certificado personal de identificación y firma reconocida de clase 1 con cargo (CPISR-1 con cargo), y el certificado de identificación y de firma electrónica reconocida de clase 1 con cargo para uso concreto (CPISR-1 Cargo Uso), son certificados reconocidos de acuerdo con lo establecido en el artículo 11.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, con el contenido prescrito por el artículo 11.2, y emitidos cumpliendo las obligaciones de los artículos 12, 13, 18 y 20 de la mencionada Ley. Funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones. Garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permite la generación de la "firma electrónica reconocida"; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada utilizando un dispositivo seguro, por lo cual, de conformidad con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplimiento de requisito alguno adicional. Además de eso, incluye una manifestación

relativa a la categoría de personal y cargo del poseedor de claves, que ha sido comprobada antes de emitir el certificado, y es correcta. Sin embargo, esta indicación no es, por sí sola, suficiente para determinar las facultades que tiene el poseedor de claves para firmar en nombre del suscriptor; por lo tanto, el usuario del certificado tendrá que comprobar las facultades y poderes de firma del poseedor mediante otros medios, diferentes al certificado. También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, sino sólo la identificación del poseedor de claves en nombre de la institución.

El certificado personal de identificación y de firma electrónica reconocida de clase 2 con cargo (CPISR-2 Cargo), es un certificado reconocido de conformidad con lo establecido en el artículo 11.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, con el contenido prescrito por el artículo 11.2, y emitido cumpliendo las obligaciones de los artículos 12, 13, 18 y 20 de la Ley referenciada. Funciona con dispositivo seguro de creación de firma electrónica, de conformidad con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones. Garantiza la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permite la generación de la "firma electrónica reconocida"; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada utilizando un dispositivo seguro, por lo cual, de conformidad con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplimiento alguno de requisito adicional. Además incluye una manifestación relativa al cargo del poseedor de claves, que ha sido comprobada antes de emitir el certificado, y es correcta. Aun así, esta indicación no es, por sí sola, suficiente para determinar las facultades que tiene el poseedor de claves para firmar en nombre del suscriptor; por ello, el usuario del certificado ha de comprobar las facultades y poderes de firma del poseedor mediante otros medios, diferentes del certificado. También puede ser utilizado en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, sino sólo la identificación del poseedor de claves, en nombre de la Institución.

El certificado personal de cifrado de clase 1 con cargo (CPX-1 Cargo) es un certificado reconocido de conformidad con lo que se establece en el artículo 6 y 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica. Funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y cumple lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones. Garantiza la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permite cifrar documentos y recibir mensajes de datos confidenciales, en cualquier formato. Además incluyen una manifestación relativa a la categoría de personal y cargo del poseedor de claves, que ha sido comprobada antes de emitirse el certificado, y es correcta. Sin embargo, esta indicación no es, por sí sola, suficiente para determinar las facultades que tiene el poseedor de claves para firmar en nombre del suscriptor; por tanto, el usuario del certificado comprueba las facultades y poderes de firma del poseedor de claves por otros medios, diferentes del certificado. También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, sino solamente la identificación del poseedor de claves, en nombre de la institución.

El certificado personal de identificación y firma reconocida de clase 2 para estudiantes (CPISR-2 de Estudiante), y el certificado personal de identificación y firma de clase 2 para estudiantes extranjeros (CPISR-2 de Estudiante Extranjero), son certificados reconocidos de acuerdo con lo establecido en el artículo 11.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, con el contenido prescrito por el artículo 11.2, y emitidos cumpliendo las obligaciones de los artículos 12, 13, 18 y 20 de la mencionada Ley. Funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones. Garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permiten la generación de la "firma electrónica reconocida"; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada utilizando un dispositivo seguro, por lo cual, de conformidad con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplimiento de requisito alguno adicional. Además, incluyen una manifestación relativa a la condición de estudiante adscrito a un centro del suscriptor del certificado, que ha sido comprobada antes de emitir el certificado, y es correcta. Esta indicación no es, por sí sola, suficiente para determinar las facultades que tiene el poseedor de claves para firmar en nombre del suscriptor; por tanto, el usuario del certificado comprueba las facultades y poderes de firma del poseedor mediante otros medios, distintos del certificado. También se puede utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, sino sólo la identificación del poseedor de claves.

El certificado personal de cifrado de clase 2 para estudiante (CPX-2 de Estudiante), y el certificado personal de cifrado de clase 2 para estudiante extranjero (CPX-2 de Estudiante Extranjero), son certificados reconocidos de conformidad con lo que se establece en el artículo 6 y 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica. Funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y que cumplen lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones. Garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permiten cifrar documentos y recibir mensajes de datos confidenciales, en cualquier formato.

El certificado personal de cifrado de clase 2 con cargo (CPX-2 Cargo) es un certificado reconocido de conformidad con lo que se establece en el artículo 6 y 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica. Funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y cumple lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones. Garantiza la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permite cifrar documentos y recibir mensajes de datos confidenciales, en cualquier formato.

El certificado personal de identificación, cifrado y firma avanzada, con cargo, de empleado público, de clase 1 (CPIXSA-1Cargo EP) es un certificado reconocido de conformidad con lo establecido con los artículos 6 y 11.1, con el contenido prescrito en el artículo 11.2 y emitido cumpliendo las obligaciones de los artículos 12, 13 y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica. Garantiza la identidad del suscriptor y el poseedor de

la clave privada de identificación y firma, y permite la generación de la “firma electrónica avanzada”.

1.1.1.3. Certificados de entidad

La EC-UR emite los siguientes tipos de certificados de entidad:

- Certificados de entidad de firma electrónica reconocida de clase 1 (CEISR-1), de acuerdo con lo establecido en el artículo 7 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, que permite que Instituciones públicas y privadas, corporaciones de derecho público y personas jurídico-públicas (colectivamente denominadas “entidades”) firmen documentos con dispositivo seguro de creación de firma, mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos.
- Certificados de entidad de cifrado de clase 1 (CEX-1), de acuerdo con lo establecido en el artículo 7 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, que permite que Instituciones públicas y privadas, corporaciones de derecho público y personas jurídico-públicas (colectivamente denominadas “entidades”) puedan cifrar o recibir mensajes de datos confidenciales, en cualquier formato.
- Certificados de entidad de identificación, cifrado y firma electrónica avanzada (CEIXSA) de acuerdo con lo establecido en el artículo 7 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, que permite que Instituciones públicas y privadas, corporaciones de derecho público y personas jurídico-públicas (colectivamente denominadas “entidades”) firmen documentos electrónicamente, mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos y puedan cifrar y recibir mensajes de datos y documentos confidenciales, en cualquier formato.

Adicionalmente, en función de los requerimientos técnicos y de las necesidades de los usuarios, es posible que estos tipos de certificados puedan incorporar otras funcionalidades que, en todo caso, serán identificadas en una política específica de certificación que será desarrollada o aprobada por el Consorci AOC.

1.1.1.4. Certificados de dispositivo

La EC-UR emite los siguientes tipos de certificados de dispositivo:

- Certificado de dispositivo servidor seguro de clase 1 (CDS-1), que se utiliza por una aplicación informática, servidor de SSL o de TLS, para identificarse ante las aplicaciones cliente que se conectan y para proteger el secreto de las comunicaciones entre el cliente y el servidor.
- Certificado de dispositivo servidor seguro de clase 1 Extended Validation (CDS-1 EV), que se utiliza por una aplicación informática, servidor de SSL o de TLS, para que se identifique ante las aplicaciones cliente que se conectan y para proteger el secreto de las comunicaciones entre el cliente y el servidor, ofreciendo la validación automática en el navegador.
- Certificado de dispositivo de sede electrónica nivel medio de clase 1 Extended Validation (CDS-1 SENMEV), que sirve para identificar y garantizar una comunicación segura con la sede electrónica de un ente, entendiéndose sede

electrónica en los términos del artículo 10 de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.

Este certificado puede utilizarse para la conexión segura de los ciudadanos a páginas web oficiales, la autenticación de un lugar web, el alojamiento de registros electrónicos, la consulta y autorización de registros de representación, etc, ofreciendo la validación automática en el navegador.

El certificado de nivel medio, con unas claves de 1024 bits, es recomendable para la mayoría de las administraciones públicas con previsión de los siguientes riesgos: infracción de seguridad (por ejemplo, robo de la identidad), pérdidas económicas moderadas, pérdida de información sensible o crítica, o refutación de una transacción con impacto económico significativo.

El certificado de nivel medio se entregará en soporte software.

- Certificado de dispositivo de sede electrónica nivel alto de clase 1 Extended Validation (CDS-1 SENA EV), que sirve para identificar y garantizar una comunicación segura con la sede electrónica de un ente, entendiéndose sede electrónica en los términos del artículo 10 de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.

Este certificado puede utilizarse para la conexión segura de los ciudadanos a páginas web oficiales, la autenticación de un lugar web, el alojamiento de registros electrónicos, la consulta y autorización de registros de representación, etc, ofreciendo la validación automática en el navegador.

El certificado de nivel alto, con unas claves de 2048 bits, es recomendable para aquellas administraciones públicas que, habiendo realizado previamente un análisis de riesgos, precisan medidas adicionales de seguridad, al contemplar los siguientes riesgos: infracción de seguridad, pérdidas económicas importantes, pérdida de información altamente sensible y crítica o refutación de una transacción con impacto económico muy significativo.

El certificado de nivel alto deberá ser almacenado en un HSM (hardware criptográfico).

- Certificado de dispositivo seguro de controlador de dominio de clase 1 (CDSCD-1), se utiliza por una aplicación informática, servidor SSL o TLS, para autenticar en una red Windows a los usuarios que pertenecen a un determinado dominio, mediante un certificado digital de firma con tarjeta criptográfica.
- Certificado de dispositivo de aplicación (CDA), que almacenado en un servidor y requerido por una aplicación, firma documentos o mensajes.
- Certificado de dispositivo de sello electrónico de Administración, órgano o entidad de derecho público nivel medio de clase 1 (CDA-1 SENM), se utiliza para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada, en los términos descritos en el artículo 18 de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.

El certificado de nivel medio, con unas claves de 1024 bits, es recomendable para la mayoría de las administraciones públicas que pueden tener los siguientes riesgos: infracción de seguridad (p.ex. robo de la identidad), pérdidas económicas moderadas, pérdida de información sensible o crítica o refutación de una transacción con impacto económico significativo.

- Certificado de dispositivo de sello de Administración, órgano o entidad de derecho público nivel alto de clase 1 (CDA-1 sello nivel alto), se utiliza para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada, en los términos descritos en el artículo 18 de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.

Este certificado puede utilizarse para el intercambio de datos entre administraciones, la identificación y autenticación de un sistema, servicio web o aplicación, el archivo electrónico automatizado, las compulsas y copias electrónicas, entre otros.

El certificado de nivel alto, con unas claves de 2048 bits, es recomendable para aquellas administraciones públicas que, habiendo realizado previamente un análisis de riesgos, precisan medidas adicionales de seguridad, ya que contemplan los siguientes riesgos: infracción de seguridad, pérdidas económicas importantes, pérdida de información altamente sensible y crítica o refutación de una transacción con impacto económico muy significativo.

El certificado de sello electrónico de nivel alto se cargará directamente en la PSIS (Plataforma de servicios de identificación y firma), al menos mientras no se disponga del hardware criptográfico HSM necesario para el nivel de seguridad requerido.

- Certificado de dispositivo de firma de aplicaciones informáticas de clase 1 (CDP-1), que se utiliza para firmar electrónicamente las aplicaciones informáticas o software a transmitir por medio de internet. Así los usuarios finales pueden firmar documentos como applets, scripts, ejecutables, etc.

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-UR.

La EC-UR emite certificados dentro de la jerarquía de certificación operada por el Consorci AOC. Por tanto, dispone de una Declaración de Prácticas de Certificación (DPC) de acuerdo con la Política General de Certificación del Consorci AOC.

Esta DPC incluye los procedimientos que aplica la EC-UR 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-UR”.

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

1.3.6.1.4.1.15096.1.2.7

1.2.2. Identificación de políticas de certificación cubiertas por esta DPC

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

- **CIPISR** – Certificado de infraestructura de operador, emitido por la EC-UR
Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.15
Clase 2. OID: 1.3.6.1.4.1.15096.1.3.1.16
- **CIC** – Certificado de infraestructura de Entidad de Certificación Vinculada, emitido por la EC-UR
CIC-1. OID: 1.3.6.1.4.1.15096.1.3.1.11
CIC-2. OID: 1.3.6.1.4.1.15096.1.3.1.12
CIC-3. OID: 1.3.6.1.4.1.15096.1.3.1.13
- **CIDS-1** – Certificado de infraestructura de servidor seguro, emitido por la EC-UR
Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.17
- **CIDA-1** – Certificado de infraestructura de aplicación, emitido por la EC-UR
Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.18
- **CIO-1** – Certificado de infraestructura de servidor de estado de certificados en línea, emitido por la EC-UR
Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.19
- **CIV-1** – Certificado de infraestructura de entidad de validación, emitido por la EC-UR
Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.20
- **CIT-1** – Certificado de infraestructura de entidad de sellos de tiempo, emitido por la EC-UR
Clase 1. 1.3.6.1.4.1.15096.1.3.1.111
- **CPISR-1 Cargo** – Certificado personal de identificación y firma electrónica reconocida con cargo, emitido por la EC-UR
Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.81.2.1
- **CPISR-1 con Cargo Extranjero** – Certificado personal de identificación y firma electrónica reconocida con cargo por extranjeros, emitido por la EC-UR
Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.81.1.1
- **CPISR-1 con Cargo Uso** – Certificado personal de identificación y firma electrónica reconocida con cargo para uso concreto, emitido por la EC-UR
Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.81.3.3
- **CPX Cargo** – Certificado personal de cifrado con cargo, emitido por la EC-UR
Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.41.1.1

Clase 2. OID: 1.3.6.1.4.1.15096.1.3.1.42.3.1

- **CPX-1 con Cargo Extranjero** – Certificado personal de cifrado con cargo para extranjeros, emitido por la EC-UR

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.41.2.1

- **CPISR-2 con Cargo** – Certificado personal de identificación y firma electrónica reconocida con cargo, emitido por la EC-UR

Clase 2. OID: 1.3.6.1.4.1.15096.1.3.1.82.3.1

- **CPISR-2 de Estudiante** – Certificado personal de identificación y firma electrónica reconocida, de estudiante, emitido por la EC-UR

Clase 2. OID: 1.3.6.1.4.1.15096.1.3.1.82.2.1

- **CPISR-2 de Estudiante Extranjero** - Certificado personal de identificación y firma electrónica reconocida para estudiantes extranjeros, emitido por la EC-UR

Clase 2. OID: 1.3.6.1.4.1.15096. 1.3.1.82.2.3

- **CPX-2 de Estudiante** – Certificado personal de cifrado de estudiante, emitido por la EC-UR

Clase 2. OID: 1.3.6.1.4.1.15096.1.3.1.42.2.1

- **CPX-2 de Estudiante Extranjero** - Certificado personal de cifrado de estudiante extranjero, emitido por la EC-UR

Clase 2. OID: 1.3.6.1.4.1.15096.1.3.1.42.2.3

- **CPIXSA-1 Cargo EP** – Certificado personal de identificación, cifrado y firma electrónica avanzada con cargo de empleado público, emitido por la EC-UR

OID: 1.3.6.1.4.1.15096.1.3.1.85

- **CEISR-1** – Certificado de entidad de identificación y firma electrónica reconocida, emitido por la EC-UR

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.121.3

- **CEX-1** – Certificado de entidad de cifrado, emitido por la EC-UR

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.131.3

- **CEIXSA-1** – Certificados de entidad de identificación, cifrado y firma electrónica avanzada emitido por la EC-UR

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.161.3

- **CDS-1** – Certificado de dispositivo servidor seguro, emitido por la EC-UR

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.51

- **CDS-1EV** - Certificado de dispositivo servidor seguro Extended Validation, emitido por la EC-UR

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.4

- **CDS-1 SENM EV**– Certificado de dispositivo servidor seguro, sede electrónica nivel medio Extended Validation emitido por la EC-UR

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.2

- **CDS-1 SENA EV**- Certificado de dispositivo servidor seguro, sede electrónica nivel alto Extended Validation emitido por la EC-UR

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.3

- **CDA-1** – Certificado de dispositivo de aplicación digitalmente asegurada, emitido por la EC-UR

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.91

- **CDA-1 SENM** -Certificado de dispositivo de aplicación digitalmente asegurada, sello electrónico nivel medio emitido por la EC-UR

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.91.1

- **CDA-1 SENA** -Certificado de dispositivo de aplicación digitalmente asegurada, sello electrónico nivel alto emitido por la EC-UR

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.91.2

- **CDP-1** – Certificado de dispositivo de firma de software, emitido por la EC-UR.

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.71

- **CDSCD-1** - certificado de dispositivo seguro de controlador de dominio, emitido por la EC-UR.

Clase 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.1

Los documentos descriptivos de estos perfiles de certificados se publican en la 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 diversas relaciones administrativas y privadas, de acuerdo con la Ley 59/2003 y la normativa administrativa correspondiente.

Los certificados de la EC-UR no se expiden al público, sino a les entidades, al personal, a los estudiantes y a los dispositivos de las universidades, los centros de investigación y otras instituciones de Catalunya, en su caso, adheridas al “Anillo Científico” o vinculadas con estas (en adelante, “las instituciones”).

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-UR.

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

1.3.2 Entidad de Certificación Raíz

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

La citada vinculación técnica se consigue mediante la emisión de certificados de infraestructura de entidad de certificación vinculada (CIC).

1.3.3 EC-UR

El Departamento de Universidades, Investigación y Sociedad de la Información (DURSI), la Fundación Catalana para la Investigación y la Innovación (FCRI), las universidades públicas (UB, UAB, UPC, UPF, UdG, URV y UdL), la universidad no presencial (UOC), la Asociación Catalana de Entidades de Investigación (ACERO), la Administración Abierta de Cataluña (AOC), la Agencia Catalana de Certificación (CATCert) y el Centro de Supercomputación de Cataluña (CESCA), firmaron un convenio el 23 de Octubre de 2003 con el objetivo de que las universidades y centros de investigación incorporen la firma electrónica para incrementar la seguridad de sus comunicaciones telemáticas mediante la creación de la EC-UR, vinculada a la jerarquía de entidades de certificación de las entidades públicas de Cataluña, que emite los certificados a las Instituciones.

La huella digital del certificado de la EC-UR es la siguiente:

d7 af fd f4 7f df f6 86 5d db f1 46 d8 86 4c 70 6c fa 00 32

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.

El proceso de creación de entidades de registro es responsabilidad del administrador de la Entidad de Certificación. Mediante acuerdo o convenio se constituye la entidad de registro. El Consorci AOC verifica que la Entidad de Registro cuenta con los recursos materiales y humanos necesarios, y de la designación del personal responsable. Asimismo, es responsable, en todo caso, de la formación del personal que emita los certificados como operadores de la entidad de registro y, a tal efecto, de la emisión de los certificados de operador correspondientes (típicamente, CIPISR). El Consorci AOC validará las peticiones de certificados de las Entidades de Registro examinando la solicitud y haciendo las comprobaciones necesarias para el cumplimiento de la Política General de Certificación y de la Declaración de Prácticas de Certificación.

En certificados de clase 1, la Entidad de Registro y el suscriptor podrán ser la misma organización y, en consecuencia, habitualmente la Entidad de Registro podrá actuar también como solicitante del certificado.

En certificados de clase 2, la Entidad de Registro y el suscriptor deberán ser necesariamente organizaciones diferentes, ya que la Entidad de Registro tiene que actuar siempre por cuenta de la Entidad de Certificación Vinculada.

El CESCO actúa como Entidad de Registro de todas las Instituciones suscriptoras que soliciten certificados y no se hayan constituido en Entidad de Registro. En este caso, deben aportar los necesarios datos personales y corporativos, legalmente certificados, para la emisión de los certificados.

1.3.5 Usuarios finales

Los usuarios finales son las personas (físicas o jurídicas) que obtienen y utilizan los certificados dispositivo emitidos por la EC-UR; 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 esta DPC son las personas autorizadas por las entidades suscriptoras.

Pueden ser solicitantes:

- a) La persona que será el futuro poseedor de claves o el futuro suscriptor del certificado
- b) Una persona autorizada por el futuro suscriptor
- c) Una persona autorizada por la Entidad de Registro
- d) Una persona autorizada por la Entidad de Certificación.

La autorización podrá realizarse tanto de forma expresa como tácita y, en aquellos casos en los que la entidad de certificación lo considere conveniente, tendrá que formalizarse documentalmente.

1.3.5.2 Suscriptores de certificados

Los suscriptores son las instituciones y las personas, físicas o jurídicas, así identificadas en el campo "Subject" del certificado.

El suscriptor tiene licencia de uso del certificado y, cuando se trata de una institución u otra persona jurídica, y el certificado es personal, actúa siempre a través de un poseedor de claves, debidamente autorizado, y que figura identificado en el certificado.

1.3.5.3 Poseedores de claves

Los poseedores de claves son las personas físicas que poseen de forma exclusiva las claves privadas de los certificados, que se encuentran debidamente autorizadas para ello por el suscriptor y debidamente identificados en el certificado mediante su nombre y apellidos o mediante un pseudónimo.

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 físicas y jurídicas que reciben firmas electrónicas y certificados digitales y tienen que verificarlos, como paso previo a confiar.

Los verificadores, aunque pueden confiar absolutamente en la identidad del poseedor de claves y en su relación con la institución suscriptora de su certificado, tienen que practicar otras comprobaciones adicionales si quieren confiar en el acto jurídico del cual se da fe en el documento o mensaje firmado por el poseedor.

Por ejemplo, es necesario comprobar que un poseedor sin un cargo concreto está facultado legalmente, o mediante una previsión estatutaria o un apoderamiento o habilitación concretos, antes de confiar en el acto documentado, ya que el certificado no aporta esta garantía.

En cambio, sí se puede confiar siempre en el cargo, de forma que todo lo que puede hacer un determinado cargo mediante un documento en soporte papel, por escrito, también lo puede hacer electrónicamente, sin que sea necesaria ninguna comprobación adicional.

1.4. Uso de los certificados

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

1.3.6 Usos típicos de los certificados

1.4.1.1. Certificados de infraestructura

1.4.1.1.1. Certificado de Infraestructura personal de identificación y firma reconocida (CIPISR)

Los certificados de infraestructura personal de identificación y firma reconocida (CIPISR) son emitidos a operadores de Entidades de Registro para las tareas de emisión y gestión del ciclo de vida de certificados de una Entidad de Certificación.

Los certificados de infraestructura de identificación son certificados reconocidos de acuerdo con lo que establece el artículo 11.1, con el contenido prescrito en el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Los CIPISR funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y que dan cumplimiento a lo dispuesto en la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Por este motivo, los CIPISR garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permiten la generación de la firma electrónica reconocida; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada usando un dispositivo seguro, por la cual cosa, de acuerdo con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma manuscrita por efecto legal, sin necesidad de cumplir con otro requisito adicional.

Los CIPISR son certificados de operador y su uso exclusivo es la operación de los componentes de la infraestructura de clave pública de CATCert como, por ejemplo, los componentes usados por las Entidades de Registro para aprobar y generar certificados, o para revocar-los, o para el servicio de atención a usuarios para suspender certificados.

Los CIPISR correspondientes a la Entidad de Certificación serán emitidos por la propia Entidad de Certificación, con la aprobación previa de CATCert

Los CIPISR correspondientes a cada Entidad de Certificación Vinculada a la Entidad de Certificación serán emitidos por la propia Entidad de Certificación, con la aprobación previa de la Entidad de Certificación.

1.4.1.1.2. Requisitos específicos para el certificado de entidad de certificación (CIC)

Los certificados de entidad de certificación (CIC) son emitidos por la Entidad de Certificación Raíz, a organizaciones que operan una Entidad de Certificación 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 de infraestructura, personales, de identidad y de dispositivo.
- Emisión y firma de listas de revocación de certificados (LRC). Los CIC se obtienen después de un proceso de admisión de la Entidad de Certificación Vinculada a los servicios de certificación de la Agència Catalana de Certificació, que se describe en la declaración de prácticas de certificación (DPC) de la entidad de certificación raíz de la jerarquía.

1.4.1.1.3. Requisitos específicos para el certificado de infraestructura de dispositivo de servidor seguro de clase 1 (CIDS-1)

Los certificados de infraestructura de dispositivo servidor seguro de clase 1 (CIDS-1) se emiten a Entidades de Certificación, responsables de la operación de servidores seguros SSL o TLS, con los siguientes usos:

- Autenticación de servidor
- Cifrado de las comunicaciones entre cliente y servidor

Los certificados CIDS son certificados ordinarios, y que garantizan la identidad de la Entidad de Certificación y del servidor concreto donde funcionan.

1.4.1.1.4. Requisitos específicos para el certificado de infraestructura de aplicación digitalmente asegurada de clase 1 (CIDA-1)

Los certificados de infraestructura de dispositivo de aplicación digitalmente asegurada (CIDA) se emiten a Entidades de Certificación responsables de la operación de aplicaciones informáticas que se identifican digitalmente, firman electrónicamente webservices u otros protocolos y que reciben documentos y mensajes cifrados.

Los certificados CIDA son certificados ordinarios, y que garantizan la identidad de la Entidad de Certificación y la integridad y la autenticidad de los datos firmados. También permiten la recepción de información cifrada.

La clave privada del CIDA podrá estar archivada por la entidad de certificación de forma que, en ciertas circunstancias, pueda recuperarse y acceder a la información cifrada, bajo demanda de la Entidad de Certificación.

1.4.1.1.5. Requisitos específicos para el certificado de infraestructura de servidor de estado de certificados en línea de clase 1 (CIO-1)

Los certificados de infraestructura de servidor de estado de certificados en línea (CIO) se emiten a Entidades de Certificación, responsables de la operación de un servidor *OCSP Responder* para firmar sus respuestas sobre el estado de validez de los certificados.

Los certificados CIO son certificados ordinarios, que garantizan la identidad de la Entidad de Certificación y del servidor *OCSP Responder* y la integridad y la autenticidad de los datos firmados.

1.4.1.1.6. Requisitos específicos para el certificado de entidad de sellos de tiempos (CIT-1)

Los certificados de infraestructura de entidad de sellos de tiempos (CIT) se emiten a Entidades de Certificación, responsables de la operación de un servidor para firmar los sellos de tiempos que emiten.

Los certificados CIT son certificados ordinarios, que garantizan la identidad de la Entidad de Certificación y del servidor de firma de sellos de tiempos y la integridad y la autenticidad de los datos firmados.

1.4.1.1.7. Requisitos específicos para el certificado de infraestructura de entidad de validación (CIV-1)

Los certificados de infraestructura de entidad de validación (CIV) se emiten a Entidades de Certificación, responsables de la operación de un servidor de entidad de validación para firmar sus informes. Los certificados CIV son certificados ordinarios, que garantizan la identidad de la Entidad de Certificación y del servidor de entidad de validación y la integridad y la autenticidad de los datos firmados.

1.4.1.2. Certificados personales

1.4.1.2.1. Certificados personales de identificación y firma electrónica reconocida de clase 1 con cargo (CPISR-1 cargo), y con cargo para extranjeros (CPISR-1 con Cargo Extranjeros), y certificados de identificación y firma

electrónica reconocida de clase 1 con cargo para uso concreto (CPISR-1 cargo uso)

Los certificados personales de identificación y firma reconocida de clase 1 con cargo, y con cargo para extranjeros, y los certificados personales de identificación y firma electrónica reconocida de clase 1 con cargo para uso concreto, son certificados reconocidos de acuerdo con lo que se establece en el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y que dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Éstos son certificados reconocidos que funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Por este motivo, estos certificados garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permiten la generación de la firma electrónica reconocida; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada utilizando un dispositivo seguro, por lo que, de acuerdo con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requerimiento adicional.

Estos certificados incluyen una manifestación relativa a la categoría de personal y/o cargo del poseedor de claves, que han sido comprobados antes de emitir el certificado, y son correctos, de acuerdo con esta Declaración de Prácticas.

Además, los tres certificados se pueden utilizar para diversos usos, entre los que se pueden indicar los siguientes:

- Identificación en servidores web basada en presentación de la credencial.
- Autenticación en sistemas de control de acceso, de sistemas operativos o centralizados.

1.4.1.2.2. Certificado personal de identificación y firma electrónica reconocida con cargo (CPISR-2 con Cargo)

El certificado personal de identificación y firma reconocida de clase 2 con cargo, es un certificado reconocido de conformidad con el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitido cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y que da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Se trata de un certificado reconocido que funciona con dispositivo seguro de creación de firma electrónica, de conformidad con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Por este motivo, este certificado garantiza la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permite la generación de la firma electrónica reconocida; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada utilizando un dispositivo seguro, por lo cual, de conformidad con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplir requisito adicional alguno.

Este certificado incluye una manifestación relativa al cargo del poseedor de claves, que ha sido comprobado antes de emitir el certificado, y es correcto y vigente mientras el certificado también se encuentre vigente.

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

- Identificación en servidores web basada en presentación del certificado.
- Autenticación en sistemas de control de acceso, de sistema operativo o centralizados.

1.4.1.2.3. Certificados personales de identificación y firma electrónica reconocida de clase 2 de estudiante (CPISR-2 estudiante) y de estudiante extranjero (CPISR-2 de Estudiante Extranjero)

Los certificados personales de identificación y firma reconocida de clase 2 de estudiante, y de estudiante extranjero, son certificados reconocidos de acuerdo con lo que se establece en el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y que dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Estos son certificados reconocidos que funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Por este motivo, estos certificados garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permiten la generación de la firma electrónica reconocida; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada utilizando un dispositivo seguro, por lo que, de acuerdo con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

Estos certificados incluyen una manifestación relativa a la condición del poseedor de claves, como estudiante adscrito a un centro del suscriptor del certificado, que han sido comprobados antes de emitir el certificado, y son correctos y vigentes mientras el certificado también se encuentre vigente.

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

- Identificación en servidores web basada en presentación del certificado.
- Autenticación en sistemas de control de acceso, de sistemas operativo, o centralizados.

1.4.1.2.4. Certificados personales de cifrado de clase 1 con cargo (CPX-1 cargo), y de clase 1 con cargo para extranjeros (CPX-1 con Cargo Extranjero)

El certificado personal de cifrado de clase 1 con cargo y el certificado personal de cifrado de clase 1 con cargo para extranjeros son certificados reconocidos de conformidad con el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitido cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y que dan cumplimiento a lo dispuesto por la normativa técnica del

Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Se trata de certificados reconocidos que funcionan con dispositivo seguro de creación de firma electrónica, de conformidad con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Los certificados personales de cifrado se utilizan exclusivamente para cifrar documentos y recibir mensajes de datos confidenciales, en cualquier formato, protegidos mediante el cifrado del texto del mensaje, por parte del remitente del mensaje.

Estos certificados garantizan la identidad del suscriptor, pero no permiten la firma electrónica de mensajes de datos.

1.4.1.2.5. Certificados personales de cifrado de clase 2 con cargo (CPX-2 cargo)

El certificado personal de cifrado de clase 2 con cargo es un certificado reconocido de conformidad con el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitido cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y que da cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Se trata de un certificado reconocido que funciona con dispositivo seguro de creación de firma electrónica, de conformidad con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Los certificados personales de cifrado con cargo se utilizan exclusivamente para cifrar documentos y recibir mensajes de datos confidenciales, en cualquier formato, protegidos mediante el cifrado del texto del mensaje, por parte del remitente del mensaje.

Estos certificados garantizan la identidad del suscriptor, pero no permiten la firma electrónica de mensajes de datos.

1.4.1.2.6. Certificados personales de cifrado de clase 2 de Estudiante (CPX-2 estudiante) y de estudiante extranjero (CPX-2 de Estudiante Extranjero)

El certificado personal de cifrado de clase 2 para estudiante y el certificado personal de cifrado de clase 2 para estudiante extranjero son certificados reconocidos de conformidad con el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitido cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y que dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Se trata de certificados reconocidos que funcionan con dispositivo seguro de creación de firma electrónica, de conformidad con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Los certificados personales de cifrado se utilizan exclusivamente para cifrar documentos y recibir mensajes de datos confidenciales, en cualquier formato, protegidos mediante el cifrado del texto del mensaje, por parte del remitente del mensaje.

Estos certificados garantizan la identidad del suscriptor, pero no permiten la firma electrónica de mensajes de datos.

Estos certificados incluyen una manifestación relativa a la condición del poseedor de claves como estudiantes adscrito a un centro del suscriptor del certificado, que ha sido comprobada antes de emitir el certificado, y es correcta y vigente mientras el certificado también se encuentre vigente.

El poseedor de la clave utiliza su clave privada para descifrar mensajes.

1.4.1.2.7. Certificados personales de identificación, cifrado y firma avanzada con cargo de empleado público de clase 1 (CPIXSA-1 Cargo EP)

El certificado personal de identificación, cifrado y firma avanzada con cargo de empleado público de clase 1 es un certificado reconocido de acuerdo con lo que se establece en el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitido cumpliendo las obligaciones de los artículos 12, 13, i 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Se utiliza para firmar sin dispositivo seguro de creación de firma, dando soporte a la firma electrónica avanzada según el artículo 3.2 de la Ley 59/2003, de 19 de diciembre.

Estos certificados pueden incluir una manifestación relativa a la categoría de personal y cargo del poseedor de claves, que han sido comprobados antes de emitir el certificado, y son correctos, cuando lo prevea una política específica.

El certificado personal de identificación y firma electrónica avanzada con cargo de empleado público de clase 1 con cargo para uso concreto, identifica, además de la persona que lo posee, la organización suscriptora, y su cargo en esta, las limitaciones materiales de uso.

Además, los tres certificados se pueden utilizar para diversos usos, entre los que se pueden indicar los siguientes:

- Identificación en servidores web basada en presentación del certificado.
- Autenticación en sistemas de control de acceso, de sistemas operativos o centralizados.

1.4.1.3. Certificados de Entidad

1.4.1.3.1. Certificados de Entidad de Identificación y Firma Electrónica Reconocida de clase 1 (CEISR-1)

Los certificados de entidad de identificación con firma reconocida de clase 1 son certificados reconocidos, no emitidos al público, de acuerdo con lo que se establece en el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 7, 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y que dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Se tratan de certificados reconocidos que funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Por este motivo, estos certificados garantizan la identidad del suscriptor y del poseedor de la clave privada de firma, siendo idóneos para ofrecer soporte a la firma electrónica

reconocida de la entidad; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada utilizando un dispositivo seguro, por lo que, de acuerdo con lo que establece el artículo 3.4 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

1.4.1.3.2. Certificados de Entidad de Cifrado de clase 1 (CEX-1)

Los certificados de entidad de cifrado de clase 1 son certificados reconocidos, no emitidos al público, que se expiden a suscriptores y se utilizan exclusivamente para cifrar documentos o recibir mensajes confidenciales, en cualquier formato, protegidos mediante el cifrado del texto del mensaje, utilizando la clave pública del suscriptor indicada en el CEX.

Los CEX corresponden a certificados con dispositivo seguro de creación de firma electrónica, para el descifrado, no expedidos al público, de acuerdo con el documento ETSI TS 101 456 v1.1.1.

El poseedor de la clave utiliza su clave privada para descifrar los mensajes.

La clave privada del CEX se archivará por la entidad de certificación de manera que, en ciertas circunstancias, pueda recuperarse y acceder a la información cifrada, incluso sin la intervención del suscriptor.

1.4.1.3.3. Certificado de Entidad de Identificación, Cifrado y Firma Electrónica Avanzada de clase 1 (CEIXSA-1)

Los certificados de entidad de identificación, cifrado y firma electrónica avanzada de clase 1 son certificados reconocidos, no emitidos al público, de acuerdo con lo que se establece en el artículo 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 7, 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y que dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Se utilizan para firmar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos, para recibir mensajes de datos confidenciales, en cualquier formato, protegidos mediante el cifrado del texto del mensaje, utilizando la clave pública del suscriptor indicada en el CEIXSA y para firma documentos sin dispositivo seguro de creación de firma, dando soporte a la firma electrónica avanzada según el artículo 3.2 de la Ley 59/2003, de 19 de diciembre.

1.4.1.4. Certificados de dispositivo

1.4.1.4.1. Certificados de dispositivo de servidor seguro de clase 1 (CDS-1)

Los certificados de dispositivo servidor seguro (CDS) se emiten a personas físicas o personas jurídicas, responsables de la operación de servidores seguros SSL o TLS, con los siguientes usos:

- Autenticación de servidor
- Cifrado de las comunicaciones entre cliente y servidor

Los certificados CDS-1 son, con carácter general, certificados ordinarios, y que garantizan la identidad de la persona jurídica responsable y del servidor concreto donde funcionan.

1.4.1.4.2. Certificados de dispositivo de servidor seguro de clase 1 Extended Validation (CDS-1 EV)

Los CDS-1 EV se emiten a las Instituciones, responsables de la operación de servidores seguros SSL o TLS, con los siguientes usos:

- Autenticación de servidor
- Cifrado de las comunicaciones entre cliente y servidor
- Validación automática del certificado mediante los navegadores web adheridos a CA/Browser Forum.

Estos son certificados ordinarios, que garantizan la identidad de la persona responsable y de los servidores concretos donde funcionan.

1.4.1.4.3. Certificado de dispositivo de sede electrónica Extended Validation (CDS-1 Sede nivel medio y alto EV)

Los CDS-1 de sede electrónica Extended Validation se emiten a las Universidades y Centros de Investigación, responsables de la operación de servidores seguros SSL o TLS, con el uso de identificar y garantizar una comunicación segura con la sede electrónica de un ente, entendiéndose sede electrónica en los términos del artículo 10 de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos. Se trata de certificados reconocidos que puede utilizarse para la conexión segura de los ciudadanos a páginas web oficiales, la autenticación de un lugar web, el alojamiento de registros electrónicos, la consulta y autorización de registros de representación, etc.

Se distinguen dos certificados:

- El certificado de nivel medio, es recomendable para la mayoría de las administraciones públicas con previsión de los siguientes riesgos: infracción de seguridad (por ejemplo, robo de la identidad), pérdidas económicas moderadas, pérdida de información sensible o crítica, o refutación de una transacción con impacto económico significativo.
- El certificado de nivel alto, almacenado en un HSM (hardware criptográfico), es recomendable para aquellas administraciones públicas que, habiendo realizado previamente un análisis de riesgos, precisan medidas adicionales de seguridad, al contemplar los siguientes riesgos: infracción de seguridad, pérdidas económicas importantes, pérdida de información altamente sensible y crítica o refutación de una transacción con impacto económico muy significativo. El certificado de sede electrónica de nivel alto se cargará directamente en la PSIS (Plataforma de Servicios de Identificación y Firma), al menos mientras no se disponga de hardware criptográfico HSM necesario para el nivel de seguridad requerido.

Estos certificados incorporan la función Extended Validation, que permite la validación automática del certificado mediante los navegadores adheridos a CA/Browser Forum.

1.4.1.4.4. Certificados de dispositivo seguro de controlador de dominio de clase 1 (CDSCD)

Los CDSCD se emiten a las Universidades y Centros de Investigación de las Instituciones responsables de la operación del controlador de dominio, con los siguientes usos:

- Autenticación del servidor
- Autenticación del usuario con tarjeta criptográfica

Los CDSCD son certificados ordinarios que garantizan la identidad de la persona responsable, de los servidores concretos donde funcionan y de los usuarios con tarjeta criptográfica que autentica.

1.4.1.4.5. Certificados de dispositivo de aplicación digitalmente asegurada de clase 1 (CDA-1)

Los CDA se emiten a las Universidades y Centros de Investigación responsables de la operación de aplicaciones informáticas que se identifican digitalmente, que firman electrónicamente webservices u otros protocolos, y que reciben documentos y mensajes cifrados.

Son certificados ordinarios, que garantizan la identidad de la persona jurídica responsable y la integridad y la autenticidad de los datos firmados. También permiten la recepción de información cifrada.

1.4.1.4.6. Certificados de dispositivo de aplicación digitalmente asegurada sello electrónico (CDA-1 sello electrónico nivel medio y alto)

Los CDA-1 sello electrónico se utilizan para la identificación y la autenticación del ejercicio de la competencia en la actuación administrativa automatizada, en los términos descritos en el artículo 18 de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.

Este certificado puede utilizarse para el intercambio de datos entre administraciones, la identificación y autenticación de un sistema, servicio web o aplicación, el archivo electrónico automatizado, las compulsas y copias electrónicas, entre otros. Se distinguen dos certificados:

- El certificado de nivel medio, es recomendable para la mayoría de las administraciones públicas que pueden tener los siguientes riesgos: infracción de seguridad (por ejemplo robo de la identidad), pérdidas económicas moderadas, pérdida de información sensible o crítica, o refutación de una transacción con impacto económico significativo.
- El certificado de nivel alto, con unas claves de 2048 bits, es recomendable para aquellas administraciones públicas que, habiendo realizado previamente un análisis de riesgos, precisan medidas adicionales de seguridad, ya que contemplan los siguientes riesgos: infracción de seguridad, pérdidas económicas importantes, pérdida de información altamente sensible y crítica o refutación de una transacción con impacto económico muy significativo. La protección de la clave privada del certificado de sello electrónico de nivel alto se realiza mediante hardware criptográfico HSM necesario para el nivel de seguridad requerido.

1.4.1.4.7. Certificados de dispositivo de firma de software de clase 1 (CDP-1)

Los CDP se emiten a personas jurídicas responsables de la edición, publicación o distribución digitales de software informático, para la firma del software, que permite instalarlo o ejecutarlo a distancia.

Estos son certificados ordinarios, y que garantizan la identidad de la persona jurídica responsable y el origen y la integridad del software firmado.

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 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. Certificado de infraestructura personal de identificación y de firma reconocida

Cualquier otro uso no especificado en la sección anterior está expresamente prohibido y su detección dará lugar a la inmediata revocación del certificado CIPISR.

1.4.2.3. Certificados personales de identificación y firma electrónica reconocida

Los certificados CPISR-1 con Cargo, CPISR-1 con Cargo Extranjeros, CPISR-1 con Cargo Uso, CPISR-2 con Cargo, CPISR-2 de Estudiante y CPISR-2 de Estudiante Extranjero, no pueden utilizarse para:

- Firmar peticiones de emisión, renovación, suspensión o revocación de certificados.
- Firmar certificados de clave pública de ningún tipo, ni listas de revocación de certificados (LRC).
- Cifrar ni descifrar mensajes o documentos.

1.4.2.4. Certificado personal de identificación, cifrado y firma avanzada

Los certificados CPIXSA-1 Cargo EP no se pueden utilizar para:

- Firmar peticiones de emisión, renovación, suspensión, habilitación o revocación de certificados.
- Firmar certificados de clave pública de ningún tipo ni listas de revocación de certificados (LRC).

1.4.2.5. Certificados personales de cifrado

Los CPX no pueden utilizarse para generar firmas electrónicas de ningún tipo de mensaje de datos.

1.4.2.6. Certificados de entidad de identificación y firma electrónica reconocida

Los certificados no pueden utilizarse para:

- Firmar peticiones de emisión, renovación, suspensión, habilitación o revocación de certificados.
- Firmar certificados de clave pública de ningún tipo, ni listas de revocación de certificados (LRC).
- Cifrar ni descifrar mensajes o documentos.

1.4.2.7. Certificados de entidad de cifrado

Los CEX no pueden utilizarse para generar firmas electrónicas de ningún tipo de mensaje de datos.

1.4.2.8. Certificados de entidad de identificación, cifrado y firma electrónica avanzada

Los CEIXSA no pueden utilizarse para:

- Firmar peticiones de emisión, renovación, suspensión, habilitación o revocación de certificados.
- Firmar certificados de clave pública de ningún tipo, ni listas de revocación de certificados (LRC).
- Realizar firma electrónica reconocida de documentos.

1.4.2.9. Certificados de dispositivo de servidor seguro

Los CDS-1 y los CDS-1 EV no pueden utilizarse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados CIC, certificados de ningún tipo o listas de revocación de certificados (LRC).

1.4.2.10. Certificado de dispositivo de servidor seguro sede electrónica

Los CDS-1 de Sede electrónica EV no pueden emplearse para asegurar servidores que no tengan la consideración legal de sede electrónica.

1.4.2.11. Certificados de dispositivo seguro de controlador de dominio (CDSCD)

Los CDSCD no pueden utilizarse para firmar peticiones de emisión, renovación, suspensión, habilitación o revocación de certificados CIC, certificados de ningún tipo o listas de revocación de certificados (LRC).

1.4.2.12. Certificados de dispositivo de aplicación digitalmente asegurada

Los CDA no pueden utilizarse para firmar peticiones de emisión, renovación, suspensión, habilitación o revocación de certificados CIC, certificados de ningún tipo, o listas de revocación de certificados (LRC).

Tampoco pueden utilizarse para asegurar aplicaciones diferentes a la identificada en el certificado.

1.4.2.13. Certificados de dispositivo de aplicación digitalmente asegurada sello electrónico

Los CDA sello no pueden emplearse para la realización de actos manuales.

1.4.2.14. Certificados de dispositivo de firma de software

Sin estipulaciones adicionales.

1.5 Administración de la Declaración de Prácticas.

1.5.1 Organización que administra la especificación

Consorti Administració Oberta de Catalunya – Consorti AOC

1.5.2 Datos de contacto de la organización

Consorti Administració Oberta de Catalunya – Consorti AOC

Domicili social: Via Laietana, 26 – 08003 Barcelona

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

Web del Consorti AOC: www.aoc.cat

Web del servicio de certificación digital del Consorti AOC:

www.aoc.cat/catcert

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

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

La persona que determina la conformidad de una DPC con la Política General de Certificación es el/la Responsable del Servicio de Certificación Digital del Consorti AOC,

basándose en los resultados de una auditoría al efecto, realizada por un tercero, bianualmente.

1.5.4 Procedimiento de aprobación

El procedimiento para la aprobación y modificación de esta declaración de prácticas será el establecido en el Convenio marco de colaboración entre el Departamento de Universidades, Investigación y Sociedad de la Información, la Fundación Catalana para la Investigación, la Universitat de Barcelona, la Universitat Autònoma de Barcelona, la Universitat Politècnica de Catalunya, la Universitat Pompeu Fabra, la Universitat de Girona, la Universitat de Lleida, la Universitat Rovira i Virgili, la Universitat Oberta de Catalunya, la Associació Catalana d'Entitats de Recerca, Serveis Públics Electrònics (CAT365), la Agència Catalana de Certificació y el Consorci Centre de Supercomputació de Catalunya, de 23 de octubre de 2003, que prevé su aprobación definitiva por la Comisión Mixta de Seguimiento y Control del Convenio Marco en su cláusula décima.

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-UR, 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-UR

La EC-UR 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-UR, 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-UR 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 9.12.1.

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-UR, pudiendo ser consultadas por los interesados.

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

2.4. Control de acceso

Sin estipulaciones adicionales.

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

[Sin estipulaciones adicionales.](#)

3.1.1.2 Perfiles dels certificadors

Los perfiles de los certificados emitidos por la EC-URse publican en la web del Consorci AOC (<http://www.aoc.cat/catcert/>).

3.1.1.3. Características de los certificados personales de clase 1 con cargo

El listado de categorías para el campo Title es el siguiente:

- "CU " Catedráticos y catedráticas de Universidad.
- "TU " Titulares de universidad
- "CEU" Catedráticos y catedráticas de Escuelas universitarias
- "TEU" Titulares de escuelas universitarias
- "PRF" Profesorado contratado
- "INV" Personal de investigación
- "PAS" Personal de Administración y Servicios
- "PDI" Personal Docente e Investigador
- "PVE" Personal Vinculado o Externo

3.1.1.4. Características de los certificados personales de clase 2 de estudiante

El listado de categorías para el campo Title para los certificados personales de clase 2 es el siguiente:

- "EST " Estudiantes.
- "EST EST" Estudiantes extranjeros

3.1.2. Significado de los nombres

Sin estipulaciones adicionalesSin estipulaciones adicionales.

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 estipulaciones adicionalesSin estipulaciones adicionales.

3.1.5. Unicidad de los nombres

Sin estipulaciones adicionales.

3.1.6. Resolución de conflictos relativos a nombres

Sin estipulaciones adicionalesSin estipulaciones adicionales.

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 estipulaciones adicionales.

3.2.2. Autenticación de la identidad de una organización

Sin estipulaciones adicionales.

3.2.2.1. Entidades de Registro

Sin estipulaciones adicionales

3.2.2.2. Suscriptores de los certificados

Sin estipulaciones adicionales.

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 operador de la Entidad de Registro introduce la información que identifica al poseedor de claves, que encuentra en el expediente asociado a la petición de suscripción.

En el caso que la Institución no disponga de información actualizada del poseedor de claves, se comprueba la identidad personalmente o se utilizan sistemas que proporcionen garantías equivalentes a la identificación con presencia física del futuro poseedor de claves, y se graba una justificación acreditativa de los siguientes elementos:

- Nombre completo
- 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).
- Cualquier otra información que pueda ser utilizada para diferenciar una persona de otra, dentro del ámbito de la Institución (por ejemplo: fotografía, correo-e, categoría, etc.).

3.2.3.2. Validación de los elementos de identificación

La información de identificación de poseedores de claves de certificados de Clase 1 se valida comparando la información de la solicitud con los registros internos de la Entidad de Registro que se asegura de la corrección de la información a certificar.

Se puede ocupar un proveedor corporativo de información de recursos humanos para esta tarea.

La información del poseedor registrada por la Institución en los últimos cinco años está actualizada.

3.2.3.3. Necesidad de presencia personal

Es necesario validar la identidad del poseedor de claves con su presencia física, que es responsabilidad de la propia Institución, y que lo hace mediante su relación funcional, laboral o profesional, según proceda.

Durante el trámite de entrega y aceptación del certificado y del correspondiente dispositivo seguro de creación de firma, se realiza la validación definitiva de la identidad de la persona de conformidad con los procedimientos operativos aprobados y la presente DPC.

3.2.3.4. Vinculación de la persona física con la Institución

Puesto que se trata de certificados corporativos, en los que la Entidad de Registro y el suscriptor coinciden, no es necesario obtener una justificación documental específica de la vinculación del poseedor de claves.

3.2.4. Información no verificada

La EC-UR 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

Sin estipulaciones adicionales.

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 certificados

4.1.1.1. Certificados personales, de identidad y de cifrado.

Antes de la emisión y entrega de un certificado, existe una solicitud de certificado, acompañada de la correspondiente documentación acreditativa de los datos a certificar.

La documentación acreditativa se genera mediante tres procesos alternativos:

1. El acto administrativo de certificación previa de los datos, por parte de la institución solicitante del certificado, ante el CESCA, que es Entidad de Registro de la Entidad de Certificación.

La EC-UR informa al suscriptor de los términos y condiciones aplicables al certificado, en lenguaje fácilmente comprensible.

La solicitud es, en cualquier caso, el primer paso que debe hacer el suscriptor para conseguir los certificados para su personal. Una Adenda al Convenio firmado entre el Consorci AOC i el CESCA determinará la persona o personas autorizadas para solicitar certificados a la EC-UR en nombre del suscriptor. Esta solicitud requiere el envío de un documento con la información exacta y comprobada (certificada) de las personas o dispositivos para las que se pide el certificado. Esta solicitud se firma por la persona autorizada por el suscriptor en la ficha. También se envía un certificado de datos. También se puede acompañar una dirección física, u otros datos, que permitan establecer contacto directo con el futuro poseedor de claves.

Toda la documentación se entrega al Responsable del servicio de certificación digital del CESCA presencialmente, o en soporte papel, mediante correo postal certificado, o en soporte electrónico, mediante correo electrónico firmado y cifrado, o también telemáticamente, siempre que sea posible por razones técnicas o de aplicativo informático.

2. El acto administrativo de registro directo por una institución constituida como Entidad de Registro de la Entidad de Certificación, de acuerdo con el convenio correspondiente firmado por el Consorci AOC, CESCA y la Institución.

Para que exista una solicitud primero disponemos de una relación entre la Institución y el poseedor de claves. Esta relación puede definirse de tres maneras:

- Si son profesores, a partir de la relación contractual entre la Institución y ellos, ya sean funcionarios o dispongan de un contrato laboral.
- Si son miembros del PAS, a partir de la relación contractual entre la Institución y ellos, ya sean funcionarios o dispongan de un contrato laboral.

- Si son estudiantes, a partir de la matrícula oficial en un programa reglado o en asignaturas individuales.

Cuando se pide un certificado CPISR-1 con cargo para profesores o miembros del PAS, un miembro del órgano competente de la Institución hace la solicitud donde consta la relación autenticada (por ejemplo, mediante un certificado administrativo) de aquellos usuarios que deben recibir un certificado, o se obtienen los datos de manera automática de los sistemas de gestión de identidad de la Institución. Este documento se envía a un responsable de la Entidad de Registro, que sigue adelante con el proceso.

Cuando se pide un certificado CPISR-2 de estudiante, un miembro del órgano competente de la Institución hace la solicitud donde consta la relación autenticada (por ejemplo, mediante una copia auténtica de la lista de los estudiantes matriculados) de aquellos usuarios que deben recibir un certificado, o se obtienen los datos de manera automática de los sistemas de gestión de identidad de la Institución. Este documento se envía a un responsable de la Entidad de Registro, que sigue adelante con el proceso.

- a) El acto administrativo de registro directo por una Institución constituida, de acuerdo con el convenio de referencia, como Entidad de Certificación Vinculada a la Entidad de Certificación, mediante su propia Entidad de Registro.
- b) Presencia notarial, de acuerdo con el artículo 13.1 de la Ley 59/2003, de Firma Electrónica

4.1.1.2. Otros certificados

Antes de la emisión y entrega de un certificado, existe una solicitud de certificado, acompañada de la correspondiente documentación acreditativa de los datos a certificar, la cual gestiona el responsable del sistema de certificación digital, encargado de la Entidad de Registro, directament al Consorci AOC.

Esta solicitud sólo puede ser realizada por los responsables de las unidades o departamentos correspondientes.

De la misma manera que para los certificados personal y de entidad, el encargado del ente subscriptor tiene que realizar la tramitación telemática, cuando proceda.

4.1.2. Procedimiento de alta: Responsabilidades de la ER

En el caso de que la Entidad de registro tenga conexión automática con los sistemas de gestión de identidad de la Institución, diariamente se genera un proceso automático que revisa las bases de datos, correspondientes a alumnos y a personal de las universidades que forman parte del Convenio de referencia, y detecta las nuevas incorporaciones, así como cualquier otra modificación de los datos incluidos en el certificado, que generará una nueva solicitud.

Por cada nueva alta en cualquiera de las dos bases de datos citadas, se genera una solicitud, según el modelo establecido en manual de procedimiento operativo de emisión de certificados, que se envía por comunicación directa vía Internet a la Autoridad de Certificación (AC) de la UR.

La comunicación realizada a la AC de la UR se procesa y, realizada la validación, si todo es correcto, se crea la solicitud a la Autoridad de Certificación. Seguidamente se genera un mensaje de respuesta informando del resultado positivo o negativo de la operación y el tipo de error detectado en caso de resultado negativo. Esta respuesta se revisa por el servicio correspondiente, que analiza y canaliza la resolución de las solicitudes que han sido rechazadas.

La Entidad de Certificación ha de asegurarse de que las solicitudes de certificado son completas, precisas y están debidamente autorizadas.

Antes de la emisión y entrega del certificado, la Entidad de Certificación informará al suscriptor de los términos y las condiciones aplicables al certificado.

En certificados de organización, este requisito se podrá cumplir librando el instrumento jurídico que vincula a la Entidad de Certificación con el suscriptor y entregando una hoja de entrega al poseedor de claves, que incluye esta información.

La citada información se comunicará en soporte perdurable, en papel o electrónicamente y en lenguaje fácilmente comprensible.

En la solicitud se podrá acompañar documentación justificativa de la identidad del suscriptor y otras circunstancias, y del poseedor de claves, de acuerdo con lo que establece la sección correspondiente de esta declaración de prácticas de certificación.

También se podrá acompañar de una dirección física o de otros datos que permitan contactar con el suscriptor.

La Entidad de Registro es la responsable de realizar el procedimiento de alta, que puede realizarse de dos maneras:

1. Procedimiento de alta cuando lo efectúa el CESCO como Entidad de Registro:

Una vez el CESCO ha recibido la adenda del convenio de colaboración con la ficha, firmados por el suscriptor, se abre el expediente, incluyendo ambos documentos.

El CESCO da de alta en una base de datos la información contenida en la ficha de suscriptor incluida en el convenio, con el fin de poder realizar consultas posteriores, principalmente sobre cuáles son las personas autorizadas para actuar en nombre de este suscriptor.

El CESCO entrega al suscriptor la documentación (modelo de formulario) necesaria con el fin de solicitar certificados o le indica la sección del web de donde la puede obtener.

2. Procedimiento de alta cuando lo efectúa la Entidad de Registro:

Un miembro del órgano competente del suscriptor hace la correspondiente solicitud donde consta la relación autenticada de los usuarios que deben recibir un certificado, haciéndola llegar a un responsable de la Entidad de Registro quien sigue adelante con el proceso, o se obtienen los datos de manera automática de los sistemas de gestión de identidad de la Institución.

4.2. Procesamiento de la solicitud de certificación

4.2.1. Certificados personales

4.2.1.1. Cuando el CESCO actúa como Entidad de Registro

Cuando el CESCO recibe una nueva solicitud de certificado, en primer lugar registra la documentación, que se añade en el expediente del suscriptor.

El CESCO se asegura que las solicitudes de certificados son completas, precisas y están debidamente autorizadas y archivadas.

Si falta algún documento, el CESCO lo comunica al suscriptor por correo electrónico firmado, para que lo aporte, ya que el proceso de solicitud de certificados queda parado hasta que no se disponga de toda la documentación.

Posteriormente, una persona autorizada por el CESCO accede al sistema de certificación y una vez identificada, introduce todos los datos que el sistema le pide, obteniéndolos del expediente anteriormente indicado y que contiene la documentación necesaria (ya sea en papel o en formato electrónico).

Una vez introducidos todos los datos, éstos se verifican de acuerdo con la información de la solicitud y la documentación del expediente.

Si la solicitud es correcta, el CESCO:

- Aprueba la solicitud.
- Genera el par de claves, en su caso dentro de la tarjeta del futuro poseedor de claves.
- Solicita a la EC-UR la generación del certificado.

Si la solicitud presenta incorrecciones que no se pueden corregir, el CESCO la deniega definitivamente.

4.2.1.2. Cuando se efectúa el procesamiento por una Entidad de Registro

La Entidad de Registro recibe una nueva solicitud de certificado proveniente del órgano competente de la Institución (por ejemplo del Departamento de Recursos Humanos, del Rectorado, del Gerente, del Departamento de Matriculación, de la Secretaría Docente, etc.).

El procedimiento sigue mediante expedientes en papel o tramitación electrónica, informática o telemática, con la firma electrónica reconocida basada en un certificado CPISR-1 con cargo emitido por la EC-UR.

El usuario (profesor, miembro del PAS o estudiante) se presenta físicamente en la Entidad de Registro, con su tarjeta.

Una vez identificado con el original del DNI, NIE, pasaporte o equivalente inserta la tarjeta en la unidad de grabación.

Si la solicitud es correcta, la Entidad de Registro:

- Aprueba la solicitud
- Genera el par de claves, dentro de la tarjeta del futuro poseedor de claves.
- Solicita a la EC-UR la generación del certificado.

4.2.2. Requisitos específicos para el CEIXSA

Una vez aprobada la solicitud, la EC-UR recibe la autorización de la Entidad de Registro, recupera la correspondiente solicitud de la tabla de solicitudes, la almacena en el directorio de certificados, siendo firmada por la EC-UR, completando así la generación del certificado.

A partir de este momento el solicitante ya puede descargar desde el web su certificado y empezar a utilizarlo.

4.2.3. Informaciones adicionales para el CDS, el CDS-1 EV, el CDSCD y el CDS-1 Sede electrónica EV

Una vez aprobada la solicitud de certificado de servidor seguro el certificado queda pendiente de descarga.

Después de la recepción, en condiciones de seguridad, de la clave pública generada por el solicitante, la EC-UR procede a la emisión del certificado.

Los certificados digitales de dispositivo se entregarán mediante un fichero que tendrá que descargarse el responsable de la Entidad de Registro.

4.2.4. Informaciones adicionales para el CIPISR

Adicionalmente, la Entidad de Certificación tendrá que:

- Incluir en el certificado las informaciones establecidas en el artículo 11 de la Ley 59/2003, de acuerdo con lo establecido en la sección 7 de esta Declaración de Prácticas de Certificación.
- Garantizar la fecha y la hora en que se expidió un certificado
- En caso que la Entidad de Certificación aporte su dispositivo seguro de creación de firma, utilizar un procedimiento de gestión de dispositivos seguros de creación de firma que asegure que dicho dispositivo es entregado de forma segura al poseedor de claves.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Asegurarse que el certificado es emitido por sistemas que utilicen protección contra falsificación y, en caso que la Entidad de Certificación genere claves privadas, que garanticen el secreto de las claves durante el proceso de generación de dichas claves.

4.2.5. Otros certificados

Las solicitudes realizadas son procesadas y se realiza la validación. En el supuesto de que todo sea correcto, se crea la solicitud en la EC-UR. Seguidamente, se genera un mensaje de respuesta informando del resultado positivo o negativo de la operación y el tipo de error detectado en caso de ser el resultado negativo.

4.3. Emisión de certificado

4.3.1. Acciones de la EC-UR durante el proceso de emisión

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.

Para cada solicitud de certificado tramitada por la Entidad de Registro, la EC-UR tiene que:

- Utilizar un procedimiento de generación de certificados que vincule de forma segura el certificado con la información de registro, incluyendo la clave pública certificada
- En caso de que la Entidad de Certificación genere el par de claves, utilizar un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves y, que la clave privada es entregada de forma segura al suscriptor, en caso de certificados individuales, o al poseedor de claves en caso de certificados de organización.
- Proteger la confidencialidad e integridad de los datos de registro, especialmente en caso de que sean intercambiados con el suscriptor, en caso de certificados individuales, con el poseedor de claves, en caso de certificados de organización o con el tercer solicitante, en su caso¹.
- Incluir en el certificado las informaciones establecidas en el artículo 11.2 de la Ley 59/2003, de acuerdo con lo establecido en la sección correspondiente de esta Declaración de Prácticas de Certificación.
- Indicar la fecha y la hora en las que se expidió un certificado.
- En caso de que la Entidad de Certificación aporte el dispositivo seguro de creación de firma, utilizar un procedimiento de gestión de dispositivos seguros de creación de firma que asegure que este dispositivo es entregado de forma segura al poseedor de claves.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garantizan la seguridad técnica y en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Tomar medidas contra la falsificación de certificados y, en caso de que la Entidad de Certificación genere claves privadas, que garanticen el secreto de las claves durante el proceso de generación de estas claves.

4.3.2. Comunicación de la emisión al suscriptor

La EC-UR comunica al suscriptor la emisión del certificado, o la incidencia correspondiente.

¹ TS 101 456: 7.3.3 e)

4.4. Aceptación del certificado

4.4.1. Responsabilidades de la Entidad de Registro

4.4.1.1. Para Certificados personales y de entidad

El CESCA es el encargado de crear el par de claves y el certificado de los suscriptores.

El CESCA también crea los correspondientes códigos PIN y PUK de las tarjetas (dispositivos criptográficos) donde se alojan el par de claves y el certificado. Para cada poseedor genera dos copias de la hoja de entrega; una para el poseedor y la otra para el suscriptor.

Estos códigos se podrán reenviar directamente al poseedor de claves, éste los podrá solicitar a través de la aplicación telemática en cualquier momento.

En la hoja de entrega y aceptación del certificado se indica a éste:

- custodiar la hoja de entrega de poseedor debidamente firmado durante 15 años,
- se pide al poseedor que esté informado sobre el tratamiento de sus datos, respecto de la normativa de protección de datos y que dé consentimiento para el tratamiento y la inclusión de ciertos datos en el certificado.

En la hoja de entrega y aceptación del poseedor, se indica a éste:

- cuál es el régimen obligatorio de uso de certificados digitales:
- la existencia de esta Declaración de Prácticas de Certificación,
- que los certificados son únicos para cada persona y están protegidos por un código secreto,
- que los certificados permiten identificarse, generar firmas electrónicas y, en su caso, descifrar mensajes,
- que tiene que custodiar la tarjeta y el código secreto,
- que en caso de indicio que su identificación puede ser conocida por otras personas tiene que notificarlo a su Entidad de Registro,
- Que en caso de necesidad de información adicional, puede dirigirse a su Entidad de Registro,
- que puede ejercer sus derechos incluidos en la ley 15/1999, de 13 de diciembre, sobre protección de datos personales,
- que sus datos podrán ser cedidos, en cumplimiento de la legislación vigente sobre firma electrónica y protección de datos personales, y
- cuáles son los certificados incluidos en la tarjeta y el código de suspensión
- que firma el documento de entrega, ya que está conforme, una vez leídas y entendidas las obligaciones y responsabilidades.

4.4.1.2. Para certificados de dispositivo

Los certificados de dispositivo se entregarán mediante un fichero que se tendrá que descargar el responsable de la entidad de registro.

L'EC-UR generará la hoja de entrega para cada poseedor de claves, EL Consorci AOC enviará mediante correo electrónico directamente a los poseedores de claves los códigos PIN y PUK, si procede, de acuerdo con el tipo de certificado.

Estos códigos se podrán reenviar directamente al poseedor de claves, que los podrá solicitar a través de la aplicación telemática en cualquier momento.

4.4.2. Conducta que constituye aceptación del certificado

El certificado se acepta mediante la firma de la hoja de entrega y aceptación del certificado de poseedor de claves.

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

A través de la aplicación telemática se podrán obtener informes de todos los certificados gestionados por la Entidad de Registro en el momento actual o hacer una recopilación histórica.

4.4.3. Publicación del certificado

Los certificados se pueden publicar sin el consentimiento previo de los poseedores de claves, excepto los certificados de clase 2 (de estudiante) que se exige 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 del par de claves por los poseedores de claves y uso de los certificados por los suscriptores

4.5.1.1. Información para todos los tipos de certificados

Los certificados se utilizan para permitir una mejor seguridad en las comunicaciones telemáticas internas de las Instituciones, como entre ellas, así como las que se realicen con el resto de la sociedad.

Los certificados se utilizan de acuerdo con su función propia y finalidad establecida, y no se pueden utilizar en otras funciones o con otras finalidades.

Se deben utilizar de acuerdo con la ley aplicable, teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

El uso del par de claves y del certificado permite al poseedor de claves identificarse, generar firmas electrónicas y, en su caso, descifrar aquellos mensajes en los que el emisor ha decidido preservar el contenido.

La extensión Key Usage se utiliza para establecer límites técnicos a los usos que puede darse a una clave privada correspondiente a una clave pública listada en un certificado X.509v3.

Sin embargo, se debe tener en cuenta que se da la circunstancia 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 estar controladas por las Entidades de Certificación.

4.5.1.2. Informaciones adicionales para los certificados personales y de dispositivo

Los certificados personales y de dispositivo no se pueden utilizar para firmar otros certificados, o información del estado de certificados, de ninguna manera.

4.5.1.3. Informaciones adicionales para los CIPISR

Los CIPISR se utilizan necesariamente con un dispositivo seguro de creación de firma electrónica, cumpliendo las características establecidas por el artículo 24 de la Ley 59/2003, de 19 de diciembre y esta Declaración de Prácticas de Certificación (DPC).

Se utiliza el par de claves exclusivamente para crear firmas electrónicas y de acuerdo con cualquier otra limitación que sea notificada.

Se es especialmente diligente en la custodia de la clave privada y el dispositivo seguro de creación de firma, con la finalidad de evitar usos no autorizados.

4.5.1.4. Informaciones adicionales para los CPISR

Los CPISR se utilizan necesariamente con un dispositivo seguro de creación de firma electrónica, que cumple las características establecidas por el artículo 24 de la Ley 59/2003, de 19 de diciembre, de firma electrónica y esta Declaración de Prácticas de Certificación (DPC).

Se utiliza el par de claves exclusivamente para crear firmas electrónicas y de acuerdo con cualquier otra limitación que sea notificada.

Se debe ser especialmente diligente en la custodia de la clave privada y del dispositivo seguro de creación de firma, con la finalidad de evitar usos no autorizados.

4.5.1.5. Informaciones adicionales para el CPIXSA

Se debe ser especialmente diligente en la custodia de la clave privada con la finalidad de evitar usos no autorizados.

4.5.1.6. Informaciones adicionales para el CPX

Estos certificados se utilizan en conjunción con un dispositivo de protección de la clave privada de descifrado, de acuerdo con las características establecidas en este documento.

4.5.1.7. Informaciones adicionales para el CEISR

Los CEISR se utilizan necesariamente con un dispositivo seguro de creación de firma electrónica, que cumple las características establecidas por el artículo 24.3 de la Ley 59/2003, de 19 de diciembre y esta Declaración de Prácticas de Certificación (DPC).

Se utiliza el par de claves exclusivamente para crear firmas electrónicas y de acuerdo con cualquier otra limitación que sea notificada.

Se debe ser especialmente diligente en la custodia de la clave privada y del dispositivo seguro de creación de firma, con la finalidad de evitar usos no autorizados.

4.5.1.8. Informaciones adicionales para el CEX

Los CEX se utilizan en conjunción con un dispositivo de protección de la clave privada de descifrado, de acuerdo con las características establecidas en este documento.

4.5.1.9. Informaciones adicionales para el CEIXSA

Se debe ser especialmente diligente en la custodia de la clave privada con el fin de evitar usos no autorizados.

4.5.1.10. Informaciones adicionales para los CDS-1, los CDS-1 EV y los CDS-1 Sede electrónica EV

Los CDS-1 y los CDS-1 EV han de utilizarse en conjunción con un dispositivo de protección de la clave privada de descifrado, de acuerdo con los requisitos establecidos en la política de certificación y las Condiciones Generales de Uso.

4.5.2. Uso por el tercero que confía en los certificados

Los certificados se utilizan de acuerdo con su función propia y finalidad establecida, sin que puedan utilizarse en otras funciones y con otras finalidades. De la misma forma, los certificados se utilizan únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

El uso del certificado permite al tercero que confía, una identificación positiva, recibir y confiar en firmas electrónicas y, en su caso, cifrar aquellos mensajes en que ha decidido preservar su contenido.

La extensión Key Usage se utiliza para establecer límites técnicos a los usos que puede darse a una clave privada correspondiente a una clave pública listada en un certificado X.509v3.

Debe tenerse en cuenta que se da la circunstancia 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 estar controladas por la EC-UR.

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

La renovación de un certificado se inicia dos meses antes de la fecha de expiración del certificado, cuando el suscriptor recibe un correo electrónico donde se le informa de los pasos a seguir para ejecutar la renovación del certificado. Este correo se vuelve a enviar 30 días antes de la expiración si el certificado aun no se ha renovado.

El proceso para la renovación de un certificado es el mismo que se sigue para la emisión de nuevos certificados.

4.8. Modificación de certificados

El solicitante de un certificado deberá requerir la modificación de los certificados cuando tenga conocimiento de cambios en la información obligatoria o la relativa a cargos, límites de uso o dispositivos usuarios de los certificados (p.ej. direcciones IP o datos de servidores o aplicaciones). Igualmente, podrá requerir la modificación del resto de los datos incluidos en el certificado. Para realizar las modificaciones, la Entidad de Registro podrá requerir la acreditación de las condiciones justificativas de la modificación. La modificación de los datos de los certificados comporta la revocación y la emisión de un nuevo certificado. A todos los efectos, la modificación se considerará renovación.

4.9. Revocación y suspensión de certificados

4.9.1. Causas de revocación de certificados

La EC-UR puede revocar un certificado por las siguientes causas:

1. Circunstancias que afectan a la información contenida en el certificado:
 - Modificación de alguno de los datos contenidos en el certificado.
 - Descubrimiento que alguno de los datos contenidos en la solicitud de certificado es incorrecta.
 - Descubrimiento que alguno de los datos contenidos en el certificado es incorrecto, así como la alteración o modificación de las circunstancias verificadas por la expedición del certificado.
2. Circunstancias que afectan a la seguridad de la clave o del certificado:
 - Compromiso de la clave privada o de la infraestructura o sistemas de la EC-UR, siempre que afecte a la confianza en los certificados emitidos a partir de este incidente.
 - Infracción, por la EC-UR, de los requisitos previstos en los procedimientos de gestión de certificados establecidos en este documento.
 - Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del suscriptor.
 - Acceso o utilización no autorizados, por parte de un tercero, de la clave privada del suscriptor.
 - El uso irregular del certificado por el suscriptor o falta de diligencia en la custodia de la clave privada.

3. Circunstancias que afectan al dispositivo criptográfico:
 - Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
 - Pérdida o inutilización del dispositivo criptográfico.
 - Acceso no autorizado por un tercero, a los datos de activación del suscriptor.
4. Circunstancias que afectan al suscriptor o el poseedor de claves:
 - Fin de la relación entre la EC-UR y el suscriptor.
 - Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al suscriptor.
 - Infracción por parte del solicitante del certificado de los requisitos preestablecidos para la solicitud de éste.
 - Infracción por parte del suscriptor de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente de la EC-UR o en este documento.
 - La extinción de la persona jurídica suscriptora del certificado, así como la finalidad de la autorización del suscriptor al poseedor de claves o el fin de la relación entre suscriptor y poseedor de claves.
 - Solicitud del suscriptor de revocación del certificado.
5. Circunstancias relativas a los certificados Extended Validation:
 - Solicitud del suscriptor.
 - La Entidad de Certificación obtiene pruebas razonables de que la clave privada del suscriptor se ha visto comprometida o que el certificado ha sido usurpado por un tercero.
 - La Entidad de Certificación recibe notificación o comunicación por parte de un tribunal o árbitro sobre la revocación del derecho a utilizar el nombre de dominio que figura en el certificado o conoce la imposibilidad de renovar el dominio.
 - La Entidad de Certificación tiene conocimiento del incumplimiento de las Condiciones Generales de Uso o de otras especificaciones establecidas en la documentación jurídica u operativa.
 - La Entidad de Certificación cesa actividades que dan soporte a la revocación de certificados Extended Validation o pierde el derecho de emitir certificados Extended Validation. Si la Entidad de Certificación puede garantizar el mantenimiento de los servicios de validación CRL y OCSP, la revocación no es necesaria.
 - Compromiso o sospecha de compromiso de las claves de cualquier Entidad de Certificación de nivel superior en la jerarquía.
 - Revocación de las publicaciones de las políticas relativas a certificados Extended Validation.
 - Notificación de la inclusión de un suscriptor en el listado de suscriptores prohibidos (también listas negras, confeccionadas para víctimas de phishing o actividades de ingeniería inversa).

6. Otras circunstancias:

- La suspensión del certificado digital por un periodo superior a 120 días.
- La finalización del servicio de la EC-UR, de acuerdo con lo establecido en la sección 5.8 de este documento.
- La finalización de la prestación de servicios por parte del Consorci AOC, de acuerdo con lo que establece la Política General de Certificación.
- Resolución judicial o administrativa que lo ordene (Art. 8.1 de la Ley 59/2003, de firma electrónica).
- La EC-UR tiene conocimiento de que los certificados CDP han realizado firmas sobre código hostil.

Si la entidad a la cual se dirige la solicitud de revocación no dispone de toda la información necesaria para determinar la revocación de un certificado, pero tiene indicios de su compromiso, puede decidir su suspensión. En este caso se considera que las actuaciones realizadas durante el periodo de suspensión no son válidas, siempre que el certificado finalmente sea revocado. Serán válidas si se levanta la suspensión (habilitación) y el certificado vuelve a pasar a la situación de válido.

El instrumento jurídico que vincula la EC-UR con el suscriptor establece que el suscriptor tiene que solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias indicadas anteriormente.

4.9.2. Legitimación para solicitar la revocación

La solicitud de revocación puede ser pedida por el suscriptor del certificado, el Consorci AOC, el CESCA o la Entidad de Registro que solicitó la emisión del certificado. Los poseedores de claves tendrán que comunicar al suscriptor las circunstancias previstas por la Ley o esta Declaración, y que pueden dar lugar a la revocación del certificado que, en su caso, deberá ser solicitada por el suscriptor.

4.9.3. Procedimientos de solicitud de revocación

El procedimiento de revocación la lleva a cabo después de una solicitud del suscriptor o de oficio por el Consorci AOC si se diera alguna de las causas establecidas en el apartado 4.9.1. En la recepción de la solicitud, el operador de la Entidad de Registro o el operador del centro de llamadas, accede a la aplicación web con un certificado de operador y procede a suspender el certificado. A continuación, el Consorci AOC o en su caso la Entidad de Registro directamente, examina la solicitud y procede a la renovación definitiva del certificado y a continuación y de forma automática e inmediata se indica la citada revocación en el estado del certificado en la lista de revocaciones.

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-URV, 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, que realiza la revocación en la aplicación telemática y, a continuación y de forma automática y casi inmediata, se incluirá esta revocación en la lista de certificados revocados. Se informa al subscriptor y, en su caso, el poseedor de claves, sobre el cambio de estado de revocación del certificado de acuerdo con el artículo 10.2 de la Ley de firma electrónica.

La EC-UR no puede reactivar el certificado una vez revocado.

Nota: Un certificado revocado no puede volver a utilizarse; eso quiere decir que no puede alzarse la revocación, ni no anularse de ninguna otra forma: es un estado definitivo del certificado.

4.9.4. Plazo temporal de solicitud de revocación

Las solicitudes de revocación se remiten de forma razonablemente inmediata cuando se tenga conocimiento de la causa de revocación.

4.9.5. Plazo máximo de procesamiento de la solicitud de revocación

La solicitud de revocación es procesada en el mínimo plazo posible.

4.9.6. Obligación de consulta de información de revocación de certificados

Los verificadores comprueban el estado de aquellos certificados en los que deseen 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-UR. El estado de vigencia también se puede comprobar online mediante el protocolo OCSP.

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

4.9.7. Frecuencia de emisión de listas de revocación de certificados (LRCs)

La EC-UR emite una LRC al menos cada 24 horas. Además se emite una nueva LRC después de cada suspensión o revocación.

Se indica en la LRC el momento programado de emisión de una nueva LRC, aunque se puede emitir una LRC antes del plazo indicado en la LRC anterior, cada vez que se revoque o se suspenda un certificado.

Los certificados revocados o suspendidos son retirados de la LRC transcurridos sesenta días desde la expiración.

4.9.8. Periodo máximo de publicación de LRCs

Las LRCs son publicadas inmediatamente en la web del Consorci AOC (<http://www.aoc.cat/catcert/>).

4.9.9. Disponibilidad de servicios de comprobación de estado de certificados

De forma alternativa los verificadores pueden consultar los certificados publicados en el directorio de la EC-UR, a través de una interficie web, que está disponible las 24 horas de los 7 días de la semana. Los verificadores de certificados digitales pueden consultar un servicio en línea 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 que se confía.

El Consorci AOC ofrece de forma gratuita un servicio *OCSP responder* para la comprobación en línea del estado de los certificados emitidos por las Entidades de Certificación que integren la jerarquía pública de certificación de Catalunya.

LA URL en la que se encuentra disponible el citado 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>.

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

El verificador que no utiliza LRC para comprobar la validez de un certificado, lo puede hacer en el directorio de la EC-UR.

Los verificadores tienen que comprobar obligatoriamente el estado de aquellos certificados en los que deseen confiar.

Una forma de verificar el estado de los certificados es consultando la LRC más reciente de la EC-UR.

La EC-UR suministra información a los verificadores en lo referente a cómo y dónde encontrar la LRC correspondiente.

4.9.11. Otras formas de información de revocación de certificados

La EC-UR también informará sobre la revocación de los certificados, mediante el protocolo OCSP, que permite conocer el estado de vigencia de los certificados on-line.

En la petición de consulta de vigencia de un certificado en línea se ha de consignar un número de serie del certificado sobre el cual se realiza la petición y los datos identificativos de la autoridad de certificación emisora.

Si la petición no está válidamente realizada o si el servicio no puede dar respuesta en el momento de la solicitud, el servicio OCSP devolverá una respuesta que identifique el motivo por el cual no se devuelve esta respuesta (solicitante no autorizado, error en la respuesta o inoperatividad temporal del prestador requerido).

Si la petición está válidamente realizada y los servicios no tienen ninguna disfunción, se responderá a la petición con la consignación de que el certificado es válido o que está

revocado (en este caso se consignará también el momento de la finalización de la vigencia del certificado).

Esta respuesta será firmada por la Entidad de Certificación con el certificado correspondiente (en este caso, el certificado de infraestructura de servidor de estado de certificados en línea –que recibe el acrónimo CIO). Esta respuesta será almacenada.

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

El compromiso de la clave privada de la EC-UR es comunicado, en la medida de lo posible, a todos los participantes en la jerarquía pública de certificación de Cataluña y a todos los terceros verificadores, mediante el directorio del Consorci AOC.

4.9.13. Causas de suspensión de certificados

Los certificados se pueden suspender:

- Cuando lo solicite el poseedor de claves, el suscriptor o un tercero autorizado (art. 9.1.a de la Ley 59/2003).
- En los casos legalmente previstos en el artículo 9.1 de la Ley de Firma electrónica, esto es, en el caso de que una resolución judicial o administrativa lo ordene.
- Cuando lo solicite el poseedor de claves o el suscriptor.
- Cuando la documentación requerida en la solicitud de revocación sea suficiente pero no se pueda identificar razonablemente al poseedor de claves.
- Cuando la documentación requerida en la solicitud de revocación no sea suficiente, aunque se pueda identificar razonablemente al poseedor de claves.
- Cuando la documentación requerida en la solicitud de revocación no sea suficiente y tampoco permitan identificar razonablemente al poseedor de claves.
- Si el suscriptor no utiliza el certificado durante un periodo prolongado de tiempo, conocido previamente.
- Si se sospecha el compromiso de una clave, hasta que éste sea confirmado. En este segundo caso, la EC-UR debe asegurarse que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.
- Cuando no se activa el certificado en un plazo de 120 días a partir de la fecha de emisión del certificado.

4.9.14. Legitimación para solicitar la suspensión

1. El poseedor de claves del certificado.
2. El suscriptor que pidió la emisión de certificados (Solicitante de la Entidad de Registro).
3. Las Entidades de Certificación o las Entidades de Registro, que emitieron el certificado.

4.9.15. Procedimientos de solicitud de suspensión

La suspensión de los certificados digitales se puede realizar de las formas que se detallan a continuación, informando en todo caso al suscriptor de acuerdo con lo previsto en el artículo 10.2 de la Ley de firma electrónica:

1. La suspensión puede ser solicitada por el poseedor de las claves y se puede llevar a cabo por medio de una llamada telefónica al 902 90 10 80.
2. La suspensión puede ser solicitada por el suscriptor del certificado y se puede realizar por vía telefónica al 902 90 10 80.
3. La suspensión puede ser solicitada por el CESCO o por la Entidad de Registro. En caso de que la Entidad de Registro disponga de autorización de el Consorci AOC, podrá realizar ella misma el proceso de suspensión. En caso contrario, realiza la tramitación de la suspensión a través del Consorci AOC.
4. La suspensión puede ser realizada por la EC-UR directamente, a través del componente LRA o RRA.

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 (en caso de que no sea el mismo poseedor).
- Información de contacto de la entidad que pide la suspensión.
- Nombre y apellidos del poseedor de claves a quien se le debe suspender el certificado digital.
- DNI del poseedor de claves a quien se le debe suspender el certificado digital.
- Organismo y departamento al que pertenece el poseedor de claves.
- Número de serie (serial number) del certificado digital que se solicita suspender.
- Motivo de la petición de suspensión.
- Código de suspensión asociado al certificado o, por defecto, pregunta y respuesta secreta escogida en el momento de activar el certificado.

Una vez suspendida la vigencia de un certificado se informará al suscriptor y, en su caso, al poseedor de claves, sobre el cambio de estado de suspensión y que el plazo máximo de la misma será de 120 días naturales (arts. 10.2 y 10.4 de la Ley 59/2003).

4.9.16. Período máximo de suspensión

El plazo máximo de suspensión será de ciento veinte días naturales.

4.9.17. Habilitación de un certificado suspendido

El suscriptor podrá habilitar el certificado que permanece suspendido, personándose e identificándose ante la Entidad de Registro, firmando el correspondiente documento de solicitud de habilitación comunicando 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 LCR se publican en la web 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 de la EC-UR.

4.10.2. Disponibilidad de los servicios

Los verificadores de certificados digitales pueden consultar un servicio en línea 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 gratuita 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>

4.10.3. Otras funciones de los servicios

Sin estipulaciones adicionales.

4.11. Fin de la suscripción

El fin de la suscripción no implica la revocación de los certificados que hayan sido emitidos, sino que estos pueden utilizarse hasta que expiren.

4.12. Depósito y recuperación de claves

4.12.1. Política y prácticas de depósito y recuperación de claves

No se practica recuperación de claves

4.12.2. Política y prácticas de encapsulamiento y recuperación de claves de sesión

Sin estipulaciones adicionales.

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

Sin estipulaciones adicionales.

5.1 Controles de seguridad física

5.1.1 Localización y construcción de las instalaciones

Sin estipulaciones adicionales.

5.1.2 Acceso físico

Sin estipulaciones adicionales.

5.1.3 Electricidad y aire acondicionado

Sin estipulaciones adicionales.

5.1.4 Exposición al agua

Sin estipulaciones adicionales.

5.1.5 Advertencia y protección de incendios

Sin estipulaciones adicionales.

5.1.6 Almacenaje de soportes

Sin estipulaciones adicionales.

5.1.7 Tratamiento de residuos

Sin estipulaciones adicionales.

5.1.8 Copia de seguridad fuera de las instalaciones

Sin estipulaciones adicionales.

5.2 Controles de procedimientos

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

5.2.1 Funciones fiables

Sin estipulaciones adicionales.

5.2.2 Número de personas por tarea

Sin estipulaciones adicionales.

5.2.3 Identificación y autenticación para cada función

Sin estipulaciones adicionales.

5.2.4 Roles que requieren separación de tareas

Sin estipulaciones adicionales.

5.3 Controles de personal

La EC-UR 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 permitan 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 de Certificación Digital.
- el Responsable de la EC-UR.
- 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.
- los Usuarios de la EC-UR.

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

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

5.3.1 Requisitos de historial, calificaciones, experiencia y autorización

Sin estipulaciones adicionales.

5.3.2 Requisitos de formación

Sin estipulaciones adicionales.

5.3.3 Requisitos y frecuencia de actualización formativa

Sin estipulaciones adicionales.

5.3.4 Secuencia y frecuencia de rotación laboral

Sin estipulaciones adicionalesSin estipulaciones adicionales.

5.3.5 Sanciones por acciones no autorizadas

Sin estipulaciones adicionales.

5.3.6 Requisitos de contratación de profesionales

Sin estipulaciones adicionales.

5.3.7 Suministro de documentación al personal

Sin estipulaciones adicionales.

5.4 Procedimientos de auditoría de seguridad

5.4.1 Tipos de acontecimientos registrados

Sin estipulaciones adicionales.

5.4.2 Frecuencia de tratamiento de registros de auditoría

Sin estipulaciones adicionales.

5.4.3 Periodo de conservación de registros de auditoría

Sin estipulaciones adicionales.

5.4.4 Protección de los registros de auditoría

Sin estipulaciones adicionales.

5.4.5 Procedimientos de generación de copias de seguridad

Se generan copias de seguridad 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 Certificación.

5.4.6 Localización del sistema de acumulación de registros de auditoría

Sin estipulaciones adicionales.

5.4.7 Notificación del acontecimiento de auditoría al causante del acontecimiento

Sin estipulaciones adicionales.

5.4.8 Análisis de vulnerabilidades

Sin estipulaciones adicionales.

5.5 Archivo de informaciones

Sin estipulaciones adicionales.

5.5.1 Tipos de acontecimientos registrados

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

La EC-UR guarda un registro de lo siguiente:

Documentos originales:

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

Fotocopias de:

- Carta de entrega de certificados CPISR y CPX
- Carta PIN y PUK, con acuse de recibo.

La EC-UR guarda, en relación con los certificados Extended Validation:

- Logs y pistas de auditoria
- Documentación relativa a peticiones, verificaciones y revocaciones de certificados Extended Validation

5.5.2 Periodo de conservación de registros

La EC-UR 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.

La EC-UR guarda los registros especificados en la sección 5.5.1 en relación con los certificados Extended Validation por un período de 7 años, contados desde el momento de la expedición del certificado.

5.5.3 Protección del archivo

Sin estipulaciones adicionales.

5.5.4 Procedimientos de generación de copias de seguridad

Sin estipulaciones adicionales.

5.5.5 Requisitos de sellado de cautela de fecha y hora

Sin estipulaciones adicionales.

5.5.6 Localización del sistema de archivo

Sin estipulaciones adicionales.

5.5.7 Procedimientos de obtención y verificación de información de archivo

Sin estipulaciones adicionales.

5.6 Renovación de claves

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

5.7 Compromiso de claves y recuperación de desastre

5.7.1 Procedimiento de gestión de incidencias y compromisos

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

En caso de compromiso la EC-UR:

- 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-UR ya no son válidos.

5.7.4 Desastre sobre las instalaciones

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

5.8 Finalización del servicio

5.8.1 EC-UR

Sin estipulaciones adicionales.

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.

Sin estipulaciones adicionales Sin estipulaciones adicionales

6. Controles de seguridad técnica

La EC-UR 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

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

6.1.1.2. Información para los certificados CPISR y CEISR

Las claves pública y privada de los certificados CPISR i CEISR se generan por parte del Consorci AOC dentro de un dispositivo seguro de creación de firma electrónica (tarjeta que recibe el poseedor de claves)

6.1.1.3. Información para los certificados CPIXSA

Las claves pública y privada de los certificados CPIXSA se generan por parte del Consorci AOC y son enviados al poseedor de claves de forma segura. Estas claves no se almacenan, de modo que el Consorci AOC no responderá por la pérdida de información en caso de suspensión, revocación o expiración del certificado.

6.1.1.4. Información para los certificados CPX y CEX

Las claves pública y privada de los certificados CPX i CEX se generan por parte del Consorci AOC y son insertadas en el dispositivo de descifrado.

Adicionalmente una copia de la clave privada se almacena en los sistemas del Consorci AOC.

6.1.1.5. Información para los certificados CEIXSA

El par de claves es generado por el futuro poseedor de claves

6.1.1.6. Información para los certificados CDS-1, CDS-1EV y CDSCD-1

La clave pública de los certificados CDS-1, CDS-1 EV y CDSCD-1 se generan bajo su responsabilidad, por parte de la Entidad de Registro. La clave privada la genera la institución que solicita el certificado.

6.1.1.7. Información para los certificados CDS-1 Sede electrónica EV

Las claves pública y privada de los certificados CDS-1 Sede electrónica EV se generan bajo su responsabilidad, por parte de la Entidad de Registro, dentro de un dispositivo seguro de creación de firma electrónica. La clave pública de los certificados se genera bajo su responsabilidad, por parte de la Entidad de Registro y la clave privada la genera la Institución que solicita el certificado y, en ningún caso, se envía a la Entidad de Registro.

6.1.1.8. Información para los certificados CDA-1 Sello electrónico

Las claves pública y privada de los certificados CDA-1 Sello electrónico se generan bajo su responsabilidad, por parte de la Entidad de Registro, dentro de un dispositivo seguro de creación de firma electrónica. La clave privada la genera la Institución que solicita el certificado y, en ningún caso, se envía a la Entidad de Registro.

6.1.1.9. Información para los certificados CDP

Las claves pública y privada de los certificados CDP se generan bajo su responsabilidad, por parte de la Entidad de Registro, dentro de un dispositivo seguro de creación de firma electrónica (tarjeta que recibe el poseedor de claves), o bien en software.

6.1.2. Envío de la clave privada al suscriptor

6.1.2.1. Información para los certificados CPISR, CEISR, CDP, CPX y CEX

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.

6.1.2.2. Información para los certificados CEIXSA

La clave privada es generada por el suscriptor en su sistema informático y no debe salir bajo ningún concepto de este sistema, por lo tanto no existe ningún envío de la clave privada, en ninguna dirección.

6.1.3. Envío de la clave pública al emisor del certificado

El método de envío de la clave pública a la EC-UR es PKCS #10

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

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

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

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

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

Los usuarios acceden al directorio para obtener las claves públicas de la EC-UR.

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-UR es al menos de 2.048 bits.

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

6.1.6. Generación de parámetros de clave pública

Sin estipulaciones adicionales.

6.1.7. Comprobación de calidad de parámetros de clave pública

Se realiza de acuerdo con el informe especial del ETSI TS 101 276, 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-UR son generados utilizando hardware criptográfico que cumple los requisitos establecidos por la especificación técnica CEN CWA 14167 o equivalente.

Los pares de claves de los suscriptores de certificados CPISR, CPX, CEISR, CEX, CDS-1 de sede electrónica de nivel alto y CDA-1 de sello electrónico de nivel alto deben generarse en el componente de Autoridad de Registro Local 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-UR 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

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 reconocidos 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, o bien directamente por el Consorci AOC cuando actúa como Entidad de Registro Virtual.

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 libraré 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-UR requiere la concurrencia de al menos 2 de forma simultánea.

Cada uno de estos dispositivos es responsabilidad de una persona concreta, única concedora 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-UR, y para su acceso es necesaria una persona adicional.

6.2.3. Depósito de la clave privada

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

Las claves privadas de los certificados de cifrado sí se podrán almacenar en la EC-UR.

6.2.4. Copia de seguridad de la clave privada

Existe copia de seguridad de la clave privada de la EC-UR 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-UR cuenta con una copia de seguridad realizada, almacenado, y recuperado 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-UR.

Los controles de seguridad a aplicar en copias de seguridad de la EC-UR 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.

No se almacenan copias de las claves privadas de los certificados.

6.2.6. Introducción de la clave privada en el módulo criptográfico

Las claves privadas de la EC-UR 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-UR.

Para certificados personales y de entidad, la clave privada del suscriptor se activa mediante la introducción del PIN en la tarjeta inteligente.

6.2.9. Método de desactivación de la clave privada

No aplicable.

6.2.10. Método de destrucción de la clave privada

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

6.2.11. Clasificación de los módulos criptográficos

Los módulos de la EC-UR 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 reconocidos y certificados de nivel alto 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 o equivalente.

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

La EC-UR archiva sus claves públicas, de acuerdo con lo establecido en la sección 5.5

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-UR 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 los datos de activación

6.4.2.1. Para certificados personales y de entidad

a) Cuando el CESCO actúa como Entidad de Registro:

Para proteger al máximo los datos de activación se distribuyen 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.

b) Cuando la Institución dispone de Entidad de Registro:

Para proteger al máximo los datos de activación, cuando el poseedor de claves se presenta físicamente ante la Entidad de Registro, esta crea en su presencia los datos de activación de firma o en todo caso, se cambian.

4.12.2.1. Para certificados de dispositivo CDS-1, CDS-1 EV, CDSDC-1 y CDS-1 Sede electrónica de nivel medio EV y CDA-1 sello electrónico de nivel alto

La distribución de los datos de activación para los certificados de dispositivo CDS-1, CDS-1 EV, CDSDC-1, CDS-1 Sede electrónica de nivel medio EV y CDA-1 Sello electrónico de nivel alto es diferente a la de los certificados personales (no tiene ni PIN ni PUK ni tarjeta), que la privada la genera el propio suscriptor que ha pedido el certificado.

6.4.3. Otros aspectos de los datos de activación

Sin estipulaciones adicionales.

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-UR 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-UR 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-UR, 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-UR está identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.
- El personal de la EC-UR 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-UR (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-UR garantiza que sus funciones de gestión de las operaciones de los módulos criptográficos son suficientemente seguras y, en particular, ha de 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 código malicioso, para garantizar la integridad y la validez de la información que procesan

La EC-UR 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 .

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

6.6.3. Evaluación del nivel de seguridad del ciclo de vida

Sin estipulaciones adicionales.

6.7. Controles de seguridad de red

Se garantiza que el acceso a las diferentes redes de la EC-UR 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-UR.

- 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 enrutadores) se encuentran ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.

6.8. Sello de tiempo

Sin estipulaciones adicionales.

7. Perfiles de certificados y listas de certificados revocados

7.1 Perfil de certificado

Sin estipulaciones adicionales.

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

7.2 Perfil de la lista de revocación de certificados

El acceso a la información relativa a la lista de revocación de certificados se publica en la web del Consorci AOC <http://www.aoc.cat/catcert/>.

8. Auditoría de conformidad

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

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

8.1 Frecuencia de la auditoría de conformidad

Sin estipulaciones adicionales

8.2 Identificación y calificación del auditor

El CESCA (ejerciendo como departamento de auditoría interna) o un Departamento de la Institución que dispone de Entidad de Registro, puede encargarse de realizar la auditoría de conformidad.

No obstante la EC-UR puede acudir a un auditor independiente externo, el cual debe 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-UR auditada.

8.4 Relación de elementos objeto de auditoría

Sin estipulaciones adicionales.

8.5 Acciones a emprender como resultado de una falta de conformidad

Sense estipulació adicional.

8.6 Tratamiento de los informes de auditoría

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

9. Requisitos comerciales y legales

9.1 Tarifas

9.1.1 Tarifa de emisión o renovación de certificados

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

9.1.2 Tarifa de acceso a certificados

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

9.1.3 Tarifa de acceso a información de estado de certificado

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

9.1.4 Tarifas de otros servicios

Sin estipulaciones adicionales Sin estipulaciones adicionales

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 del Consorci AOC como prestador de servicios de certificación.

9.2.2 Otros activos

Sin estipulaciones adicionales Sin estipulaciones adicionales.

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

En caso de uso incorrecto o no autorizado de los certificados, el Consorcio AOC (o la EC-UR) no actuará como agente fiduciario ante suscriptores y terceras personas, que deberán

dirigirse contra el infractor de las condiciones de uso de los certificados establecidas por el Consorcio AOC (o la EC-UR).

9.3 Confidencialidad

9.3.1 Informaciones confidenciales

Sin estipulaciones adicionales.

9.3.2 Informaciones no confidenciales

Sin estipulaciones adicionales.

9.3.3 Responsabilidad para la protección de información confidencial

Sin estipulaciones adicionales.

9.4 Protección de datos personales

9.4.1 Política de Protección de Datos Personales

Sin estipulaciones adicionales.

9.4.2 Datos de carácter personal no disponibles a terceros

Sin estipulaciones adicionales.

9.4.3 Datos de carácter personal disponibles a terceros

Sin estipulaciones adicionalesSin estipulaciones adicionales.

9.4.4 Responsabilidad correspondiente a la protección de los datos personales

Sin estipulaciones adicionales.

9.4.5 Gestión de incidencias relacionadas con los datos de carácter personal

Sin estipulaciones adicionales.

9.4.6 Prestación del consentimiento en el uso de los datos personales

Sin estipulaciones adicionales.

9.4.7 Comunicación de datos personales

Sin estipulaciones adicionales.

9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de los certificados e información de revocación

Sin estipulaciones adicionales.

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

Sin estipulaciones adicionales

9.5.3 Propiedad de la información relativa a nombres

Sin estipulaciones adicionales.

9.5.4 Propiedad de claves

Sin estipulaciones adicionales.

9.6 Obligaciones y responsabilidad civil

9.6.1 Entidades de Certificación

9.6.1.1 Obligaciones generales de la EC-UR

- Sin estipulaciones adicionales.

9.6.1.2 Garantías ofrecidas a suscriptores y verificadores

Sin estipulaciones adicionales.

9.6.2 Obligaciones y otros compromisos de las Entidades de Registro

9.6.2.1 Obligaciones y otros compromisos

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

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

9.6.3 Garantías ofrecidas a suscriptores y verificadores

9.6.3.1 Garantía del Consorci AOC por los servicios de certificación digital

9.6.3.2 Sin estipulaciones adicionales Exclusión de la garantía

Sin estipulación adicional

9.6.4 Suscriptores

9.6.4.1 Obligaciones y otros compromisos

Sin estipulaciones adicionales

9.6.4.2 Garantías ofrecidas por el suscriptor

Sin estipulaciones adicionales

9.6.4.3 Protección de la clave privada

Sin estipulaciones adicionales.

9.6.5 Verificadores

9.6.5.1 Obligaciones y compromisos

Sin estipulaciones adicionales.

9.6.5.2 Garantías ofrecidas por el verificador

Sin estipulaciones adicionales

9.6.6 Otros participantes

9.6.6.1 Obligaciones y garantías del directorio

Sin estipulaciones adicionales

9.6.6.2 Garantías ofrecidas por el directorio

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

9.7 Renuncias de garantías

9.7.1 Rechazo de garantías de la EC-UR

La EC-UR 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-UR

Más allá de las limitaciones de los prestadores de servicios de certificación establecidas en el artículo 23 de la Ley 59/2003, de 19 de diciembre, la EC-UR 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) suministrados por ésta.

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

9.10.3 Supervivencia

Sin estipulaciones adicionales

9.11 Notificaciones

Sin estipulaciones adicionales.

9.12 Modificaciones

9.12.1 Procedimiento para las modificaciones

Sin estipulaciones adicionales.

9.12.2 Periodo y mecanismos para notificaciones

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

9.12.3 Circunstancias en las que un OID tiene que ser cambiado

Sin estipulaciones adicionales.

9.13 Resolución de conflictos

9.13.1 Resolución extrajudicial de conflictos

Sin estipulaciones adicionales.

9.13.2 Jurisdicción competente

Sin estipulaciones adicionales.

9.14 Ley aplicable

Sin estipulaciones adicionales.

9.15 Conformidad con la ley aplicable

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

9.16 Cláusulas diversas

9.16.1 Acuerdo íntegro

Sin estipulaciones adicionales.

9.16.2 Subrogación

Sin estipulaciones adicionales.

9.16.3 Divisibilidad

Sin estipulaciones adicionales.

9.16.4 Aplicaciones

Sin estipulaciones adicionalesSin estipulaciones adicionales.

9.16.5 Otras cláusulas

Sin estipulaciones adicionalesSin estipulaciones adicionales.

ANEXO – Control documental

Control de versiones DPC EC-UR 1er semestre 2016

Proyecto:	Informe modificación del documento DPC EC-UR
Entidad de destino:	Consorci AOC
Código de referencia:	Revisión 1r semestre 2016
Versión:	Cambios de la v6.1a la v7.0 en catalán y en castellano
Fecha de la edición:	05/08/2016

Versió n	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
7.0	Totes	Revisión global. Integración de CATCert en Consorci AOC	Servei de Certificació Digital AOC	05/08/2016