Administració Oberta de Catalunya

PLIEGO DE PRESCRIPCIONES TÉCNICAS PARA LA CONTRATACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN DIGITAL
AOC-2025-2

Generalitat de Catalunya

LOCALRET

Realizado por: Servicio de Certificación Digital
Versión: 1.5
Fecha: 25/07/2024
Archivo: PPT_SCD_2025_v.1.5.docx

INDEX

1 OBJETO

El Consorci d'Administració Oberta de Catalunya (Consorci AOC) es el órgano competente en relación con la prestación de servicios de identidad digital y firma electrónica, de acuerdo con la Ley 29/2010, de 3 de agosto, del uso de los medios electrónicos en el sector público de Cataluña y con sus estatutos.

De acuerdo con esta competencia y en relación con el objeto de este contrato, debe considerarse al Consorci AOC, a todos los efectos, como Prestador Calificado de Servicios de Certificación.

En relación con el ámbito de los Servicios de Certificación Digital (SCD) y aquellos otros que son conexos, vinculados o relacionados, estamos ante unos servicios de alta criticidad y complejidad, con muchas particularidades, una gran cantidad de usuarios consumiendo los servicios de manera concurrente, así como una importante dependencia estratégica con los servicios digitales de los entes y organismos públicos del ámbito catalán usuarios de los servicios.

Por lo tanto, hay que evidenciar ya en este punto, que la imprescindible continuidad del servicio obliga a un constante análisis y adecuación normativa, como también en relación con las auditorías internas y externas que esta normativa obliga a realizar al prestador cualificado de servicios de certificación.

Al tratarse el SCD de un servicio sin solución de continuidad contractual, se iniciará un expediente de contratación que garantice la continuidad de la prestación del servicio. Así el objeto de este Pliego de prescripciones técnicas particulares es regular las condiciones de ejecución de este.

2 ALCANCE DEL SERVICIO

A pesar de considerarse como un todo la provisión del servicio de identificación digital, se ha podido identificar y considerado necesaria la estructuración del servicio en tres lotes, que a pesar de tener identidad propia y diferenciada entre ellos, no se pueden concebir de manera independiente en relación con la prestación global del servicio de certificación. En concreto:

a. Lote 1: Asesoramiento en cumplimiento de la normativa de identificación y firma electrónica y normativa de protección de datos de carácter personal, ejecución de auditorías internas y apoyo y acompañamiento interno al Consorci AOC en el proceso de ejecución de las auditorías externas.
b. Lote 2: Auditorías de conformidad de las Entidades de Registro.
c. Lote 3: Servicios de certificación digital.

3 MARCO NORMATIVO

La base normativa sobre la que debe estructurarse el servicio es, a modo de ejemplo, la indicada a continuación, siempre en el entendido de que será de aplicación la versión vigente de la legislación aplicable y toda aquella normativa que pueda surgir durante el tiempo de ejecución del contrato. Por tanto, el licitador deberá adecuar la prestación del servicio de acuerdo con los requerimientos legales establecidos en todo momento.

- **Ley 6/2020**, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- **Ley 34/2002**, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- **Reglamento (UE) nº 2016/679** del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD) y la normativa específica vinculada.
- **Ley orgánica 3/2018**, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD).
- **Real Decreto 311/2022**, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
- **Real Decreto 4/2010**, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (ENI).
- **Reglamento (UE) nº 910/2014** del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (ReIDAS).
- **ETSI EN 319 401 V3.1.1 (2024-06)** General Policy Requirements for Trust Service Providers.
- **ETSI EN 319 411-1 V1.4.1 (2023-10)** Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- **ETSI EN 319 411-2 V2.5.1 (2023-10)** Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- **ETSI EN 319 421 V1.2.1 (2023-05)** Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps.
- **ETSI EN 319 412-1 V1.5.1 (2023-09)** Certificate Profiles; Part 1: Overview and common data structures.
- **ETSI EN 319 412-2 V2.3.1 (2023-09)** Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- **ETSI EN 319 412-3 V1.3.1 (2023-09)** Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
- **ETSI EN 319 412-4 V1.3.1 (2023-09)** Certificate Profiles; Part 4: Certificate profile for web site certificates.
- **ETSI EN 319 412-5 V2.4.1 (2023-09)** Certificate Profiles; Part 5: QCStatements.
- **CA/Browser Forum V2.0.4 (17 abril 2024)** Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates
- **ETSI EN 319 403-1 V2.3.1 (2020-06)** Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers.
- **ETSI TS 119 403-2 V1.3.1 (2023-03)** Trust Service Provider Conformity Assessment; Part 2: Additional requirements for Conformity Assessment Bodies auditing Trust Service Providers that issue Publicly-Trusted Certificates

ETSI TS 119 403-3 V1.1.1 (2019-03) Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers

- **Mozilla Root Store Policy V2.9 (1 septiembre 2023)**
- **Política de Seguridad y Marco Normativo del Consorci AOC** publicado en la web www.aoc.cat

La normativa interna del Consorci AOC en materia de seguridad y del servicio objeto de licitación.

4 Lote 1: ASESORAMIENTO EN CUMPLIMIENTO DE LA NORMATIVA DE IDENTIFICACIÓN Y FIRMA ELECTRÓNICA Y NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL EJECUCION DE AUDITORÍAS INTERNAS Y APOYO Y ACOMPAÑAMIENTO INTERNO AOC EN EL PROCESO DE EJECUCIÓN DE LAS AUDITORÍAS EXTERNAS.

4.1 Descripción

Derivado de las necesidades del Consorci AOC al cumplir con los requerimientos de la normativa de identificación y firma, en especial del ReIDAS, se requiere de un proceso constante de revisión, actualización y control en las actuaciones que conforman el Servicio de Certificación Digital.

El objetivo es disponer de información actualizada, normalizada y adaptada del Servicio de Certificación Digital, ante el constado cambio que sufre el marco normativo.

El servicio requiere de acciones focalizadas en tres ejes:

- Asesoramiento en cumplimiento de la normativa de identificación y firma electrónica, de la normativa de protección de datos de carácter personal y de otras consultas jurídicas.
- Ejecución de auditorías internas en el marco ReIDAS
- Defensa ante entidades de certificación y los organismos que sean necesarios de las acreditaciones ReIDAS

4.1.1 Asesoramiento en cumplimiento de la normativa de identificación y firma electrónica, normativa de protección de datos de carácter personal y otras consultas jurídicas

Los cambios en la legislación y el marco normativo suponen un proceso continuo de adaptación y actualización de la documentación necesaria para la ejecución del Servicio de Certificación Digital. Esto requiere de un esfuerzo para dar respuesta al cumplimiento de requerimientos de los usuarios y de las partes interesadas.

El Consorci AOC requiere del apoyo en el cumplimiento de la normativa de identificación y firma electrónica, en especial con respecto a los criterios de seguridad y operaciones en entornos de certificación digital, así como en el cumplimiento de la normativa de protección de datos personales, y el apoyo en otras consultas jurídicas que el servicio pueda necesitar.

En el ámbito de la protección de datos, el asesoramiento se hará mediante informe que se someterá a la consideración del delegado de protección de datos del Consorci AOC y que habrá que aclarar o enmendar en función del resultado de esta.

Esta tarea se concreta en la redacción y/o revisión de la documentación jurídica del Servicio de Certificación Digital. La empresa adjudicataria deberá gestionar las revisiones, modificaciones, etc., adaptando a la normativa actual o a las necesidades del servicio o del Consorci AOC de la documentación jurídica auxiliar del servicio de certificación digital que incluye:

- Declaraciones de prácticas de certificación
- Políticas de certificación
- Textos de divulgación
- Perfiles de los certificados
- Condiciones específicas del servicio

Y cualquier otra que sea necesaria para el correcto desarrollo del servicio objeto de este contrato.

4.1.2 Ejecución de auditorías internas

De forma anual el Consorci AOC debe desarrollar auditorías internas sobre el marco ReIDAS por la totalidad del Servicio de Certificación Digital. Este es un requisito normativo que emana de la normativa técnica aplicable que pretende hacer una prueba de esfuerzo del servicio con el fin de garantizar los controles de seguridad pertinentes. En este punto el adjudicatario también realizará tareas de apoyo y acompañamiento en el análisis de estas.

4.1.3 Apoyo y acompañamiento interno al Consorci AOC en el proceso de ejecución de las auditorías externas

De forma bianual el Consorci AOC debe someterse al control del organismo de supervisión estatal, es decir, para validar los controles de seguridad del Servicio de Certificación Digital. De esta manera se procede a la renovación de las certificaciones necesarias para cumplir con los requerimientos del Ministerio a efectos de ser considerado como Prestador de servicios de confianza cualificado.

Anualmente, los Prestadores de servicios de certificación tienen la recomendación de realizar auditorías de control de la ejecución de sus tareas.

Cabe destacar la importancia del resultado de estas auditorías y las que en cualquier momento pueda efectuar el organismo de supervisión, dado que pueden suponer la retirada de la consideración como prestador cualificado de servicios de confianza. También hay que tener en cuenta que el resultado de las auditorías será informado a la autoridad de protección de datos correspondiente por parte del organismo de supervisión en caso de posibles infracciones de las normas sobre protección de datos.

El apoyo y el acompañamiento interno incluye el análisis y enmienda de los posibles incumplimientos advertidos en los resultados obtenidos.

4.2 Funciones

4.2.1 Funciones del adjudicatario hacia el Consorci AOC

La empresa adjudicataria presentará al jefe de servicio, la relación del personal adscrito al servicio, especificando las categorías de cada uno dentro de la estructura, que en todo caso

deberá disponer de la calificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y gestión adecuados en el ámbito de la firma electrónica.

La empresa adjudicataria aportará la información relativa a procedimientos de trabajo, trabajos efectuados y tiempos invertidos. Igualmente informará de cualquier defecto o anomalía en las instalaciones durante el desarrollo de sus actividades.

4.2.1.1 Gobernamiento de la seguridad

La finalidad del gobernamiento de la seguridad se focaliza en velar por una correcta gestión de la seguridad de la información del Consorci AOC a lo largo de todo su ciclo de vida.

Este objetivo se alcanzará mediante:

- La prescripción, seguimiento y verificación de la correcta implantación del modelo de seguridad
- El cumplimiento de los requerimientos que sean de aplicación de acuerdo con el Marco Normativo vigente de AOC y de la Generalidad de Cataluña vigente y con las modificaciones que se produzcan a lo largo de la prestación del servicio, así como del marco legal que sea de aplicación
- En relación con el tratamiento de datos de carácter personal, el adjudicatario dará cumplimiento como encargado de tratamiento a lo establecido en la normativa vigente en materia de protección de datos de carácter personal y a lo establecido en el encargo de tratamiento.
- La implantación de los controles de seguridad que permitan mitigar los riesgos a los que la información del Consorci AOC y sus sistemas están expuestos

El adjudicatario deberá tener en cuenta la clasificación de la información que trata o genera, objeto del contrato, para aplicar correctamente el marco normativo y legal del Consorci AOC en materia de seguridad.

En el caso de que el adjudicatario preste servicios o almacene información vinculada al servicio fuera de las instalaciones del Consorci AOC, deberá garantizar y demostrar la aplicación de las medidas de prevención y protección de acuerdo con los estándares de la Generalidad de Cataluña en las dependencias desde las que presta el servicio.

4.2.1.2 Gobernamiento de la continuidad y la disponibilidad

La finalidad del gobernamiento de la continuidad y la disponibilidad se centra, principalmente, en garantizar la continuidad del servicio y procesos ante cualquier situación adversa, evitando un impacto significativo en la organización.

Los objetivos que se persiguen son:

- Disponer de mecanismos para garantizar la continuidad del personal involucrado en las auditorías.
- Disponer de un plan de continuidad de los procesos, personas y sistemas de información que participan en el proceso de asesoramiento.
- Garantizar la continuidad del servicio.
- Focalizar el esfuerzo en la mitigación de riesgos relevantes.
- Coordinar a todas las personas clave para hacer frente a una situación de contingencia.
- Cumplir con los requerimientos legales / regulatorios en materia de continuidad de negocio.

4.2.2 Funciones del Consorci AOC hacia el adjudicatario

El Consorci AOC será responsable de dar accesos a las redes corporativas y colaborará en todo momento con el adjudicatario en la realización de las tareas descritas. Todas las comunicaciones se realizarán mediante la herramienta de *ticketing* que utilice el Consorci AOC y por lo tanto el Consorci AOC deberá facilitar a los usuarios o licencias que sean necesarios para el correcto desarrollo de las tareas.

El Consorci AOC facilitará toda la información de la que disponga al adjudicatario sobre los temas de seguridad y de protección de datos, así como la interlocución con los responsables de seguridad y de protección de datos respectivamente.

El Consorci AOC garantizará la interlocución tanto con el jefe de servicio de certificación como con el responsable del asesoramiento jurídico de los servicios del Consorci AOC.

4.3 Requisitos

4.3.1 Requisitos personales

Las tareas que desarrollar en este lote se han calculado a partir de la incorporación (en diferente porcentaje) de los perfiles siguientes:

- Consultor ReIDAS
- Auditor interno

En todos los casos, se calcula sobre unas 1700 horas/año persona (incluye, por tanto, tiene en cuenta los días de baja y ausencias).

El personal adscrito al servicio, en conjunto, debe disponer de los conocimientos suficientes, tanto a nivel técnico práctico como de idiomas (dominio del catalán (nivel C), castellano e inglés), que aseguren la correcta interpretación de procedimientos y normas de seguridad, lo que debe permitir una correcta aplicación de estos conocimientos.

El personal que el adjudicatario destine a este servicio deberá reunir todas las condiciones estipuladas por la normativa actualmente vigente.

El Consorci AOC puede rechazar y/o solicitar el cambio de interlocutor o responsables de proyecto. En este caso, el adjudicatario debe reemplazar al trabajador por otro suficientemente capacitado para llevar a cabo la tarea encomendada. Los costes derivados de esta incidencia irán a cargo del adjudicatario.

El Consorci AOC se reserva el derecho de no aceptar al personal que desarrolle su tarea sin una capacitación suficientemente o un comportamiento incorrecto.

Habrá que presentar una tabla de correlación entre los medios requeridos y los presentados por parte del adjudicatario.

El adjudicatario debe hacerse cargo de todos los materiales y útiles para la correcta ejecución de los servicios encomendados, debidamente identificados como de su propiedad.

El Consultor EIDAS propuesto por el adjudicatario deberá disponer de un número de teléfono que permita su localización en jornada laboral del calendario laboral de Barcelona, por parte del personal responsable del Consorci AOC.

El auditor debe demostrar ser competente para llevar a cabo la auditoría. Esto incluye la realización de juicios técnicos exigidos, la definición de políticas y su implementación y la imparcialidad.

La empresa adjudicataria acreditará documentalmente que el personal que se asigne al servicio haya realizado previamente al inicio de las tareas, los diferentes cursos en relación con la formación específica para el servicio, por la que se determinan los programas de formación de seguridad.

En caso de baja de cualquiera de los miembros del equipo, el adjudicatario deberá sustituirlo en menos de 15 días laborables de acuerdo con los responsables del Consorci AOC. Cualquier cambio en uno de los miembros del equipo a instancias del adjudicatario deberá ser pactado con el Consorci AOC, que deberá validar tanto la baja como el currículo de la nueva persona a incorporar. Si el cambio es a instancias del adjudicatario, habrá que acordar el calendario de cambio con el Consorci AOC con el fin de minimizar el impacto en los desarrollos en curso. Quedan fuera de estos compromisos los periodos de vacaciones y permisos de todos los miembros del equipo.

El Consorci AOC realizará, en su caso, entrevistas a las personas del equipo de proyecto propuesto y, si es necesario, pedirá alternativas a las personas presentadas.

El Consorci AOC se reserva el derecho a solicitar el cambio de cualquiera de los miembros del equipo sin necesidad de justificación con una antelación de 20 días naturales a la fecha de sustitución.

El Consorci AOC se reserva el derecho a pedir una declaración personal de cada uno de los auditores para garantizar su formación y conocimientos.

Para poder conocer la calificación profesional, el licitador presentará el currículo profesional de los candidatos que propongan por estos perfiles. El licitador justificará documentalmente la calificación profesional del personal destinado con la presentación de la documentación compulsada que se detalla a continuación: tarjeta de identidad profesional y títulos profesionales. En el currículo profesional de cada perfil que proponga para las funciones definidas, constará como mínimo:

- nombre y apellidos
- calificación educativa y categoría profesional
- experiencia y formación
- evaluación de la competencia: conocimientos de la tecnología y marco legal aplicable.
- seguimiento del desempeño
- fecha de la actualización más reciente de cada registro

4.4 Condiciones

4.4.1 Asesoramiento en cumplimiento de la normativa de identificación y firma electrónica, normativa de protección de datos de carácter personal y otras consultas jurídicas

Debido a las necesidades recurrentes de modificación de la documentación del Servicio de Certificación Digital (SCD) políticas, se ha decidido establecer un calendario fijo de actualizaciones de la documentación.

- La primera actualización se producirá durante el primer semestre de cada ejercicio.
- La segunda actualización se producirá durante el segundo semestre de cada ejercicio.

Las horas previstas en esfuerzo anual por este concepto y perfiles implicados se muestran en el Pliego de Cláusulas Administrativas. Se calculan unas 1.700 horas/año persona (incluye, por tanto, los días de baja y ausencias).

Tareas que ejecutar:

1. Actualización según recomendaciones ETSI
   Conocimiento actualizado de la normativa de identificación y firma electrónica, en especial del ReIDAS Gestión del cambio (análisis de la capacidad)
   Detección de necesidades
   Plan de acciones que suponen las necesidades

2. Actualización documentación reguladora del servicio de certificación digital
   Gestión del cambio (análisis de la capacidad)
   Detección de necesidades de las DPC y Políticas
   Plan de acciones que suponen las necesidades
   Redacción de los apartados de cumplimiento normativo de la documentación
   Asesoramiento del resto de apartados

3. Actualización según normativa: autonómica, estatal, europea e internacional
   Gestión del cambio (análisis de la capacidad)
   Actualización trimestral de los acuerdos anuales DATASHIELD
   Plan de acciones que suponen los acuerdos
   Resolución de incidentes derivados

4. DATASHIELD (acuerdos internacionales)
   Actualización trimestral de los acuerdos anuales DATASHIELD
   Plan de acciones que suponen los acuerdos
   Resolución de incidentes derivados

5. Ejecución de Auditorías internas
   Disponer de Auditores acreditados
   Cumplir el alcance de la auditoría
   Generar un programa, plan y un informe

6. Apoyo en la superación de auditorías:
   Conocimientos del sector
   Conocimiento de las normas del alcance

Atención a consultas en 48 horas demora máxima

4.4.1.1 Planificación del asesoramiento, revisión y propuestas de mejora

Las fases del calendario de actualización ordinaria de la documentación serán las siguientes:

Primer semestre:

- **Enero y febrero,** fase de recogida de propuestas de modificación.
- **Marzo,**
  1. la **primera quincena** se dedicará a la fase de análisis, comprobación y propuesta de calendario
  2. la **segunda quincena** se dedicará a la comprobación y redacción de las modificaciones.
- **Abril,**
  1. la **primera quincena** se trasladará la propuesta modificada al equipo del servicio del Consorci AOC.
  2. la **segunda quincena** se realizará una reunión con el Área proponente, análisis de los cambios y aprobación del documento.
- **Mayo**,
  - 1- en **la primera quincena** es realización de una segunda reunión, si procede, y preparación de los documentos modificados definitivos en catalán, castellano e Inglés
  - 2- la segunda quincena se trasladarán los cambios acordados al adjudicatario del lote 3 de esta licitación.
- **Junio**, fase de publicación en la web del Consorci AOC y envío a todos los organismos que sea necesario.

En cuanto al segundo semestre:

- **Julio y agosto,** fase de recogida de propuestas de modificación.
- **Septiembre,**
  - 1. la **primera quincena** se dedicará a la fase de análisis, comprobación y propuesta de calendario
  - 2. la **segunda quincena** se dedicará a la comprobación y redacción de las modificaciones.
- **Octubre,**
  - 1. la **primera quincena** se trasladará la propuesta modificada al equipo del servicio del Consorci AOC.
  - 2. la **segunda quincena** se realizará una reunión con el Área proponente, análisis de los cambios y aprobación del documento.
- **Noviembre,**
  - 1. en **la primera quincena** es realización de una segunda reunión, si procede, y preparación de los documentos modificados definitivos en catalán, castellano e Inglés
  - 2. la segunda quincena se trasladarán los cambios acordados al adjudicatario del lote 3 de esta licitación.

- **Diciembre,** fase de publicación en la web del Consorci AOC y envío a todos los organismos que sean necesarios.

A pesar de estas dos revisiones anuales planificadas, se puede dar el caso de que haya que llevar a cabo otras modificaciones, por motivos de urgencia o de necesidad del servicio, también se tendrán que realizar en un periodo máximo de un mes desde la fecha de la detección de la necesidad.

4.4.1.2 Fase de recogida de propuestas de modificación

Las propuestas de modificación o actualización de la documentación se pueden presentar por el jefe de servicio correspondientes, o bien de oficio por el propio adjudicatario o a recomendación de los adjudicatarios de los demás lotes que conforman el presente contrato.

Todas las propuestas se realizarán mediante un ticket en la herramienta corporativa del Consorci AOC

Todas las propuestas recibidas serán archivadas en una carpeta creada a tal efecto, indicando la fecha de recepción de la propuesta, la descripción de la modificación propuesta y su justificación. Esta carpeta será la carpeta de documentación reguladora dentro del directorio corporativo. Esta ubicación, durante el período de vigencia del contrato puede sufrir modificaciones.

4.4.1.3 Fase de análisis, comprobación y redacción de modificaciones

Todas las modificaciones propuestas tienen que ser analizadas, en su caso realizando las comprobaciones técnicas necesarias y, en caso de resultar necesaria la modificación propuesta, redactado su texto.

Las comprobaciones podrán incluir consultas a otros adjudicatarios de los otros lotes del contrato u otras áreas del Consorci AOC o a otros departamentos u organismos, a los efectos necesarios para producir un texto correcto y actualizado.

El análisis de las modificaciones propuestas debe registrarse en un documento de control de revisiones de cada documento afectado, que debe tener los siguientes contenidos mínimos:

- Una sección con el histórico de versiones del documento, que debe indicar la versión vigente (publicada) del documento, y la versión en revisión.
- Una sección con las modificaciones propuestas, para cada versión del documento, por la oficina de políticas, que debe indicar la fecha de la modificación, la sección afectada y la descripción o justificación del cambio propuesto.
- Una sección con la disposición de las modificaciones propuestas, para cada versión del documento, por el servicio afectado, que debe indicar la fecha de la modificación, la sección afectada y la descripción o justificación del cambio propuesto.

4.4.1.4 Fase de comentario y aprobación

El/los documento/s, con sus modificaciones propuestas, debe ser entregado/s al jefe de servicio correspondiente y al resto de áreas a las que se hayan solicitado comprobaciones y otras informaciones técnicas, para su comentario, en las fechas acordadas en el calendario establecido.

Se podrán realizar modificaciones adicionales en función de los comentarios recibidos, sin perjuicio de los periodos establecidos por las siguientes fases del procedimiento, y según se establezca en el calendario programado y se editará una versión final del/los documento/s, que será/a aprobada por el jefe del servicio correspondiente.

4.4.1.5 Fase de publicación

El/los documento/s aprobado/s debe/n ser publicado/s en la página web del Consorci AOC en el apartado de regulación correspondiente (actualmente en https://epscd.aoc.cat/regulacio).

El Jefe del servicio, mediante la herramienta de ticketing interna del Consorci AOC enviará a la persona responsable de la página web los documentos en versión catalana, castellana e inglesa para que los publique en el apartado correspondiente. Esta fase puede variar tanto en la ubicación de la publicación como en las personas responsables de la ejecución de esta.

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

4.4.2 Ejecución de Auditorías internas

Anualmente, se deberá programar, planificar y ejecutar como mínimo una Auditoría interna con el fin de verificar el cumplimiento de la normativa de identificación y firma electrónica, en especial el ReIDAS, a la totalidad del Servicio de Certificación Digital.

Las horas previstas en esfuerzo anual por este concepto y perfiles implicados se muestran en el Pliego de Cláusulas Administrativas. Se calculan unas 1.700 horas/año persona (incluye, por tanto, los días de baja y ausencias).

Tras acordar la fecha de auditoría, se deberá hacer llegar un plan de auditoría a todos los implicados donde conste:

- Objetivo y alcance
- Criterios de auditoría
- Equipo auditor
- Documentos de referencia
- Agenda con tiempo de inicio o duración
- Temas de confidencialidad
- Riesgos de la auditoría
- Instrucciones de resolución y seguimiento

La Auditoría interna debe cumplir criterios de objetividad y debe ser realizada por un auditor acreditado.

Por otra parte, el auditor debe ser imparcial y debe ser percibido como tal, con la finalidad de dar confianza a sus actividades y resultados.

Por lo tanto, se evitará:

- Intereses propios
- Autor revisión de una actividad llevada a cabo por la misma persona
- Defensa u oposición
- Exceso de familiaridad
- Intimidación
- Competencia

La planificación de la auditoría deberá llevarse a cabo con una antelación mínima de un mes para poder gestionar la disponibilidad de los implicados.

La auditoría se realizará conforme los procedimientos de auditoría establecidos en el Consorci AOC.

El adjudicatario deberá realizar un informe de auditoría donde consten:

- Los hallazgos
- Áreas de mejora
- Observaciones
- Las no conformidades

Las no conformidades deberán estar referenciadas al punto de requisito de norma que incumplen y que hay que resolver.

Finalmente, el adjudicatario deberá proponer al Consorci AOC medidas correctoras para poder resolver los incumplimientos de norma encontrados.

4.4.3 Defensa ante Auditorías externas

El Consorci AOC, como Prestador de Servicios de Confianza ejecuta una auditoría bienal (o cuando sea establecido) por parte de una entidad acreditada externa para obtener un nivel de cumplimiento adecuado respecto a los requisitos especificados en el Reglamento (UE) Nº 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, y sus guías de referencia (Reglamento ReiDAS).

El alcance de la certificación comprende lo que dictamine el organismo de supervisión nacional estatal en cada momento.

El Consorci AOC, a través de la entidad certificadora, informará con antelación al adjudicatario sobre la planificación de las auditorías externas.

El adjudicatario deberá hacer la defensa ante auditorías externas que realice el Consorci AOC. Con el fin de realizar correctamente esta defensa, habrá que tener un amplio conocimiento del marco legal que aplica, los requisitos legales y requerimientos internos del Consorci AOC, así como del resultado de las auditorías internas realizadas previamente.

La defensa incluye la asistencia a la auditoría, la participación en la presentación de evidencias y la propuesta de acciones correctivas con el fin de solucionar las No conformidades encontradas.

Las horas previstas en esfuerzo anual por este concepto y perfiles implicados se muestran en el Pliego de Cláusulas Administrativas. Se calculan unas 1.700 horas/año persona (incluye, por tanto, los días de baja y ausencias).

4.5 Acuerdos de nivel de servicio (ANS)

El funcionamiento del servicio objeto de esta contratación estará sujeto a un sistema de control de calidad ejercido por el Consorci AOC.

El funcionamiento de este control de calidad está ligado a las Condiciones Generales de los Servicios del Consorci AOC, las Condiciones Particulares de los Servicios de Certificación

Digital y el marco normativo aplicable. Los criterios de valoración y puntuación de la calidad del servicio se mencionan a continuación en cada ANS aplicable.

Esta puntuación es importante, ya que aparte de ser una medida de calidad de funcionamiento del servicio, también puede constituir una causa justificada de rescisión del contrato por parte del Consorci AOC.

Los acuerdos de nivel de servicio (ANS) para el seguimiento del servicio objeto de este lote serán:

a. Actualización según recomendaciones ETSI
Número de incidentes por falta de conocimiento por debajo del 5%.

b. Actualización de la normativa reguladora del servicio de certificación digital (Declaración de prácticas de certificación, políticas de certificación, etc.)
Número de revisiones detectadas, tiempo entre detección y modificación

c. Entrega de informes de servicio entregado los primeros 5 días operativos del mes siguiente al que se está validando
Se considerará desviación si el informe se entrega a partir del 5º día operativo del mes.

d. Actualización según normativa: autonómica, estatal, europea e internacional.
Número de incidentes por falta de conocimiento por debajo del 5%

e. DATASHIELD (acuerdos internacionales)
Número de incidentes por falta de conocimiento en el caso de Auditorías internas por debajo del 5%.
Plazo de ejecución de acuerdo con lo previsto en normativa y valor añadido de las propuestas de mejora.

f. Apoyo en la superación de auditorías:
Número de no conformidades de auditoría por debajo del 5%.

g. Consultas sobre el marco normativo del Servicio de Certificación Digital: plazo máximo de evaluación y primera respuesta 5 días laborables. En el caso de consultas sobre certificados urgentes se reducirá a 2 días

4.6 Seguimiento del servicio

El objetivo de este ámbito de seguimiento es garantizar la integración de la calidad, seguridad y continuidad, en todo el ciclo de vida, de los procesos, servicios y soluciones, mediante la prescripción, seguimiento, validación y verificación de la eficaz implantación de los controles definidos.

4.6.1 Gobernamiento y mejora del servicio

El adjudicatario es el responsable de generar y entregar los informes y métricas de reporting (en adelante información) que se determinen en los diferentes ámbitos del gobernamiento del servicio objeto de este lote. Estos deben permitir al Consorci AOC gobernar, controlar y gestionar los servicios prestados por el adjudicatario, tanto desde una óptica individual, como transversal y global.

El formato y el contenido mínimo de la información a elaborar por el adjudicatario en todos los ámbitos de gobernamiento es el definido en el Anexo "Anexo _1_Plantilla Informe Seguimiento".

El Consorci AOC podrá solicitar, durante la vigencia del contrato cambios en la estructura y contenido de la información para ajustarse a las necesidades de seguimiento de los servicios.

El adjudicatario deberá proporcionar al Consorci AOC, además de los informes periódicos de seguimientos de los ANS, la información (evidencias) con base en la que se hayan elaborado, para que el Consorci AOC la pueda incorporar a su herramienta de gestión.

El objetivo de este ámbito de gobernamiento es garantizar la integración de la calidad, en todo el ciclo de vida, de los procesos, servicios y soluciones, mediante la prescripción, seguimiento, validación y verificación de la eficaz implantación de los controles definidos.

El licitador propondrá los mecanismos necesarios para permitir al Consorci AOC comprobar que se mantienen los niveles de calidad esperados.

4.6.1.1 Incidencias y problemas

Se entiende para incidencia cualquier suceso que no forma parte de la operativa normal de un servicio y que provoca, o puede provocar, la interrupción, el mal funcionamiento o la degradación en la calidad del servicio.

El objetivo principal del proceso de gestión de incidencias es restaurar el normal funcionamiento del servicio tan pronto como sea posible, minimizando el impacto adverso sobre las operaciones de negocio/clientes y organización, asegurando que el servicio se mantenga en los mejores niveles posibles de calidad y disponibilidad.

El proceso soporta todos los servicios que el Consorci AOC presta al usuario dentro del alcance del pliego y por tanto su alcance es la resolución de todas las incidencias que puedan afectar a estos servicios.

Se entiende por problema cualquier causa subyacente, aún no identificada, de una serie de incidentes o de un incidente aislado de importancia significativa.

El objetivo principal de la Gestión de Problemas es minimizar el impacto negativo que tienen las incidencias sobre el negocio, y prevenir la recurrencia de incidencias relacionadas con estos errores. Para conseguir esta meta, la Gestión de Problemas llega hasta la causa a raíz de las incidencias y luego inicia acciones que corrigen la afectación de servicio.

El adjudicatario participará activamente en el proceso de Gestión de Problemas siendo el Responsable de todos los problemas que puedan salir de los servicios que está prestando al Consorci AOC.

Es responsabilidad del adjudicatario la aplicación y seguimiento de los procedimientos asociados a la gestión de problemas surgidos de los servicios que presta, así como el seguimiento y gestión del estado de estos hasta la corrección de la afectación de servicio.

Ante la detección de problemas graves y con impacto directo a negocio, el proveedor de servicio deberá notificar el problema al Jefe del servicio Consorci AOC.

El licitador describirá la metodología propuesta para atender:

- Registro de incidencias y problemas
- Clasificación y asignación
- Investigación y diagnosis

• Seguimiento y coordinación
• Resolución y recuperación
• Cierre de incidencias y problemas

4.6.2 Órganos de Gestión

4.6.2.1 Reuniones de Dirección.

Las reuniones de Dirección se realizarán con el objetivo de establecer un control y una visión estratégica y amplia sobre el desarrollo global del servicio.

Las reuniones podrán ser presenciales y/o virtuales. En el caso de las presenciales, pueden realizarse tanto en la sede del Consorci AOC, como de la empresa adjudicataria. En todo caso, es necesario que el adjudicatario disponga de los recursos necesarios en cualquiera de las modalidades de reunión previstas.

Las reuniones de dirección se convocarán trimestralmente, aunque a petición del poder adjudicador y en circunstancias concretas de afectación crítica del servicio, podrán ser convocadas en cualquier momento durante la vigencia del contrato, convocadas con una antelación mínima de 3 días laborables, según el calendario laboral aplicable al personal del Consorci AOC.

4.6.2.2 Reuniones de Seguimiento.

El gestor del servicio del adjudicatario y el Jefe del Servicio del SCD del Consorci AOC realizarán una reunión de seguimiento del servicio, que será periódica y como mínimo de carácter mensual, aunque a petición del Consorci AOC y en circunstancias concretas de afectación crítica del servicio, podrán ser convocadas en cualquier momento durante la vigencia del contrato, con una antelación mínima de 1 día laborable, según el calendario laboral aplicable al personal del Consorci AOC.

Las reuniones podrán ser presenciales y/o virtuales. En el caso de las presenciales, pueden realizarse tanto en la sede del Consorci AOC como de la empresa adjudicataria. En todo caso, es necesario que el adjudicatario disponga de los recursos necesarios en cualquiera de las modalidades de reunión previstas.

Esta reunión se hará antes del décimo día laborable (de lunes a viernes excepto festivos) de cada mes. En esta reunión se revisará el informe mensual, el funcionamiento de los procesos, se generarán propuestas de mejora del servicio y se hará un seguimiento de todo lo relacionado con la prestación. A título de ejemplo se indican algunos de los aspectos incluidos como posible contenido de la reunión:

- Evaluar la situación de ejecución del servicio objeto del contrato a partir del seguimiento de la evolución de los objetivos e indicadores formulados, así como el nivel de cumplimiento de los acuerdos de nivel de servicio que estén vinculados.
- Revisar y poner en común las incidencias que se hayan producido en el mes inmediatamente anterior, ya sea en relación con la prestación efectiva del servicio como en relación con el modelo de gestión vinculado.
- Revisar y poner en común novedades, jornadas y/o documentación relevante para la ejecución del servicio, con el fin de generar una dinámica de participación que impacte de manera positiva en la gestión del conocimiento y sea aplicable a la propia prestación del servicio.

Antes de cada reunión de seguimiento y con la antelación establecida en el correspondiente acuerdo de nivel de servicio establecido el referente del servicio del adjudicatario pondrá a disposición del Jefe del Servicio del Consorci AOC el informe de seguimiento detallado propuesto en el "Anexo _1_Plantilla Informe Seguimiento" que incluye, como mínimo, información sobre:

- Estado de cumplimiento de las tareas en relación con las planificaciones realizadas y las posibles desviaciones que se hayan producido. Número de actuaciones realizadas de acuerdo con el objeto y alcance del lote. Número de consultas realizadas (por tipología, teléfono, correo, etc..).
- Mejoras aplicables al servicio de certificación digital.
- Información de cumplimientos sobre los acuerdos de nivel de servicio establecidos.

Se utilizará una herramienta de gestión del Consorci AOC que permitirá y facilitará la participación de los diferentes actores implicados en la ejecución del servicio. Esta herramienta se convierte en clave para mantener coordinados a todos los actores participantes, detectar las necesidades a cubrir, así como detectar mejoras tanto en la prestación del servicio como en el modelo de gestión vinculado. El referente del servicio es el principal responsable del mantenimiento de la herramienta de gestión del servicio y debe reflejar todos los cambios, actualizaciones, documentos, etc., con el máximo rigor posible, con el fin de tener un acceso inmediato a la información actualizada de la prestación del servicio y permitir una visión con el mayor detalle posible a los diferentes actores que participan en la gestión de este lote.

4.7 Devolución del servicio

Una vez finalizado el contrato el adjudicatario deberá garantizar que ha cumplido con todos los compromisos establecidos en este lote.

- Informe de situación de cumplimiento normativo del Consorci AOC. En este informe se detallará qué asesoramientos en cumplimiento normativo de identificación y firma electrónica y de protección de datos personales se han hecho en el último año del servicio y cuál es el estado actual.
- En el caso de que exista, la planificación de acciones previstas hacia cumplimiento normativo en materia de identificación y firma electrónica y de protección de datos personales.
- Informes de auditorías internas realizados durante los últimos tres años en el Consorci AOC.
- Estado y seguimiento de las propuestas de acciones de las auditorías internas y de las auditorías ReIDAS.
- Análisis de riesgos y oportunidades detectados en el momento de la finalización del servicio de asesoramiento y propuestas de actuaciones.

El adjudicatario deberá devolver toda la información confidencial propiedad del Consorci AOC, así como la generada a partir de la prestación del servicio.

El adjudicatario deberá finalizar todas las tareas que le hayan sido encomendadas y aceptadas antes de la finalización del contrato.

5 Lote 2: AUDITORÍAS DE CONFORMIDAD

5.1 Descripción

El objetivo de realizar auditorías a las Entidades de Registro que conforman el Servicio de Certificación Digital del Consorci AOC (SCD).

Este servicio engloba 3 subservicios:

- Entidades de registro T-CAT: es un ente o departamento que col·labora con el Consorci AOC en la emisión de certificados digitales a las administraciones públicas catalanas.
- Entidades de Registros idCAT : es un ente o departamento que col·labora con el Consorci AOC, en el registro de las identidades digitales para la ciudadanía, concretamente para emitir y gestionar certificados idCAT y el idCAT en el móvil actualmente.
- Entidades de registro o Entes suscriptores: es un ente o departamento que colabora con el Consorci AOC en los trámites de identificación, registro y autenticación para la emisión de certificados digitales, siguiendo los procedimientos y las relaciones con los titulares de los certificados.

Todas estas entidades de registro deben cumplir con los requerimientos y procedimientos de emisión y gestión de los certificados idCAT y T-CAT que se realizan y que cumplen con los procedimientos que el Consorci AOC proporciona a las Entidades de Registro (ER's), así como las condiciones específicas del servicio y la normativa propia del servicio de certificación digital como toda aquella que le afecte o pueda afectar, directamente.

5.2 Funciones

El adjudicatario deberá hacerse cargo de la realización de las auditorías a las ER's (entes suscriptores y entidades de registro T-CAT e idCAT.

El adjudicatario deberá llevar a cabo auditorías presenciales y virtuales a las ER's, siguiendo el procedimiento que el Consorci AOC establezca, de manera acordada con el adjudicatario. El procedimiento actual se describe en el anexo 4**.**

A principios de cada año el Consorci AOC acordará con el adjudicatario la selección de las ER's que deberán auditarse durante ese año, en base a los criterios descritos en el citado documento; y con el objetivo de que todas las ER's se sometan, como mínimo, a una auditoría presencial cada 2 años, siempre que haya habido emisiones de certificados. También se acordará la planificación de las correspondientes auditorías.

A modo de resumen el adjudicatario deberá :

- Realizar la planificación inicial de la realización de las auditorías
- La preparación y organización previa de cada auditoría: con el apoyo del Consorci AOC y de acuerdo con el responsable del servicio de cada entidad de registro
- El desplazamiento a la entidad de registro (cuando sea necesario) para realizar la auditoría
- La redacción del informe de auditoría y entrega al Consorci AOC para su validación
- Un informe final de conclusiones (clasificado por tipo de ER) una vez al año.

La empresa adjudicataria presentará al jefe de servicio, la relación del personal adscrito al servicio, especificando las categorías de cada uno dentro de la estructura.

La empresa adjudicataria asignará a una persona con perfil de jefe de auditoría, cuyas principales responsabilidades serán:

- La gestión y seguimiento diario del servicio, así como la resolución de conflictos y redimensionamiento temporal o permanente del mismo.
- Mantenimiento del registro de la evolución del servicio para posteriormente poder elaborar los informes de servicio y justificar el cumplimiento de los ANS.
- Seguimiento y control de los recursos asignados al servicio.
- Realizar el control de costes, la estimación de esfuerzos y su seguimiento.
- Analizar cualquier desviación y situaciones de gravedad dentro de la calidad, plazos o alcance del servicio
- Analizar las modificaciones en alcance y coste del servicio que se puedan derivar, e interpretar estas modificaciones respecto al contrato vigente. En caso de que no impliquen una modificación contractual, debe tener la autoridad para formalizar e implementar internamente en su organización los acuerdos tomados.
- Asegurar la buena colaboración con otros proveedores del Consorci AOC con quien se debe relacionar con el fin de mejorar el servicio de negocio final.

La empresa adjudicataria aportará la información relativa a procedimientos de trabajo, trabajos efectuados y tiempos invertidos. Igualmente informará de cualquier defecto o anomalía en las instalaciones durante el desarrollo de sus actividades.

5.2.1.1 Gobernamiento de la seguridad

La finalidad del gobernamiento de la seguridad se focaliza en velar por una correcta gestión de la seguridad de la información del Consorci AOC a lo largo de todo su ciclo de vida.

Este objetivo se alcanzará mediante:

- La prescripción, seguimiento y verificación de la correcta implantación del modelo de seguridad
- El cumplimiento de los requerimientos que sean de aplicación de acuerdo con el Marco Normativo vigente de AOC y de la Generalidad de Cataluña vigente y con las modificaciones que se produzcan a lo largo de la prestación del servicio, así como del marco legal que sea de aplicación
- En relación con el tratamiento de datos de carácter personal, el adjudicatario dará cumplimiento como encargado de tratamiento a lo establecido en la normativa vigente en materia de protección de datos de carácter personal y a lo establecido en el encargo de tratamiento.
- La implantación de los controles de seguridad que permitan mitigar los riesgos a los que la información del Consorci AOC y sus sistemas están expuestos

El adjudicatario deberá tener en cuenta la clasificación de la información que trata o genera, objeto del contrato, para aplicar correctamente el marco normativo y legal del Consorci AOC en materia de seguridad.

En el caso de que el adjudicatario preste servicios o almacene información vinculada al servicio fuera de las instalaciones del Consorci AOC, deberá garantizar y demostrar la aplicación de las medidas de prevención y protección de acuerdo con los estándares de la Generalidad de Cataluña en las dependencias desde las que presta el servicio.

5.2.1.2 Gobernamiento de la continuidad y la disponibilidad

La finalidad del gobernamiento de la continuidad y la disponibilidad se centra, principalmente, en garantizar la continuidad del servicio y procesos ante cualquier situación adversa, evitando un impacto significativo en la organización.

Los objetivos que se persiguen son:

- Disponer de mecanismos para garantizar la continuidad del personal involucrado en las auditorías.
- Disponer de un plan de continuidad de los procesos, personas y sistemas de información que participan en el proceso de auditoría.
- Garantizar la continuidad del servicio.
- Focalizar el esfuerzo en la mitigación de riesgos relevantes.
- Coordinar a todas las personas clave para hacer frente a una situación de contingencia.
- Cumplir con los requerimientos legales / regulatorios en materia de continuidad de negocio.

5.2.2 Funciones del Consorci AOC hacia el adjudicatario

El Consorci AOC será responsable de dar accesos a las redes corporativas y colaborará en todo momento con el adjudicatario en la realización de las tareas descritas. Todas las comunicaciones se realizarán mediante la herramienta de *ticketing* que utilice el Consorci AOC y por lo tanto el Consorci AOC deberá facilitar a los usuarios o licencias que sean necesarios para el correcto desarrollo de las tareas.

El Consorci AOC facilitará toda la información de la que disponga al adjudicatario sobre los temas de seguridad y de protección de datos, así como la interlocución con los responsables de seguridad y de protección de datos respectivamente.

El Consorci AOC garantizará la interlocución tanto con el jefe de servicio de certificación como con el responsable del asesoramiento jurídico de los servicios del Consorci AOC.

5.3 Requisitos

5.3.1 Requisitos generales

El adjudicatario deberá hacerse cargo de:

- Elaborar un plan operativo de ejecución de las auditorías de conformidad, ya sean virtuales o presenciales y teniendo en cuenta las economías de escala en los desplazamientos. Es decir, realizar todas las auditorías de una misma organización aprovechando el desplazamiento o bien la interlocución, así como aprovechando la proximidad para realizar más de una auditoría a la misma jornada.
- Elaborar un plan de auditoría y comunicarlo a la entidad a auditar 30 días antes de la ejecución de esta.
- Ejecutar las auditorías de conformidad.
- Disponer de auditores acreditados
- Elaborar un informe de auditoría
- Remitir el *Checklist* de seguimiento y el informe de auditoría al Consorci AOC en un plazo máximo indicado en el punto “5.5 a Plazo de entrega del checklist y evidencias de auditoría”, tras la ejecución de la auditoría, al responsable del servicio de certificación digital

- Entregar un informe de auditoría a cada ER auditada en el plazo máximo indicado en el punto “5.5 1-bb Plazo de entrega de informes”, tras la ejecución de la auditoría.
- Evaluar la conformidad de las acciones ejecutadas para garantizar la corrección de las desviaciones.
- Realizar un informe con un resumen de la visión global del grado de cumplimiento de los procedimientos de las ER, una vez al año.

5.3.2 Requisitos personales

Las tareas que desarrollar en este lote se han calculado a partir de la incorporación (en diferente porcentaje) de los perfiles siguientes:

- Jefe de auditoría
- Auditor acreditado

Para poder ofrecer todos los servicios objeto de este lote en un escenario de consumo máximo, se han previsto, por cada perfil, las horas de dedicación indicadas en el pliego de cláusulas administrativas.

En ambos casos, se calcula sobre unas 1.700 horas/año persona (incluye, por tanto, se tienen en cuenta los días de baja y ausencias).

El personal adscrito al servicio, en conjunto, debe disponer de los conocimientos suficientes acreditados, tanto a nivel técnico práctico como de idiomas (dominio del catalán (nivel C), castellano y el inglés), que aseguren la correcta interpretación de procedimientos y normas de seguridad, lo que debe permitir una correcta aplicación de estos conocimientos.

El personal que el adjudicatario destine a este servicio deberá reunir todas las condiciones estipuladas por la normativa actualmente vigente.

El Consorci AOC puede rechazar y/o solicitar el cambio de interlocutor o responsables de proyecto. En este caso, el adjudicatario debe reemplazar al trabajador por otro suficientemente capacitado para llevar a cabo la tarea encomendada. Los costes derivados de esta incidencia irán a cargo del adjudicatario.

El Consorci AOC se reserva el derecho de no aceptar al personal que desarrolle su tarea sin una capacitación suficientemente o un comportamiento incorrecto.

El adjudicatario debe hacerse cargo de todos los materiales y útiles para la correcta ejecución de los servicios encomendados, debidamente identificados como de su propiedad.

El Jefe de auditoría propuesto por el adjudicatario deberá disponer de un número de teléfono que permita su localización en jornada laboral del calendario laboral de Barcelona, por parte del personal responsable del Consorci AOC.

Para poder conocer la calificación profesional, el licitador presentará el currículo profesional de los candidatos que propongan por estos perfiles. El licitador justificará documentalmente la calificación profesional del personal destinado con la presentación de la documentación compulsada que se detalla a continuación: tarjeta de identidad profesional y títulos profesionales. En el currículo profesional de cada perfil que proponga para las funciones definidas, constará como mínimo:

- nombre y apellidos
- calificación educativa y categoría profesional
- experiencia y formación

- evaluación de la competencia: conocimientos de la tecnología y marco legal aplicable.
- seguimiento del desempeño
- fecha de la actualización más reciente de cada registro

En caso de baja de cualquiera de los miembros del equipo, el adjudicatario deberá sustituirlo en menos de 15 días laborables de acuerdo con los responsables del Consorci AOC. Cualquier cambio en uno de los miembros del equipo a instancias del adjudicatario deberá ser pactado con el Consorci AOC, que deberá validar tanto la baja como el currículo de la nueva persona a incorporar. Si el cambio es a instancias del adjudicatario, habrá que acordar el calendario de cambio con el Consorci AOC con el fin de minimizar el impacto en los desarrollos en curso. Quedan fuera de estos compromisos los periodos de vacaciones y permisos de todos los miembros del equipo.

El Consorci AOC realizará, en su caso, entrevistas a las personas del equipo de proyecto propuesto y, si es necesario, pedirá alternativas a las personas presentadas.

El Consorci AOC se reserva el derecho a solicitar el cambio de cualquiera de los miembros del equipo sin necesidad de justificación con una antelación de 20 días naturales a la fecha de sustitución.

El Consorci AOC se reserva el derecho a pedir una declaración personal de cada uno de los auditores para garantizar su formación y conocimientos.

El auditor debe demostrar ser competente para llevar a cabo la auditoría. Esto incluye la realización de juicios técnicos exigidos, la definición de políticas y su implementación y la imparcialidad.

5.4 Condiciones

Las entidades de registro se encuentran distribuidas por toda la geografía catalana en ayuntamientos, consejos comarcales, diputaciones, universidades, etc...

El número máximo de auditorías de entidades de registro a realizar en el marco del presente contrato, en modalidad presencial o virtual, será el definido en las unidades por tipologías definidas en el apartado B3 del Pliego de cláusulas Administrativas. A continuación se exponen las volumetrías y condiciones aplicables a las tipologías de auditoría definidas :

- Auditorías presenciales ER T-CAT : actualmente hay 72 ER T-CAT operativas.
- Auditorías presenciales ER idCAT: existen 282 entidades de registro idCAT de las cuales un 70% se auditará virtualmente y un 30% presencialmente, según las volumetrías de emisiones
- Auditorías virtuales Entidad de Registro (ente suscriptores): estas auditorías siempre serán virtuales a excepción de necesidad de presencia por problemas en la primera auditoría virtual: 2.200 organismos
- Auditorías virtuales Entidades de Registro idCAT: existen 282 entidades de registro idCAT de las cuales un 70% se auditará virtualmente y un 30% presencialmente, según las volumetrías de emisiones.

Cada 2 años el Consorci AOC, como prestador de servicios de certificación, debe garantizar que las entidades de registro con emisiones deben haber pasado una auditoría. Esta carencia se puede ver afectada por cambios en el marco normativo o según los procesos de mejora continua a los que está obligado el servicio.

Los esfuerzos en horas previstos por cada perfil y cada tipo de auditoría se exponen en el pliego de cláusulas administrativas.

5.4.1 Programa de auditorías

Anualmente el adjudicatario, procederá a una programación de entidades a auditar.

Cuando un organismo sea entidad de registro T-CAT e idCAT se aprovechará para realizar las auditorías en un mismo desplazamiento, en el caso de que se determine la necesidad de una auditoría presencial.

En el caso de las auditorías virtuales, también se aprovechará el contacto con la organización para realizar las auditorías de control que sea necesarias.

El equipo de auditoría deberá estar en permanente contacto con las personas que forman el Servicio de Certificación Digital y con el adjudicatario de los demás lotes del presente contrato.

El programa de trabajo y el calendario propuesto será elaborado por el proveedor. Sin embargo, el Consorci AOC podrá decidir qué auditorías son prioritarias.

El adjudicatario deberá haber realizado la totalidad de las auditorías planificadas en los periodos bianuales que marca el reglamento eIDAS.

El proveedor generará un plan operativo del proyecto que deberá contener toda la información necesaria para asegurar la calidad de las auditorías realizadas.

5.4.2 Planificación y preparación de la auditoría

El objetivo de este paso es obtener la máxima información posible de la entidad de registro antes de abordar con éxito la auditoría. Esto incluye:

- Obtener la ficha de suscriptor y de entidad de registro donde figuran todos los participantes del servicio en el ente con su rol y toda la documentación que sea necesaria.
- Conocer el número de certificados emitidos
- Disponer de la fecha de la última auditoría y resultados (en el caso de que los haya)
- Conocer cualquier cambio que haya podido afectar al servicio.
- Disponer del listado de incidencias sufridas
- Disponer del informe de revisión de gestión.

Una vez cerrada la fecha de auditoría con la entidad de registro, se deberá enviar un correo-e con la planificación detallada de la misma al responsable de servicio.

El plan de auditoría deberá incluir los siguientes puntos:

- Objetivo y alcance
- Criterios de auditoría
- Equipo auditor
- Documentos de referencia
- Agenda con tiempo de inicio o duración
- Temas de confidencialidad
- Riesgos de la auditoría
- Instrucciones de resolución y seguimiento

La comunicación del plan de auditoría a la entidad de registro deberá realizarse con 30 días de antelación a la realización de esta.

Toda esta primera parte se puede hacer mediante teléfono y correo-e con la entidad de registro con un correo electrónico corporativo que suministrará el Consorci AOC, pero siempre deberá quedar una constancia por escrito.

El estado de cada actuación debe estar siempre disponible para el Consorci AOC mediante las herramientas propias del Consorci AOC

5.4.3 Realización propiamente de la auditoría

La realización de la auditoría se realizará conforme los procedimientos de auditoría establecidos y que encontraréis en el anexo 4.

5.4.3.1 Las pautas que seguir en la auditoría presencial será la siguiente:

Términos y condiciones: Poner a disposición de los suscriptores, las entidades de registro y partes interesadas los términos y condiciones de cada uno de los servicios prestados. Estos términos y condiciones especificarán:

- Las obligaciones del suscriptor y las entidades de registro, si existen,
- El período de tiempo que se guardan los *logs* del servicio de confianza
- Las limitaciones de responsabilidad
- Marco legal aplicable
- Procedimiento de quejas y resolución de conflictos
- Información de contacto del servicio de confianza
- Compromiso sobre la disponibilidad

Hay que informar a los suscriptores, las entidades de registro y a las partes interesadas de los términos y condiciones antes de iniciar la relación contractual. Además, estos términos y condiciones deben estar disponibles a través de medios de comunicación no perecederos, con un lenguaje comprensible y que se puedan transmitir electrónicamente.

Operación y gestión del servicio

- Los servicios deben ser accesibles a todos los solicitantes, cuyas actividades están dentro de su campo de operación declarado y que aceptan cumplir sus obligaciones especificadas en los términos y condiciones del servicio.
- Disponer de políticas y procedimientos para la resolución de conflictos o reclamaciones de clientes u otras partes interesadas
- Contrato en vigor con el Consorci AOC.

Recursos humanos involucrados: El ente debe asegurarse de que el personal que da el servicio es responsable y da confianza al servicio dado.

- El personal estará cualificado para hacer el trabajo encomendado y habrá recibido formación sobre seguridad y protección de datos personales adecuados al servicio ofrecido y el puesto de trabajo.
- Se dispondrá de una ficha de personal actualizada con la formación recibida (conocimiento, experiencia y calificaciones) o experiencia en el puesto de trabajo que se irá actualizando cada año, en función de actualizaciones sobre nuevas amenazas o nuevas prácticas de seguridad.
- Se describirán sanciones disciplinarias para aquellos trabajadores que incumplan las políticas o procedimientos establecidos.
- Las funciones de seguridad y las responsabilidades estarán descritas claramente en la descripción de los puestos de trabajo que estarán

disponibles para todo el personal implicado. Las funciones de confianza, de las que depende la seguridad de la operación del servicio, deben estar claramente identificadas. Las funciones de confianza serán nombradas por la dirección y serán aceptadas por la dirección y por la persona implicada.

- Todo el personal (temporal o fijo) dispondrá de su descripción del puesto de trabajo donde constará la sensibilidad de posición en función de los derechos y nivel de acceso, formación y sensibilización.
- Se dispondrá de procedimientos y procesos de gestión alineados con los de seguridad de la información.
- Todo el personal con funciones de confianza debe estar libres de conflictos de intereses que puedan perjudicar la imparcialidad de las operaciones del servicio.
- Las funciones de confianza incluyen:
    - Operador del sistema: Responsable para operar el sistema de confianza en el día a día. Autorizado para realizar la copia de seguridad.
- El personal no tendrá acceso a las funciones de confianza hasta que no se hayan cumplido todos los controles necesarios.

Gestión de activos: El ente deberá asegurarse del nivel apropiado de protección de los activos, incluyendo los activos de información.

- Mantener un listado actualizado de activos de información con la asignación de la clasificación correspondiente con la evaluación de riesgos realizada.
- Todos los materiales se tratarán de manera segura según su clasificación de riesgo. Los materiales que contengan datos sensibles se destruirán de manera segura cuando ya no sean necesarios.

Control de acceso digital: El acceso al sistema estará limitado al personal autorizado.

- El acceso a la información y a las funciones del sistema de aplicación deben estar restringidos de acuerdo con la política de acceso.
- El personal del ente debe identificarse y autenticarse antes de utilizar aplicaciones críticas relacionadas con el servicio.
- El personal del ente es responsable de sus actividades.
- Debe existir un protocolo o política de borrado seguro de datos confidenciales en dispositivos con el fin de evitar el acceso no autorizado.

Control de acceso físico: Se debe controlar el acceso físico a los componentes del sistema del ente, cuya seguridad es crítica para la provisión del servicio de confianza y minimizar los riesgos relacionados con la seguridad física.

- Acceso físico limitado a los componentes del sistema del ente que son críticos para la prestación del servicio.
- Se deben implementar controles para evitar la pérdida, daño o compromiso de activos e interrupción de las actividades.
- Se deben implementar controles para evitar el compromiso o robo de información y de las instalaciones de procesados de la información.
- Los componentes que son críticos para la prestación del servicio deben estar localizados en un perímetro de seguridad protegido físicamente

contra la intrusión y se debe controlar el acceso a través de un perímetro de seguridad y alarma.

Seguridad operacional: El ente debe utilizar sistemas de confianza y productos protegidos contra modificaciones y debe asegurarse de la seguridad técnica y fiabilidad de los procesos realizados por ellos.

- Hay que aplicar un procedimiento y registro de gestión de cambios para versiones, modificaciones y correcciones de software.
- La integridad de los sistemas del ente debe estar protegidos contra virus, software malicioso y software no autorizado.
- Los materiales utilizados en los sistemas del ente deben gestionarse de manera segura para protegerlos de daños, robos, accesos no autorizados y obsolescencia.
- Deben protegerse contra la obsolescencia y el deterioro, los materiales utilizados durante el tiempo en que deban conservarse los registros.
- Se deben implementar y establecer los procedimientos para las funciones administrativas y de confianza que impactan a la provisión de los servicios.
- El ente debe aplicar procedimientos para asegurarse de lo siguiente:
    - Los despliegues de seguridad que están disponibles se aplican en un tiempo razonable.
    - No se aplican despliegues de seguridad que introducen vulnerabilidades o inestabilidades mayores que los beneficios que puedan aportar.
    - Se documentan las razones por las que no se aplica un despliegue de seguridad.

Seguridad de las redes: El ente debe proteger su red y sus sistemas de los ataques.

- El ente mantendrá todos los sistemas que son críticos para la operación del ente en una o más zonas seguras.
- El ente debe someterse o realizar un escáner de vulnerabilidad periódico en direcciones IP publicadas y privadas identificadas por el ente y registrar pruebas de que cada persona o entidad realizaba cada escaneo de vulnerabilidad con las habilidades, las herramientas, la competencia, el código ético y la independencia necesario para proporcionar un informe fiable.
- El ente debe someterse a una prueba de penetración en sus sistemas en la instalación y después de la infraestructura o las actualizaciones o modificaciones de las aplicaciones que determine el ente como significativas. El ente registrará pruebas de que cada prueba de penetración fue realizada por una persona o entidad con las habilidades, las herramientas, la competencia, el código ético y la independencia necesarias para proporcionar un informe fiable.

Gestión de incidentes: Se debe controlar la actividad del sistema relacionada con el acceso a los sistemas informáticos, el uso de sistemas informáticos y las solicitudes de servicio.

- Las actividades de seguimiento deberían tener en cuenta la sensibilidad de cualquier información recogida o analizada

- Las actividades anormales del sistema que indican una posible vulneración de seguridad, incluida la intrusión en la red del ente, deben detectarse e informarse como alarmas.
- Los sistemas de TI del ente deben supervisar los siguientes acontecimientos:
  - Puesta en marcha y apagado de las funciones de registro; i
  - Disponibilidad y utilización de los servicios necesarios con la red del ente.
- El ente debe actuar de manera oportuna y coordinada para responder rápidamente a incidentes y limitar el impacto de las violaciones de la seguridad. El ente debe designar personal de rol de confianza para hacer un seguimiento de las alertas de eventos de seguridad potencialmente críticos y garantizar que se registren incidentes relevantes de acuerdo con los procedimientos del ente.
- El ente debe establecer procedimientos para notificar a las partes apropiadas de acuerdo con las normas reguladoras aplicables de cualquier incumplimiento de la seguridad o pérdida de integridad que tenga un impacto significativo en el servicio de confianza prestado y en los datos personales mantenidos en él, dentro de las 24 horas posteriores al momento en que se identifica el incumplimiento.
- Cuando el incumplimiento de la seguridad o pérdida de integridad pueda afectar negativamente a una persona física o jurídica a la que se ha prestado el servicio fiduciario, el ente también notificará a la persona física o jurídica el incumplimiento de la seguridad o la pérdida de integridad sin demora indebida .
- Se deben controlar los sistemas del ente, incluida la supervisión o la revisión periódica de los registros de auditoría para identificar evidencias de actividad maliciosa que implican mecanismos automáticos para procesar los registros de auditoría y personal de alertas de posibles eventos de seguridad críticos.
- El ente abordará cualquier vulnerabilidad crítica que no se haya tratado previamente por el mismo, dentro del plazo de 48 horas después de su descubrimiento. Si esto es efectivo en función del efecto en términos de costes, el ente debe crear e implementar un plan para mitigar la vulnerabilidad o documentará la base por la que la vulnerabilidad no debe ser tratada.
- Se deben utilizar los procedimientos de información y respuesta de los incidentes de manera que se minimice el daño causado por incidentes de seguridad y mal funcionamiento.

Alineación con el Plan de continuidad de negocio del Consorci AOC: El ente debe tener definido y mantener un plan de continuidad que promulgará en caso de desastre.

Cumplimiento legal y normativo: El ente debe asegurarse de que opera dentro del marco legal aplicable.

- Procedimiento de cumplimiento de marco legal donde se pueda demostrar cómo se gestiona el marco legal.
- El ente debe asegurarse de que los servicios son accesibles a personas con discapacidad.

– Cumplimiento del marco legal vigente en protección de datos personales. Gestión de la identificación:

Gestión del cambio: Procedimiento transversal donde se planifiquen los cambios, se registren y se lleve un seguimiento.

5.4.3.2 Las pautas que seguir por la auditoría virtual serán:

- Hacer un muestreo de los certificados personales generados, entre un 5% y un 10% del total.
- Hacer un muestreo de los certificados de dispositivo y aplicación generados (casos de ER T-CAT y ente suscriptor), entre un 6% y un 10%.
- Solicitar al responsable del servicio la documentación del muestreo para analizar.
- La auditoría deberá comprobar que los datos del certificado generado son los mismos que el certificado solicitado o que el DNI u otros documentos identificativos. En los casos de hoja de entrega de T-CAT se comprobará que están debidamente firmados, archivados.
- Comprobar la seguridad del tratamiento de datos personales en cumplimiento de la legislación vigente.

5.4.4 Documentación que entregar

Para cada ERD, se entregará un informe de auditoría según el formato definido previamente entre el proveedor y el Consorci AOC que tendrá una estructura similar a los informes de ejemplo que se distribuyen junto con este pliego en los anexos 2 al 5.

Toda la documentación y comunicaciones estarán redactadas en catalán normalizado.

Estos informes se irán entregando de forma individual tras la realización de la auditoría en el plazo indicado en el punto "5.5 a Plazo de entrega del checklist y evidencias de auditoría". Todas estas entregas serán validadas por el Consorci AOC en las fases pertinentes y formarán parte del acta de aceptación parcial correspondiente.

El Consorci AOC deberá recibir por parte de el adjudicatario, el ***Checklist* de seguimiento, las evidencias asociadas y el informe de auditoría** indicando cuáles son las no conformidades encontradas y las evidencias que lo demuestran en el plazo máximo indicado en "5.5 1-bb informes tras la ejecución de la auditoría, para su evaluación y gestión diligente.

Aparte de los informes de auditoría de cada ER, se realizará otro informe con un resumen de la visión global del grado de cumplimiento de los procedimientos de las ER, donde se incluirán tablas y gráficos que permitan detectar fácilmente los puntos que en general han sido más problemáticos, al final de cada año de servicio.

Toda la documentación generada durante la ejecución del contrato, incluyendo los documentos de trabajo y las evidencias recogidas, serán propiedad del Consorci AOC, y el adjudicatario no podrá facilitarla a terceros. Esta documentación se irá guardando en las carpetas de red del Consorci AOC.

Los informes de auditoría que se consideren "incompletos" por parte del Consorci AOC deberán repetirse, excepto en el caso de que se pueda demostrar que la ER no ha cumplido con la obligación de ofrecer de forma abierta toda la información necesaria al auditor. Para evitar esto se recomienda realizar una buena planificación y concienciación a los ente en la primera fase de la auditoría.

5.4.5 Finalización de la auditoría

En la recepción de las correcciones por parte de cada ER, el auditor evaluará la conformidad de las acciones ejecutadas para garantizar la corrección de las desviaciones.

Se deberá tener especial cuenta para:

- Establecer medidas para controlar el progreso de las no conformidades graves.
- Realizar las revocaciones de oficio de los certificados emitidos de manera errónea. (con los procedimientos establecidos, comunicación al responsable, etc...).
- En caso de que el ER idCAT no haga la recopilación de los DNI's será necesario que envíen el correo de plantilla para que el suscriptor lo lleve al ER. En caso de que no lo lleve en 90 días, el proveedor deberá comunicarlo al Consorci AOC quien procederá a la revocación de oficio de aquel certificado.

Una vez evaluado, el auditor considerará cerrado el proceso de auditoría.

5.4.6 Herramienta para la realización remota de auditorías a las ER

El licitador propondrá una herramienta, software o plataforma, para la realización remota de las auditorías. Esta herramienta debe permitir :

- El envío de los cuestionarios por cada tipo de auditoría a la entidad receptora.
- La carga y custodia de las evidencias que provea la entidad auditada.
- La carga de las preguntas y cuestionarios que el Consorci AOC indique.
- El seguimiento en tiempo real de los cuestionarios enviados, devueltos, pendientes... por cada tipo de auditoría.
- La visualización del cronograma y calendario previsto para cada tipo de auditoría y por cada fase (cuestionarios, informes y alegaciones).

El adjudicatario pondrá a disposición suficientes licencias para el uso de la herramienta por parte del equipo de auditoría. También el licenciamiento de la herramienta deberá permitir que se puedan auditar todas las entidades destinatarias de auditoría por año.

La ubicación de los servidores y los datos de esta herramienta deberán cumplir los requisitos de protección de datos aplicables indicados en este documento.

5.4.7 La gestión de la seguridad y el cumplimiento normativo

El adjudicatario, de forma coordinada con el área de seguridad del Consorci AOC, deberá dar cumplimiento al marco legal y normativo vigente (definido en el punto 3 MARCO NORMATIVO). En este apartado se remarcan aquellos aspectos de seguridad considerados de mayor relevancia dentro del alcance del servicio y que habrá que tener operativos para la puesta en marcha de este.

En concreto, aplican medidas proporcionales para el tratamiento de auditoría de los datos que pertenecen a los subsistemas "Subsistema de emisión y revocación de certificados" y "Subsistema de EACAT y MUX" definidos en el punto "6.4.10.9 Auditoría externa", apartado Esquema nacional de seguridad.

5.4.7.1 Cumplimiento normativo y legal

El adjudicatario deberá cumplir con todos los requerimientos que sean de aplicación de acuerdo con el marco normativo de seguridad vigente y de todas las actualizaciones posteriores que se produzcan, así como a todo el marco legal en materia de ciberseguridad

que sea de aplicación (por ejemplo, Esquema Nacional de Seguridad y GDPR – General Data Protection Regulation, eIDAS - electronic IDentification, Authentication and trust Services)).

El adjudicatario deberá incorporarse al modelo de cumplimiento normativo del Consorci AOC. En este modelo se integran las posibles auditorías que el Consorci AOC determinen realizar, así como el seguimiento de los planes de acción derivados de las mismas. También se incluye en este modelo el cumplimiento por parte del adjudicatario de planes de acción relativos a normativas o estándares el Consorci AOC y su seguimiento recurrente. El adjudicatario deberá disponer de los recursos adecuados para llevar a cabo la ejecución de las tareas que le correspondan en el modelo de cumplimiento, dando respuesta en los plazos marcados por el Consorci AOC.

El adjudicatario deberá garantizar el acceso del personal autorizado del Consorci AOC a la información de seguridad (procedimientos, registro de incidentes, rastros, etc.). Toda la información de seguridad deberá estar siempre disponible para este personal, autorizado y previamente identificado. El Consorci AOC y el adjudicatario establecerán conjuntamente los mecanismos para facilitar el acceso del personal autorizado a esta información, estableciendo los controles de seguridad mínimos.

5.4.7.2 Requisitos de protección de datos

El licitador en su oferta deberá detallar las medidas de seguridad y las medidas de privacidad desde el diseño y por defecto que se establecen para dar cumplimiento a los requerimientos establecidos en el Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de estos datos y a Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales por cada uno de los ámbitos especificados en el apartado "5.4 Condiciones del presente PPT y por todo el ciclo de vida de los datos, incluido su bloqueo en cumplimiento de lo establecido en la LLOPDiGDD. Habrá que estar en las guías aprobadas por la Autoridad Catalana de protección de Datos, la Agencia Española de Protección de Datos y el Comité Europeo de Protección de Datos (CEPD).

El adjudicatario deberá revisar anualmente y cuando se produzca alguna modificación en el tratamiento de los datos, el Análisis de Riesgos por los derechos y libertades de los titulares de los datos y adoptar las medidas de seguridad que, en su caso, sea necesario implantar para preservarlos.

5.5 Acuerdos de nivel de servicio

El funcionamiento del servicio objeto de esta contratación estará sujeto a un sistema de control de calidad ejercido por el Consorci AOC, siguiendo los Acuerdos de nivel de servicio

a. Plazo de entrega del checklist y evidencias de auditoría
   Máximo 15 días

b. Plazo de entrega de informes
   Máximo 15 días

c. Desviación en el cumplimiento de planificación
   5% de programa de auditorías

Esta puntuación es importante, ya que aparte de ser una medida de calidad de funcionamiento del servicio, también puede constituir una causa justificada de rescisión del contrato por parte del Consorci AOC.

Sin prejuicio de lo descrito en este documento en el punto 5.2, el adjudicatario anualmente deberá presentar al Consorci AOC un informe con un plan de mejora para el Consorci AOC resultante de las auditorías realizadas.

5.6 Seguimiento del servicio

El objetivo de este ámbito de seguimiento es garantizar la integración de la calidad, seguridad y continuidad, en todo el ciclo de vida, de los procesos, servicios y soluciones, mediante la prescripción, seguimiento, validación y verificación de la eficaz implantación de los controles definidos.

5.6.1 Gobernamiento y mejora del servicio

El adjudicatario es el responsable de generar y entregar los informes y métricas de reporting (en adelante información) que se determinen en los diferentes ámbitos del gobernamiento del servicio objeto de este lote. Estos deben permitir al Consorci AOC gobernar, controlar y gestionar los servicios prestados por el adjudicatario, tanto desde una óptica individual, como transversal y global.

El formato y el contenido mínimo de la información a elaborar por el adjudicatario en todos los ámbitos de gobernamiento es el definido en el Anexo 5.

El Consorci AOC podrá solicitar, durante la vigencia del contrato cambios en la estructura y contenido de la información para ajustarse a las necesidades de seguimiento de los servicios.

El adjudicatario deberá proporcionar al Consorci AOC, además de los informes periódicos de seguimientos de los ANS, la información (evidencias) con base en la que se hayan elaborado, para que el Consorci AOC la pueda incorporar a su herramienta de gestión.

El objetivo de este ámbito de gobernamiento es garantizar la integración de la calidad, en todo el ciclo de vida, de los procesos, servicios y soluciones, mediante la prescripción, seguimiento, validación y verificación de la eficaz implantación de los controles definidos.

El licitador propondrá los mecanismos necesarios para permitir al Consorci AOC comprobar que se mantienen los niveles de calidad esperados.

5.6.1.1 Gestión de incidencias y problemas

Se entiende para incidencia cualquier suceso que no forma parte de la operativa normal de un servicio y que provoca, o puede provocar, la interrupción, el mal funcionamiento o la degradación en la calidad del servicio.

El objetivo principal del proceso de gestión de incidencias es restaurar el normal funcionamiento del servicio tan pronto como sea posible, minimizando el impacto adverso sobre las operaciones de negocio/clientes y organización, asegurando que el servicio se mantenga en los mejores niveles posibles de calidad y disponibilidad.

El proceso soporta todos los servicios que el Consorci AOC presta al usuario dentro del alcance del pliego y por tanto su alcance es la resolución de todas las incidencias que puedan afectar a estos servicios.

Se entiende por problema cualquier causa subyacente, aún no identificada, de una serie de incidentes o de un incidente aislado de importancia significativa.

El objetivo principal de la Gestión de Problemas es minimizar el impacto negativo que tienen las incidencias sobre el negocio, y prevenir la recurrencia de incidencias relacionadas con estos errores. Para conseguir esta meta, la Gestión de Problemas llega hasta la causa a raíz de las incidencias y luego inicia acciones que corrigen la afectación de servicio.

El adjudicatario participará activamente en el proceso de Gestión de Problemas siendo el Responsable de todos los problemas que puedan salir de los servicios que está prestando al Consorci AOC.

Es responsabilidad del adjudicatario la aplicación y seguimiento de los procedimientos asociados a la gestión de problemas surgidos de los servicios que presta, así como el seguimiento y gestión del estado de estos hasta la corrección de la afectación de servicio.

Ante la detección de problemas graves y con impacto directo a negocio, el proveedor de servicio deberá notificar el problema al Jefe del servicio Consorci AOC.

El licitador describirá la metodología propuesta para atender:

- Registro de incidencias y problemas
- Clasificación y asignación
- Investigación y diagnosis
- Seguimiento y coordinación
- Resolución y recuperación
- Cierre de incidencias y problemas

5.6.2 Órganos de Gestión

5.6.2.1 Reuniones de Dirección.

Las reuniones de Dirección se realizarán con el objetivo de establecer un control y una visión estratégica y amplia sobre el desarrollo global del servicio.

Las reuniones podrán ser presenciales y/o virtuales. En el caso de las presenciales, pueden realizarse tanto en la sede del Consorci AOC, como de la empresa adjudicataria. En todo caso, es necesario que el adjudicatario disponga de los recursos necesarios en cualquiera de las modalidades de reunión previstas.

Las reuniones de dirección se convocarán trimestralmente, aunque a petición del Consorci AOC y en circunstancias concretas de afectación crítica del servicio, podrán ser convocadas en cualquier momento durante la vigencia del contrato, convocadas con una antelación mínima de 3 días laborables, según el calendario laboral aplicable al personal del Consorci AOC.

5.6.2.2 Reuniones de Seguimiento.

El gestor del servicio del adjudicatario y el Jefe del Servicio del SCD del Consorci AOC realizarán una reunión de seguimiento del servicio, que será periódica y como mínimo de carácter mensual, aunque a petición del Consorci AOC y en circunstancias concretas de afectación crítica del servicio, podrán ser convocadas en cualquier momento durante la

vigencia del contrato, con una antelación mínima de 1 día laborable, según el calendario laboral aplicable al personal del Consorci AOC.

Las reuniones podrán ser presenciales y/o virtuales. En el caso de las presenciales, pueden realizarse tanto en la sede del Consorci AOC como de la empresa adjudicataria. En todo caso, es necesario que el adjudicatario disponga de los recursos necesarios en cualquiera de las modalidades de reunión previstas.

Esta reunión se hará antes del décimo día laborable (de lunes a viernes excepto festivos) de cada mes. En esta reunión se revisará el informe mensual, el funcionamiento de los procesos, se generarán propuestas de mejora del servicio y se hará un seguimiento de todo lo relacionado con la prestación. A título de ejemplo se indican algunos de los aspectos incluidos como posible contenido de la reunión:

- Evaluar la situación de ejecución del servicio objeto del contrato a partir del seguimiento de la evolución de los objetivos e indicadores formulados, así como el nivel de cumplimiento de los acuerdos de nivel de servicio que estén vinculados.
- Revisar y poner en común las incidencias que se hayan producido en el mes inmediatamente anterior, ya sea en relación con la prestación efectiva del servicio como en relación con el modelo de gestión vinculado.
- Revisar y poner en común novedades, jornadas y/o documentación relevante para la ejecución del servicio, con el fin de generar una dinámica de participación que impacte de manera positiva en la gestión del conocimiento y sea aplicable a la propia prestación del servicio.

Antes de cada reunión de seguimiento y con la antelación establecida en el correspondiente acuerdo de nivel de servicio establecido el referente del servicio del adjudicatario pondrá a disposición del Jefe del Servicio del Consorci AOC el informe de seguimiento detallado propuesto en el "Anexo _1_Plantilla Informe Seguimiento" que incluye, como mínimo, información sobre:

- Estado de cumplimiento de las tareas en relación con las planificaciones realizadas y las posibles desviaciones que se hayan producido. Número de actuaciones realizadas de acuerdo con el objeto y alcance del lote. Número de consultas realizadas (por tipología, teléfono, correo, etc..).
- Mejoras aplicables al servicio de certificación digital.
- Información de cumplimientos sobre los acuerdos de nivel de servicio establecidos.

Se utilizará una herramienta de gestión del Consorci AOC que permitirá y facilitará la participación de los diferentes actores implicados en la ejecución del servicio. Esta herramienta se convierte en clave para mantener coordinados a todos los actores participantes, detectar las necesidades a cubrir, así como detectar mejoras tanto en la prestación del servicio como en el modelo de gestión vinculado. El referente del servicio es el principal responsable del mantenimiento de la herramienta de gestión del servicio y debe reflejar todos los cambios, actualizaciones, documentos, etc., con el máximo rigor posible, con el fin de tener un acceso inmediato a la información actualizada de la prestación del servicio y permitir una visión con el mayor detalle posible a los diferentes actores que participan en la gestión de este lote.

5.7 Devolución del servicio

Una vez finalizado el contrato el adjudicatario deberá garantizar que ha cumplido con todos los compromisos establecidos.

A la finalización del servicio, el adjudicatario deberá presentar la siguiente documentación al Consorci AOC:

- Informe del muestreo de entidades de registro auditadas durante los últimos dos años del servicio.
- Cierre de informes de auditoría en un plazo previsto máximo de acuerdo con lo definido en el punto de ANS para esta tipología tras la finalización del servicio.
- Listado actualizado de la planificación de auditorías a ente suscriptores (auditorías no realizadas).
- Listado actualizado de comunicaciones de auditorías a ente suscriptores (auditorías planificadas ya comunicadas).
- Informe final de conclusiones (clasificado por tipo de ER) desde el último informe final de conclusiones hasta la finalización del servicio.
- Informe donde consta la evaluación de la conformidad de las acciones ejecutadas por cada ente suscriptor para garantizar la corrección de las desviaciones detectadas y la identificación de aquellas acciones que no han sido evaluadas por el adjudicatario.

El adjudicatario deberá devolver toda la información confidencial propiedad del Consorci AOC, así como la generada a partir de la prestación del servicio.

6 Lote 3: SERVICIOS DE CERTIFICACIÓN DIGITAL

6.1 Descripción

El Consorci AOC es órgano competente en relación con la prestación de servicios de identidad digital y firma electrónica, de acuerdo con la Ley 29/2010, de 3 de agosto, del uso de los medios electrónico en el sector público de Cataluña y con sus estatutos.

De acuerdo con esta competencia y en relación con el objeto de este contrato, debe considerarse al Consorci AOC, a todos los efectos, como Prestador calificado de servicios de certificación.

En relación con el ámbito de los Servicios de Certificación Digital y aquellos otros que son conexos, vinculados o relacionados, estamos ante unos servicios de alta criticidad y complejidad, con muchas particularidades, una gran cantidad de usuarios consumiendo los servicios de manera concurrente, así como una importante dependencia estratégica con los servicios digitales de los entes y organismos públicos del ámbito catalán usuarios de los servicios.

6.1.1 Catálogo de servicios objeto del contrato

El catálogo de servicios incluidos en el ámbito de esta licitación estará formado, principalmente, por los siguientes:

6.1.1.1 Servicios a precio unitario y mantenimiento de aplicaciones informáticas

Se consideran Servicios bajo demanda con un coste unitario: son los servicios asociados a elementos tangibles (físicos) y no tangibles (digitales) establecidos en el catálogo de servicios del Consorci AOC, a un coste unitario.

Bajo estas categorías se incluye el siguiente catálogo de servicios:

Concepto	Descripción breve
Adquisición de soportes criptográficos (tarjetas)	Diseño T-CAT estándar
Servicio de emisión ordinaria de soportes criptográficos (incluye envío al ente solicitante)	T-CAT estándar
Servicio de emisión urgente de soportes criptográficos (T-CAT Estándar e incluye envío urgente al ente solicitante)	Diseño personalizado (sólo grabar chip)
Servicio de emisión urgente de soportes criptográficos (diseño personalizado e incluye envío urgente al ente solicitante)	T-CAT estándar
Servicios de programación	Precio/hora programador

Las volumetrías por cada servicio y año son las indicadas en el pliego de cláusulas administrativas.

6.1.1.2 Servicios a tanto alzado

Incluye todos los gastos generales necesarios para garantizar el buen funcionamiento del servicio con un volumen de la demanda de los servicios de hasta 700.000 certificados vigentes para usuarios únicos independientemente de la entidad de certificación emisora, así como los certificados de aplicación, personales e infraestructura y aquellos incluidos en el catálogo de certificados en cada momento, y que no impliquen manipulación directa por parte del adjudicatario categorizada en los servicios a precio unitario.

Concretamente:

- La financiación de los gastos en hardware y software, de puesta en marcha, de transición, de optimización y de devolución del servicio (si procede). En concreto:
  - La provisión de dispositivos criptográficos HSM por el entorno de las entidades de certificación según especificado en el punto 6.4.3.4.3.
  - La provisión de las herramientas de observación de los Acuerdos de Nivel de Servicio. En particular de la herramienta para la observación del ANS de emisiones y provisión de servicios (punto 6.5.2) y de la herramienta para la observación de los ANS de capacidad y disponibilidad (puntos 6.5.2.4 i 6.5.2.3).
- Durante la fase de transición incluye la adaptación y/o integración de interfaces, web, portales, infraestructura y EERR avanzadas.
- Durante la fase de transformación y optimización, incluye la mejora de las interfaces de las aplicaciones de usuario final.
- El servicio de soporte de 2º y 3er nivel dirigido a suscriptores y operadores.
- Mantenimiento de la documentación asociada al servicio, manuales, faq's, procedimientos, etc..
- Las auditorías y otras evaluaciones periódicas a que se tenga que someter el servicio.
- La operación de la Entidad de Registro T-CAT del Consorci AOC según definido en el punto 6.4.6.
- La generación de paquetes de certificados de pruebas con datos estándares.
- La generación de certificados de preproducción solicitados.
- La homologación de impresoras, tarjetas criptográficas y softwares asociados.
- La incorporación de hasta dos (2) perfiles de certificado adicional por año según establecido en el punto 6.4.3.2. (incluye la redacción, implantación y reconocimientos y todas las tareas asociadas)
- La gestión de los reconocimientos de los servicios de certificación.
- Facturación de los certificados y control de la facturación.
- Gastos de funcionamiento ordinario, de gestión operativa y explotación del servicio, incluyendo específicamente:
  - Emisión de facturas a los suscriptores y seguimiento
  - Gestión de los stocks de tarjetas, papelería y material fungible, incluida la distribución a las entidades de registro
  - Envío de los certificados
  - Adquisición del material fungible y de papelería necesario
  - Todas las tareas necesarias para el funcionamiento del servicio
- Adecuación al marco normativo vigente en cada momento así como las traducciones necesarias.
- La creación de hasta 20 nuevas ER IDCAT según las condiciones definidas en el punto "6.4.5 Modelo de registro idCAT certificado". Incluye la puesta en marcha (sin desplazamiento).
- La creación de hasta 3 nuevas ER T-CAT estándar con impresora de tarjetas con soporte criptográfica y según las condiciones definidas en el punto "6.4.4.1 Entidad de registro T-CAT". Incluye la puesta en marcha estándar con apoyo presencial.

- El apoyo a hasta 15 formaciones virtuales de operadores de ER idCAT o TCAT. Las sesiones serán con un máximo de 25 alumnos, según las condiciones definidas en el punto 6.4.8.
- El apoyo a hasta 5 formaciones presenciales de operadores ER T-CAT. Las sesiones serán con un máximo de 30 alumnos y duración de hasta 4 horas, según las condiciones definidas en el punto 6.4.8.

Los siguientes servicios no son objeto de este contrato:

- El servicio de apoyo de primer nivel.
- La compra de las impresoras de plástico y criptográficas para las entidades de registro, los recambios ni el servicio de mantenimiento de este hardware.

6.2 Funciones

El adjudicatario del presente lote deberá permitir al Consorci AOC prestar los servicios descritos en las Políticas de Certificación y la Declaración de Prácticas de Certificación del Consorci AOC, publicadas en http://epscd.aoc.cat/regulacio; y a las condiciones generales y específicas en el apartado funciones del Consorci AOC:

https://www.aoc.cat/serveis-aoc/condicions-prestacio-serveis-aoc/

Condiciones generales del Consorci AOC (versión del 13/03/2019):

https://www.aoc.cat/wp-content/uploads/2015/11/condicions-generals-de-prestacio-de-serveis_13032019.pdf

Condiciones específicas Er-T-CAT (punto 4, versión del 4/9/2015):

https://www.aoc.cat/wp-content/uploads/2015/11/Condicions-espec%C3%ADfiques-dels-Serveis-AOC_ER_T-CAT.pdf

Condiciones específicas ER-idCAT (versión del 23/6/16):

https://www.aoc.cat/wp-content/uploads/2015/11/Condicions-espec%C3%ADfiques-dels-Serveis-AOC_ER_idCAT.pdf

Un extracto de las funciones que el Consorci AOC traslada al adjudicatario y que se enumeran en las condiciones específicas como prestador del servicio son:

- Emitir, entregar, administrar, suspender, revocar y renovar certificados en los casos y por los motivos descritos en la Declaración de Prácticas de Certificación de las Entidades de Certificación de la Jerarquía Pública de Certificación de Cataluña.
- Ejecutar los servicios con los medios técnicos y materiales adecuados, y con personal que cumpla las condiciones de calificación y experiencia establecidas en la Declaración de Prácticas de Certificación de las Entidades de Certificación de la Jerarquía Pública de Certificación de Cataluña
- Cumplir los niveles de calidad del servicio, de conformidad con lo establecido en la Declaración de Prácticas de Certificación de las Entidades de Certificación de la Jerarquía Pública de Certificación de Cataluña, en los aspectos técnicos, operativos y de seguridad.
- Notificar al suscriptor, como mínimo con dos meses de antelación a la fecha de expiración de los certificados, la posibilidad de renovarlos, así como la suspensión, habilitación o revocación de los certificados.
- Comunicar a las terceras personas que lo soliciten el estado de los certificados, de acuerdo con lo establecido en la Declaración de Prácticas de Certificación de las

Entidades de Certificación de la Jerarquía Pública de Certificación de Cataluña para los diferentes servicios de verificación de certificado.
- Emitir un certificado para cada operador nombrado por el ente usuario después de la aprobación de la solicitud del certificado correspondiente.
- Impartir la necesaria formación al personal del ente usuario en especial a los operadores, para la ejecución de sus tareas.
- Comunicar al ente usuario cualquier cambio que se produzca en las Políticas de Certificación y en la Declaración de Prácticas de Certificación de las Entidades de Certificación de la Jerarquía Pública de Certificación de Cataluña.
- El Consorci AOC garantiza que las claves privadas de las Entidades de Certificación de la Jerarquía Pública de Certificación de Cataluña, utilizadas para emitir certificados, no ha sido comprometida, salvo que el Consorci AOC haya comunicado lo contrario, de acuerdo con lo estipulado en la Declaración de Prácticas de Certificación de las Entidades de Certificación de la Jerarquía Pública de Certificación de Cataluña.

El adjudicatario deberá poner a disposición las infraestructuras necesarias para la correcta prestación de los servicios de acuerdo con unos determinados requisitos (punto). **¡Error! No se encuentra el origen de la referencia.**) y condiciones (punto 6.4) expuestos en el presente documento, regidos por unos Acuerdos de nivel de servicio determinados (punto 6.5), con un determinado modelo de seguimiento del servicio (punto 6.6) y en las fases propuestas (punto 6.4.2, 6.7 i 6.8).

A continuación se presenta una estructuración de las funciones y responsabilidades del adjudicatario y del Consorci AOC en un marco de actuación común, para asegurar el cumplimiento de las obligaciones de cada una de las partes. Es un marco de relación que permite acordar el contenido y nivel de la prestación de los servicios, así como el seguimiento de la prestación real en los aspectos contractuales, estratégicos, tácticos y operativos.

Los licitadores pueden ampliar, mejorar y detallar, partiendo de las directrices aquí marcadas, la organización propuesta y el esquema específico de la relación con el Consorci AOC, así como los mecanismos de control propios de cada servicio y/o función transversal.

El modelo de relación propuesto en este lote (punto 6.6) se sustenta en una estructura de competencias y funciones que recaen sobre un esqueleto de responsables del adjudicatario, los cuales se relacionarán con el Consorci AOC a 2 niveles: directivo y operativo. Actuarán como interlocutores con el Consorci AOC, y serán el vínculo entre la estructura del Consorci AOC y la organización interna del proveedor.

El adjudicatario asignará al Consorci AOC los responsables que sostendrán el Modelo de Relación. El equipo de responsables deberá disponer del dimensionado, la formación y los medios adecuados para desarrollar las funciones y responsabilidades asignadas.

6.2.1 Estructura de responsabilidades del adjudicatario

La estructura de responsabilidades y competencias mencionada se concreta en los siguientes responsables. El equipo de responsables deberá disponer del dimensionado, la formación y los medios adecuados para desarrollar las funciones y responsabilidades asignadas.

Por parte del adjudicatario:

- Responsable de cuenta: Es la figura de referencia en el marco del contrato entre el Consorci AOC y el adjudicatario, y será el último responsable de la prestación del conjunto de servicios y proyectos del adjudicatario. Esta figura se mantendrá durante toda la vida del contrato: en la gestión comercial, durante la provisión del servicio y

hasta la devolución de este. Debe ser garante de la existencia de los mecanismos de relación en su organización para llevar a cabo los acuerdos tomados entre el Consorci AOC y el adjudicatario.

- Responsable de servicios: El proveedor asignará un responsable, cuyas principales responsabilidades serán:
  - La gestión y seguimiento diario del servicio, así como la resolución de conflictos y redimensionamiento temporal o permanente del mismo.
  - Mantenimiento del registro de la evolución del servicio para posteriormente poder elaborar los informes de servicio y justificar el cumplimiento de los ANS.
  - Seguimiento y control de los recursos asignados al servicio.
  - Realizar el control de costes, la estimación de esfuerzos y su seguimiento.
  - Analizar cualquier desviación y situaciones de gravedad dentro de la calidad, plazos o alcance del servicio
  - Analizar las modificaciones en alcance y coste del servicio que se puedan derivar, e interpretar estas modificaciones respecto al contrato vigente. En caso de que no impliquen una modificación contractual, debe tener la autoridad para formalizar e implementar internamente en su organización los acuerdos tomados.
  - Asegurar la buena colaboración con otros proveedores del Consorci AOC con quien se debe relacionar con el fin de mejorar el servicio de negocio final.

- Responsable de Control de Gestión: Es la figura que consolidará y aportará al Consorci AOC las informaciones objetivas y también las subjetivas, valoradas (información fiable y de calidad y analizada en base al conocimiento del modelo) que permitan la toma de decisiones operativas y estratégicas a lo largo de la vida del contrato. Será responsable de que el Consorci AOC reciba los informes de gestión acordados, tanto con indicadores económico-financieros como otros, así como de realizar el seguimiento del modelo económico acordado con el adjudicatario.

- Responsable Jurídico: Será el interlocutor principal con el Consorci AOC en materia jurídico-legal por los servicios prestados por el adjudicatario.

- Responsable de Facturación: Deberá facilitar la información relativa al proceso de facturación, según el modelo y formato definido por el Consorci AOC, así como colaborar en el proceso de la conciliación. Velará y asegurará que el proveedor:
  - Facilita la información relativa al proceso de facturación al Consorci AOC y también a los entes suscriptores del Servicio de Certificación Digital, según los modelos y formatos definidos por el Consorci AOC:
  - Presentará las facturas y el detalle por cada elemento / concepto de los importes facturados, adecuándose a los siguientes criterios:
    - Detalle completo de todos los elementos de coste facturados, identificando las unidades de coste.
    - Preinscripción y codificación de los elementos de coste facturados.
    - El formato de codificación y criterios de tipificación se validarán de forma conjunta.
  - Colabora en el proceso de la conciliación de la facturación en el Consorci AOC.

- Responsable de Arquitectura e innovación: Es el responsable de coordinar y armonizar la aplicación de la arquitectura corporativa en los sistemas de información y servicios a construir o mantener por el proveedor. Sus principales responsabilidades son:

- Velar por el cumplimiento de los principios asociados a los diferentes dominios, y por el cumplimiento de los estándares de arquitectura corporativa TIC.
- Proponer nuevas arquitecturas TIC a la vez que se mantienen y/o evolucionan las existentes (función de innovación).
- Velar por la coherencia en la aplicación de la arquitectura corporativa TIC.
- Identificar los componentes reutilizables y promocionar tanto la generación como el uso.
- Proporcionar un mecanismo de control, fundamental para asegurar el cumplimiento efectivo de los estándares de arquitectura corporativa TIC.

- Responsable de Operación de Apoyo y de Provisión del Servicio: Es el responsable del cumplimiento de los procesos de gestión de peticiones, incidencias, problemas y eventos (apoyo) y de gestión de configuración e inventario, cambios, versiones y despliegues (provisión). Como principales funciones deberá:
  - Asegurar la toma de decisión operativa directa entre el Consorci AOC y su organización.
  - Asegurar la coordinación con el CAU (de 1er nivel, del Consorci AOC; y también de 2º y 3º nivel, del adjudicatario) para todos los procesos.
  - Asegurar una buena relación y coordinación entre los equipos bajo su responsabilidad con el fin de cumplir las actividades asociadas a todos los procesos de gestión definidos, y con responsabilidad sobre el adjudicatario.

- Responsable de Calidad: Será responsable de:
  - Asegurar la existencia de un plan de calidad para los servicios y aplicaciones.
  - El aseguramiento de la calidad.
  - La verificación de la ejecución del control de la calidad.

- Responsable de Seguridad: Será responsable de:
  - Actuar como enlace entre el adjudicatario y los diferentes agentes implicados (Consorci AOC, CESICAT) cuando se traten temas de seguridad.
  - Garantizar, liderar e impulsar el cumplimiento del marco normativo de seguridad del Consorci AOC dentro de su organización, asegurando la correcta implantación de los niveles de seguridad y sus correspondientes medidas (técnicas, organizativas, y jurídicas); así como las directrices en materia de seguridad establecidas por el Consorci AOC.
  - Coordinar reuniones de seguimiento periódicas con el Consorci AOC y el CESICAT para informar del grado de adecuación de las aplicaciones al modelo de seguridad establecido, identificar los riesgos más relevantes y proponer planes de acción para su mitigación.
  - Que todo el personal del adjudicatario que prestará servicios en el Consorci AOC, pase por un plan de formación en materia de seguridad, focalizándose en el marco normativo del Consorci AOC y los procedimientos de seguridad que le sean de aplicación.
  - Asegurar la información regular al Consorci AOC según los plazos marcados, de todo lo relacionado con la seguridad (incidentes, medidas correctoras, riesgos, nuevos proyectos, iniciativas, etc...).
  - Hay que asegurar que todo el personal del proveedor que tenga que tratar datos o sistemas de tratamiento de datos de nivel sensible o superior firmen un Acuerdo de Confidencialidad Individual. El Consorci AOC podrá auditar este aspecto.
  - Coordinación operativa con los equipos operativos del Consorci AOC ante incidentes o posibles amenazas de ciberseguridad (Entrega de evidencias para la gestión e investigación de incidentes de seguridad, apoyo para la aplicación rápida de medidas de protección y contención ante amenazas o ciberincidentes, disponer de información vinculada a la aplicación (URLs, usuario de aplicación, logs, etc.))

- Responsable de Continuidad: Será el responsable de:
  - Garantizar y liderar dentro de su organización la correcta implantación de los planes de continuidad y disponibilidad (tanto de servicios tecnológicos como de negocio) acordados con el Consorci AOC.
  - Que todo el personal del adjudicatario que prestará servicios en el Consorci AOC, pase por un plan de formación en materia de continuidad, focalizándose en el marco normativo del Consorci AOC y los procedimientos de continuidad que le sean de aplicación.
  - El desarrollo de todas las medidas en este ámbito (técnicas, organizativas, y jurídicas) necesarias para alcanzar el nivel de cumplimiento exigido por el Consorci AOC.
  - Asegurar la información regular al Consorci AOC según los plazos marcados, de todo lo relacionado con la Continuidad y Disponibilidad (incidentes, medidas correctoras, riesgos, nuevos proyectos, iniciativas, etc...)

- Programador:
  - Liderar la fase de construcción de los cambios a realizar: entre otros, realizar las clases, interfaces y demás código necesario para el desarrollo de la aplicación atendiendo a los criterios fijados para cada desarrollo (calidad, robustez, eficiencia, etc.)
  - Ejecución exhaustiva del plan de pruebas definido por el proyecto.
  - Colaboración puntual, si así se cree conveniente, en las fases de toma de requerimientos, fase de análisis y diseño y fase de implantación.
  - Escribir, depurar y mantener el código fuente realizado, de manera que deberá comentar correctamente el código, para que éste sea mantenible. Los comentarios deben seguir las recomendaciones del estándar definido por java.
  - Generar la documentación (javadoc) a partir de los propios comentarios del código (se puede utilizar una herramienta del estilo JavaDoc Tool).
  - En los casos de incidencias complejas deberá participar activamente en el diagnóstico y ejecución del plan de acción a seguir por la resolución de la incidencia.

6.2.2 Estructura de responsabilidades del Consorci AOC

Por parte del Consorci AOC, los roles que participarán en la relación contractual:

- Responsable de Transición de la operación: Será el responsable de presentar la planificación, alcance y metodología de ejecución de los diferentes planes de transición del servicio. Impulsará. Asegurará la ejecución de estos según la dirección establecida por el Consorci AOC, de manera coordinada con los responsables del resto de proveedores del Consorci AOC. Informará del grado de avance, los riesgos y planes de mitigación correspondientes, y asegurará el acompañamiento por parte del proveedor en la gestión del cambio. El Responsable de Transición desarrollará, alineará, sincronizará y gobernará de forma global los planes de transición de la operación.

- Responsable de Seguridad del Consorci AOC.

- Jefe del Servicio de Certificación Digital

- Jefe de Proyecto del Área de Tecnología

- Responsable de Asesoramiento Jurídico de Servicios del Consorci AOC.

- Responsable del sistema del Consorci AOC
- Representante de la Dirección

6.2.3 Recursos tecnológicos provistos por el Consorci AOC

- Hardware y software:
  - HSM's jerarquía PRO y CONT y offline. Con modelo de seguridad a transferir.
  - Documentación jurídica
  - Código de las aplicaciones de las Entidades de Registro T-CAT e idCAT
  - Hardware de las ER : impresoras y lectores
  - Stock de tarjetas criptográficas.
  - Configuración de la PKI actual (EJBCA).
- Repositorios de información:
  - Carpetas de Sharepoint del Consorci AOC por documentación del servicio.
  - GIT por el código.
- Herramientas control ANS:
  - ANS disponibilidad: ISM
  - ANS evolutivos y peticiones del servicio : JIRA del Consorci AOC
  - ANS soporte: Zendesk del Consorci AOC

El Consorci AOC durante la vigencia del contrato se reserva el derecho de cambiar los recursos tecnológicos descritos en este punto.

6.2.4 Recursos tecnológicos que proveer por el adjudicatario

- Entornos para alojamiento de las claves y aplicaciones:
  - Entorno de Producción
  - Entorno de contingencia
  - Entorno de Preproducción
- Hardware, software y comunicaciones:
  - Necesario por prestación de los servicios objeto del contrato.
- Herramientas de control ANS:
  - ANS disponibilidad: Opensearch o equivalente
  - ANS indicadores de servicio : OpenSearch o equivalente.
  - ANS disponibilidad y capacidad : OpenSearch o equivalente.

6.3 Requisitos

6.3.1 Requisitos personales

Las tareas que desarrollar en este lote se han calculado a partir de la incorporación (en diferente porcentaje) de los perfiles siguientes:

- Responsable
- Técnico
- Programador

Para poder ofrecer todos los servicios objeto de este lote en un escenario de consumo máximo, es decir, de todos los servicios previstos en "Precio unitario y desarrollo y mantenimiento de aplicaciones informáticas" y también los de "tanto alzado", se han calculado los volúmenes de horas por año y categoría definidas en el punto B1 del pliego de cláusulas administrativas.

En todos los casos, se calcula sobre unas 1.700 horas/año persona (incluye, por tanto, se tienen en cuenta los días de baja y ausencias).

El personal adscrito al servicio, en conjunto, debe disponer de los conocimientos suficientes acreditados, tanto a nivel técnico práctico como de idiomas (dominio del catalán (nivel C), castellano y el inglés), que aseguren la correcta interpretación de procedimientos y normas de seguridad, lo que debe permitir una correcta aplicación de estos conocimientos.

El personal que el adjudicatario destine a este servicio deberá reunir todas las condiciones estipuladas por la normativa actualmente vigente.

El Consorci AOC puede rechazar y/o solicitar el cambio de interlocutor o responsables de proyecto. En este caso, el adjudicatario debe reemplazar al trabajador por otro suficientemente capacitado para llevar a cabo la tarea encomendada. Los costes derivados de esta incidencia irán a cargo del adjudicatario.

El Consorci AOC se reserva el derecho de no aceptar al personal que desarrolle su tarea sin una capacitación suficientemente o un comportamiento incorrecto.

Habrá que presentar una tabla de correlación entre los medios requeridos en el punto "6.2.1 adjudicatario y los presentados por parte del adjudicatario.

El adjudicatario debe hacerse cargo de todos los materiales y útiles para la correcta ejecución de los servicios encomendados, debidamente identificados como de su propiedad.

El Responsable de servicios propuesto por el adjudicatario deberá disponer de un número de teléfono que permita su localización en jornada laboral del calendario laboral de Barcelona, por parte del personal responsable del Consorci AOC.

Para poder conocer la calificación profesional, el licitador presentará el currículo profesional de los candidatos que propongan por estos perfiles. El licitador justificará documentalmente la calificación profesional del personal destinado con la presentación de la documentación compulsada que se detalla a continuación: tarjeta de identidad profesional y títulos profesionales.

En caso de baja de cualquiera de los miembros del equipo, el adjudicatario deberá sustituirlo en menos de 15 días laborables de acuerdo con los responsables del Consorci AOC. Cualquier cambio en uno de los miembros del equipo a instancias del adjudicatario deberá ser pactado con el Consorci AOC, que deberá validar tanto la baja como el currículo de la nueva persona a incorporar. Si el cambio es a instancias del adjudicatario, habrá que acordar el calendario de cambio con el Consorci AOC con el fin de minimizar el impacto en los desarrollos en curso. Quedan fuera de estos compromisos los periodos de vacaciones y permisos de todos los miembros del equipo.

El Consorci AOC realizará, en su caso, entrevistas a las personas del equipo de proyecto propuesto y, si es necesario, pedirá alternativas a las personas presentadas.

El Consorci AOC se reserva el derecho a solicitar el cambio de cualquiera de los miembros del equipo sin necesidad de justificación con una antelación de 20 días naturales a la fecha de sustitución.

El Consorci AOC se reserva el derecho a pedir una declaración personal de cada uno de los auditores para garantizar su formación y conocimientos.

El adjudicatario deberá presentar al Consorci AOC, la ficha personal de cada responsable, técnico y programador que proponga por las funciones definidas, donde constará:

- nombre y apellidos
- calificación educativa y categoría profesional
- experiencia y formación
- evaluación de la competencia: conocimientos de la tecnología y marco legal aplicable.
- seguimiento del desempeño
- fecha de la actualización más reciente de cada registro

6.3.2 Catálogo de certificados del Consorci AOC

El catálogo de certificados digitales que el Consorci AOC ofrece actualmente a los usuarios del Servicio de Certificación Digital (SCD), mediante los servicios que prestará el adjudicatario de este lote, es el que se puede consultar en el punto "1.1.1. Tipos y clases de certificados" de la Declaración de Prácticas de Certificación publicada en la web del servicio en epscd.aoc.cat.

Correspondencia a las categorías de Servicios eIDAS:

- TrustedList/SvcInfoExt/ForeSignatures : T-CAT personales e idCAT.
- TrustedList/SvcInfoExt/ForeSeals : Sellos electrónicos y Dispositivo aplicación.

Aparte de las categorías eIDAS también se realizan certificados de operador tanto idCAT como T-CAT.

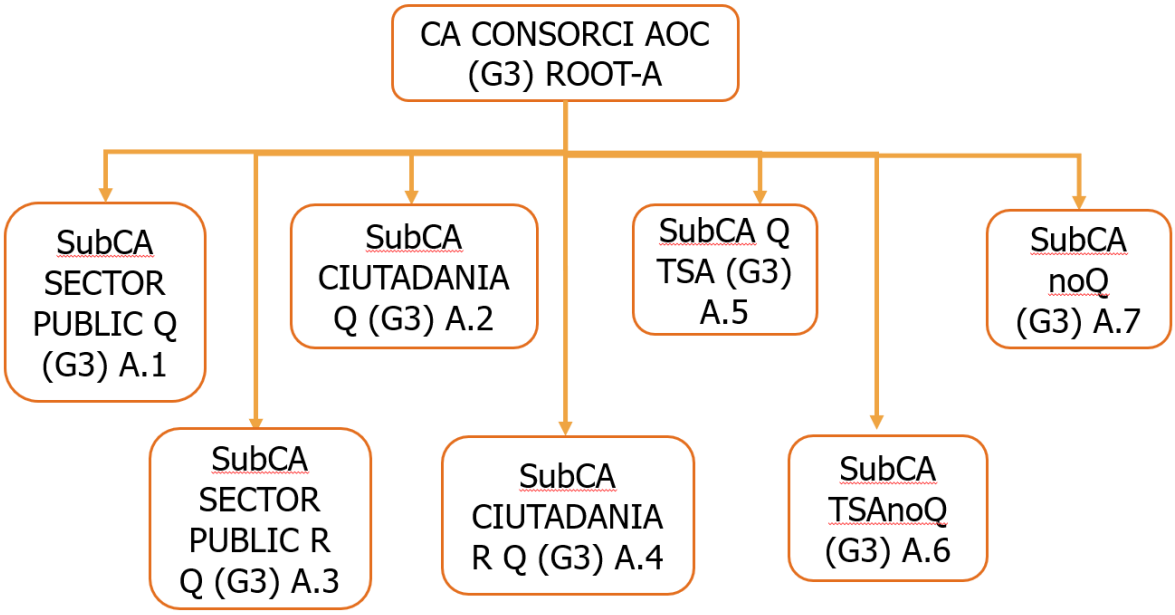
El histórico de volumetrías del servicio se puede consultar en el documento Anexo 6.

El Consocio AOC se reserva el derecho de modificar su catálogo de certificados cuando lo considere oportuno.

6.3.3 Explotación de la Jerarquía de los Servicios Públicos de Certificación de Cataluña

La siguiente figura muestra la estructura de la actual Jerarquía de los Servicios Públicos de Certificación de Cataluña en el ámbito de explotación de este contrato y que está formada por :

- Una Entidad de Certificación raíz (Root CA), que es la EC-ACC,
- La jerarquía de la primera generación estaba formada por cinco Entidades de Certificación de 2º nivel (la EC-GENCAT, el EC-AL, el EC-UR, el EC-Parlamento y el EC-IDCAT) y dos Entidades de Certificación de 3º nivel (la EC-SAFP y el EC-URV). Estas entidades están finalizadas.
- La jerarquía de la segunda generación formada por dos Entidades de Certificación de 2º nivel (el EC-SECTORPUBLIC y la EC-CIUDADANÍA) que concentran todas las emisiones de los tipos de certificados que forman parte del catálogo de certificados ofrecido por el Consorci AOC.
- La jerarquía de tercera generación se emitió en 2022 y está formada por siete entidades de certificación subordinadas y una Entidad de Certificación raíz. En el ámbito de este contrato están la nueva raíz y las subCAs A1, A2, A5, A6 y A7.



6.3.3.1 Infraestructura de Hosting y Hardware / Continuidad de servicios de jerarquía y claves

La infraestructura de la actual jerarquía de Entidades de Certificación (en adelante, ECs) está desplegada en los siguientes entornos:

Producción:

- EC raíz (Offline, desconectada de internet): en un "CPD" (del adjudicatario actual, situado en la provincia de Barcelona).
- ECs subordinadas: en alta disponibilidad, en un "CPD" (del adjudicatario actual, situado en la provincia de Barcelona).

De contingencia:

- ECs raíz y subordinadas: en el CPD primario del Consorci AOC, en la provincia de Barcelona, y operado por el adjudicatario actual.

De Preproducción (e Integración):

- EC raíz y subordinadas de preproducción: en un CPD titularidad del adjudicatario actual.

Los dispositivos actuales que dan servicio cumplen el marco normativo aplicable y están certificados como FIPS 140-2 nivel 3 o EAL4+. Estos equipos se han mantenido en todo momento y, en algunos casos mientras los contratos de apoyo del fabricante lo han permitido, bajo garantía del fabricante. El detalle exacto de los dispositivos se puede consultar en el ANEXO 11 sobre el inventario de activos (hardware y licencias contratadas).

Los actuales custodios de las tarjetas que permiten la operación de los dispositivos criptográficos asociados a estas EC's son personal directivo o con roles de Seguridad asignados en el Servicio de Certificación del Consorci AOC y también personal del adjudicatario actual.

6.3.3.2 Aplicación PKI actual de la de la Jerarquía de los Servicios Públicos de Certificación de Cataluña

La aplicación que soporta a la Infraestructura de clave pública (PKI) de la actual Jerarquía de los Servicios Públicos de Certificación de Cataluña ofrece las funcionalidades y el rendimiento que se exponen a continuación:

6.3.3.2.1 Emisión de Listas de Revocación de Certificados (CRL's)

Cada Entidad de Certificación (en adelante EC), genera sus listas de revocación (en adelante, CRL's, el acrónimo en inglés de Lista de Revocación de Certificados) en las condiciones – de periodicidad, vigencia, etc. – que se establecen en su Declaración de Prácticas de Certificación, publicada en: http://epscd.aoc.cat/regulacio y siempre de acuerdo con la normativa aplicable.

6.3.3.2.2 Servicio de Consulta de Estado de Certificados en Línea (OCSP)

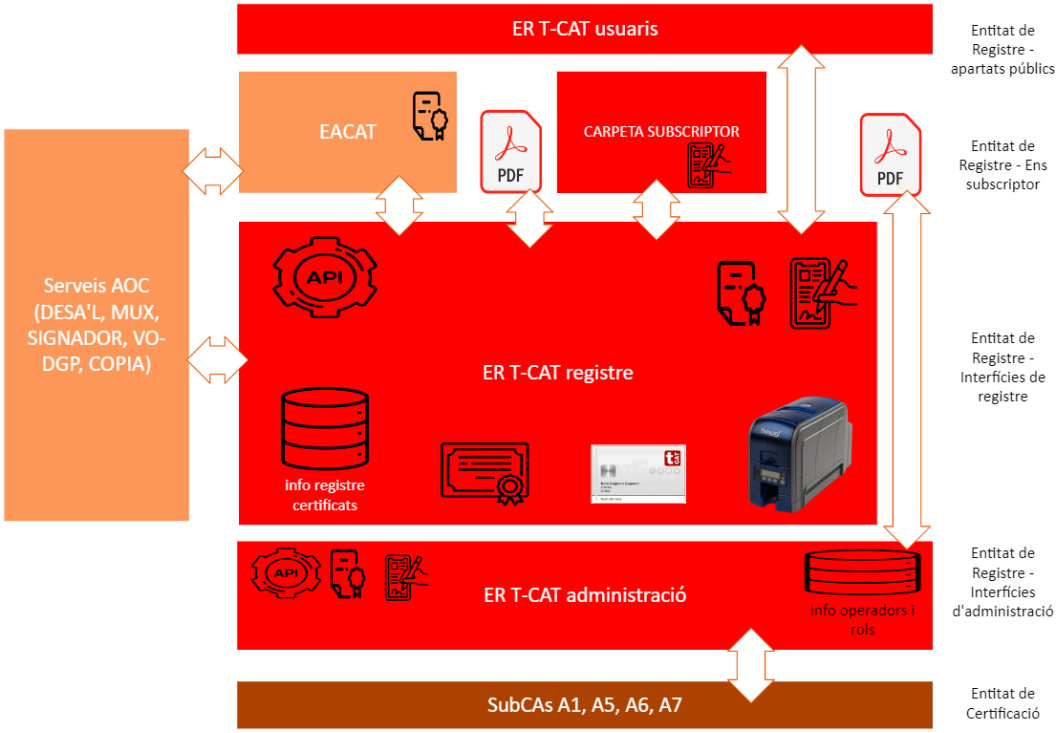
La infraestructura PKI deberá proveer servicios de validación a través del protocolo de Consulta de Estado de Certificados en Línea (en adelante, OCSP, el acrónimo en inglés de Consulta de Estado de Certificados en Línea).

Para cada EC configurada en el servicio OCSP, se dispone de una clave con usos de firma de respuestas OCSP emitida por esta EC. Así, permitiendo que un único servicio pueda dar respuestas sobre certificados emitidos por todas las EC's de la jerarquía, firmadas con una clave de la misma EC que emitió el certificado que se quiere validar (tal como hace actualmente el servicio publicado en: http://ocsp.catcert.cat), el servicio es interoperable con la validación de los certificados SSL que hacen los navegadores.

Para cada EC configurada en el servicio OCSP, el servicio OCSP no podrá responder el estado desconocido (UNKNOWN) por certificados que no ha emitido, de acuerdo con la normativa vigente aplicable.

6.3.4 El Servicio de Certificación Digital del sector público catalán (T-CAT)

El Servicio de Certificación Digital para trabajador público (en adelante, T-CAT) es el servicio que se ofrece para la emisión de certificados del sector público catalán. Los certificados T-CAT son los que se emiten desde las Entidad de Certificación de Sector Publico. Como perfiles de certificado se incluyen los certificados de firma electrónica y de sello electrónico.



6.3.4.1 Modelo de Registro

Todo el proceso de solicitud, emisión y entrega de los certificados T-CAT actual se realiza por medios digitales y almacenando evidencias documentales electrónicas y seguras en cada paso. Para llevar a cabo esto, hay tres componentes lógicos principales con responsabilidades funcionales concretas asignadas. Se describen a continuación en el mismo orden que se utilizan en el caso de una solicitud, emisión y entrega de un certificado T-CAT.

1) Módulo ASCD de EACAT : canal de entrada de las solicitudes de certificados T-CAT y de la documentación para la gestión de los roles de todo el sistema de registro. Este módulo está integrado dentro del Servicio EACAT ofrecido por el Consorci AOC. Por lo tanto, se utiliza por todos los ente adscritos a EACAT y susceptibles de solicitar un certificado digital T-CAT. Existe un vídeo demostrativo del proceso disponible aquí. Las responsabilidades del componente son:

   a. Generar y archivar la documentación electrónica de solicitud de certificados digitales (envío de certificados) con la firma de las personas autorizadas a realizar este trámite en el ente solicitante.

   b. Canalizar y archivar la documentación electrónica de gestión de los roles del sistema de Registro de la SCD T-CAT.

   c. Asignación de un número de referencia único para el seguimiento del trámite. Actualmente es un número de registro asignado por el servicio de registro unificado (MUX) del Consorci AOC.

   d. Notificación de los cambios de estado de la tramitación. En particular de la aceptación y de la finalización del envío de certificados.

e. Archivo de la documentación y las comunicaciones generadas por el trámite en un Sistema de Gestión Documental (SGD). Actualmente el gestor SGD utilizado es el que dispone el Consorci AOC con el servicio propio DESA'L.

f. Control de acceso a los trámites de la ASCD a través del sistema de autenticación y autorización T-CAT con los siguientes roles: editor de solicitudes, solicitante de certificados personales, solicitante de certificados de dispositivo y certificador de datos.

2) Web operadores de registro: módulos web y conectores de la entidad de registro. Es utilizado por una octogenaria de entidades que hacen el rol de Entidad de Registro de la SCD T-CAT.

a. Módulo peticionario: módulo de carga de peticiones al sistema de registro. Dispone de un canal de entrada web y de un canal de entrada automático vía conector REST que es el que utiliza el módulo ASCD de EACAT.

b. Módulo aprobador: módulo web para la aprobación de las solicitudes.

c. Módulo generador: módulo basado en un software instalado en un ordenador cliente para la generación de los certificados. Si el soporte del certificado T-CAT es una tarjeta criptográfica, este módulo interacciona con una impresora de tarjetas. En caso de que sea de soporte software, este módulo no interviene porque aquella petición de certificado pasa directamente a estar lista para entrega a través de la carpeta del suscriptor (descrito a continuación).

d. Módulo gestor de certificados: módulo para la gestión del estado del certificado (suspensión, habilitación y revocación). También dispone de un canal de entrada web y de un canal de entrada automático vía un conector REST.

3) Carpeta del suscriptor : módulo para la gestión digital segura del proceso de entrega de los certificados T-CAT por parte del ente solicitante de los certificados. Su uso también es por parte de todos los ente susceptibles de solicitar un certificado digital T-CAT (unos 2.500).

a. Este módulo custodia los originales digitales no firmados del contrato de aceptación de las condiciones del servicio de certificación que firma el suscriptor del certificado T-CAT

b. Custodia de los códigos de activación (PIN y PUK en caso de tarjeta; contraseña en caso de certificados en formato p12) originales de los certificados T-CAT.

c. La persona designada dentro del ente solicitante que hace uso de este módulo se denomina Responsable del Servicio y es un rol dentro del sistema de certificación T-CAT.

d. El Responsable del Servicio es el encargado de hacer firmar los contratos de aceptación de las condiciones de uso de los certificados T-CAT, entregar los certificados (según el procedimiento definido para cada tipo de certificado T-CAT) y custodiar la documentación firmada en el archivo en papel de su Ente.

e. El responsable también deja evidencia en el sistema de la firma en papel y, con este acto, genera el envío de los códigos de activación al suscriptor.

f. Finalmente, la carpeta del suscriptor también permite al suscriptor titular de un certificado T-CAT, la recuperación de los códigos de activación originales a través de una interfaz web.

En los próximos puntos se describen más en detalle cada uno de los componentes y módulos mencionados.

6.3.4.2 Roles del sistema T-CAT

Los Roles implicados en la emisión y gestión de certificados T-CAT dividen en dos por residir en dos niveles de registro diferente dentro del proceso de emisión. Son los "Roles en el portal de operadores de registro y la Carpeta del Suscriptor" y los "Roles web Operadores / Entidad de registro T-CAT". Los primeros se recogen en los documentos "FICHA ENS Suscriptor" y los segundos en el "FICHA ER T-CAT" que se encuentran en la web del Consorci AOC en "https://www.aoc.cat/serveis-aoc/catcert-t-cat-administracions/".

6.3.4.2.1 Roles en el portal de operadores de registro y la Carpeta del Suscriptor

Están definidos en la web del Consorci AOC en "https://www.aoc.cat/knowledge-base/quins-tipus-de-rols-hi-ha-a-la-part-del-servei-de-certificacio-digital-a-leacat/".

6.3.4.2.1.1 Responsable del servicio de certificación digital

Los responsables del servicio de certificación digital son las personas con un rol de gestión, y no un perfil de elevado grado de responsabilidad; estos actúan como enlace entre el ente y su Entidad de Registro T-CAT. Entre sus funciones, se responsabilizan de entregar los certificados digitales a los titulares, de hacerles firmar la documentación legal, de archivarla convenientemente y también de informarles de sus obligaciones y responsabilidades. Es necesario que haya un mínimo de dos personas con el rol responsable del servicio de certificación digital, pero puede haber todos los que se deseen con el fin de garantizar la continuidad del servicio.

6.3.4.2.1.2 Certificador de datos

Los certificadores de datos son las personas que se responsabilizan de justificar la veracidad de los datos de los certificados. Recomendamos que este rol sea el perfil del ente con capacidad para dar fe de los datos personales que debe contener el certificado digital. Por ejemplo: el/la secretario/a de un ayuntamiento, el/la jefe/ a de recursos humanos o cargos similares. Es necesario que haya un mínimo de dos personas con el rol de certificador, pero puede haber todos los que se deseen para garantizar la continuidad del servicio.

6.3.4.2.1.3 Solicitante de certificados personales o de entidad

Persona con autoridad dentro del ente para solicitar la emisión, renovación, habilitación y revocación de certificados personales o de entidad (p.e. el alcalde, un teniente de alcalde o

un concejal en el ayuntamiento o el director de servicios de un departamento de la Generalitat). Es necesario que haya un mínimo de dos personas con el rol de solicitante de certificados personales, pero puede haber todos los que se deseen para garantizar la continuidad del servicio.

6.3.4.2.1.4 Solicitante de certificados de dispositivo y aplicación

Persona con autoridad dentro del ente para solicitar la emisión, renovación, habilitación y revocación de certificados de dispositivo y aplicación (p.ej. el/la jefe/ a de informática). Es necesario que haya un mínimo de dos personas con el rol de solicitante de certificados de dispositivo, pero puede haber todos los que se deseen para garantizar la continuidad del servicio.

6.3.4.2.1.5 Editor de solicitudes en EACAT

Los editores de solicitudes son las personas que pueden cumplimentar, aunque no firmar, solicitudes de emisión, renovación, habilitación y revocación de certificados digitales a través de EACAT, de forma que queden preparadas para la firma de un usuario con el rol de solicitante de certificados. Recomendamos que los editores de solicitudes sean de perfil administrativo y que haya un mínimo de dos personas con este rol, aunque puede haber todos los que se deseen para garantizar la continuidad del servicio:

6.3.4.2.2 Roles web Operadores / Entidad de registro T-CAT

Hay establecidos cuatro roles de operador (peticionario, aprobador, generador y gestor de certificados), uno de coordinador del servicio (responsable del servicio) y tres figuras asociadas (responsable de seguridad física, responsable de seguridad lógica y archivero). A continuación se explica la función que realiza cada uno de los roles:

6.3.4.2.2.1 Peticionario

Persona encargada de introducir los datos de las solicitudes de los certificados en la aplicación de petición de certificados. Hay que tener en cuenta que cuando una petición entra por la EACAT este rol desaparece y queda para casos de extraordinarios (nuevos ente o ente no dados de alta en EACAT o en caso de problemas técnicos que impidan hacer uso de la plataforma.)

6.3.4.2.2.2 Aprobador

Persona encargada de revisar los datos de las solicitudes introducidas por el peticionario y aprobar (validar) o denegar (devolver al peticionario) la petición en consecuencia. En el caso de peticiones introducidas por EACAT, no se tratará de una tarea de revisión del trabajo del peticionario, que no existe, pero si será necesario comprobar que no hay errores evidentes, pruebas de los entes que solicitan certificados, etc.

6.3.4.2.2.3 Generador

Persona encargada de generar los certificados una vez aprobadas las peticiones.

6.3.4.2.2.4 Gestor de certificados

Persona encargada de habilitar y revocar los certificados digitales durante su ciclo de vida (la suspensión sólo es telefónica). Hay que tener en cuenta que cuando una petición entra por EACAT, este rol desaparece y queda para casos de emergencia (en los que no sea posible usar EACAT).

6.3.4.2.2.5 Depositario AOC

Operador con permisos para efectuar la entrega y la descarga de certificados cedidos por los entes al Consorci AOC.

6.3.4.2.2.6 Responsable del servicio

El responsable del servicio se encarga de la coordinación y buen funcionamiento de la Entidad de Registro, en caso de que lleguen solicitudes en papel o PDF firmado, recibe la documentación, valida la identidad y la autoridad del solicitante, verifica la documentación, notifica al suscriptor el inicio de la tramitación, abre los expedientes, archiva la documentación y notifica al peticionario el inicio del proceso. Además, actúa como enlace entre la organización y el Consorci AOC.

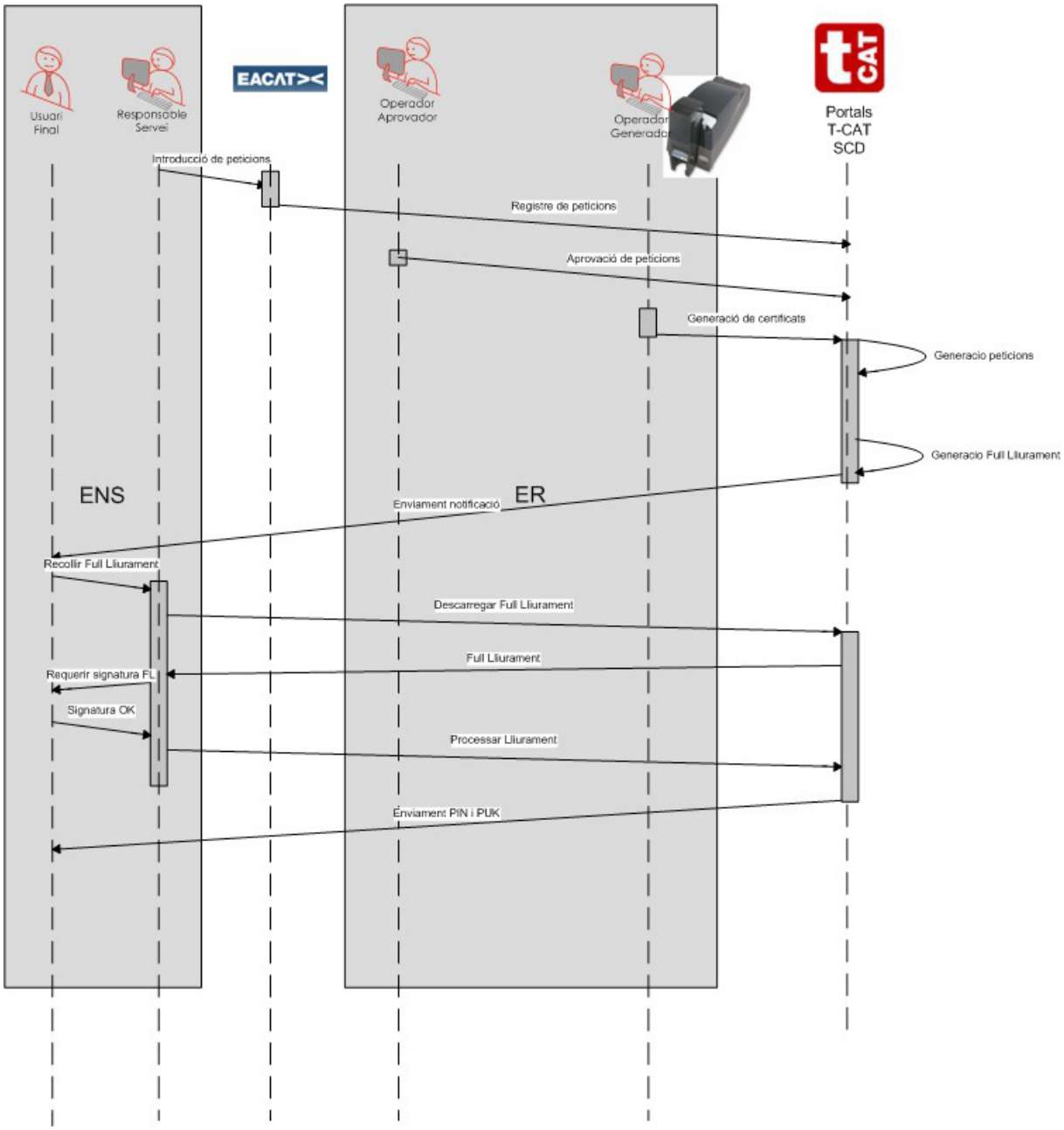
6.3.4.3 El Servicio de emisión de certificados T-CAT

Los procedimientos operativos de las ER's de T-CAT se encuentran en el apartado ¿Quién Sueldo? Del Servicio El Consorci AOC de la web del Consorci AOC.

Mediante los siguientes diagramas de relaciones, se ilustran los procesos de emisión de certificados digitales en sus diferentes formatos (T-CAT y T-CATP). Los esquemas muestran los roles que intervienen y su localización física a lo largo del proceso.

6.3.4.3.1 Procedimiento de emisión T-CAT

El siguiente diagrama de flujo representa el procedimiento de emisión estándar de una tarjeta T-CAT a través de EACAT, solicitada por un ENS, emitida por su ER correspondiente y con el PIN enviado por correo electrónico:

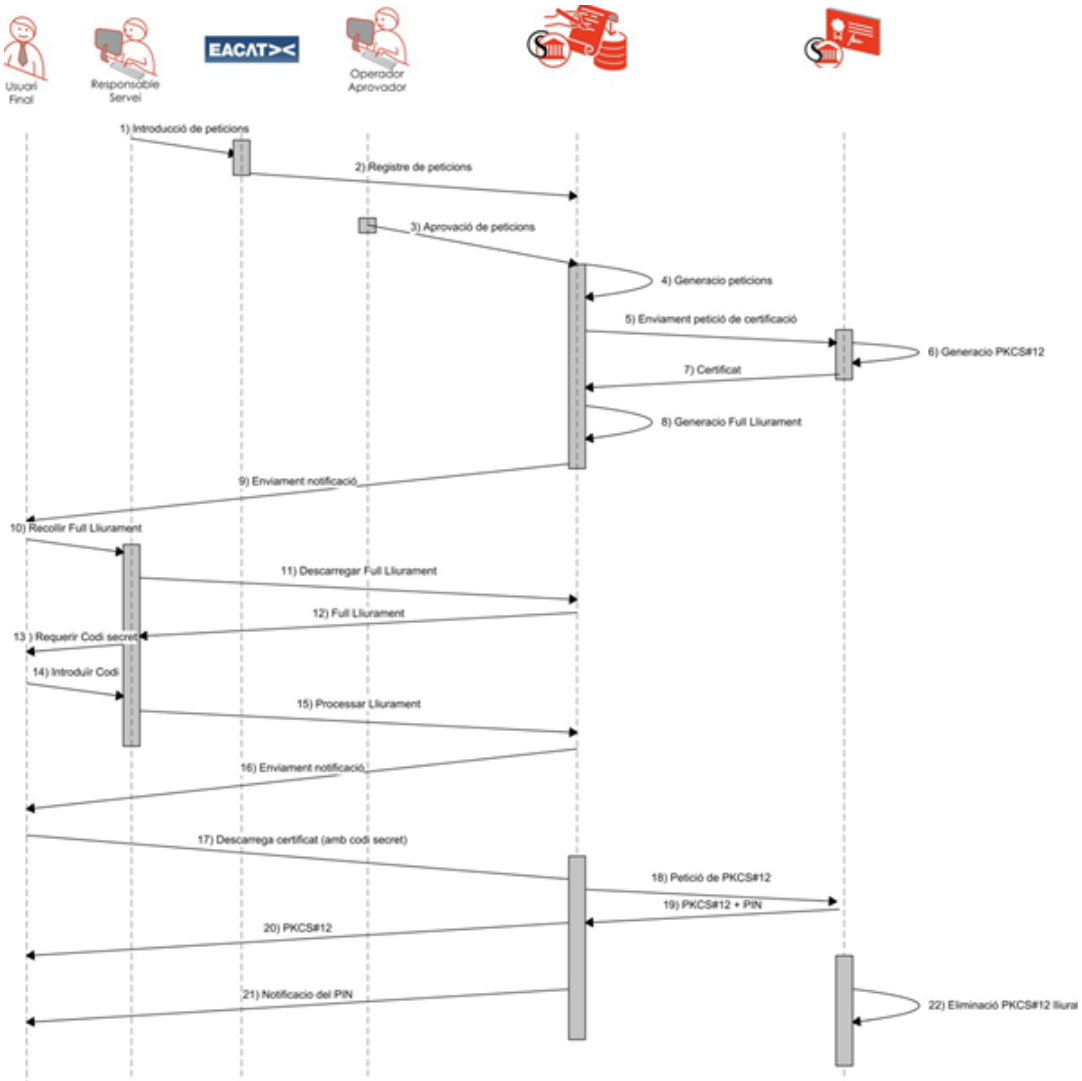


El diagrama de flujo puede introducir las variantes/excepciones:

- Los certificados de dispositivo servidor o aplicación se generan automáticamente por el software sin la intervención del Módulo Generador
- Existen variantes de emisión masiva que utilizan conectores automáticos para carga masiva de datos, consulta de estados y emisión masiva desatendida, entre otras funcionalidades.
- Algunas entidades grandes son ER a la vez y se hacen sus tarjetas. Se puede dar el caso de que no carguen las peticiones al sistema vía EACAT, sino a través de los conectores directamente.
- Más información de módulos y funcionalidades personalizadas en el Anexo 9.

6.3.4.3.2 Procedimiento de emisión T-CAT-P (Software)

El siguiente diagrama de flujo representa el procedimiento de emisión estándar de un certificado T-CAT-P en software con la solicitud a través de EACAT.



6.3.4.3.3 Diseños y personalización de tarjetas

El sistema de Certificación digital T-CAT soporta actualmente estas categorías de diseños de plásticos de tarjetas.

6.3.4.3.3.1 Estándar T-CAT

Diseño de tarjeta estándar aprobado por el Consorci AOC. Soporta banda magnética e impresión de texto sin foto, sólo por la parte de delante.

6.3.4.3.3.2 Personalizado por Ente

Diseño de tarjeta personalizado para cada ente de acuerdo con sus requisitos estéticos. El formato lo acuerda cada ente con el fabricante de tarjetas y personaliza con foto. El Consorci AOC, en este caso, sólo genera el certificado al chip criptográfico.

La relación de qué nos tienen tarjeta personalizada se recoge en el anexo "Annex_9_Resum_caracteristiques_ERs_TCAT".

6.3.4.3.4 Solución tecnológica para el Servicio de emisión de tarjetas

El servicio de emisión de certificados y personalización completa de la tarjeta, en un solo paso, es posible gracias a una aplicación hecha a medida por este servicio. Esta aplicación graba el certificado y personaliza la tarjeta con los datos que se han cargado en el sistema de Registro. Es decir, siguen el mismo camino de carga en el sistema y validación que los datos que se incorporarán a los certificados digitales. De esta manera se consigue hacer de la emisión y personalización de la tarjeta un proceso atómico y en un solo paso.

Para gestionar la impresión y los procesos asociados a través de la impresora criptográfica, es necesario instalar en las estaciones de registro que operan el módulo generador, un software de cliente desarrollado a medida y que requiere una instalación específica y la homologación previa de todos los componentes que componen el equipo. Por esta razón, los ordenadores cliente que utilizan la aplicación para las ER's del SCD del Consorci AOC para el módulo generador son equipos dedicados y homologados con el fin de garantizar que la aplicación de emisión funcionará correctamente. Actualmente el software de emisión es compatible con las últimas versiones de Windows.

En cuanto a las impresoras criptográficas, también se ha homologado cada modelo de impresora soportado con el software de emisión y personalización. Además, también se ha validado la compatibilidad con cada versión de sistema operativo y resto de software. Actualmente, la aplicación es compatible con las impresoras que se especifican en el documento de inventario y en el documento de funcionalidades de las EERR adjuntos.

6.3.4.3.5 Modelo de provisión y mantenimiento del hardware de emisión de la SCD T-CAT

Tal y como se ha mencionado en los puntos anteriores, la complejidad inherente al hecho de mantener una aplicación de generación con capacidad de generación y alta personalización de la tarjeta ha motivado la homologación de unos equipos y componentes de software concretos con el fin de mantener el correcto logro del objetivo funcional. Del mismo modo, en su inicio se proveyeron los equipos para los diferentes entes que se establecían como ER. De esta manera y, en general, se ha provisto un equipo PC, una impresora láser para la impresión de documentación, en su caso, y una impresora criptográfica para su uso en la emisión de certificados de la SCD T-CAT.

Estos equipos se han mantenido en todo momento y, en algunos casos mientras los contratos de apoyo del fabricante lo han permitido, bajo garantía del fabricante.

Adicionalmente, también se ofrece un servicio de mantenimiento del hardware y software de las ER's: actualmente el Consorci AOC apoya (incluso in situ, cuando es necesario) al personal técnico de los entes que operan las ER's. En caso de que el hardware de la ER haya sido provisto por el Consorci AOC, también se ofrecen servicios de mantenimiento de este (reparación, reposición, etc.) en condiciones que garantizan el acuerdo de nivel de servicio por el servicio ordinario de emisión y renovación de certificados comprometido con los usuarios.

6.3.4.3.6 Modelos de provisión de los soportes criptográficos

Hay dos grandes modelos de provisión de los soportes criptográficos en la SCD T-CAT actual. Son éstos:

6.3.4.3.6.1 T-CAT estándar

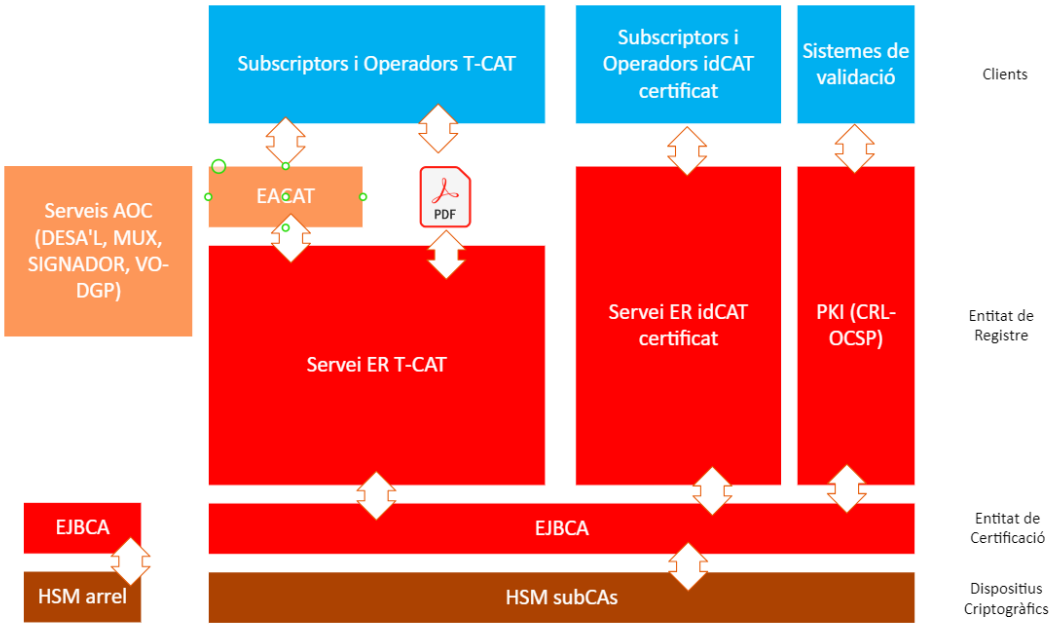
Adquirida por el Consorci AOC directamente al fabricante de acuerdo con los requisitos del Consorci AOC. Esta tarjeta es la que utilizan la mayoría de ERs colaboradoras de los Consejos Comarcales que dan servicio a las ERs vinculadas asignadas a su ámbito y también por la ER del Consorci AOC. En el caso de las ERs colaboradoras que utilizan este modelo de tarjeta, es el Consorci AOC quien les envía periódicamente un stock de tarjetas para su uso.

6.3.4.3.6.2 Tarjeta personalizada

Adquirida por cada ER colaboradora directamente al fabricante y de acuerdo con sus especificaciones negociadas con el fabricante. Adopta un chip homologado por el Consorci AOC y una personalización de foto, en su caso.

6.3.4.4 Descripción de componentes e interfaces de software del Servicio de Certificación Digital (T-CAT e idCAT)

El siguiente esquema muestra la estructura de sistemas que utiliza el Consorci AOC para gestionar los servicios de certificación digital:



- En azul oscuro se muestran clientes agrupados por operadores del sistema de portales o como clientes y/o suscriptores.
- En rojo se muestran los componentes de la SCD, ya sean productos comerciales o desarrollados a medida :
    - Servicio ER-T-CAT: portal, conectores y software de la Entidad de Registro de Certificados T- CAT para trabajadores públicos y de las Entidades de Certificación del Consorci AOC
    - Servicio ER idCAT: portal y conectores de idCAT
    - PKI-EPSCD : servicios de OCSP, CRL e información pública (DPC, claves públicas, etc..)
- En marrón: la capa criptográfica (HSMs) de la EC raíz y subCA
- En naranja, integraciones con servicios del Consorci AOC:
    - EACAT (Extranet de las Administraciones Públicas Catalanas) : canal de entrada único de la tramitación interadministrativa, incluida la de los certificados digitales. Incluye tramitación en PDF de solicitudes de certificados y operadores del sistema.
    - Servicios AOC: registro de entrada/salida (MUX), repositorio documental (DESA'L), aplicaciones de firma (SIGNADOR), servicio de digitalización (COPIA), acceso a datos de la DGP (VO-DGP), etc..

6.3.4.5 La Entidad de Registro T-CAT del Consorci AOC

El Consorci AOC opera una Entidad de Registro (en adelante ER) que es la que centraliza las peticiones de certificados digitales en tarjeta criptográfica de todos los entes que no están vinculados a una ER Colaboradora. Desde el ER del Consorci AOC también se generan algunos certificados con requisitos de validaciones más elevados, como son los perfiles de representante.

Cuando el volumen de solicitudes recibidas supera las 100 tarjetas, el sistema las permite derivar al fabricante de las tarjetas para que haga la producción masiva del lote y gestione los correspondientes envíos postales a los entes suscriptores. La producción en la fábrica permite las mismas personalizaciones y servicios avanzados que se incorporan desde las estaciones de generación de las ER Colaboradoras.

El procesado del fichero de lote se realiza a través de una personalización del software del módulo Generador que opera únicamente desde el ER del Consorci AOC. Consta de un proceso de intercambio de datos de forma segura y, entre otros datos, se intercambian las claves públicas a certificar, los certificados una vez emitidos, los PINs y PUKs de las tarjetas para almacenarlos en la carpeta del suscriptor, etc.. Todo el proceso de registro por lotes informa los mismos datos al sistema que una emisión normal y, de esta manera, se consigue que las tarjetas emitidas por lotes o desde las estaciones de generación, tengan la misma funcionalidad y operativa en la fase de la entrega (carpeta del suscriptor).

6.3.4.6 Gestión documental del Servicio de Certificación T-CAT

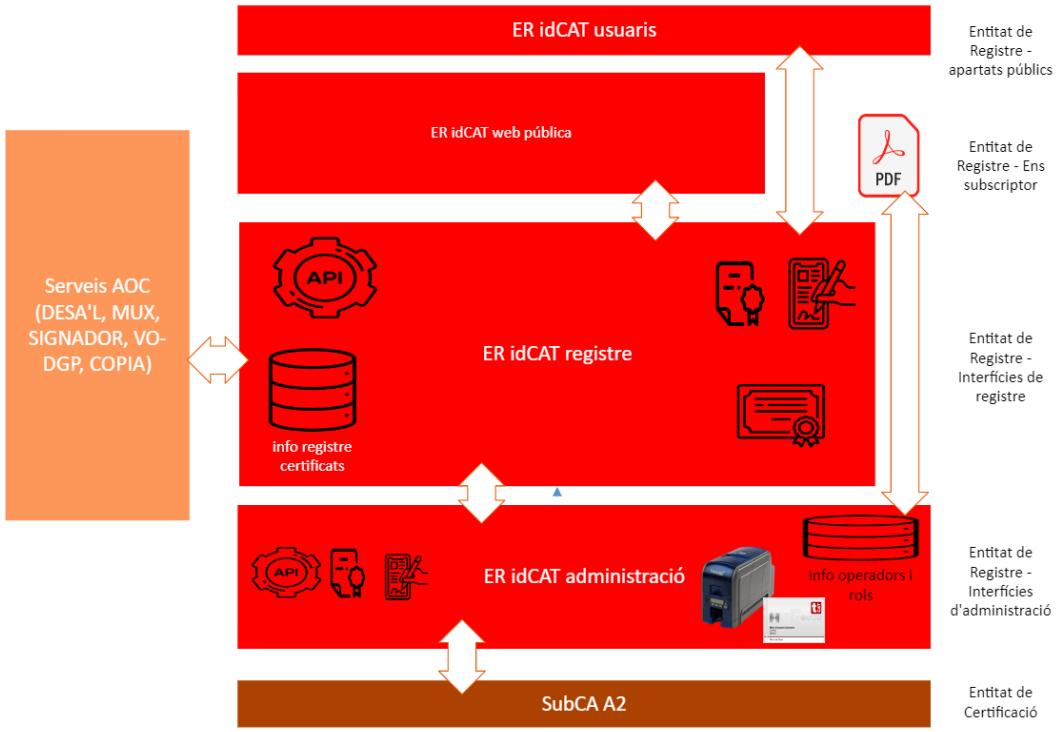
El software de la ASCD de EACAT, que gestiona el trámite de solicitud de certificados T-CAT y las fichas de suscriptores, se integra con el gestor documental del Consorci AOC (llamado DESA'L) para la gestión de la documentación derivada del trámite.

El módulo ASCD de EACAT se utiliza también para generar las comunicaciones de finalización o rechazo de la tramitación solicitada, con el fin de informar a los solicitantes del trámite de su estado. Cabe recordar que se asigna un número de registro de entrada desde el módulo ASCD de EACAT y este es el número que se utiliza para hacer el seguimiento del expediente.

La documentación de la fase de entrega, es decir, el contrato de aceptación de las condiciones de aceptación de la emisión de los certificados digitales se hace en el archivo de cada ER vinculada. Cada Responsable del Servicio de cada ER vinculada es responsable de descargar el contrato y hacerlo firmar al suscriptor del certificado, en el caso de los personales, o firmarlo él mismo en el caso de los certificados de dispositivo. En ambos casos, esta documentación en papel es custodiada por el archivero de la ER vinculada durante el periodo legalmente exigido.

6.3.5 El Servicio de Certificación Digital para la ciudadanía (idCAT certificado)

Por su parte, los operadores de las ERs idCAT trabajan empleando un único aplicativo que es el Web idCAT (www.idcat.cat). El equipo del operador del ER, aparte de la de disponer de un lector para sus tarjetas con el certificado de operador, debe disponer de la instalación de la aplicación de firma por emisión y revocación. La web idCAT consta de tres grandes módulos funcionales:



6.3.5.1 La web del ciudadano

Desde donde se puede hacer la solicitud, búsqueda de entidades de registro para hacer la validación presencial, la descarga, la revocación y la renovación del certificado digital de ciudadano. La descarga del certificado se realiza en formato pkcs#12.

6.3.5.2 La Web de los Operadores

Desde donde se hace el flujo de emisión, con la correspondiente generación de documentación del contrato a firmar por el ciudadano; se controlan los permisos de los operadores del servicio idCAT; y se hace la gestión del ciclo de vida del certificado para su suspensión, habilitación o revocación. El flujo de emisión consta de las fases de registro de los datos del ciudadano que solicita el certificado por parte de un operador identificado, la validación de estos datos con la base de datos de la Policía (a través del servicio de Vía Abierta del Consorci AOC, modalidad DGP) para que se pueda emitir el certificado y la generación de la documentación.

Finalmente, la documentación contractual en papel generada y firmada por los ciudadanos suscriptores del servicio es custodiada por el archivero de la ER idCAT durante el periodo legalmente aplicable.

6.3.6 La Web de los Operadores de Certificación o de administración

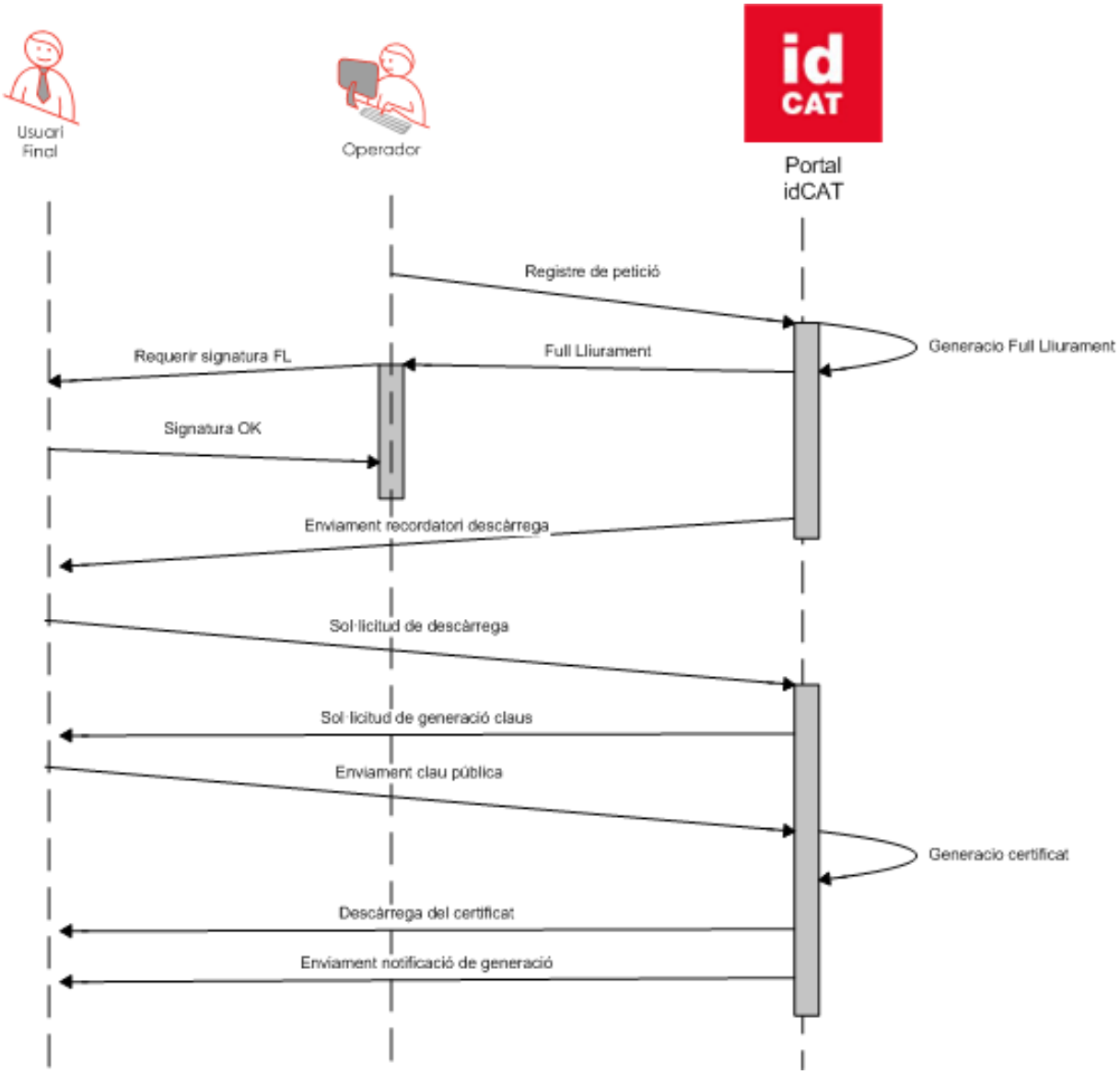
Desde donde se controlan los permisos de los operadores del servicio idCAT y se generan los certificados en tarjeta para operadores del sistema.

Dimensiones ER idCAT:

- Número de ERs: 393
- Número de operadores de las ERs idCAT: 4.125

6.3.6.1 Procedimiento de solicitud y emisión idCAT certificado

La siguiente figura representa el flujo de solicitud de emisión y descarga en modo prevalidación. El usuario no carga los datos desde casa y lo hace el operador en el ER.



El flujo puede introducir la variante del modelo de "solicitud" previa. Es decir con carga de datos previa a la aplicación por parte del ciudadano y el operador recupera la solicitud para validarla.

6.3.6.2 Gestión documental del Servicio de Certificación idCAT

La documentación de la fase de entrega, es decir, el contrato de aceptación de las condiciones de aceptación de la emisión de los certificados digitales se hace en el archivo de cada ER vinculada. Cada Responsable del Servicio de cada ER vinculada es responsable de descargar el contrato y hacerlo firmar al suscriptor del certificado. En ambos casos, esta documentación en papel es custodiada por el archivero de la ER vinculada durante el periodo legalmente exigido.

6.4 Condiciones

6.4.1 Condiciones generales y específicas de Prestación de los servicios objeto del contrato por parte del Consorci AOC

El adjudicatario deberá ofrecer los servicios objeto del contrato de acuerdo con las condiciones generales y específicas definidas por el Consorci AOC en esta documentación:

https://www.aoc.cat/condicions-prestacio-serveis-aoc/

Condiciones generales Consorci AOC:

https://www.aoc.cat/wp-content/uploads/2023/06/CON_GENERALS-PRESTACIO-SERVEIS_29062023.pdf

Condiciones específicas ER T-CAT:

https://www.aoc.cat/wp-content/uploads/2021/10/CON_especifiques-ER-TCAT_01102021.pdf

Condiciones específicas ER idCAT:

https://www.aoc.cat/wp-content/uploads/2024/01/CON_Condicions-especifiques-ER-idCAT_24012024.pdf

Los ANS descritos en las condiciones anteriores se especifican en el punto 6.5 más adelante.

A continuación se exponen los detalles en relación con las Fases de la ejecución del contrato, el servicio de explotación que incluye, alojamiento, explotación de aplicación y servicios adicionales; y evolutivos.

6.4.2 Fases de la ejecución del contrato

Se prevé, pues, que la planificación aproximada para la prestación de los servicios objeto de este contrato sea, en el escenario mejor:

<table>
<tr><td colspan="4">2025</td><td rowspan="2">2026</td><td rowspan="2">2027</td><td rowspan="2">2028</td><td rowspan="2">2029</td></tr>
<tr><td>T1</td><td>T2</td><td>T3</td><td>T4</td></tr>
<tr><td>Fase de transició de l'operació del Servei</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="7">Fase de prestació del Servei</td></tr>
<tr><td></td><td></td><td></td><td></td><td colspan="4">Fase d'Adeqüació del Servei</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Fase de devolució del Servei</td></tr>
</table>

1) Transición de la operación del servicio: desde la adjudicación del contrato y, como máximo, hasta la finalización del 1er trimestre de 2025. Esta fase se describe en detalle en el punto "6.8 - actual del presente documento.

2) Prestación del servicio de certificación: desde principios del mes de abril de 2025 y hasta la finalización del contrato. Como puntos clave para tener en cuenta en este período, hay que mencionar:

   a) La auditoría bienal EIDAS vigente a la celebración de este contrato tuvo lugar en fecha 28 de marzo de 2013. Por tanto, la primera auditoría EIDAS completa en el ámbito temporal de este contrato debe tener lugar en fecha 28 de marzo de 2025.
   b) Sin perjuicio de lo mencionado en el punto anterior, Mozilla requiere el envío de auditorías anuales de revisión de los servicios. En este contexto, el Consorci AOC deberá pasar una auditoría que cubra el periodo entre el 28 de marzo de 2024 y 28 de marzo de 2025. En su caso, esta auditoría deberá obtenerse en paralelo a la de preparación para el inicio de emisiones del traspaso del servicio que se describe en el punto "6.8 - Transición de la operación del servicio actual"

3) Adecuación del servicio: desde el 1 de enero de 2026 hasta la finalización del contrato, el adjudicatario llevará a cabo las adecuaciones del servicio previstas o sobrevenidas (normativas, de seguridad, tecnológicas, organizativas, etc.) previstas en este pliego o que se considere convenientes en cada momento para adecuar su prestación, previo acuerdo con el Consorci AOC sobre el alcance, la planificación, el impacto en clientes y el coste de los cambios – entre otros; sin que pueda suponer costes emergentes para el Consorci AOC.

4) Devolución del servicio: las tareas preparatorias se iniciarán un año antes de la finalización del contrato. Esta fase se describe en detalle en el punto "6.7 servicio del presente documento.

La oferta de los licitadores debe describir la planificación que proponen detallando, entre otros, los siguientes aspectos:

- Descripción de los principales hitos de cada fase.
- Plan de contingencia/alternativo, para las fases que se consideren críticas.
- Calendario previsto para cada fase e hito destacado.
- En su caso, adelantos o mejoras en el calendario de alguna fase.

6.4.3 Explotación de la Jerarquía Pública de Certificación Digital de Cataluña

6.4.3.1 Operación de la Jerarquía de Certificación

El adjudicatario deberá alojar y operar las Entidades de Certificación raíz y subordinadas (en adelante, ECs), cuya titularidad es del Consorci AOC, como Prestador de Servicios de Certificación para los entes del Sector Público de Cataluña.

El adjudicatario queda obligado a la adecuación y plena conformidad de los servicios de la Jerarquía Pública de Servicios de Certificación Digital de Cataluña al Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas en el mercado interior (en adelante, "ReIDAS"), y a las normas técnicas que se aprueben para su aplicación. En este sentido, el contratista deberá obtener a su costa y en los plazos establecidos en la normativa aplicable, la evaluación periódica de la conformidad y cumplir con el resto de las obligaciones del Consorci AOC como prestador de servicios de confianza cualificado, así como asumir cualquier cambio que en cada momento exija el supervisor nacional o que deriven de la normativa española que se

dicte para dar cumplimiento o para aplicar el ReIDAS. En ningún caso esta obligación de adecuación se considerará modificación del contrato.

El adjudicatario deberá llevar a cabo las necesarias acciones de comunicación y difusión de las claves y certificados de las EC's del Consorci AOC a los usuarios del servicio y a terceras partes.

El adjudicatario deberá apoyar para las cuestiones relacionadas con las ECs del Consorci AOC a los supervisores que sean convenientes en cada momento:

- Ministerio de Industria, Comercio y Turismo, como a supervisor EIDAS a España.
- Principales fabricantes de software de uso generalizado: Google, Microsoft, Mozilla, Apple, Adobe, Java, etc.

El adjudicatario deberá mantener los actuales reconocimientos de los certificados emitidos por estas ECs mientras haya certificados vigentes.

El adjudicatario deberá someterse a las auditorías de cumplimiento que faciliten el reconocimiento de los certificados emitidos por estas ECs; incluyendo las auditorías ETSI.

En relación con el desarrollo de la nueva jerarquía de certificación de tercera generación, el adjudicatario deberá continuar desarrollándola hasta cerrar la de segunda generación, antes de la fecha máxima de emisión permitida por la vigencia de la subCA.

Más allá del cese de las actividades de emisión de las Ecs del Consorci AOC, durante la vigencia del contrato, el adjudicatario deberá continuar prestando los servicios para la gestión del ciclo de vida de los certificados: suspensión, activación, revocación, publicación de la información de revocación, etc., de acuerdo con lo establecido en la Declaración de Prácticas de Certificación del Consorci AOC.

6.4.3.2 Prestación de los Servicios del Catálogo de Certificados del Consorci AOC

Independientemente de la jerarquía de certificación (ECs) utilizada por la emisión en cada momento del contrato, el adjudicatario deberá ajustar a la normativa vigente el catálogo de perfiles de certificados del Catálogo de Certificados del Consorci AOC en el momento de la adjudicación.

El catálogo de certificados de la SCD se podrá modificar durante la vigencia del contrato, para adecuarlo a los cambios normativos que se produzcan; o para atender demandas específicas de los usuarios del servicio. El primer caso no generará costes emergentes para el Consorci AOC; en el segundo caso, la creación de hasta dos (2) perfiles nuevos por año no generará costes emergentes para el Consorci AOC sino que estos estarán incluidos en el importe fijo del servicio. En el caso de eliminación de algún perfil, el adjudicatario estará obligado a mantener el soporte a los certificados emitidos con el perfil en cuestión durante la vigencia del contrato y hasta la extinción de la vigencia de todos los certificados del mismo perfil.

Para garantizar la alineación de los certificados a emitir con los requerimientos de la legislación de administración electrónica, el contratista debe mantener, en su propuesta, la diferenciación entre certificados de clase 1 y de clase 2 o de persona vinculada. Los certificados de clase 1 corresponderán, como mínimo, con los certificados de sello electrónico y de empleado público, mientras que el resto de los certificados podrán ser también de clase 2. Esta restricción se podrá eliminar en función de las condiciones de implementación del nuevo Reglamento europeo, para lo que el contratista deberá hacer una propuesta, una vez adecuado a la nueva regulación, y recibir la conformidad previa del Consorci AOC.

El adjudicatario deberá gestionar los necesarios reconocimientos de los perfiles de certificados que conformen el catálogo del Servicio de Certificación Digital (SCD) del Consorci AOC a los principales navegadores, fabricantes de software y validadores.

6.4.3.3 Aplicación PKI

Será necesario que la aplicación de gestión de la infraestructura de clave pública (PKI) aportada esté certificada Comomon Criteria EAL 4+.

De esta manera se asegura que la solución aportada minimice los riesgos derivados de las necesidades de integración de la solución PKI aportada por el adjudicatario con el software de la entidad de Registro T-CAT e idCAT y las aplicaciones y conectores desplegados en el actual sistema de la SCD; por lo tanto, que minimice los principales riesgos del proyecto relativos a la gestión del cambio de los usuarios del servicio.

Se requiere que la aplicación de gestión de certificados esté configurada para aproximarse tanto como sea posible a la política de seguridad CIMC (Certificate Issuing and Management Componentes Protection Profile).

Las credenciales de acceso a cualquier parte o transacción de la aplicación serán siempre con tarjeta criptográfica y asignada nominalmente a un titular (Modelo basado en CWA 14167).

La solución de infraestructura de clave pública (PKI) aportada por el adjudicatario deberá permitir la devolución del servicio a la finalización del contrato, por si en un futuro se requiere transferir el servicio a un nuevo gestor.

En caso de incapacidad para proveer el servicio, desaparición o cese de las actividades del adjudicatario, éste deberá entregar al Consorci AOC el código fuente y configuraciones del software de la PKI utilizado para la operación de las ECs que conforman la jerarquía de certificación del Consorci AOC.

El punto "6.4.2 - Fases de la ejecución del contrato", establece la fecha a partir de la cual toda la gestión del servicio deberá realizarse con la solución PKI aportada por el adjudicatario.

La nueva solución PKI deberá incorporar servicios de publicación del estado de los certificados emitidos que, como mínimo, ofrezcan las funcionalidades y el rendimiento de los sistemas actuales según se ha definido en "6.3.3.2.1 Emisión de Listas de Revocación de Certificados (CRL's))" y "6.3.3.2.2 Servicio de Consulta de Estado de Certificados en Línea (OCSP))".

6.4.3.4 Infraestructura tecnológica

6.4.3.4.1 Entornos

Con el fin de cumplir con los requisitos de continuidad de los servicios definidos en el plan de continuidad del Consorci AOC que se exponen en el punto "6.4.11 disponibilidad de acuerdo con los ANS definidos en el apartado "6.5.2.2 ANS de continuidad", el adjudicatario deberá desplegar la infraestructura en los siguientes entornos:

6.4.3.4.1.1 Producción :

Entorno completo con características de escalabilidad, balanceo de carga y alta disponibilidad. El dimensionado de los equipos debe garantizar la capacidad de proceso de la carga de peticiones de usuarios prevista.

Los elementos de seguridad perimétricos deben garantizar el acceso controlado a los usuarios del sistema.

6.4.3.4.1.2 Contingencia:

En el entorno de contingencia, con requisitos de seguridad equivalentes a los de producción, el adjudicatario deberá alojar los sistemas necesarios para garantizar, la continuidad de todos los servicios objeto de este contrato que se ofrecen en el entorno de Producción. También por la entidad de certificación raíz.

6.4.3.4.1.3 Preproducción:

Despliegue de un entorno estable completo, destinado a la formación, a las pruebas funcionales y a la realización de pruebas de rendimiento. Toda su actividad no tendrá impacto en el conjunto de datos reales ni afectará al rendimiento de los otros entornos.

6.4.3.4.1.4 Entorno de pruebas/formación :

Despliegue de un entorno estable completo destinado a la formación y con la misma versión de aplicación desplegada que a Producción. Toda su actividad no tendrá impacto en el conjunto de datos reales ni afectará al rendimiento de los otros entornos.

6.4.3.4.1.5 Desarrollo:

Despliegue de un entorno diseñado para la realización de las actividades relacionadas con el desarrollo y el mantenimiento de los sistemas que forman el Servicio. Sin requerimientos especiales de estabilidad ni disponibilidad.

El entorno de desarrollo puede estar diversificado siempre que se garantice la seguridad en el control de acceso y que no se utilicen datos reales.

6.4.3.4.2 CPD's

Dado que los custodios de las tarjetas de administración (ACS) de los dispositivos criptográficos (HSM's) en los que se alojarán las claves de las EC's del Consorci AOC será personal vinculado al propio Consorci AOC, y con el objetivo de minimizar los desplazamientos que estos deban hacer cada vez que sea necesario realizar una intervención sobre estos dispositivos que requiera que los custodios se personen para aportar y hacer uso de las tarjetas en cuestión; se requiere que el CPD principal (CPD-1) esté ubicado en el área metropolitana de Barcelona.

La infraestructura técnica dentro del CPD principal debe ser exclusiva del adjudicatario, y debe encontrarse en una cámara con condiciones de seguridad y nivel de protección contra

cualquier agresión física que pueda afectar a los equipos informáticos o de telecomunicaciones y deberá ser conforme a los requisitos que, sobre este aspecto, imponen las normas técnicas aplicables a los prestadores de servicios de confianza que emiten certificados calificados; como por ahora, la ETSI EN 319 411-2 y otras más específicas que el licitador puede indicar si dispone de ella.

El CPD de contingencia (CPD-2), con requisitos de seguridad equivalentes a los de producción, el adjudicatario deberá alojar los sistemas necesarios para garantizar, la continuidad de todos los servicios objeto de este contrato que se ofrecen en el entorno de Producción. También por la entidad de certificación raíz. Para los ANS de activación del Plan de Recuperación de Desastres (PRD), se requiere que este CPD también esté en la provincia de Barcelona y a una distancia de seguridad mínima de 15 kms. del CPD principal (CPD-1).

6.4.3.4.3 Hardware y software dedicado

Las claves de las EC's del Consorci AOC deberán generarse y mantenerse dentro de dispositivos criptográficos (HSM) de uso exclusivo para el Consorci AOC. También la aplicación PKI de gestión de certificados, debe ser por uso dedicado a las EC's del Consorci AOC. La configuración será en alta disponibilidad por el entorno de Producción de las EC en línea (o EC subordinadas) y, si la capacidad lo permite, también por contingencia. En cuanto a los entornos de la EC raíz, el servicio se ofrecerá con un dispositivo por cada entorno (producción y contingencia).

El Consorci AOC prevé un escenario en el que el adjudicatario pueda reutilizar los HSM actuales que dan servicio a las EC's subordinadas. El hardware que se pondrá a disposición se recoge en el anexo "Annex_11_Actius SCD-AOC.pdf"

A lo largo de la vigencia del presente contrato, se ha previsto (en el importe a tanto alzado) que anualmente el adjudicatario adquiera y renueve estos dispositivos, junto con los eventuales servicios de migración de llaves entre los dispositivos antiguos y los nuevos, en su caso. La instalación de estos nuevos dispositivos y las tareas críticas de migración se llevarán a cabo en las instalaciones del adjudicatario para, en última instancia, hacer su puesta en funcionamiento a lo largo de la ejecución del presente contrato y sus prórrogas.

Se prevé, por tanto, que si se ejecuta todo el contrato hasta su duración máxima, se puedan renovar completamente la plataforma criptográfica. De cara a la correcta devolución del servicio, estos dispositivos deberán mantenerse con la garantía del fabricante durante toda la vigencia del contrato por parte del adjudicatario.

6.4.3.4.4 Uso de activos del Consorci AOC

El documento anexo "Annex_11_Actius SCD-AOC.pdf" del pliego de prescripciones técnicas, muestra la relación de activos que apoyan los servicios de certificación de la jerarquía actual y la aplicación de registro.

El Consorci AOC cederá al adjudicatario el uso del hardware que se relaciona en este documento en el apartado Hardware dedicado; y también los dispositivos criptográficos actuales. El hardware virtualizado se cederá en soporte digital. La cesión del hardware compartido físico se puede negociar con el adjudicatario, si es de su interés. Las prestaciones y volúmenes del hardware como servicio y el almacenamiento necesario se indican como referencia.

En relación con la Entidad de registro, el Consorci AOC dispone del código de todos los componentes de interfaces de usuario. También de la información para la integración con los

diferentes servicios de backend ofrecidos por los diferentes componentes enumerados en el punto "6.3.3". También las fichas de alta de los ENS y ER con su información verificada y los operadores y roles que las componen.

En caso de dar de baja los activos cedidos, el adjudicatario deberá notificarlo al Consorci AOC, para que éste pueda actualizar convenientemente su inventario de activos.

6.4.4 Explotación del software de la Entidad de registro T-CAT

El adjudicatario deberá alojar, operar y mantener el software de la Entidad de registro T-CAT propiedad del Consorci AOC.

La línea maestro del modelo de registro T-CAT tiene el objetivo de equilibrar la proximidad con los suscriptores, para mantener un nivel alto del servicio, y la racionalización de este, para ajustar el gasto al mínimo necesario.

El nivel de servicio deseado quedaría definido por los siguientes atributos:

- Rapidez en el proceso de registro y proximidad con los usuarios suscriptores.
- Mantener la capacidad de personalización de las EERR distribuidas por el territorio sin sacrificar en exceso la usabilidad y la facilidad del proceso actual.
- Mantener el actual nivel de digitalización y seguridad del proceso de solicitud, emisión y entrega de certificados actual.

Los objetivos de esta premisa no son otros que:

- Cumplir ANS para la entrega de las tarjetas, distinguiendo entre el servicio estándar, el personalizado y el servicio avanzado.
- Instruir un modelo económicamente autosuficiente, con una política de precios públicos de constitución y mantenimiento, que permitan financiar la estructura necesaria para el nuevo modelo de Registro.
- Instruir un modelo de proceso de servicio de certificación digital a ciudadanos y trabajadores públicos independiente de la tecnología de certificación con altos niveles de digitalización, seguridad y usabilidad.

Tal y como se ha expuesto en los puntos anteriores, el Servicio de Certificación Digital T-CAT se compone de tres elementos principales:

- Aplicación ASCD de EACAT: para hacer la tramitación de solicitud y modificación de roles en el servicio de forma digital, segura y con mecanismos para hacer el seguimiento del trámite.
- Web de Operadores de la Entidad de registro: para las operaciones de registro de datos de suscriptores, emisión de tarjetas, documentación y gestión del ciclo de vida del certificado digital por medios web y también mediante conectores automáticos.
- Carpeta del suscriptor: para hacer la entrega de los certificados T-CAT de forma segura y enviando los códigos de activación por correo electrónico.

El Consorci AOC valora mucho el modelo actual de prestación del servicio y el nivel de digitalización conseguido en el proceso de la SCD T-CAT actual. Por ello pide mantener funcionalidades claves en este proceso para garantizar la persistencia de este modelo. Al mismo tiempo, quiere minimizar el impacto en los usuarios operadores de la SCD actual sin perder de vista el objetivo de racionalización. Por todo ello, se pide que:

Con el objetivo de mantener la EACAT como mecanismo de entrada de las tramitaciones relativas al SCD T-CAT y por el elevado volumen de usuarios que utilizan esta aplicación, se

requiere que el adjudicatario mantenga todas y cada una de las funcionalidades a alto nivel y propósito de esta aplicación ASCD dentro de la SCD T-CAT.

Para llevarlo a cabo, el Consorci AOC requiere al adjudicatario hacer una nueva aplicación fuera de EACAT que cumpla las funcionalidades que cubre actualmente la ASCD. El Consorci AOC entregará un prototipo "cloud-native" operativo para que el adjudicatario lo pueda acabar de desarrollar, alojar e integrar con el nuevo EACAT 3.0. Este prototipo ha sido desarrollado a partir de las historias funcionales existentes y con mejoras de la experiencia de usuario de acuerdo con las indicaciones del Consorci AOC.

Con el objetivo de facilitar el mantenimiento al adjudicatario y generarle ahorros, el Consorci AOC prevé que el adjudicatario pueda cambiar la capa de la web de operadores actual de la SCD T-CAT para su tecnología de entidad de registro. Los requisitos funcionales de esta nueva capa a proveer se detallarán en próximos puntos.

En cuanto a la Carpeta del suscriptor, también se pide al adjudicatario que mantenga la funcionalidad de este componente del proceso de la SCD.

La aplicación ASCD y la Carpeta del Suscriptor han nacido en sistemas diferentes y heterogéneos. El adjudicatario puede proponer unificar estas capas de servicios de valor añadido en un solo software de registro que unifique los sistemas y que será devuelto al Consorci AOC en la fase de retorno del servicio. Para llevar a cabo esta transformación, se permite al adjudicatario que la pueda ejecutar durante la fase de transformación y optimización y no es necesario que lo haga durante la de transición. Los desarrollos realizados en esta capa de valor añadido deben ir enfocados al objetivo de garantizar el retorno del servicio al Consorci AOC de tal manera que futuras transiciones de tecnologías de certificación no impacten en la experiencia de usuario de los suscriptores de la SCD.

En cuanto a los roles enumerados en el punto "6.3.4.2 Roles del sistema T-CAT sobre esta parte de la aplicación (ASCD y Carpeta del Suscriptor), se pide que el adjudicatario los mantenga con el fin de aprovechar la labor de creación de roles que lleva haciendo el Consorci AOC desde hace tiempo y para minimizar el impacto en los usuarios actuales.

6.4.4.1 Entidad de registro T-CAT

Tal y como ya se ha dicho en puntos anteriores, el adjudicatario podrá cambiar la capa de Registro actual por la que él disponga. Esta capa de software se sitúa, en términos de pasos en el proceso de emisión, entre la ASCD y la Carpeta del suscriptor. Los requisitos que pone el Consorci AOC para esta transformación son que la capa de ER sea capaz de:

Sustituir las responsabilidades del módulo peticionario actual por mecanismos de entrada vía web y automáticos para la carga de datos de solicitudes para su validación y generación.

Disponer de una interfaz web y automática para hacer la validación de datos de una solicitud (actual módulo aprobador). Las solicitudes que vengan por EACAT vendrán ya prevalidadas y, por lo tanto, este módulo y rol puede ser simplificado para estos casos.

Disponer de un módulo de generación de certificados. Este módulo se corresponde con el actual módulo generador. Debe soportar la generación de certificados en tarjeta de forma personalizada y también del resto de certificados del catálogo de servicios solicitado. La funcionalidad de generación de tarjetas y de su personalización se describe en los próximos apartados específicos.

Este módulo de generación de certificados puede soportar, a decisión del adjudicatario y sólo para algunas ER concretas, un mecanismo de emisión por lotes enviados al fabricante. O alternativamente, para hacer una aplicación aparte con este propósito. En todo caso, el

adjudicatario deberá contemplar este servicio y podría aprovechar el actual esquema de mensajería para el intercambio de datos para hacer esta personalización de lotes de tarjetas al fabricante.

Disponer de un módulo de gestión de estados de los certificados. Este módulo debe poder ser utilizado vía web o bien vía conector automático. Se corresponde con el actual módulo de gestor de certificados.

Tener conectores de consulta de estado de certificados para dar respuesta a las necesidades de los conectores actuales. En concreto, las consultas pueden ser sobre un certificado en particular o múltiples certificados (los asociados a una ER, por ejemplo, que se puedan pedir a modo de informe) y se pueden solicitar consumir de forma síncrona o asíncrona (caso de los informes diarios).

6.4.4.1.1 Módulo generador: el servicio de personalización de tarjetas en las ER's colaboradoras

Partiendo del escenario de diseños que se describe en el punto "6.3.4.3.6 Modelos de provisión de los soportes criptográficos", el adjudicatario deberá ajustar el servicio de creación de nuevas ER para la personalización de tarjetas a estos modelos de prestación del servicio:

6.4.4.1.1.1 ER T-CAT estándar:

ER con impresora de plásticos (no criptográfica) que graba certificados en una tarjeta con diseño estándar T-CAT definido por el Consorci AOC. Este tipo de ER es el que dará continuidad, en el nuevo modelo de prestación del servicio, a las ER T-CAT con tarjeta estándar actual.

La tarjeta T-CAT estándar que se utilizará en estas ER será provista por el adjudicatario a la ER bajo una serie de condicionados que se definen en próximos puntos.

En caso de que la ER tenga impresora, la impresión de la tarjeta en estas ER será sólo por la cara de delante y sin ninguna otra personalización ni foto. La impresora que realiza esta impresión, por lo tanto, puede no tener lector/grabador de chips criptográficos.

No será responsabilidad del adjudicatario la provisión de la impresora. No obstante, sí se le pedirán servicios relacionados con la homologación, el mantenimiento y la formación relacionados con las impresoras de tarjetas.

El proceso de grabación del chip y el proceso de impresión pueden hacerse en un mismo paso o hasta un máximo de dos pasos, de cara a mantener la usabilidad y la facilidad del sistema actual donde se hace en un solo paso.

La aplicación de impresión de la tarjeta será desarrollada y mantenida por el adjudicatario. Para que esta aplicación funcione correctamente de acuerdo con el nivel de servicio acordado, el adjudicatario mantendrá un listado de software e impresoras homologadas para funcionar con su aplicación y sistemas operativos usuales en cada momento de la prestación del servicio. Los servicios de instalación y validación de la aplicación de personalización de tarjetas para la puesta en marcha de la ER serán ofrecidos por el adjudicatario. No se prevé que el adjudicatario provea el hardware (PC) para alojar estas aplicaciones locales de grabación y personalización en las entidades de registro.

Se pretende que las aplicaciones de grabación de chip y personalización funcionen con equipos (PC) estándar provistos por los propios Ente que son o serán Entidades de Registro.

El objetivo de este hecho es no tener que ofrecer mantenimiento a nivel de hardware a estos equipos PC o lectores asociados al ER.

A pesar de no tener que proveer el hardware PC, sí que el adjudicatario deberá mantener una configuración homologada de sistema operativo y componentes de hardware para el uso de estas aplicaciones para garantizar su operatividad y acuerdo de nivel de servicio aplicable al ER. Esta configuración se pasará a los entes que quieran establecerse como ER para que puedan adquirir el hardware necesario. La aplicación de generación de tarjetas mantendrá la funcionalidad de generar el certificado dentro del chip y cambiar los códigos de pin y PUK de la tarjeta. También se integrará con la Carpeta del suscriptor para guardar el pin y PUK generados en el momento de la generación del certificado dentro del chip. También cargará en la carpeta del suscriptor el documento con el contrato para la entrega del certificado y otros datos adicionales que puedan ser necesarios.

En uno mismo Nos puede haber más de un punto de registro. Aunque, en la medida de lo posible, la replicación de la instalación será llevada a cabo por los propios Ente, el adjudicatario apoyará la replicación. Tampoco se aplicarán costes por licenciamiento adicional del software de la estación de registro en este contexto, en su caso.

La aplicación de generación dejará rastros en el sistema que faciliten el diagnóstico de incidencias puntuales de generación. También dispondrá de un conjunto de scripts para hacer test unitarios de cada componente que compone la estación (lector externo, impresión, etc..) con el fin de facilitar el diagnóstico de incidencias en el CAU remoto.

6.4.4.1.1.2 ER T-CAT personalizada sin características avanzadas

ER con impresora de plásticos (no criptográfica) que no utiliza la tarjeta estándar del Consorci AOC. Aparte de requerir el nivel de servicio y funcionalidades de una ER estándar, puede requerir un nivel de prestación de servicio más elevado debido al nivel de personalizaciones que requiere la tarjeta que se genera.

Estas ER pactan sus diseños con los fabricantes y pueden requerir unos mapas y niveles de personalización más elevados.

Las personalizaciones soportadas por el modelo personalizado y que se salen del modelo estándar pueden ser únicamente la foto del suscriptor y la impresión de datos (de dentro o de fuera del proceso de registro del certificado) por la parte de delante o de detrás.

También se pueden emitir certificados directamente en la tarjeta sin necesidad de impresión, en estos casos.

6.4.4.1.2 Principios generales del modelo de provisión de tarjetas y hardware para las ER T-CAT y el servicio de mantenimiento asociado a las mismas

La impresora de tarjetas no está incluida en el servicio de creación de ER T-CAT que se solicita y será siempre provista por el ente que se quiera constituir como ER en base a los requisitos que le facilite el adjudicatario. Los fungibles de esta impresora tampoco les proveerá el adjudicatario.

Los licitadores ofrecerán como servicio la adquisición de tarjetas T-CAT estándar u otros modelos concretos. Este servicio incluirá la provisión del plástico, el envío a la ER y la gestión del stock. Esta gestión se hará desde la ER ubicada en las instalaciones del adjudicatario.

La papelería y material divulgativo será adquirido por el adjudicatario para su distribución a las ER estándar y para el uso en la propia ER de sus oficinas.

El adjudicatario se hará cargo del mantenimiento y la transición de las ER actuales abiertas al nuevo modelo durante la fase de transición. Para ello, se acordará con el Consorci AOC la asignación de las nuevas tipologías de ER a cada una (estándar o personalizada).

6.4.4.1.3 ER vinculadas

De acuerdo con lo expuesto hasta ahora, las ER vinculadas deben seguir sin tener necesidad de disponer de hardware específico para seguir haciendo su función y roles dentro de la SCD y de seguir utilizando las mismas interfaces o muy similares. El objetivo de que no haya que hacer formación a los operadores de estas ER o que, en todo caso, sea mínima, es fundamental para garantizar la continuidad del modelo de registro T-CAT.

6.4.4.1.4 Interfaces y conectores

El adjudicatario deberá mantener todas las interfaces actuales que hay interconectadas con clientes y que están definidas en el punto "6.3.4.4 Descripción de componentes e interfaces de software del Servicio de Certificación Digital (T-CAT e idCAT)"De este documento.

En particular, son especialmente críticas las que son utilizadas por clientes y sistemas externos a la SCD y, para estos casos, habrá que mantener exactamente la misma funcionalidad y operativa actuales así como las medidas de seguridad pertinentes y aplicables.

De forma pactada con cada cliente de la SCD y de cada conector, se podrá migrar el servicio que se ofrece actualmente a alguna nueva modalidad transformada.

6.4.4.2 Topología de la red de Entidades de Registro T-CAT

Las Entidades de Registro T-CAT presentan las siguientes variantes:

6.4.4.2.1 EERR Virtuales / vinculadas

En el entorno T-CAT las ER's virtuales o vinculadas son todos los entes suscriptores del servicio que no disponen de la impresora criptográfica necesaria para grabar el chip e imprimir la personalización gráfica de las tarjetas. Las ER vinculadas usan la ASCD de EACAT para la certificación de datos de certificados T-CAT y la entrega de los certificados T-CAT a través de la carpeta del suscriptor.

El número de ER's Virtuales o vinculadas (entes dados de alta en el sistema) actualmente es de 2.200.

6.4.4.2.2 ER's T-CAT

En el entorno T-CAT, se entiende por ER T-CAT, una ER que dispone de infraestructura para la emisión de certificados en soporte tarjeta.

El número de ER's T-CAT es de 68 entidades de registro (de las cuales hay que tienen varios puntos de atención, etc...).

Las ER's T-CAT se clasifican en dos tipologías según el nivel de funcionalidades y personalizaciones incorporadas a la tarjeta:

- ER estándar T-CAT: Entidad de registro con o sin impresora que emite los certificados T-CAT en soporte tarjeta. El tipo de tarjeta es el estándar T-CAT que permite personalización de la parte de delante de la tarjeta con datos del certificado (típicamente nombre, organización y departamento al que está adscrito el titular de la T-CAT, aunque puede haber variantes de los campos impresos).

- ER con tarjeta personalizada: ER con o sin impresora que emite certificados T-CAT personales en soporte tarjeta, pero con una tarjeta diferente de la T-CAT estándar. En caso de que imprima la tarjeta, lo puede hacer con un mapa de campos personalizado por la parte de delante o de detrás de la tarjeta y puede incluir foto.

La información relativa a las personalizaciones y funciones que incorpora cada ER a las tarjetas que emite se recoge en el documento "Annex_9_Resum_caracteristiques_ERs_TCAT". Este mismo documento también contiene información relativa a las necesidades de las diferentes ERs.

6.4.4.3 Servicio de emisión de soportes criptográficos

Los modelos de chips criptográficos soportados y homologados actualmente para la emisión de certificados son:
- Sm@rt cafe 7.0 del fabricante G&D
- CHIPDOC V2 ON JCOP 3 P60 in SSCD configuration, version V7b4_2

El modelo "Sm@rt cafe 7.0 del fabricante G&D" sin embargo, ya no se usa para emitir certificados calificados porque salió de la lista de calificados en julio de 2023.

Durante la vigencia del contrato se prevé que habrá que homologar al menos una nueva tarjeta para la caducidad del dispositivo criptográfico.

6.4.5 Modelo de registro idCAT certificado

El idCAT ofrece diferentes mecanismos de autenticación y firma. Es objeto de este contrato el modelo de servicio de idCAT en modalidad certificado en software (formato PKCS#12). En concreto, los procesos de registro de identidad, validación presencial por parte de operadores del servicio y entrega del certificado al titular del certificado digital en formato pkcs#12. También son objeto de este contrato, las integraciones del proceso de registro con el servicio de vídeo-identificación y con el servicio de custodia de certificados remotos ofrecido por el Consorci AOC. No es objeto de este contrato la provisión de la tecnología y servicios para la vídeo-identificación de los titulares de certificados idCAT ni de los servicios de custodia de los certificados remotos. El Consorci AOC ofrece estos servicios a través de los contratos "AOC 2020 71" y "AOC-2024-17", respectivamente.

El Consorcio está desplegando el registro de usuarios basado en vídeo-identificación de forma integrada y alternativa con el proceso de solicitud previa a la validación presencial de la identidad. Este servicio se encuentra en proceso de construcción previa a la acreditación por parte del supervisor EIDAS. El adjudicatario del presente contrato deberá mantener la integración para poder llamar al servicio de vídeo-identificación y recuperar los datos de la validación de identidad para continuar con el proceso de entrega.

Se solicita también, en el ámbito del servicio aplicable al alcance de este contrato, la implementación de las propuestas de maquetación del conjunto de webs en el alcance del servicio IdCAT que haga el Consorci AOC al adjudicatario. Las propuestas de cambio llegarán validadas por los responsables de Accesibilidad y Experiencia de Usuario del Consorci AOC.

Los cambios en esta parte de la aplicación se consensuarán con el Consorci AOC a lo largo de todas las fases de prestación del Servicio.

En relación con el punto anterior, actualmente el Consorci AOC también está en proceso de cambiar la página web principal del servicio idCAT, bajo el dominio de www.idcat.cat, para presentar las modalidades del servicio idCAT. Esta web se alojará en sistemas del Consorci AOC y redirigirá a los usuarios que deseen un idCAT en modalidad certificado a los que aloje el adjudicatario del presente contrato.

En relación con la parte de la web de operadores, el Consorci AOC pedirá al adjudicatario cambiar la web de operadores actual por una versión en estado de prototipo funcional, desarrollada con tecnologías basadas en microservicios y que ha sido validada a nivel de experiencia de usuario. El requisito fundamental será que se siga manteniendo el grado actual de separación tecnológica entre el componente de Registro y el componente de Entidad de Certificación. El adjudicatario debe velar por que este modelo se mantenga en la solución que proponga. También que el impacto en el alto volumen de operadores actualmente formados sea el mínimo posible a raíz de este cambio.

Las ER idCAT no tienen requisitos específicos de hardware PC ni lectores. Esto viene dado por el hecho de que toda la interacción con la aplicación es web y se hace desde un navegador. Por tanto, el adjudicatario no deberá proveer este hardware sino que deberá mantener unas mesas de compatibilidad y requisitos de componentes de hardware y software compatibles con el servicio de entidad de registro.
El adjudicatario incluirá en sus servicios, el de creación de una entidad de registro idCAT. Los servicios en que se desglosará este servicio de creación serán básicamente dos: el soporte por medios electrónicos para la configuración de los lugares de Registro por parte del propio ente y la formación por medios electrónicos de los operadores.

A nivel de soportes de emisión, el idCAT debe seguir pudiendo emitir con el soporte actual en formato software, con generación de claves en la CA y entrega en formato PKCS#12. También deberá permitir la gestión de las credenciales de firma remota mediante la redirección del usuario a los sistemas de información de la solución de firma remota.

Por último, el adjudicatario deberá continuar las integraciones iniciadas con el sistema de repositorio de datos del Consorci AOC a través del servicio DESA'L con el fin de dar cumplimiento a las obligaciones de custodia de datos derivados de la normativa aplicable.

En el documento anexo "Annex_8_llistat_ER idCAT" se enumeran las Entidades de Registro activas a fecha de elaboración de este documento.

6.4.6 Servicio de Entidad de Registro T-CAT del Consorci AOC

El adjudicatario creará una ER del tipo estándar en sus oficinas desde donde podrá ofrecer los servicios que se ofrecen actualmente en el ER del Consorci AOC definidos en el punto "□o
La Entidad de Registro T-CAT del Consorci AOC".

Esta ER alojará la interconexión con el sistema de lotes por solicitudes masivas de cara a poder servirlas dentro de la ANS establecido.

Esta ER soportará el servicio de emisión en soporte tarjeta en modalidad urgente y ordinaria con los compromisos de ANS que aplican ahora al ER del Consorci AOC definidos en "6.5.2 ANS de Explotación del Servicio".

Desde esta ER se gestionarán los stocks de tarjetas y papelería que se enviarán al resto de ER estándar del territorio.

6.4.7 El servicio de apoyo

Actualmente el servicio se estructura en 3 niveles:

1er nivel: formado por personal subcontratado, externo al Consorci AOC. Este nivel se encarga de resolver incidencias tipificadas, documentadas y de acuerdo con procedimientos definidos en el portal de soporte y en la web del Consorci AOC y de resolución sencilla.

2º nivel: formado por personal subcontratado, externo al Consorci AOC. Se encarga de resolver incidencias que requieren intervención de personal con cierta cualificación técnica y que no se encuentran documentadas y ni disponen de procedimientos en el portal de soporte ni en la web del Consorci AOC. En el caso del SCD este 2º nivel ya lo ofrecerá la empresa adjudicataria del servicio de certificación digital del Consorci AOC.

3er nivel: es personal de la empresa adjudicataria del servicio de certificación digital del Consorci AOC.

Se derivarán al nivel 3 las incidencias que no se puedan resolver en el nivel 2.

6.4.7.1 Ámbitos de atención y apoyo a prestar por el proveedor:

El adjudicatario deberá ofrecer el servicio de apoyo a:
- Operadores de las Entidades de Registro (registradores)
- Usuarios finales (ciudadanos y empleados públicos)
- Integradores y otro personal técnico al servicio de los ente del sector público de Cataluña

También deberá hacer el mantenimiento del material de soporte correspondiente (FAQ's, algunos manuales técnicos y operativos, vídeos, etc.). Estos cambios habrá que realizarlos con la máxima celeridad. Se requerirá al adjudicatario que provea y mantenga, sin costes emergentes por el Consorci AOC, herramientas de auto diagnóstico y de autoservicio dirigidas a los usuarios del servicio, que mejoren la capacidad de respuesta de los primeros niveles de soporte y mejoren la percepción del servicio por parte de los usuarios.

6.4.7.2 Canales de entrada de peticiones

Los usuarios formularán sus peticiones por los canales habituales:

- Servicio de atención telefónica, por resolución de dudas e incidencias: 900 90 50 90
- Mediante formulario web habilitado al efecto.

El nivel 1 derivará al adjudicatario las peticiones referentes al servicio objeto de este contrato, generando el ticket correspondiente con la herramienta de ticketing que emplea el Consorci AOC para el apoyo al resto de sus servicios (qué actualmente es "ZENDESK") la cual asignará un número identificador de la petición.

El Consorci AOC cederá al adjudicatario las licencias de usuarios de la herramienta de ticketing que sean necesarias para que las pueda emplear el personal de la empresa adjudicataria que prestará el servicio de soporte, en los casos que desde la AOC se les solicite intervención para solventar alguna incidencia.

6.4.7.3 Horario de atención

El horario del servicio de apoyo de 3er nivel a prestar por el adjudicatario será, como mínimo, de 8.00 a 17.00 horas, de lunes a viernes, excepto festivos del calendario laboral de Cataluña. De forma ocasional se podría ampliar este horario para alguna campaña especial.

6.4.8 Servicios de formación

A demanda del Consorci AOC, el adjudicatario deberá ofrecer los siguientes servicios de formación en relación con los servicios objeto del presente contrato:

Cursos virtuales:
- Cursos dirigidos a usuarios finales, sobre los Usos y la difusión del certificado digital.
- Cursos dirigidos a los responsables del servicio de ente suscriptor para procesos de entrega, mantenimiento, custodia, etc...
- Cursos para formar operadores de las ER T-CAT o idCAT.

Estos cursos se harán utilizando la plataforma virtual del Consorci AOC, gestionada por el propio Consorci AOC, con los requerimientos de la plataforma.

El adjudicatario deberá llevar a cabo la tutoría y la gestión de las inscripciones de los alumnos de los cursos virtuales, así como la resolución de las incidencias que puedan aparecer.

El Consorci AOC pondrá a disposición del adjudicatario los materiales de que dispone, y que fueron elaborados para las formaciones que actualmente está realizando. Aunque la adaptación, el mantenimiento, e incluso la creación de nuevos materiales formativos, deberá hacerlo el adjudicatario, dentro del ámbito de este contrato.

En cuanto al servicio de formación, se realizan estas sesiones con estos formatos:
- 4 cursos virtuales para operadores T-CAT.
- 14 cursos virtuales para operadores idCAT.
- Curso virtual abierta para ente suscriptor.
- De forma puntual cursos a medida presenciales.

El servicio de certificación digital lleva a cabo acciones de formación y divulgación dirigidas tanto a usuarios finales (titulares de los certificados digitales) como a operadores y técnicos de apoyo a las Entidades de Registro.

6.4.9 Servicios organizativos

Los servicios de carácter organizativo no definidos específicamente hasta ahora y que intervienen en la prestación del servicio de certificación digital son los siguientes:

- Servicios jurídicos:
  - Redacción y mantenimiento de la Documentación Jurídica (Política de certificación, Declaraciones de prácticas de certificación de cada EC, Condiciones de uso de cada perfil de certificado, etc.) de forma coordinada con la Responsable de Asesoramiento Jurídico de Servicios del CAOC junto con el adjudicatario del lote1 del presente contrato.
  - Informes ad-hoc relativos a la prestación ordinaria del servicio.
- Apoyo a la operativa de las Entidades de Registro
  - Gestión de la red de las ER's
  - Gestión de la configuración de permisos al sistema

- Generación de informes sobre los datos de actividad del servicio e integración con el sistema de Business Intelligence del Consorci AOC.
- Facturación a clientes del servicio: entes suscriptores y también intermediarios por todos los conceptos: consumo de certificados, materiales, mantenimiento de las ER's, formaciones, auditorías, proyectos, etc.
- Gestión de los envíos postales de los soportes criptográficos y otros materiales necesarios para el funcionamiento ordinario de las ER's.
- Gestión de stocks y de la contratación para la adquisición de los soportes criptográficos, papelería, etc.

6.4.9.1 Facturación de la documentación entregable

El Consorci AOC es el propietario de toda la documentación elaborada por el adjudicatario referente al servicio prestado por el adjudicatario.

El Consorci AOC será el responsable de la validación y aprobación de los documentos elaborados por el adjudicatario.

El adjudicatario deberá mantener la documentación actualizada en el sistema de gestión documental que el Consorci AOC proporcione para tal efecto.

Asimismo el adjudicatario deberá mantener un registro de la documentación enviada al Consorci AOC con el detalle de las versiones, fechas y destinatarios. Este registro estará a disposición del Consorci AOC en el repositorio de información que el Consorci AOC haya designado a tal efecto.

También se pide que se haga un registro de todos los ficheros que entregue al Consorci AOC o que sean generados por cualquier petición concreta.

6.4.9.2 Gestión de la adquisición y provisión de materiales y servicios

La gestión del aprovisionamiento define el modelo de provisión de los servicios bajo demanda objeto del contrato y la política de adquisición de los materiales necesarios para la prestación del servicio bajo demanda de los ente suscriptores.

Los licitadores deberán describir en sus ofertas su propuesta para la gestión de la provisión de materiales, cuando la adquisición la haga el adjudicatario (como los soportes criptográficos, papelería, fungibles de las ERs, etc.); y también las propuestas para la gestión de los materiales adquiridos por el Consorci AOC, fuera del alcance de este contrato (las impresoras para las ERs colaboradoras de los Consejos Comarcales, etc.).

Las ofertas de los licitadores también deberán describir su propuesta de modelo de provisión de servicios (para la gestión, por ejemplo, de las solicitudes de apertura de nuevas ER's T-CAT colaboradoras, etc.).

Las propuestas deben contemplar el uso de la herramienta de Apoyo del Consorci AOC para apoyar estas gestiones.

6.4.9.2.1 Gestión del catálogo de productos y servicios

El catálogo de servicios habilita y define la relación entre el Consorci AOC y el adjudicatario, detallando los servicios entregados, su operativa de petición, el ámbito de estos, los niveles de servicio comprometidos y el coste.

Los licitadores deberán exponer a sus ofertas su propuesta de procedimientos y, en su caso, de herramientas para definir y mantener actualizado el catálogo de servicios objeto de este con-trato.

6.4.9.3 Gestión de la facturación

Los licitadores deberán describir a sus ofertas su propuesta para la gestión de la facturación, en los siguientes ámbitos:

6.4.9.3.1 Del adjudicatario al Consorci AOC:

El Pliego de cláusulas Administrativas del presente contrato establece los requerimientos y las condiciones sobre la facturación del adjudicatario hacia el Consorci AOC.

6.4.9.3.2 Del Consorci AOC a los entes suscriptores del Servicio de Certificación Digital

El licitador describirá en su oferta - más allá de su propuesta para la generación y el envío de las facturas dirigidas a los entes suscriptores del SCD y de los correspondientes mecanismos de reporting ya fijados en este pliego - su propuesta de coordinación con el Consorci AOC para que éste pueda hacer el seguimiento y el resto de las actividades relativas a la gestión de la facturación; incluyendo la coordinación entre el Consorci AOC y el adjudicatario para la gestión de los abonos.

Al inicio del contrato, el envío de las facturas deberá hacerlo el adjudicatario de acuerdo con un extracto mensual y durante los 10 días hábiles del mes siguiente a la generación del certificado.

Las facturas se emitirán en formato electrónico siempre que sea posible a través de una plataforma de facturación y contendrán la información especificada por el Consorci AOC para facilitar la gestión de su aprobación por parte del ente destinatario. En ningún caso se incluirán datos de carácter personal sin un tratamiento adecuado para la pseudonimización. Se permitirá identificar el pedido y cada elemento del pedido a partir de datos como:

- el nombre del responsable del servicio del ente destinatario.
- un número de referencia: código de contratación interno, nº de expediente u otra (si se ha especificado en la solicitud)

El adjudicatario deberá efectuar un seguimiento de la facturación enviada juntamente con el departamento de gestión económica del Consorci AOC. La gestión del cobro de las facturas será responsabilidad del Consorci AOC.

6.4.9.4 Función presupuestaria

El licitador deberá describir en su oferta cómo prevé dar apoyo a la función presupuestaria, especialmente en caso de que sea necesario llevar a cabo acciones extraordinarias para cubrir eventualidades no previstas.

El adjudicatario elaborará los informes presupuestarios sobre los servicios contratados, con periodicidad inicial anual, de acuerdo con el calendario que el Consorci AOC establezca.

Los informes presupuestarios elaborados deben permitir disponer de información suficiente para la previsión anual general de la gestión del servicio.

6.4.10 La gestión de la seguridad y el cumplimiento normativo

El adjudicatario, de forma coordinada con el área de seguridad del Consorci AOC, deberá dar cumplimiento al marco legal y normativo vigente (definido en el punto 3 MARCO NORMATIVO). En este apartado se remarcan aquellos aspectos de seguridad considerados de mayor relevancia dentro del alcance del servicio y que habrá que tener operativos para la puesta en marcha de este.

6.4.10.1 Clasificación de la información

El adjudicatario deberá tener en cuenta la clasificación de la información de las aplicaciones, objeto del contrato, realizada por el Consorci AOC, para aplicar correctamente el marco normativo y legal indicado anteriormente.

6.4.10.2 Cumplimiento normativo y legal

El adjudicatario deberá cumplir con todos los requerimientos que sean de aplicación de acuerdo con el marco normativo de seguridad vigente y de todas las actualizaciones posteriores que se produzcan, así como a todo el marco legal en materia de ciberseguridad que sea de aplicación (por ejemplo, Esquema Nacional de Seguridad y GDPR – General Data Protection Regulation, eIDAS - electronic IDentification, Authentication and trust Services)).

El adjudicatario deberá incorporarse al modelo de cumplimiento normativo del Consorci AOC. En este modelo se integran las posibles auditorías que el Consorci AOC determinen realizar, así como el seguimiento de los planes de acción derivados de las mismas. También se incluye en este modelo el cumplimiento por parte del adjudicatario de planes de acción relativos a normativas o estándares el Consorci AOC y su seguimiento recurrente. El adjudicatario deberá disponer de los recursos adecuados para llevar a cabo la ejecución de las tareas que le correspondan en el modelo de cumplimiento, dando respuesta en los plazos marcados por el Consorci AOC.

El adjudicatario deberá garantizar el acceso del personal autorizado del Consorci AOC a la información de seguridad (procedimientos, registro de incidentes, rastros, etc.). Toda la información de seguridad deberá estar siempre disponible para este personal, autorizado y previamente identificado. El Consorci AOC y el adjudicatario establecerán conjuntamente los mecanismos para facilitar el acceso del personal autorizado a esta información, estableciendo los controles de seguridad mínimos.

6.4.10.3 Requisitos de protección de datos

El licitador en su oferta deberá detallar las medidas de seguridad y las medidas de privacidad desde el diseño y por defecto que se establecen para dar cumplimiento a los requerimientos establecidos en el Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de estos datos y a Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales por cada uno de los ámbitos especificados en el apartado "6.3.3 Cataluña del presente PPT y por todo el ciclo de vida de los datos, incluido su bloqueo en cumplimiento de lo establecido en la LLOPDiGDD. Habrá que estar en las guías aprobadas por la Autoridad Catalana de protección de Datos, la Agencia Española de Protección de Datos y el Comité Europeo de Protección de Datos (CEPD).

El adjudicatario deberá revisar anualmente y cuando se produzca alguna modificación en el tratamiento de los datos, el Análisis de Riesgos por los derechos y libertades de los titulares de los datos y adoptar las medidas de seguridad que, en su caso, sea necesario implantar para preservarlos.

6.4.10.4 Gestión de trazas

El adjudicatario deberá cumplir con la norma de gestión de rastros vigente. El adjudicatario deberá asegurar que almacena todas las trazas que le son de aplicación de acuerdo con su clasificación de información y al marco normativo y legal aplicable definido en el punto "3 MARCO NORMATIVO".

Las trazas deberán ser accesibles en modo lectura y se asegurará el marcaje de las trazas con requerimientos específicos de conservación según la legislación aplicable.

El adjudicatario, teniendo en cuenta el nivel de clasificación de seguridad de la aplicación expuesto en el punto 6.4.10.9 Auditoría externa, deberá facilitar los mecanismos para que las trazas sean accesibles y estén integradas con el repositorio de trazas de seguridad que determine el Consorci AOC.

Traslado al Consorci AOC de los datos y rastros generados como mucho en periodicidad anual. Como mínimo certificados emitidos, listas de revocación (CRL), firmas de aprobación o entrega.

6.4.10.5 Comunicaciones seguras de acceso a las aplicaciones objeto de la licitación

El adjudicatario deberá garantizar que todas las aplicaciones web objeto del contrato (tanto internet como intranet) utilicen canales de comunicación seguros HTTPS/TLS.

6.4.10.6 Arquitectura, pruebas de recuperación de desastres y pruebas de recuperación de backups

El adjudicatario deberá:

- Garantizar que el diseño de la arquitectura de la solución permite alcanzar los requerimientos de disponibilidad/continuidad requeridos.
- Participar en la preparación y ejecución de las pruebas de recuperación de desastres (PRDs) y en las pruebas de recuperación de backups, realizando pruebas que certifiquen la capacidad de recuperación esperada.

6.4.10.7 Seguridad de las instalaciones desde las que se presta el servicio

El adjudicatario velará por el cumplimiento de las medidas de seguridad expuestas en las Condiciones Generales de Prestación de los servicios y en la Declaración de Prácticas de Certificación del Consorci AOC y podrá ser auditado de forma anual para valorar el grado de cumplimiento e identificar riesgos de seguridad.

6.4.10.8 Seguridad en el cloud

En el caso de que alguno de los servicios o herramientas de apoyo a la prestación de este esté ubicados en la nube, el adjudicatario deberá garantizar igualmente el cumplimiento de los requerimientos de seguridad que establece el marco normativo indicado en este pliego. En concreto, será necesario que estos entornos estén incluidos en el alcance de la auditoría de ENS y EIDAS que lleve a cabo el adjudicatario.

6.4.10.9 Auditoría externa

El adjudicatario deberá disponer, a partir del inicio de la fase de transición y hasta la finalización del contrato, de la certificación de cumplimiento , conforme al Esquema Nacional de Seguridad de nivel ALT, así como una auditoría sobre el cumplimiento de la normativa de protección de datos de carácter personal.

Se adjunta información de relevancia a tener presente para el logro de este requerimiento:

- Esquema Nacional de Seguridad (ENS):
    - Para dar cumplimiento con los requisitos en materia de integridad, disponibilidad, autenticidad, trazabilidad, confidencialidad de la información, según dispone el ENS y de acuerdo con los parámetros aprobados por el Consorci AOC dentro de la categorización del servicio en los dominios del ENS:

Sistema SCD						
Denominación del activo esencial	C	I	D	A	T	DP
Ascensos repositorio de jerarquía de claves del entorno principal (HSMs)	A	A	A	M	M	N/A
Ascensos repositorio de jerarquía de claves del entorno de contingencia (HSMs)	A	A	A	M	M	N/A
Ascensos de emisión y revocación de certificados del entorno principal (PKI + CRL + OCSP)	M	M	A	M	B	M
Ascensos de emisión y revocación de certificados del entorno de contingencia (PKI + CRL + OCSP)	M	M	A	M	B	M
Subsistema de Información pública (claves públicas y documentación jurídica)	B	B	A	M	M	NA
Ascensos de apoyo	B	M	M	B	B	B
Subsistema de EACAT y MUX	B	B	A	M	M	M
Valor máximo registrado	A	A	A	M	M	M
La valoración del sistema es Alta (C=A, I=A, D=A, A=M, T=M, DP=M)						

    - Los subsistemas marcados en color azul, dado que se encontrarán completamente bajo la responsabilidad del adjudicatario, serán objeto de auditoría de activo o subsistema de acuerdo con ENS por parte del adjudicatario a lo largo de la vigencia del contrato. Los otros dos puntos, dado que están parcialmente en AOC, la auditoría se coordinará con AOC y se ejecutará en también a lo largo de la vigencia del contrato.
    - RTO y RPO segundos definido en el punto "6.5.2.2 ANS de continuidad".

- Accesibilidad:
    - Cumplimiento normativo normas accesibilidad aplicables.

- Plan de Seguridad del Consorci AOC:
    - Política de seguridad y normas derivadas (ver punto "3 MARCO NORMATIVO").

- Acreditación voluntaria del PSC:
    - Auditoría interna del % de certificados emitidos por parte del propio adjudicatario.
        - A nivel de rastros : de solicitud, aprobación, emisión, entrega.
        - A nivel de producto con certlint o herramientas equivalentes
    - el Consorci AOC se somete con periodicidad bianual a las auditorías que le permiten renovar los sellos EIDAS mencionados en el punto "“6.4.12 Auditorías del Prestador de Servicios de Certificación Consorci AOC".

- Auditorías periódicas de las ERs : el adjudicatario de este lote deberá aplicar las medidas derivadas del resultado de las auditorías del adjudicatario del lote de auditorías de las ER.

6.4.11 La gestión de la continuidad y la disponibilidad

La finalidad de la gestión de la continuidad y la disponibilidad se centra, principalmente, en garantizar la continuidad de los servicios y procesos ante cualquier situación adversa, evitando un impacto significativo en la organización.

Los objetivos que se persiguen son:

- Disponer de Planes de Continuidad que permitan gestionar de forma eficiente una situación de emergencia.
- Garantizar la continuidad de los procesos y servicios considerados críticos, cuya indisponibilidad podría tener un impacto irreversible.
- Probar los Planes de Continuidad como medida de garantía de su efectividad ante una situación real de contingencia.
- Focalizar el esfuerzo en la mitigación de riesgos relevantes.
- Coordinar a todas las personas clave para hacer frente a una situación de contingencia.
- Cumplir con los requerimientos legales / regulatorios en materia de continuidad de negocio.
- Alinearse con la metodología del Consorci AOC y buenas prácticas del mercado (ISO 27002, BS25999/ISO22301, NIST sp 800-30,34, PAS 77, ITIL, ISO/PAS 22399:2007)

El adjudicatario deberá entregar al Consorci AOC su política de continuidad.

El adjudicatario deberá documentar, desarrollar e implantar las medidas de disponibilidad necesarias para cubrir los indicadores de nivel de servicio de disponibilidad que se requieren en "6.5.2.3 ANS de disponibilidad ". Esta documentación deberá entregarse al Consorci AOC.

El adjudicatario deberá implantar medidas sobre los activos implicados que le permitan elaborar y entregar al Consorci AOC un Plan de Continuidad del servicio de Recuperación ante Desastres (en adelante, PRD) para garantizar los niveles de servicio establecidos en el punto "6.5.2.2 ANS de continuidad" de este documento y que derivan del documento de análisis de impacto de negocio (en inglés, Business Impact Analysis o BIA) elaborado por el Consorci AOC en relación a este servicio.

El adjudicatario deberá mantener actualizado al PRD ante cambios propios o por causas de terceros.

El adjudicatario deberá proveer soluciones tecnológicas que permitan alcanzar los objetivos fijados en el PRD, siendo éstas certificadas mediante pruebas de recuperación periódicas.

El adjudicatario participará en las pruebas de recuperación y alta disponibilidad que el Consorci AOC planifique. Deberá elaborar el plan de pruebas y ejecutarlas el día de la prueba, en su caso, coordinadamente con los equipos que realizan las pruebas de continuidad.

Toda la información del PRD deberá estar siempre disponible para el personal del Consorci AOC autorizado y previamente identificado. Se establecerán los mecanismos para facilitar el acceso del personal autorizado del Consorci AOC a esta información, estableciendo los controles de seguridad mínimos exigidos por el Consorci AOC.

6.4.12 Auditorías del Prestador de Servicios de Certificación Consorci AOC

Tal y como se establece en las obligaciones esenciales del contrato, el adjudicatario queda obligado a la adecuación y plena conformidad de los servicios ofrecidos al Consorci AOC al Reglamento del Parlamento Europeo y del Consejo relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas en el mercado interior (en adelante, "ReIDAS"), y a las normas técnicas que se aprueben para su aplicación.

En este sentido, el contratista deberá cumplir, sin costes emergentes por el Consorci AOC, con el resto de las obligaciones correspondientes a su condición de prestador de servicios de confianza cualificado. Esto incluye tanto las evaluaciones periódicas y planificadas, como las inspecciones que puedan sobrevenir.

Más concretamente: el adjudicatario deberá someterse a las auditorías de cumplimiento que faciliten los reconocimientos de los certificados emitidos. También deberá someterse, en su caso, a las inspecciones que el Supervisor Nacional de acuerdo con EIDAS requiera, sean rutinarias o extraordinarias. Sin costes emergentes para el Consorci AOC, dado que estos conceptos están incluidos en los servicios que prestará el adjudicatario.

6.4.13 Servicio de Mantenimiento Evolutivo

Al tratarse de un servicio alojado por el adjudicatario, el mismo incluirá, dentro del precio de adjudicación del contrato, y durante toda la vigencia de este, un servicio de mantenimiento evolutivo por adecuaciones del servicio. La estimación de las dedicaciones a las que se destinará este servicio se describe en el punto "6.4.13.5 evolutivo a continuación.

El alcance de este mantenimiento será el código de la entidad de registro (T-CAT e idCAT), con la funcionalidad descrita en los puntos "6.3.4 El Servicio de Certificación Digital del sector público catalán (T-CAT)y "6.3.5 El Servicio de Certificación Digital para la ciudadanía (idCAT certificado)así como los datos de los perfiles de certificados y las personalizaciones del producto de PKI actual descritos en el punto "6.3.2 Catálogo de certificados del Consorci AOC y "6.3.3 Explotación de la Jerarquía de los Servicios Públicos de Certificación de Cataluña ", respectivamente. Esta información se encuentra y custodia al gestor de código GIT del Consorci AOC y se pondrá a disposición del adjudicatario en fase de transición para su revisión, mantenimiento y evolución a lo largo de toda la vigencia del contrato.

La tipología de cambios y adecuaciones a aplicar se definen en los subpuntos a continuación del presente. La metodología que aplicar se define a continuación en el punto "6.4.13.1 Metodología". Toda la gestión de estos cambios e intercambios de documentos relacionados se hará a través de la herramienta JIRA del Consorci AOC.

Los acuerdos de nivel de servicio aplicables a las solicitudes de Servicio de mantenimiento evolutivo se definen en el punto "6.5.3 ANS de los Servicios de Programación ".

Para todas las situaciones de adecuación del servicio se deberán cumplir los siguientes requisitos:

- Previa a la aplicación de la actualización del servicio, el adjudicatario se compromete a realizar una copia de seguridad de todos los datos, evitando la pérdida de información.
- Antes de ejecutar la actualización del servicio en Producción, será necesario disponer de la conformidad del Consorci AOC mediante un ticket en la herramienta de gestión de cambios (JIRA). En este ticket se confirmarán los puntos de control definidos en los

puntos sucesivos, así como la fecha y hora de cuándo será realizada la instalación de la actualización.
- Las actualizaciones del servicio tendrán que ser realizadas en la ventana temporal indicada por el Consorci AOC. En general, en el entorno de Producción los miércoles a partir de las 15:00 y en el entorno de Preproducción los jueves a partir de las 10:00.
- Si se produjera una bajada en el rendimiento del servicio como consecuencia de la puesta en marcha de algún cambio, el adjudicatario deberá tratarlo como un error del servicio.

6.4.13.1 Metodología

La propuesta metodológica debe prever como mínimo:

6.4.13.1.1 Toma de requerimientos

El objetivo de esta fase es que el adjudicatario disponga de la lista de todos los requerimientos a satisfacer con el fin de llevar a cabo el evolutivo propuesto.

El tipo de requerimientos a satisfacer podrá ser de diversa índole. Los requerimientos más relevantes son:

- Requerimientos funcionales: tienen que ver con las funcionalidades que se desea incorporar o modificar en la aplicación.
- Requerimientos técnicos: tienen que ver con posibles requerimientos de carácter tecnológico; por ejemplo, quizás para conseguir lo evolutivo hay que utilizar una versión determinada de una librería de un tercero. Otro caso, puede ser que se marque como requerimiento que una consulta en base de datos hay que hacerla sobre una tecnología determinada (quizás sobre MySQL).
- Requerimientos de calendario: tienen que ver con plazos de entrega del evolutivo.
- Requerimientos de contexto: tienen que ver con la importancia que pueda tener el evolutivo, el posible impacto sobre los clientes, la prioridad de lo evolutivo respecto al resto de solicitudes en curso y/o previamente planificadas, etc.
- Requerimientos de Seguridad: incorporar todos los controles de seguridad que, por el tipo de información tratada, debe incorporar el evolutivo

Será responsabilidad del adjudicatario velar y preocuparse de recaudar todos y cada uno de los requerimientos que afectan a la solicitud de evolutivo.

Con el fin de facilitar este trabajo se llevará a cabo las siguientes acciones:

- Se hará llegar al adjudicatario un documento, lo llamaremos **ficha de inicio de evolutivo**, con una descripción lo más detallada posible de lo evolutivo que se desea. Este documento será consensuado por ambas partes.
- El adjudicatario revisará con detenimiento este documento y gestionará todas las dudas que surjan hasta obtener todos los requerimientos solicitados. Si bien puede haber varias reuniones a tal efecto se valorará que el adjudicatario obtenga los requerimientos con las mínimas reuniones posibles.
- Resultado del ejercicio anterior el adjudicatario elaborará un documento, lo llamaremos **"Documento de requerimientos"**, donde se recojan todos los requerimientos para abordar lo evolutivo, agrupados según la tipología descrita anteriormente.
- El Consorci AOC revisará este documento y se gestionarán los cambios pertinentes hasta su formalización.

6.4.13.1.2 Fase de preanálisis

El objetivo de esta fase es obtener una estimación del impacto, tanto económico como técnico, del evolutivo deseado.

En base al "Documento de requerimientos", el adjudicatario procederá a hacer un preanálisis de los cambios que implicaría realizar a la aplicación con el fin de conseguir el evolutivo deseado.

Del resultado de este ejercicio se realizará otro documento, **"Documento de preanálisis"**, el cual contendrá como mínimo la siguiente información:

- Descripción del preanálisis.
- Descripción de la solución propuesta: descripción del diseño técnico, en líneas generales, que se seguiría.
    - En caso de que el adjudicatario vea varias alternativas, explicarlas e indicar las ventajas e inconvenientes de cada una.
- Estimación del coste en horas que implicará el evolutivo. Incluirá la suma de la estimación de las horas de dedicación de los recursos humanos que el adjudicatario ha propuesto para la prestación del servicio que será necesario para realizar el evolutivo...
- Calendario con la planificación estimada del proyecto. A pesar de estar en una fase de preanálisis el adjudicatario deberá hacer el esfuerzo de elaborar un calendario, lo más cuidadoso posible, con la planificación del proyecto. Como mínimo, contendrá la información referente a la fase de análisis, diseño, construcción del sistema, e implantación y aceptación.

6.4.13.1.3 Fase de análisis

El objetivo de esta fase es realizar un análisis del cambio evolutivo a realizar. Hay que asegurar que la solución adoptada cumple todos y cada uno de los requerimientos recogidos en el documento de requerimientos, por lo que será imprescindible la aprobación del documento de preanálisis antes de iniciar esta fase.

El adjudicatario deberá realizar un análisis exhaustivo, de como mínimo, los siguientes ítems:

- Análisis funcional y técnico
- Definición de las Interfaces de usuario
- Definición de las medidas de seguridad
- Descripción de pruebas de validación: hay que describir las pruebas que se llevarán a cabo con el fin de validar el cambio evolutivo. Como mínimo, habrá que detallar el siguiente tipo de pruebas a realizar:
    - Pruebas unitarias: consiste en pruebas realizadas a nivel unitario (pe. sobre una única clase). La finalidad es detectar posibles mal funcionamiento de una clase o componente.
    - Pruebas de integración: consiste en pruebas de interacción entre clases y/o componentes. Consisten en garantizar la correcta integración de todos los componentes y clases del proyecto.
    - Pruebas funcionales: el objetivo de estas pruebas es garantizar que las funcionalidades de lo evolutivo tienen el comportamiento esperado. Hay que describir todas las pruebas funcionales que garanticen haber testeado todas las funcionalidades de lo evolutivo. También hay que definir pruebas para testear la aplicación ante un mal uso del usuario, y asegurar que el control de errores de la aplicación es correcto.

- Pruebas de rendimiento, en su caso.
- Pruebas de seguridad: uso de herramientas de análisis dinámico (OWASP) y análisis estático para la identificación de vulnerabilidades de seguridad en el código.
- Pruebas de regresión: el objetivo es garantizar que las funcionalidades existentes antes de hacer lo evolutivo siguen funcionando correctamente.

Como resultado del ejercicio anterior el adjudicatario elaborará un documento, lo llamaremos "**Documento de análisis funcional"**.

6.4.13.1.4 Fase de diseño

El objetivo de la fase de diseño es detallar el diseño técnico que se utilizará con el fin de desarrollar el evolutivo deseado.

- Las tareas que comportará esta fase son:
- Definición de la Arquitectura del Sistema
- Diseño técnico
- Especificación Técnica de Planificación de Pruebas

Como resultado del ejercicio anterior el adjudicatario elaborará un documento, lo llamaremos "Documento de diseño".

6.4.13.1.5 Fase de construcción del sistema

Las tareas que comportará esta fase son:

- Generación del código de los diversos componentes (p.e. clases): esto es programar/tocar todo el código necesario. Será necesario que todo el código esté comentado con detalle, por medio del ***"javadocs"***.
- Ejecución de pruebas unitarias
- Ejecución de pruebas de integración
- Ejecución de pruebas funcionales y de regresión.
- Ejecución de pruebas de rendimiento, en su caso.
- Ejecución de análisis dinámico y estático de seguridad.
- Elaboración de documentación: puede variar según lo evolutivo, pero generalmente se pedirá un manual de usuario.
- Definición de la formación (si es necesario)

Como resultado del ejercicio anterior el adjudicatario elaborará un documento, lo llamaremos "**Documento de plan de pruebas**", el cual contendrá todas las pruebas definidas en la fase de análisis con el estado de la prueba (superada o no superada). También se indicará el porcentaje entre las pruebas superadas respecto a las totales.

El Consorci AOC, o en quien delegue, podrá ejecutar cualquier tipo de análisis (dinámico, estático) que considere oportuno en cualquier momento para determinar si el nivel de seguridad del evolutivo cumple los requisitos de seguridad previo el paso a producción. En estos casos el adjudicatario deberá proveer de un usuario de prueba para la completa ejecución de los análisis.

Como mínimo, se realizará una sesión conjunta entre el personal del adjudicatario y el Consorci AOC para verificar que el plan de pruebas está al 100% correcto. En caso de que después de la sesión todavía haya pruebas de validación no superadas habrá que volver a

planificar otra sesión. Este proceso se iterará hasta que el 100% de las pruebas sea satisfactorio.

Para dar por cerrada esta fase, el adjudicatario deberá entregar la siguiente documentación:

- Entrega de todo código fuente y todos los componentes necesarios para implantar el evolutivo . Será necesario que el código esté comentado con detalle, por medio del ***"javadocs".***
- Entrega del compilable.
- "Guía de implantación del cambio": este documento contendrá el detalle de todas y cada una de las instrucciones técnicas que hay que ejecutar con el fin de implantar el evolutivo en cuestión.

6.4.13.1.6 Fase de implantación y aceptación

En base a las entregas de la fase anterior se procederá a realizar la implantación del evolutivo sobre los diferentes entornos. En primer término, en el entorno de desarrollo. Procederá a realizar la ejecución del plan de pruebas. Caso satisfactorio procederá a promocionar el cambio en el entorno de preproducción y posteriormente al de producción.

En caso de que en este proceso los resultados obtenidos no sean los esperados (es decir, los que se obtuvieron en el entorno de desarrollo del adjudicatario) el adjudicatario deberá dar el apoyo necesario, si es necesario presencial, para solventarlo.

Por ejemplo, habrá que corregir todas las vulnerabilidades de seguridad identificadas para cumplir con los umbrales fijados por el Consorci AOC. Cuando se superen estos umbrales de aceptación, el evolutivo podrá promocionarse a producción.

Una vez se haya realizado la ejecución del plan de pruebas con el 100% de las pruebas funcionando en el entorno de preproducción y producción se dará el proyecto por cerrado. A partir de ese instante entrará en vigor el periodo de garantía del evolutivo.

A partir de este momento ya debe entrar en vigor la etapa de apoyo, es responsabilidad del adjudicatario realizar las tareas necesarias de traspaso, formación y documentación de proyecto, de operación, y procedimental para que los nuevos desarrollos ya puedan ser objeto del servicio de apoyo 24x7.

6.4.13.2 Mantenimiento correctivo

Actualmente, el software desplegado demanda unos servicios de evolución y personalización.

Estos servicios se dedican al mantenimiento evolutivo periódico y a la resolución de incidencias derivadas del día a día de las aplicaciones asociadas a la SCD. Incluyen tareas como:

- Diagnóstico de problemas e incidencias derivadas de datos incorrectos cargados al sistema y que generan problemas en el tratamiento de estas.
- Tercer nivel de resolución de incidencias.
- Mejoras menores de gestión de la SCD.
- Apoyo a la prestación y seguimiento del servicio.
- Apoyo a integraciones de clientes y entidades de registro.
- Otras peticiones

El servicio de mantenimiento correctivo incluirá la resolución de aquellos errores de los componentes tecnológicos de la solución y el posible mal funcionamiento que hayan sido construidos por el licitador que haya resultado adjudicatario y que formen parte de la solución.

6.4.13.3 Mantenimiento técnico – legal

El servicio de mantenimiento técnico-legal incluirá el mantenimiento normativo que actualice la versión de la plataforma para que se cumplan con los requisitos legales. El adjudicatario deberá garantizar que la solución aportada se mantenga conforme a las normas y especificaciones técnicas sobre la materia objeto del contrato definidas en el punto 3 sobre el MARCO NORMATIVO y elaboradas por las organizaciones y organismos de normalización europeos, en particular por el Comité Europeo de Normalización (CEN) y el Instituto Europeo de Normas de Telecomunicación (ETSI), así como la Organización Internacional de Normalización (ISO) y la Unión Internacional de Telecomunicaciones (UIT).

Las prestaciones incluidas en el ámbito y el importe de los servicios recurrentes, en referencia a este aspecto, deberán incluir como mínimo:

- La actualización de versiones que incluyan modificaciones y/o ampliaciones obligatorias de los protocolos publicados y aprobados por los foros citados anteriormente.
- Realizar las adaptaciones necesarias en el servicio, a efectos de cumplimiento de la normativa.
- Hacer una propuesta de cambios, en caso de ser necesario por modificaciones normativas, en relación con los flujos de facturación electrónica definidos inicialmente, garantizando en todo momento que los mismos se encuentren de acuerdo con la normativa.
- En todo caso, toda modificación derivada de un cambio normativo debe estar implementada en un plazo que asegure el alineamiento con la legislación aplicable.
- La actualización de versiones que resulten de cambios introducidos por problemas de interoperabilidad con otros fabricantes (Microsoft, Mozilla, Java, Google, Apple)
- La actualización de versiones debidas al mantenimiento correctivo del software.
- Realizar las explicaciones y aclaraciones referentes a estas actualizaciones, mediante la herramienta de gestión de evolutivos (JIRA).

6.4.13.4 Mantenimiento evolutivo

El servicio de mantenimiento evolutivo incluirá aquellas modificaciones solicitadas por el Consorci AOC, al margen de las contempladas anteriormente en los puntos "6.4.13.2 correctivo y "6.4.13.3 Mantenimiento técnico – legal".

6.4.13.5 Tareas previstas en el ámbito del mantenimiento evolutivo

Las tareas que se realizarán dentro del alcance de este Servicio de Mantenimiento Evolutivo se determinan en función de la demanda de los usuarios de los servicios, de los responsables de estos o de las diferentes incidencias que tienen lugar a lo largo de la duración del contrato y que generan necesidades de mejora. En todo caso, siempre tendrán que tener encaje en las tipologías de tareas los puntos “6.4.13.2 Mantenimiento correctivo”, “6.4.13.3 legal y "6.4.13.4 Mantenimiento evolutivo”. En base a los periodos anteriores y con las nuevas demandas previstas en el momento de redacción de este documento, se estiman estas tareas y dedicaciones según cada tipo de tarea en el pliego de cláusulas administrativas.

Las tareas del tipo "Mantenimiento correctivo" y "Mantenimiento técnico - legal", en caso de que vengan derivadas de incidencias o adecuaciones técnicas-legales de obligado cumplimiento por la prestación del servicio, serán asumidas por el adjudicatario y, por tanto, deben estar previstas en el importe a tanto alzado del contrato.

6.5 Acuerdos de nivel de servicio

El funcionamiento de los servicios objeto de este lote estará sujeto a un sistema de control de calidad ejercido por el Consorci AOC, siguiendo los Acuerdos de nivel de servicio descritos y cuantificados en este apartado. En todos los casos satisfacen o exceden (por la naturaleza del servicio) los ANS definidos en las Condiciones generales de prestación de los Servicios y Condiciones de prestación específicas del Servicio de Certificación Digital del Consorci AOC (publicadas en https://www.aoc.cat/condicions-prestacio-serveis-aoc/).

A continuación se definen los ámbitos e indicadores por los Acuerdos de Nivel de Servicios (ANS) aplicables al presente lote :

- ANS de Explotación del Servicio:
  - Indicadores de cumplimiento de los niveles de servicio recogidos en las Declaraciones de Prácticas de Certificación[1] que aplican a cada Entidad de Certificación en los siguientes ámbitos:
    - Publicación de información y directorio de certificados de las EC's
    - Procedimientos de Identificación y autenticación previos a la emisión de certificados
    - Cumplimiento de los procesos relativos a la operación del ciclo de vida de los certificados (p.ej. publicación de la CRL).
  - ANS de emisión y gestión de los certificados:
    - Plazos de entrega en el servicio de emisión y renovación de T-CAT por los dos niveles (ordinario y urgente).
    - Observado con herramienta de ticketing/JIRA al cloud o a partir de trazas del sistema de emisión.
  - ANS de disponibilidad:
    - Disponibilidad continuada 24x7 de los servicios web
    - Nivel de disponibilidad superior al 99%.
    - Observado con ISM y splunk, o herramienta equivalente.
  - ANS de capacidad :
    - En transacciones por segundo (tps) por los servicios web de OCSP, CRL y descarga de los certificados de la jerarquía (claves públicas).
    - Tiempo de respuesta por debajo de 3 segundos en el 95% de los casos.
    - Observado con splunk, o herramienta equivalente.
  - ANS de calidad:
    - Auditorías trimestrales del 3% de las solicitudes de emisión y gestión de certificados.
    - Evolución de las CRLs
    - Observado con auditoría interna.

[1]Las Declaraciones de Prácticas de Certificación de las ECs del Consorci AOC se encuentran publicadas en: https://epscd.aoc.cat/regulacio

- ANS de Continuidad del Servicio : Indicadores relativos a la gestión del plan de contingencia, tal como se describen en "6.4.11 La gestión de la continuidad y la disponibilidad"

- ANS de los servicios relacionados:
  - Servicio de soporte a usuarios
  - Servicio de facturación
  - Servicio de formación a operadores de las ER

- ANS adecuaciones/evolutivos (incluye doc. jurídica y FFLL, etc.)

La medida de los ANS se hará con herramientas de AOC o provistas por el adjudicatario para la monitorización continua (p.ej. herramienta ISM para el caso de la disponibilidad) a partir de transacciones automáticas o interacciones humanas simuladas.

Los informes de Seguimiento requeridos (punto 6.6) incluirán los valores de estos indicadores definidos por el período correspondiente.

Se prevén penalidades por incumplimiento de estos ANS en el Pliego de Cláusulas Administrativas.

6.5.1 Modelo de medida del nivel de servicio

Con el fin de disponer de la información necesaria para una gestión y gobernamiento homogéneo del Servicio de Certificación, en los puntos sucesivos se define un Modelo de medida del nivel de servicio mínimo que debe permitir la valoración de los Acuerdos de los Niveles de Servicio (ANS) y su mejora continua.

El Modelo de Medida del Nivel de Servicio estructura un conjunto de indicadores, organizados de forma jerárquica, que permiten medir los diferentes aspectos de un servicio. Entre ellos (de inferior a superior):

- Métricas. Las métricas serán medidas base del recuento de datos operativos. Pueden ser meramente informativas o afectar a uno o varios de los indicadores de medida.

- Indicadores de medida (IM). Son indicadores calculados a partir de los valores de varias métricas. Un indicador de medida puede afectar a uno o más indicadores de rendimiento.

- Indicadores de rendimiento (IR). Agrupan diferentes indicadores de medida e informan sobre determinados aspectos que componen el servicio. Un indicador de rendimiento sólo puede afectar a un indicador objetivo.

- Indicadores objetivo (IO). Agrupan diferentes indicadores de rendimiento relacionados con un ámbito específico del servicio. A priori se han definido por todos los servicios los siguientes indicadores objetivo:
  a. Coste
  b. Tiempo
  c. Recursos
  d. Calidad
  e. Alcance

- Indicador de nivel de servicio (NS). Este indicador mide de forma global el nivel de desempeño del servicio aprovisionado, en base a los indicadores objetivo.

El Modelo de medida del nivel de servicio se implantará de forma progresiva a lo largo de la ejecución del contrato. En el momento inicial de su implantación, se definirán únicamente las Métricas y los Indicadores de Medida (IM). Será sobre estas dos tipologías de indicadores sobre las que se realizará la medida del cumplimiento de los ANS de los servicios prestados, y cuando proceda, la aplicación de las penalidades asociadas a su incumplimiento.

A lo largo del contrato, el Consorci AOC definirá y consensuará con los proveedores la relación jerárquica de los Indicadores de Medida (IM) definidos en el modelo, respecto al resto de niveles de indicadores (Indicadores de rendimiento [IR] e Indicadores objetivo [IO]), con el fin de alcanzar la medida del Indicador de Nivel de Servicio (NS).

Los licitadores deberán describir en sus ofertas su propuesta de Modelo de medida del nivel de servicio.

6.5.1.1 Indicadores

Se definen indicadores mínimos para medir el nivel de servicio, de manera que el Consorci AOC pueda comprobar que se cumplen los niveles de servicio establecidos.

Estos indicadores hacen referencia a los ámbitos de cumplimiento indicados y deben permitir:

- Medir objetivos concretos del servicio
- Evaluar el grado de cumplimiento de los objetivos
- Tener una idea clara del impacto o importancia del incumplimiento del objetivo

Las características que definir por cada indicador serán:

- Criticidad: determina si el indicador de medida es o no crítico
- Fórmula de obtención/herramienta: fórmula a aplicar para el cálculo del valor del indicador de medida, identificando las variables que intervienen en el cálculo (métricas) y, en su caso, la referencia a la herramienta que permite la automatización y extracción de los datos.
- Umbrales de grado para la definición de los tramos: estos tramos permiten la obtención del indicador de medida. Estos umbrales de grado pueden tener asociados valores de mejora en el tiempo.

Es necesario que los licitadores describan a sus ofertas su propuesta inicial de indicadores para la medida del nivel de servicio a partir del mínimo propuesto en este apartado.

6.5.1.2 Fuentes de información para la obtención de los niveles de servicio

El Consorci AOC dispone de un sistema de información para el cálculo de los indicadores de nivel servicio. El proveedor deberá proporcionar al Consorci AOC los datos que requiera para este propósito.

A lo largo de la prestación del servicio, ante cualquier modificación de los indicadores y niveles de servicio con el objetivo de dar un mejor servicio; el Consorci AOC juntamente con el proveedor consensuarán y planificarán la introducción de los cambios correspondientes en el Modelo de medida del nivel de servicio.

Algunas de las causas que pueden conllevar estas modificaciones son: las variaciones de entorno tecnológico, de entorno funcional y de condiciones de negocio, los cambios de alcance y volumen, la evolución de las transformaciones, las innovaciones y las mejoras del servicio.

6.5.1.3 Aplicación de los acuerdos de nivel de servicio

Los Acuerdos de Nivel de Servicio definidos para cada ámbito del servicio serán de obligado cumplimiento a lo largo del contrato. Considerando los siguientes condicionantes:

- En la etapa de Transición de la operación del servicio, se aplicarán al adjudicatario los ANS definidos por este contrato a medida que vaya prestando de forma efectiva los diferentes servicios sobre los que aplican y siempre y cuando haya acuerdo mutuo entre el adjudicatario y el Consorci AOC.

- A lo largo de la fase de Transición de la operación, los órganos de gestión del servicio harán una revisión de las métricas e indicadores definidos en el pliego, con el fin de adaptarlos a las necesidades del servicio. Los ANS que resulten en la definición inicial y de las revisiones sucesivas serán aplicables en las fases de prestación ordinaria del servicio, adecuación y en la fase de Devolución.

- Los Acuerdos de Nivel de Servicio se podrán revisar y modificar semestralmente siempre y cuando haya acuerdo mutuo entre el adjudicatario y el Consorci AOC.

- Para el cálculo del nivel ofrecido por parte del adjudicatario se excluirán los incrementos de tiempo provocados por la actuación ineludible de una tercera parte (p.ej. Interrupciones sobre sistemas dependientes del Consorci AOC, apoyo a incidencias por parte de empresas terceras, entregas de informes por parte de un auditor, etc.).

6.5.2 ANS de Explotación del Servicio

Indicadores/valores de niveles de servicio recogidos en las Declaraciones de Prácticas de Certificación que aplican a cada Entidad de Certificación en los siguientes ámbitos derivados de las normas de negocio:

- Publicación de información y directorio de certificados de las Entidades de Certificación.
- Acuerdos de nivel de servicios relativos a los procedimientos de identificación y autenticación previos a la emisión de certificados
- Cumplimiento de los procedimientos relativos a la operación del ciclo de vida de los certificados.
- Revocación en caso de sospecha de mal uso en 24 horas de certificado SSL.
- Emisión de la CRL de la EC raíz cada 6 meses.
- Emisión del resto de CRLs cada 24 h, máximo 7 días de vigencia.

En general, son procesos de criticidad alta por el servicio y, por lo tanto, de seguimiento especial.

6.5.2.1 ANS del Servicio de emisión o cambio de estado de certificados T-CAT

El periodo de entrega de los certificados que emite la entidad de registro del Consorci AOC es de un máximo de 16 días laborables a partir de la fecha de llegada de la documentación correctamente cumplimentada y firmada, exceptuando para los certificados de seudónimo y representante que será un máximo de 20 días laborables. En el caso del servicio urgente el plazo será de cuatro días laborables y se limita a cinco peticiones por ente y semana. En el caso de los certificados de seudónimo y representando la urgencia sólo aplicará a renovaciones o en caso de pérdida, robo, etc.

Actualmente, el servicio ordinario de emisión y renovación de certificados T-CAT ofrecido por el Consorci AOC tiene el compromiso de entregar los certificados en el plazo de 16 días naturales, que se cuentan a partir de la recepción de la documentación correctamente cumplimentada y firmada.

Sin embargo, se pone a disposición de los usuarios un servicio de emisión y renovación urgente de certificados para todos aquellos que, por motivos de urgencia no puedan esperar al plazo ordinario de 16 días laborables. Dada la naturaleza del servicio, éste se limita a cinco certificados por ente y semana que se entregarán en el plazo de 4 días laborables, contados a partir de la recepción correcta de la solicitud.

Las ERs colaboradoras de los Consejos Comarcales garantizan un acuerdo de nivel de servicio que mejora el del Consorci AOC:

- Certificados ordinarios: en un máximo de 5 días laborables
- Certificados urgentes: un máximo de 2 días laborables

La medida y obtención se hará a través de herramientas de gestión de peticiones del Consorci AOC o, en su defecto, del adjudicatario. Estos deben reflejar el estado de la tramitación en cada momento de los envíos de certificados o solicitudes de cambios de estado. También se incluirán las peticiones de gestión de datos de entidades u operadores del sistema.

6.5.2.2 ANS de continuidad

Indicadores/valores de negocio RTO (Recovery Time Objective) y RPO (Recovery Point Objective) derivados del Plan de Continuidad del Servicio de Certificación Digital del Consorci AOC tal y como se describen en el documento de Análisis de Impacto en el negocio (en inglés BIA) en relación con los Servicios de emisión/gestión de certificados y los Servicios de Facturación (OCSP y CRL):

- Servicio de emisión/gestión de certificados
  - RTO: entre 24 y 4 h
  - RPO: entre 24 y 4 h.
- Servicios de validación:
  - RTO: entre 4 y 0 h
  - RPO: entre 4 y 0 h.

El cumplimiento de este ANS se observará a partir del resultado de las pruebas del Plan de Recuperación de Desastres (PRD) de periodicidad semestral y de las pruebas de recuperación de copias de seguridad trimestrales de acuerdo con la política de copias de seguridad definida en el marco normativo del Consorci AOC.

6.5.2.3 ANS de disponibilidad

La disponibilidad de los servicios web objeto de este contrato, de acuerdo con las condiciones generales de prestación de servicios del Consorci AOC y a la categorización de estos en el Plan de continuidad del Consorci AOC, debe ser continuada 24x7 y con estos niveles de disponibilidad :

- Servicios de emisión/gestión de certificados: 99 %
  - Web operadores idCAT y T-CAT
  - Conectores de carga y consulta de peticiones

- Servicios de validación: 99,9%
  - Publicación CRL
  - OCSP
  - Web de documentación jurídica

- Claves públicas.

Las excepciones al nivel de disponibilidad serán las actuaciones de operaciones planificadas e incidencias de terceros que puedan afectar al servicio.

Las herramientas para la observación de este ANS serán las propias del Consorci AOC (ISM) o una herramienta para el seguimiento de la disponibilidad tipo Splunk provista por el adjudicatario.

6.5.2.4 ANS de capacidad

El nivel de servicio mínimo de capacidad se cuantifica mediante los indicadores de usuarios concurrentes o transacciones por segundo y se definen estos valores por cada servicio:

- Servicios de emisión/gestión de certificados (usuarios concurrentes) :
  - Web operadores idCAT : 5
  - Web operadores T-CAT : 5
  - Conectores de carga y consulta de peticiones : 5

- Servicios de validación (transacciones por segundo) :
  - CRL :
    - Promedio día: 2
    - Picos máximos : 60
  - OCSP :
    - Promedio día: 45
    - Picos máximos : 200
  - Descarga de los certificados de jerarquía (Claves públicas) :
    - Promedio día: 1
    - Picos máximos : 200

El tiempo de respuesta deberá estar por debajo del umbral de los 3 segundos en el 95% de los casos.

La herramienta para la observación de este ANS será una herramienta para el seguimiento de la disponibilidad tipo Splunk provista por el adjudicatario.

6.5.2.5 ANS de calidad del servicio de emisión y gestión de certificados

El nivel de servicio mínimo de calidad de la prestación será:

- Por el servicio de emisión y gestión de certificados, se cuantifica en el 98% de prestación correcta y se obtendrá de la auditoría de las trazas del sistema y de la documentación generada en una muestra de entre el 3% y 5% de los certificados objeto de auditoría del lote de auditoría de las Entidades de Registro (lote 2 del presente contrato).
- Por la adecuación y correspondencia de los certificados emitidos en los perfiles definidos correspondientes a cada momento, cuantificado en un 98%, mediante la comparación con herramientas automáticas, sobre una muestra de entre el 3% y 5% de los certificados emitidos en cada periodo objeto de seguimiento. Se propone utilizar la herramienta certlent (https://github.com/awslabs/certlint) para la comparación automática.

6.5.2.6 ANS del Servicio de Apoyo

El adjudicatario, en la prestación el servicio de apoyo de 2º y 3º nivel deberá alinearse con el Consorci AOC para que éste pueda cumplir el ANS comprometido por su CAU. Este ANS es el que se especifica a continuación:

Las incidencias se catalogarán, según su criticidad, en las categorías que se describen a continuación:

- 0 (bloqueante): una incidencia se catalogará con criticidad bloqueando (0), si impide la utilización total de alguno de los servicios del Consorci AOC.
- 1 (alta): una incidencia se catalogará con criticidad alta (1) si impide la utilización de una parte concreta de alguno de los servicios del Consorci AOC y la afectación por el negocio es elevada
- 2 (media): una incidencia se catalogará con criticidad media (2) si impide la utilización de una parte concreta de alguno de los servicios del Consorci AOC, y la afectación por el negocio es relativamente baja
- 3 (baja): una incidencia se catalogará con criticidad baja (3) si no impide la utilización ni parcial ni total de alguno de los servicios del Consorci AOC

Se define el tiempo de respuesta de una incidencia como el número de horas que transcurren desde que el usuario comunica una incidencia al CAU y éste la acepta o bien la escala al nivel superior. La aceptación comportará la aprobación de proceder a resolver la incidencia, según los acuerdos de nivel de servicio establecidos.

El tiempo de respuesta máximo permitido de una incidencia dependerá del nivel de criticidad de la incidencia. En la siguiente tabla se muestran los tiempos de respuesta y los tiempos de resolución máximos permitidos en función del nivel de criticidad de la incidencia.

En la siguiente tabla se muestran los tiempos máximos permitidos por la resolución de una incidencia en función del nivel de criticidad:

Criticidad Incidencia	Tiempo de respuesta (horas)	Tiempo de resolución (horas)	Horario	% de resolución dentro del tiempo comprometido
0 Bloqueando	0,5	2	horario supervisado (24x7)	95 %
1 Alta	1	16	horario garantizado (de 8 a 15h)	95 %
2 Media	2	40	horario garantizado (de 8 a 15h)	95 %
3 Baja	4	64	horario garantizado (de 8 a 15h)	95 %

Para el cálculo del tiempo de resolución de una incidencia se excluirán los posibles incrementos de tiempo provocados por la intervención inevitable en el proceso de resolución por parte de terceros.

6.5.3 ANS de los Servicios de Programación

Las condiciones de ejecución relativas a los ANS que se definen en este apartado sobre los servicios de programación se encuentran en el punto "6.4.13.1sobre la metodología del mantenimiento evolutivo.

6.5.3.1 Acuerdos de nivel de servicio del desarrollo

Los niveles mínimos de prestación del servicio tendrán que ser:

- La fecha de entrega planificada es de cumplimiento obligatorio una vez cerrada y acordada la orden de trabajo. Un mínimo del 95 % de las peticiones acordadas con la dirección funcional del proyecto deberán ser entregadas y ser aceptadas por la dirección del proyecto en la fecha de entrega prevista.
- Porcentaje de evolutivos sin errores. Un mínimo del 95% de los evolutivos entregados dentro del plazo deben entregarse sin errores.
- Plan de pruebas de vulnerabilidades. Un mínimo del 98% de los evolutivos entregados deberán superar el plan de pruebas de vulnerabilidades sin errores.
- Plan de pruebas sin errores. Un mínimo del 98% de los evolutivos entregados deberán superar el plan de pruebas ejecutado por personal del Consorci AOC sin errores.

Excepcionalmente y con previo aviso, se podrá requerir la ejecución de desarrollos evolutivos urgentes que no seguirán el procedimiento previo de valoración y que deberán comenzarse en el mismo día o el día siguiente.

6.5.3.2 Requerimientos de nivel de servicio en el mantenimiento correctivo y resolución de incidencias

Resolución de incidencias sin errores:

- Porcentaje de la resolución de incidencias sin errores en el plazo.
  - Cálculo: (A/B)*100

    A: Número total de incidencias resueltas sin error en el plazo

    B: Total de incidencias resueltas en el plazo
- Nocturnidad: Mensual
- El porcentaje de incidencias sin error en el plazo establecido deberá ser como mínimo del 90%.
- El nivel ofrecido por quien resulte adjudicatario del servicio constituirá un Acuerdo de Nivel de Servicio (ANS), cuyo cumplimiento se medirá durante toda la duración de la prestación del servicio.

6.5.3.3 Tiempo de respuesta en el mantenimiento evolutivo

En relación con el servicio de mantenimiento evolutivo, se definen los siguientes tiempos con el fin de fijar un Acuerdo de Nivel de Servicio:

- Tiempo de toma de requerimientos: es el número de días laborables que transcurren desde que Consorci AOC entrega al adjudicatario el documento "**Ficha de inicio de evolutivo**" y el momento en que el adjudicatario entrega el "**Documento de requerimientos**".

Los días que no sea posible realizar las reuniones oportunas para hacer la toma de requerimientos por indisponibilidad del adjudicatario se tendrán en cuenta para hacer el cálculo de los tiempos de toma de requerimientos.

- Tiempo preanálisis: es el número de días laborables que transcurren desde que el Consorci AOC aprueba el "**Documento de requerimientos**" y el momento en que el adjudicatario entrega el "**Documento de preanálisis**".

En la siguiente tabla se muestran los tiempos descritos anteriormente máximos permitidos en función del nivel de prioridad:

Nivel de prioridad	ANS: tiempo máximo permitido prisa requerimientos (en días)	ANS: tiempo máximo permitido fase preanálisis (en días)
Urgente	1	2
Normal	5	7
Baja	10	10

6.5.3.4 Desviaciones en el mantenimiento evolutivo

En relación con el servicio de mantenimiento evolutivo, se define la desviación en la entrega de un evolutivo como el número de días laborables que transcurren desde la fecha acordada entre Consorci AOC y el adjudicatario para finalizar la fase de construcción y la fecha en la que finalmente finaliza esta fase.

La desviación en la entrega de un evolutivo no será superior al 10% de la estimación, realizada en la fase de preanálisis, del esfuerzo (coste en horas o días) necesario para realizar la fase de análisis, diseño y construcción del evolutivo. Por ejemplo, si la fecha acordada para finalizar la fase de construcción es el 14 de abril y el esfuerzo estimado de la fase de análisis, diseño y construcción es de 10 días laborables (80 horas), la desviación permitida será de 1 día (10% de 10 días), y por lo tanto, la fecha máxima permitida de entrega será el 15 de abril.

6.6 Seguimiento del servicio

El objetivo de este ámbito de seguimiento es garantizar la integración de la calidad, seguridad y continuidad, en todo el ciclo de vida, de los procesos, servicios y soluciones, mediante la prescripción, seguimiento, validación y verificación de la eficaz implantación de los controles definidos.

6.6.1 Gobernamiento y mejora del servicio

El adjudicatario es el responsable de generar y entregar los informes y métricas de reporting (en adelante información) que se determinan en el punto "6.5 servicio y que aplican a los diferentes ámbitos del gobernamiento del servicio objeto de este lote. Estos deben permitir al Consorci AOC gobernar, controlar y gestionar los servicios prestados por el adjudicatario, tanto desde una óptica individual, como transversal y global.

El formato y el contenido mínimo de la información a elaborar por el adjudicatario en todos los ámbitos de gobernamiento es el definido en el anexo "Anexo _1_Plantilla Informe Seguimiento".

El Consorci AOC podrá solicitar, durante la vigencia del contrato cambios en la estructura y contenido de la información para ajustarse a las necesidades de seguimiento de los servicios.

El adjudicatario deberá proporcionar al Consorci AOC, además de los informes periódicos de seguimientos de los ANS, la información (evidencias) con base en la que se hayan elaborado, para que el Consorci AOC la pueda incorporar a su herramienta de gestión.

El licitador propondrá los mecanismos necesarios para permitir al Consorci AOC comprobar que se mantienen los niveles de calidad esperados.

6.6.1.1 Gestión de incidencias y problemas

Se entiende para incidencia cualquier suceso que no forma parte de la operativa normal de un servicio y que provoca, o puede provocar, la interrupción, el mal funcionamiento o la degradación en la calidad del servicio.

El objetivo principal del proceso de gestión de incidencias es restaurar el normal funcionamiento del servicio tan pronto como sea posible, minimizando el impacto adverso sobre las operaciones de negocio/clientes y organización, asegurando que el servicio se mantenga en los mejores niveles posibles de calidad y disponibilidad.

El proceso soporta todos los servicios que el Consorci AOC presta al usuario dentro del alcance del pliego y por tanto su alcance es la resolución de todas las incidencias que puedan afectar a estos servicios.

Se entiende por problema cualquier causa subyacente, aún no identificada, de una serie de incidentes o de un incidente aislado de importancia significativa.

El objetivo principal de la Gestión de Problemas es minimizar el impacto negativo que tienen las incidencias sobre el negocio, y prevenir la recurrencia de incidencias relacionadas con estos errores. Para conseguir esta meta, la Gestión de Problemas llega hasta la causa a raíz de las incidencias y luego inicia acciones que corrigen la afectación de servicio.

El adjudicatario participará activamente en el proceso de Gestión de Problemas siendo el Responsable de todos los problemas que puedan salir de los servicios que está prestando al Consorci AOC.

Es responsabilidad del adjudicatario la aplicación y seguimiento de los procedimientos asociados a la gestión de problemas surgidos de los servicios que presta, así como el seguimiento y gestión del estado de estos hasta la corrección de la afectación de servicio.

Ante la detección de problemas graves y con impacto directo a negocio, el proveedor de servicio deberá notificar el problema al Jefe del servicio Consorci AOC.

El licitador describirá la metodología propuesta para atender:

- Registro de incidencias y problemas
- Clasificación y asignación
- Investigación y diagnosis
- Seguimiento y coordinación
- Resolución y recuperación
- Cierre de incidencias y problemas

6.6.2 Órganos de Gestión

6.6.2.1 Reuniones de Dirección.

Las reuniones de Dirección se realizarán con el objetivo de establecer un control y una visión estratégica y amplia sobre el desarrollo global del servicio.

Las reuniones podrán ser presenciales y/o virtuales. En el caso de las presenciales, pueden realizarse tanto en la sede del Consorci AOC, como de la empresa adjudicataria. En todo caso, es necesario que el adjudicatario disponga de los recursos necesarios en cualquiera de las modalidades de reunión previstas.

Las reuniones de dirección se convocarán trimestralmente, aunque a petición del Consorci AOC y en circunstancias concretas de afectación crítica del servicio, podrán ser convocadas en cualquier momento durante la vigencia del contrato, convocadas con una antelación mínima de 3 días laborables, según el calendario laboral aplicable al personal del Consorci AOC.

6.6.2.2 Reuniones de Seguimiento.

El gestor del servicio del adjudicatario y el Jefe del Servicio del SCD del Consorci AOC realizarán una reunión de seguimiento del servicio, que será periódica y como mínimo de carácter mensual, aunque a petición del Consorci AOC y en circunstancias concretas de afectación crítica del servicio, podrán ser convocadas en cualquier momento durante la vigencia del contrato, con una antelación mínima de 1 día laborable, según el calendario laboral aplicable al personal del Consorci AOC.

Las reuniones podrán ser presenciales y/o virtuales. En el caso de las presenciales, pueden realizarse tanto en la sede del Consorci AOC como de la empresa adjudicataria. En todo caso, es necesario que el adjudicatario disponga de los recursos necesarios en cualquiera de las modalidades de reunión previstas.

Esta reunión se hará antes del décimo día laborable (de lunes a viernes excepto festivos) de cada mes. En esta reunión se revisará el informe mensual, el funcionamiento de los procesos, se generarán propuestas de mejora del servicio y se hará un seguimiento de todo lo relacionado con la prestación. A título de ejemplo se indican algunos de los aspectos incluidos como posible contenido de la reunión:

- Evaluar la situación de ejecución del servicio objeto del contrato a partir del seguimiento de la evolución de los objetivos e indicadores formulados, así como el nivel de cumplimiento de los acuerdos de nivel de servicio que estén vinculados.
- Seguimiento de la seguridad y el cumplimiento normativo con la prescripción, seguimiento y verificación de la correcta implantación del modelo de seguridad de acuerdo con los requisitos enumerados en el punto "6.4.10 La gestión de la seguridad y el cumplimiento normativo ".
- Seguimiento de la continuidad y la disponibilidad con la prescripción, seguimiento y verificación de los requisitos, acuerdos de nivel de servicio y condiciones definidas en el presente lote.
- Revisar y poner en común las incidencias que se hayan producido en el mes inmediatamente anterior, ya sea en relación con la prestación efectiva del servicio como en relación con el modelo de gestión vinculado.
- Revisar y poner en común novedades, jornadas y/o documentación relevante para la ejecución del servicio, con el fin de generar una dinámica de participación que impacte de manera positiva en la gestión del conocimiento y sea aplicable a la propia prestación del servicio.

Antes de cada reunión de seguimiento y con la antelación establecida en el correspondiente acuerdo de nivel de servicio establecido el referente del servicio del adjudicatario pondrá a disposición del Jefe del Servicio del Consorci AOC el informe de seguimiento detallado propuesto en el "Anexo _1_Plantilla Informe Seguimiento" que incluye, como mínimo, información sobre:

- Estado de cumplimiento de las tareas en relación con las planificaciones realizadas y las posibles desviaciones que se hayan producido. Número de actuaciones realizadas de acuerdo con el objeto y alcance del lote.
- Mejoras aplicables al servicio de certificación digital.
- Información de cumplimientos sobre los acuerdos de nivel de servicio establecidos.

Se utilizará una herramienta de gestión del Consorci AOC que permitirá y facilitará la participación de los diferentes actores implicados en la ejecución del servicio. Esta herramienta se convierte en clave para mantener coordinados a todos los actores participantes, detectar las necesidades a cubrir, así como detectar mejoras tanto en la prestación del servicio como en el modelo de gestión vinculado. El referente del servicio es el principal responsable del mantenimiento de la herramienta de gestión del servicio y debe reflejar todos los cambios, actualizaciones, documentos, etc., con el máximo rigor posible, con el fin de tener un acceso inmediato a la información actualizada de la prestación del servicio y permitir una visión con el mayor detalle posible a los diferentes actores que participan en la gestión de este lote.

Durante la fase de Transición de la operación, la periodicidad y alcance de estos comités podrá ser modificada, y adicionalmente se establecerán unos comités específicos ejecutivos y de seguimiento, definidos en el apartado siguiente.

6.6.2.3 Modelo de relación en la fase de Transición de la operación

Con el objetivo de minimizar los riesgos que puedan ocasionar incidencias que afecten a la continuidad del servicio, el modelo de relación en las fases de Transición de la operación, del servicio será diferenciado pero coordinado con el modelo de relación del seguimiento del servicio definido previamente.

Se proponen los siguientes órganos de gestión adicionales:

Órgano de gestión	Principales actividades
Comité de planificación y estrategia transición	• Establecimiento y seguimiento del plan global de Transición.
Comité de Transición de la operación	• Interlocución, a los efectos de la coordinación de los planes y actividades de transferencia de servicios y conocimiento, seguimiento y coordinación del proceso de inventario. • Proposición de acciones relacionadas con la transición (fijación y cambio de prioridades, cambio de planes individuales, gestión de procesos y criterios de traspaso de servicios, gestión del riesgo, etc.).

La periodicidad de estos órganos será variable y se definirá al inicio de la prestación del servicio, siendo revisable en función de los planes y proyectos de transición.

Los mencionados órganos de gestión podrán designar los grupos de trabajo operativos que sean necesarios para desarrollar adecuadamente sus funciones.

6.6.2.3.1 Gobernamiento de la fase de Transición de la operación

El Gobierno de la fase de Transición de la operación tiene como finalidad el gobierno y la dirección de la planificación, la coordinación, el seguimiento, y la implantación de todos los procesos que conformarán esta fase de cara a la prestación del nuevo servicio de certificación digital por parte del adjudicatario.

La actuación del Responsable de transición del Consorci AOC será transversal a todas las estructuras organizativas que estén implicadas en los procesos relacionados con esta fase; asumiendo el liderazgo del proceso global de la transición de la operación y ejerciendo las responsabilidades de gobierno y control necesarias.

El Responsable de transición será quien fijará, en última instancia, el calendario de desarrollo de los diferentes planes, de acuerdo con el adjudicatario; con las necesidades y prioridades del Consorci AOC, y con el impacto en el Servicio de Certificación Digital y/o las interrelaciones entre los diferentes servicios tecnológicos que conforman el servicio de negocio.

En el ámbito operativo, el Responsable de transición asegurará, durante los diferentes procesos y actividades de las fases de Transición de la operación, la interlocución y la coordinación técnica y funcional del adjudicatario con el Consorci AOC.

El adjudicatario será responsable de la ejecución y el aseguramiento del avance según la planificación y el alcance marcado por el Responsable de transición de los procesos y actividades que deberá abordar. El adjudicatario reportará al Responsable de transición, quién será el único órgano de dirección y control de todo el plan de transición de la operación.

El adjudicatario será el responsable de identificar los posibles riesgos asociados a sus proyectos de transición de la operación; así como de analizarlos, y de proponer y ejecutar los planes de mitigación correspondientes; que reportará al Responsable de transición. Este realizará el seguimiento, evaluación, y gestión de estos riesgos, y asegurará su mitigación; tanto de los riesgos identificados individualmente en cada uno de los procesos y actividades de las fases, como de los riesgos globales de todo el plan, cuya identificación es responsabilidad del Responsable de transición.

El Responsable de transición gestionará los conflictos entre el Consorci AOC y el adjudicatario, que pudieran causar impactos en los procesos y actividades de estas fases.

El Responsable de transición asegurará la consecución de las tareas necesarias asociadas a la gestión del cambio relativa al proceso de transición de la operación. El adjudicatario será responsable de un plan de acompañamiento del cambio, y apoyará al Responsable de transición en este ámbito.

Los licitadores deben proponer la definición, planificación y alcance de los diferentes planes de transición del servicio objeto de este contrato en base a lo establecido en el marco normativo aplicable y, en concreto, el punto "6.8 Transición de la operación del servicio actual de acuerdo con los requisitos y condiciones mínimas allí definidos. El Consorci AOC realizará, dentro del ámbito de los procesos de estas fases, las acciones de control necesarias para verificar la consecución de las metas marcadas para estas fases. Estas evaluaciones se coordinarán mediante el comité de planificación y estrategia de transición.

El adjudicatario puede proponer herramientas para la gestión de la transición de la operación más allá de las definidas y requeridas en este pliego de prescripciones técnicas.

6.7 Devolución del servicio

El adjudicatario deberá garantizar que se pueda llevar a cabo la transferencia de la operación del servicio a un proveedor alternativo.

El adjudicatario deberá entregar al Consorci AOC el código fuente de los desarrollo realizados por sus servicios dentro del marco de este contrato (de interfaces de usuario y de otras personalizaciones). También deberá proveer la correspondiente documentación relativa a los desarrollos y control de versiones.

El adjudicatario deberá proveer las licencias de uso de la solución PKI aportada. En caso de que esto suponga un coste adicional sobre el precio del contrato, el licitador deberá desglosarlo en su oferta económica; de lo contrario, se entenderá que el precio de la oferta incluye la adquisición de las licencias necesarias para el funcionamiento de la solución más allá de la finalización del contrato.

El adjudicatario deberá proveer el hardware dedicado y las máquinas virtuales operativas, que sean necesarios para el funcionamiento de la solución más allá de la finalización del contrato. En caso de que esto suponga un coste adicional sobre el precio del contrato, el licitador deberá desglosarlo en su oferta económica; de lo contrario, se entenderá que el precio de la oferta del licitador incluye la adquisición del hardware dedicado necesario para el funcionamiento de la solución más allá de la finalización del contrato y que el coste de este se ha amortizado durante el periodo de vigencia del contrato.

El adjudicatario preparará y mantendrá actualizados manuales de operación detallados de los sistemas, que pondrá a disposición del Consorci AOC durante la fase de Devolución del servicio.

Debido a la naturaleza regulada de la prestación contractual, y en los términos fijados por la legislación vigente, el contratista queda obligado, sin coste adicional, a mantener operativos los siguientes servicios más allá del plazo fijado para la prestación contractual:

- Los certificados de autoridad de certificación y el resto de los certificados de infraestructura deben permanecer vigentes, sin que se pueda proceder a su revocación hasta la expiración de todos los certificados de usuarios y servicios finales que avalen – excepto por petición expresa del Consorci AOC.

- Los servicios de información de estado de certificados, en forma de lista de revocación de certificados (CRL) y servicio de consulta en línea de certificados (OCSP), deben permanecer operativos hasta la expiración de los certificados correspondientes, y durante un periodo de tres meses adicionales.

El adjudicatario también deberá aportar la total colaboración que sea necesaria para la devolución o transferencia del servicio a la Administración o al prestador que ésta determine, durante el plazo imprescindible, que no será superior a tres meses más allá del plazo fijado para la prestación contractual: salvo la falta de colaboración por el contratista o la aparición de factores imprevisibles, en caso de que este plazo quedará automáticamente ampliado hasta la total finalización de la devolución o transferencia.

6.8 Transición de la operación del servicio actual

Durante la fase de Transición de la operación del servicio actual, el adjudicatario pondrá en marcha su infraestructura y hará la transferencia de la operación de los sistemas que deberán apoyar a la PKI del Consorci AOC, de manera que, a la finalización de esta fase, la prestación efectiva del servicio de emisión de certificados del Consorci AOC la lleve a cabo, a todos los efectos, el adjudicatario.

Dado que el marco normativo aplicable rige en todo momento, incluso durante la reubicación física de las de los activos del Servicio de Certificación Digital a un nuevo CPD, el Consorci AOC, por tanto, debe asegurar que el acceso físico a los entornos seguros está limitado y autorizado correctamente, que el equipamiento está operado bajo el control de múltiples personas y que los accesos no autorizados serán detectados en todo momento.

Es por ello por lo que en caso de que el licitador, en su oferta, proponga un cambio en el personal de operación del servicio o un cambio de ubicación de los dispositivos que alojan las claves privadas de las entidades de certificación, será necesario que aporte en su oferta un plan de traspaso auditado por un tercero y que dé cumplimiento a la normativa aplicable. En concreto, el plan deberá dar respuesta a los requisitos de la Root Store Policy de Mozilla a la que está adherido el Servicio de Certificación Digital del Consorci AOC (https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/). Concretamente, en los apartados en relación con la transición de la operación del servicio actual, lo que se determina, en los puntos relativos al cambio de personal operador (8.2 Change in Operational Personnel) y cambio de ubicación segura (8.3 Change in Secure Location). Se incorporan aquí los requisitos más relevantes en relación con la transición de la operación derivados de las versiones vigentes en el momento de la redacción de este pliego a modo de ejemplo del cumplimiento que habrá que evidenciar, como mínimo:

- La revisión previa de los activos y documentación del Servicio para, en su caso, adecuarlos a los cambios derivados.
- La notificación a la comunidad Mozilla del plan de cambio.
- Completar el plan de traspaso presentado a la oferta y aprobado por el auditor correspondiente.
- Detener la emisión de certificados en la ubicación actual antes del cambio.
- Auditar el estado de los activos críticos (claves privadas) para confirmar que están listos para el traslado y para asegurar que las claves están bien protegidas en el origen.
- La ceremonia de transferencia debería estar registrada en vídeo y disponer de la presencia de un testigo auditor en todo momento durante el intercambio físico de los dispositivos criptográficos y las tarjetas de administración de estos.
- En la nueva ubicación habrá que también hacer una auditoría para confirmar que la transferencia ha sido satisfactoria, que la clave privada se ha mantenido protegida durante la transferencia y que las claves privadas pueden reanudar las emisiones. Este requisito se puede cumplir con una auditoría puntual en el tiempo que denote que los sistemas están apunto por la emisión (PITRA – Point-in-time Readiness Audit).
- Envío de las auditorías a la comunidad Mozilla.
- En caso de que haya algún problema durante el cambio, informarle a la comunidad Mozilla también.

El objetivo de estos pasos es evidenciar que el adjudicatario cumple con los requisitos derivados del marco normativo aplicable y, en concreto, con los requisitos derivados de la citada política del Mozilla/CCADB .

Tal y como establece el punto "6.4.12 Auditorías del Prestador de Servicios de Certificación Consorci AOC", el coste de la auditoría del proceso de traspaso debe estar incluida en los servicios que el adjudicatario debe ofrecer en el presente contrato.

El calendario y metas de seguimiento específico según establece el punto "6.6.2.3 operación y "6.6.2.3.1 operación serán:

- Para la fase de revisión de activos y documentación actual del Consorci AOC, el nuevo adjudicatario dispondrá de un plazo de 3 semanas.

- Como muy tarde a los 3 meses desde la adjudicación, se evaluará si es viable iniciar las actividades de las EC's del Consorci AOC a la nueva ubicación en base a los resultados obtenidos en los controles técnicos y de seguridad previstos a tal efecto.

La fecha límite para que el adjudicatario inicie la operación de los sistemas que actualmente apoyan el Servicio de Certificación Digital del Consorci AOC es el 1 de abril de 2020. Para facilitar esta transición, el Consorci AOC agotará el contrato vigente con el proveedor saliente. Se alienta, por tanto, al adjudicatario a aprovechar este marco contractual para asumir la operativa y el control del servicio con el apoyo del proveedor saliente.

En particular, en relación con el cumplimiento del Esquema Nacional de Seguridad, se requiere que el adjudicatario haya completado la auditoría de cumplimiento de acuerdo con los términos y alcance definidos en el punto "6.4.10 normativo de forma previa a la transición de la operación del servicio.

El adjudicatario comenzará a ingresar por los servicios bajo demanda con precio unitario, correspondientes a la emisión de certificados digitales, a partir del momento en que inicie esta prestación empleando la solución PKI aportada por él.

Durante la fase de Transición de la operación el adjudicatario deberá mantener la ANS de los servicios actuales por los servicios que se vayan transfiriendo.

7 Definiciones, acrónimos y enlaces de interés

7.1 Definiciones

DISPOSITIVO: Soporte donde se graban los certificados emitidos, por ejemplo, una tarjeta cripto-gráfica específica, un fichero PKCS#12 en un directorio, o una memoria USB. El sistema debe utilizar los diferentes dispositivos físicos vía interfaz PKCS#11.

ENS. Organismo con usuarios que necesitan y utilizan los certificados emitidos.

ENTIDAD DE REGISTRO. Oficina donde hay operadores del sistema. Una Entidad de Registro puede peticionar o ver certificados de uno o varios entes sobre los que está autorizado. Al mismo tiempo, puede tramitar certificados de una o varias Entidades de Certificación y de uno o varios perfiles de certificado de cada Entidad de Certificación. Cada Entidad de certificación tiene un tipo especial de Entidad de Registro (código 000) que puede tratar certificados de cualquier ente.

LOT. Conjunto de peticiones de certificación agrupadas bajo un mismo identificador y que permite realizar operaciones globales por todos sus elementos.

OPERADOR. Persona o software, identificado mediante un certificado digital, que puede acceder al sistema del SCD y realizar las funciones definidas por sus roles.

PERFIL DE CERTIFICADO. Certificado o conjunto de certificados que emite el sistema. En la definición del perfil se podrán especificar cosas como: certificados a emitir (por ejemplo firma y cifrado), datos necesarios para el certificado, datos de gestión (direcciones, etc.), datos para la personalización gráfica del soporte (fotografía, diseño, etc.), reglas de unicidad que aplican a los certificados, etc.
En caso de que un perfil genere más de un certificado, el sistema permitirá realizar las operaciones del ciclo de vida (revocación, suspensión, consulta, etc.) de manera conjunta y transparente desde el punto de vista de los operadores.
El sistema dispone de diferentes Entidades de Certificación que al mismo tiempo emiten diferentes perfiles cada una. Dentro del concepto perfil Cada perfil se puede generar sobre uno o varios dispositivos diferentes.

POSEEDOR DE CLAVES. Usuario titular del certificado y que será el responsable de su uso.

RESPONSABLE DE SERVICIO. Es el interlocutor y gestor principal ante el servicio por un ente.

ROL. Propiedad asociada a un Operador y que define las operaciones que puede hacer. Un operador puede tener más de un rol, siempre que estos no sean incompatibles.

SISTEMA ONLINE. Parte del sistema del SCD que permite generar certificados de manera completa a partir de los datos de la petición.

SISTEMA LOTES. Parte del sistema del SCD que permite generar los ficheros a partir del envío de información en forma de Lot al fabricante de tarjetas, En este esquema las tareas logísticas quedan repartidas entre el fabricante de tarjetas y la AOC. Este sistema sólo es aplicable a un conjunto reducido de certificados y perfiles, siempre en soporte tarjeta criptográfica.

DOCUMENTUM. Producto comercial de gestión documental

7.2 Acrónimos

ASCD. Automatización de la Solicitud de Certificados Digitales, módulo de EACAT
CRL. Certificate Revocation List
CRT. Fichero binario de certificado digital
CSR. Certificado Signing Request
EACAT. Extranet de las Administraciones Públicas Catalanas
EAPC. Escuela de Administración Pública de Cataluña
EC. Entidad de Certificación
EC-ACC. Entidad de certificación Agencia Catalana de Certificación
EC-AL. Entidad de certificación Administración Local
EC-GENCAT. Entidad de certificación GENCAT
EC-IDCAT. Entidad de certificación idCAT
EC-PARLAMENTO. Entidad de certificación Parlamento
EC-SAFP. Entidad de certificación Secretaría de Administración y Función Pública
EC-UR Entidad de certificación Universidades e Investigación
EC-URV. Entidad de certificación Universidad Rovira i Virgili
eIDAS / ReIDAS. Electronic Identification and Signature (Electronic Trust Services), de la Comisión Europea
ER. Entidad de Registro
ERC. Entidad de Registro Colaboradora
ERV. Entidad de Registro Virtual
GEDA-e. Gestor Documental interno del Consorci AOC para el alojamiento de la documentación de la SCD
GEXAM. Gestión de Exámenes, aplicación de la EAPC
LDAP. Directorio de datos (Lightweight Directory Access Protocol)
LRA. Local Registration Authority
MINETUR. Ministerio de Industria, Energía y Turismo
MUX. Servicio de Registro Administrativo Unificado del Consorci AOC
OCSP. Servicio de Consulta de Estado de Certificados en línea (Online Certificate Status Protocol)
PSC. Prestador de Servicios de Certificación
SCD. Servicio de Certificación Digital
SGD. Sistema de Gestión Documental
SOCEX. Servicio de Obtención del Certificado de Cifrado. Conector del SCD del Consorci AOC
T-CAT. Nombre comercial de la familia de certificados personales y de dispositivo destinados al sector público catalán
T-CAT P. Certificado personal de trabajador público en formato software

7.3 Enlaces de interés

Documentación Reguladora del Servicio de Certificación digital del Consorci AOC : https://epscd.aoc.cat/regulacio

Portal de apoyo Servicio T-CAT : https://suport-tcat.aoc.cat/hc/ca
Portal de soporte Servicio idCAT : https://suport-idcat.aoc.cat/hc/ca
Portal de apoyo Servicio ER T-CAT : https://suport-ertcat.aoc.cat/hc/ca
Portal de soporte Servicio ER idCAT : https://suport-eridcat.aoc.cat/hc/ca

8 ANEXOS

- Annex_1_ Plantilla Informe Seguiment.pdf
- Annex_2_1_ChekingAuditoria_ER_T-CAT_V6_2024.pdf
- Annex_2_2_ChekingAuditoria_ER_T-idCAT_presencial_2024.pdf
- Annex_3_AutoavaluacióEntitatsRegistre_virtual_definitiu_2024.pdf
- Annex_4_D1121 AuditoriaConformitatSCD_definitiu_2024.pdf
- Annex_5_ModelInformeAuditoriaConformitatV1_2024.pdf
- Annex_6_volumetries_emissions_2024.pdf
- Annex_7_llistat_ER_T_CAT_2024.pdf
- Annex_8_llistat_er_idcat_2024.pdf
- Annex_9_Resum_caracteristiques_ERs_TCAT.pdf
- Annex_10_Descripcio_plataforma_SCD.pdf
- Annex_11_Actius SCD-AOC.pdf
- Annex_12_ Inventari_ER.pdf

Consorci
Administració Oberta
de Catalunya

Informe de seguimiento del Servicio nombre_sistema mes año

Generalitat
de Catalunya

LOCALRET

Realizado por:Responsable de Servicio X
versión:
fecha: 09/07/2024
archivo:Documento1

Index

1 Seguimiento de Servicio

1.1 visión general

1.1.1 Cuadro de situación servicio

tipología	Pendientes inicio periodo	en periodo		Pendientes fin período
		entradas	cerradas	
incidencia	14	14	16	12
Petición a medida	10	8	12	3
petición estándar	21	10	17	14
total	**36**	**26**	**34**	**28**

1.1.2 Cuadro de incidencias por tipología (si los hay definidas)

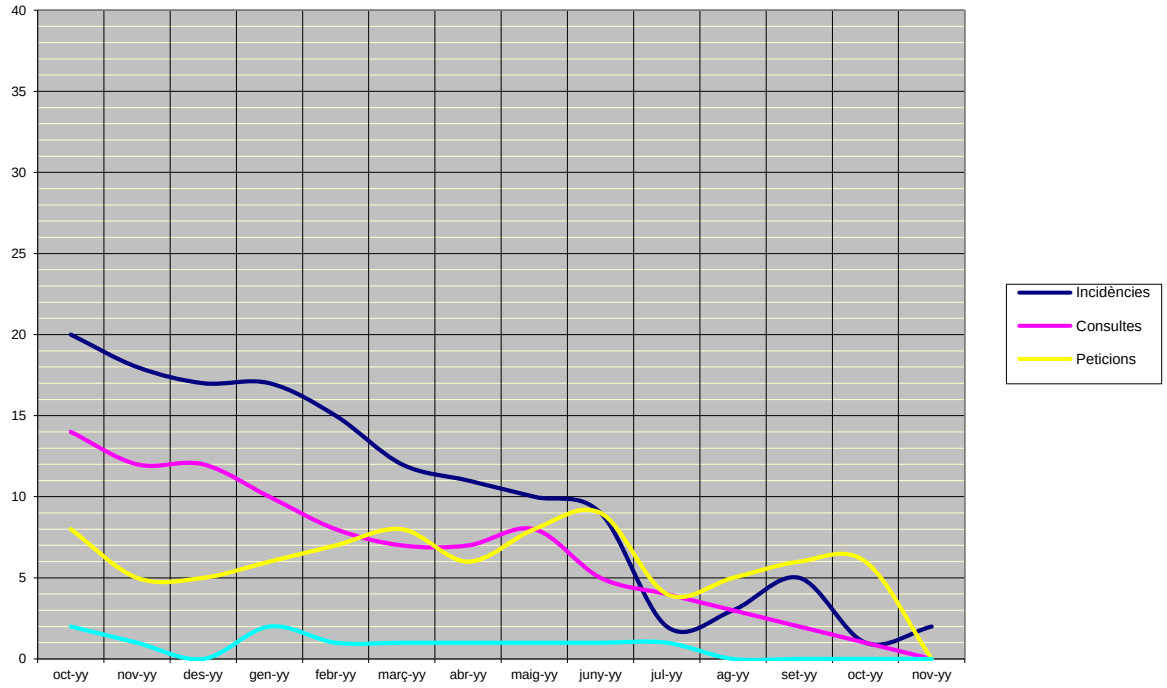
tipología	Pendientes inicio periodo	en periodo		Pendientes fin período
		entradas	cerradas	
tipo 1	1	2	1	2
tipo 2	14	14	16	12
tipo 3	10	8	12	6
total	**25**	**24**	**29**	**20**

1.1.3 Cuadro de incidencias por prioridad

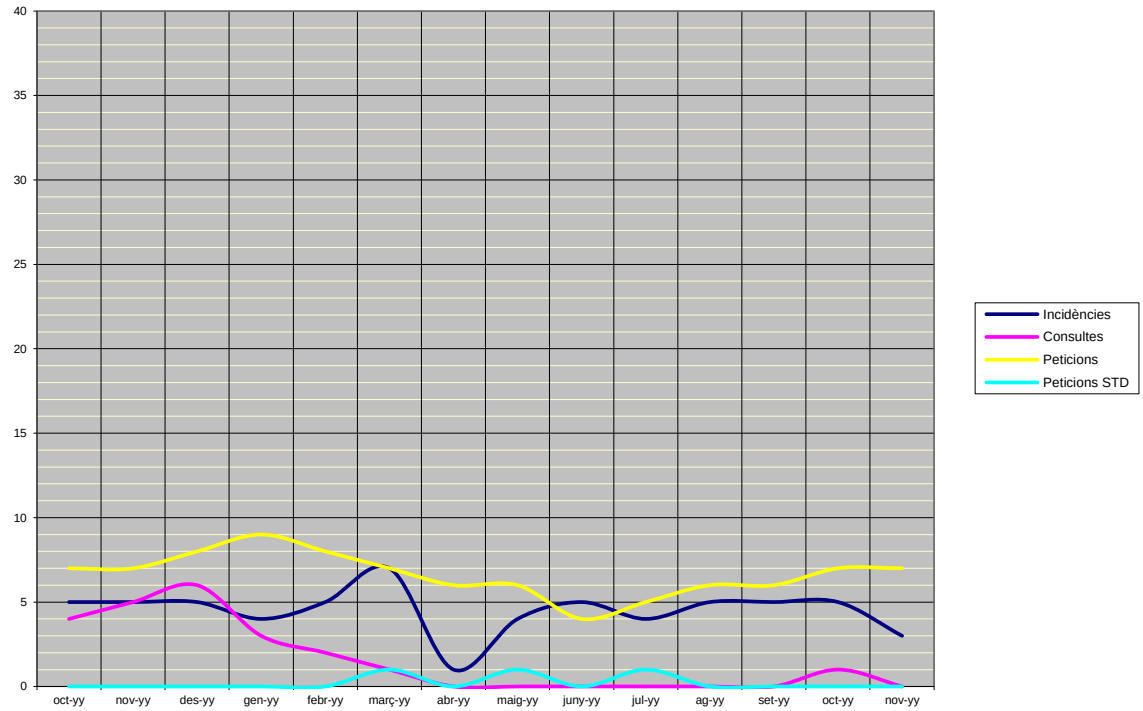
prioridad	Pendientes inicio periodo	en periodo		Pendientes fin período
		entradas	cerradas	
crítica	0	0	0	0
alta	0	0	0	0
importante	1	2	1	2
baja	10	8	12	6
total	**25**	**24**	**29**	**20**

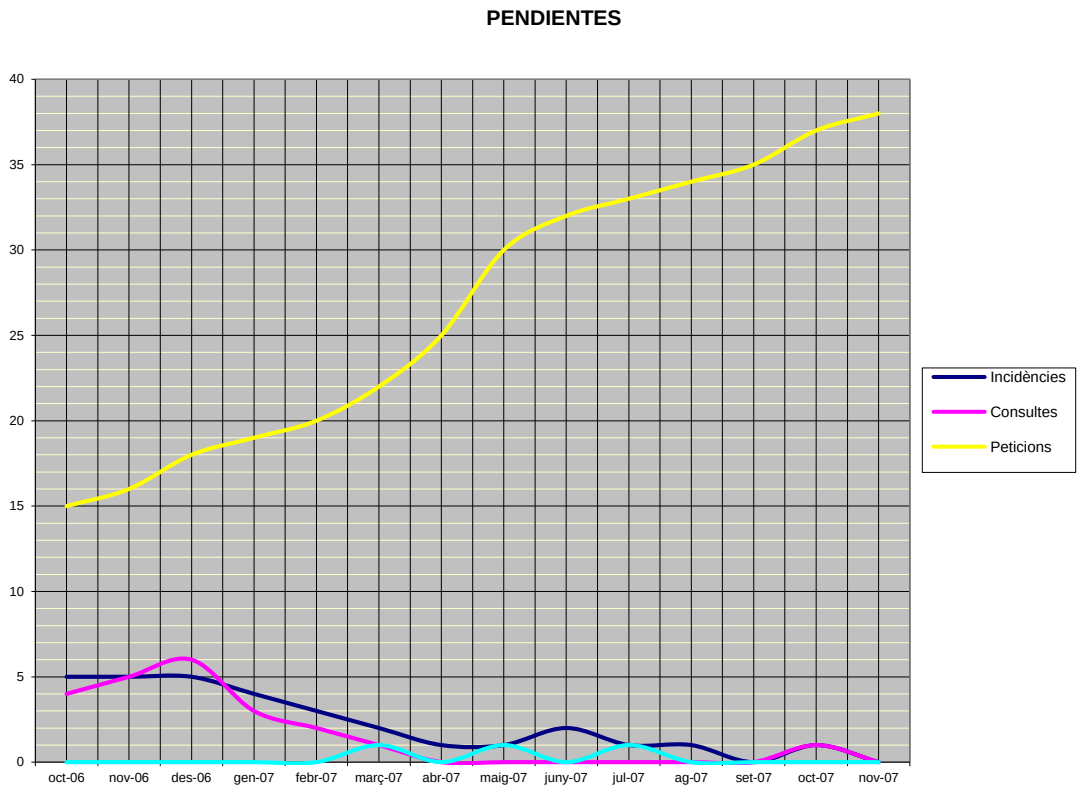
1.1.4 Gráficas de evolución

ENTRADAS



CERRADAS





1.2 Cuadro de Cumplimiento ANS

actuaciones	acuerdo Establecido	Tiempo de respuesta				total
		Dentro ANS'S		*Fuera ANS s*		
		número	*%*	*número*	*%*	
crítica	4 horas	1	100%	0	0%	1
alta	1 día	0	0%	0	0%	0
media	4 días	0	0%	0	0%	0
baja	N / A	0	0%	0	0%	0
Totales (número y cumplimiento ANS)		***1***	***100%***	***0***	***0%***	***1***

1.2.1 Gráfica evolución cumplimiento ANS

1.3 Temas cerrados en el periodo

1.3.1 Peticiones estándar (si los hay definidas)

actuaciones	acuerdo Establecido	Tiempo de respuesta				total
		Dentro ANS'S		*Fuera ANS s*		
		número	*%*	*número*	*%*	
petición 1	3 días	4	100%	0	0%	4
petición 2	2 días	0	0%	2	100%	2
petición 3	N / A	5	0%	0	0%	5
petición 4	N / A	0	0%	0	0%	0
petición 5	N / A	2	50%	2	50%	4
petición 6	N / A	1	100%	0	0%	1
petición 7	N / A	0	0%	0	0%	0
Totales (número y cumplimiento ANS)		***12***	***75%***	***4***	***25%***	***16***

1.3.2 Peticiones a medida

Peticiones a medida cerradas								
código	nombre	fecha petición	valoración		Fecha aprov.	Previsión		fecha finalización Real
			fecha	Coste (*)		Inicio	final	
3874	petición 1	18.10.17	02.27.18	1,25	03.09.18	04.11.18	04.27.18	04.27.18
1987	petición 2	03.06.18	03.13.18	7				04.27.18

(*) Unidad de medida (jornada / s)

1.3.3 incidencias

código	nombre	prioridad	fecha apertura	fecha cierre
11446	incidencia 1	crítica	01.03.18	03.10.18
12167	incidencia 2	crítica	01.03.18	03.12.18
18277	incidencia 3	alta	01.03.18	03.15.18

1.4 Temas pendientes a final de periodo

1.4.1 Peticiones a medida pendientes

Peticiones a medida abiertas									
código	**nombre**	**fecha petición**	**valoración**		**Fecha aprov.**	**Previsión**		**estado**	**asignada**
			fecha	**Coste (*)**		**Inicio**	**final**		
6787	petición 1	18.10.17	02.27.18	1,25	03.09.18	04.11.18	04.27.18	escalada	técnico 1
18672	petición 2	03.06.18	03.13.18	7				en Espera	técnico 2
19078	petición 3	03.09.18						escalada	técnico 3

(*) Unidad de medida (jornada / s)

1.4.2 incidencias pendientes

código	**nombre**	**prioridad**	**fecha**	**estado**	**asignada**
11446	incidencia 1	crítica	01.03.18	escalada	técnico 1
12167	incidencia 2	crítica	01.03.18	escalada	técnico 2
18277	incidencia 3	alta	01.03.18	en espera	técnico 3

Comentarios de las causas de posibles retrasos

2 seguimiento facturación

2.1 Facturas presentadas.

2.2 Coste previsto de los evolutivos en curso.

2.3 Costes disponibles.

3 Temas a destacar del período

4 Plan de acciones

acciones			
Descripción	**responsable**	**fecha inicio**	**estado**
petición 1	SE	15 / Mayo / 18	en curso
petición 2	SE	6 / julio / 18	en curso
petición 3	SE	26 / septiembre / 18	Finalizado septiembre / 2018
petición 4	PRJ	11 / julio / 18	Finalizado 29 / octubre / 2018
petición 5	SE	1 / octubre / 2018	en curso

5 Características del servicio

5.1 Horarios de servicio

5.2 Teléfonos y personas de contacto.

5.3 Descripción categorías incidencias

Consorci
Administració Oberta
de Catalunya

datos Generales	
Entidad de Registro	
Responsable del servicio	
auditor AOC	
fecha auditoría	

Informe de auditoría de Entidad de Registro T-CAT

áreas	Id. control		control	tipo Control	valoración	Evidencia / Observación
REQUISITOS DE GESTIÓN DOCUMENTAL Y ARCHIVO	1.1.		Tramitación de los expedientes			
		1	**Metodología de archivo y trazabilidad**	**OBL**	no evaluado	
		2	**El contenido de los expedientes es el adecuado (Solicitud de emisión, acuse de recibo de correos y copia de la hoja de entrega y aceptación de certificados firmada por el titular, en los casos en que se haya tramitado en papel).**	**OBL**	no evaluado	
		3	**La información de los expedientes seleccionados se corresponde con la información de los certificados emitidos.**	**OBL**	no evaluado	
		4	**Los expedientes están impresos con papel que cumple la Norma UNE-EN ISO 9706: 1999.**	OPT	no evaluado	
	1.2.		Archivo de gestión			
		1	**Los archivadores y / o armarios de gestión permanecen cerrados con llave cuando el personal del servicio no está presente.**	**OBL**	no evaluado	
		2	**El acceso a los archivadores sólo se permite al personal autorizado.**	**OBL**	no evaluado	
	1.3.		Transferencia al archivo central			
		1	**Existe un procedimiento de transferencia de expedientes que define la periodicidad, el responsable y el modo de envío físico al archivo central.**	OPT	no evaluado	
	1.4.		archivo Central			
		1	**Los controles de seguridad física del archivo son adecuados.**	**OBL**	no evaluado	
		2	**Metodología de archivo y trazabilidad**	**OBL**	no evaluado	

REQUISITOS OPERATIVOS	2.1.		documentación Requerida			
	1	Disponen de una ficha de suscriptor actualizada y ha sido enviada en los últimos 2 años		OBL	no evaluado	
	2	Disponen de una ficha de entidad de registro actualizada y ha sido enviada en los últimos 2 años		OBL	no evaluado	
	3	Disponen de términos y condiciones donde constan:	Las obligaciones de los suscriptores, periodo de tiempo de archivo de logs, marco legal y compromiso sobre disponibilidad	OBL	no evaluado	
	4	Disponen de términos y condiciones donde constan:	Procedimiento de quejas y resolución de conflictos	OBL	no evaluado	
	5	La entidad informa previamente a los suscriptores y partes interesadas sobre los términos y condiciones antes de iniciar la relación contractual		OBL	no evaluado	
	6	Los términos y condiciones se encuentran disponibles en medios no perecederos con un lenguaje comprensible y se pueden transmitir electrónicamente.		OBL	no evaluado	
	7	Los servicios deben ser accesibles a todos los solicitantes		OBL	no evaluado	
	8	Disponen de políticas y procedimientos para la resolución de conflictos o reclamaciones de clientes u otras partes interesadas		OBL	no evaluado	
	9	Se dispone de la Ficha de identidad y se ha revisado el cumplimiento		OBL	no evaluado	
	10	Disponen de un procedimiento de gestión de incidentes		OBL	no evaluado	
	11	Disponen de un procedimiento de cumplimiento legal y normativo (compliance)		OBL	no evaluado	
	12	Mantener un listado actualizado de activos de información con la asignación de la clasificación correspondiente con la evaluación de riesgos realizada.		OBL	no evaluado	
	13	Se dispone de un procedimiento y registro de gestión de cambios para versiones, modificaciones y desarrollos.		OBL	no evaluado	
	14	Existe un procedimiento de reinicio y recuperación del sistema en caso de fallo ..		OBL	no evaluado	
	15	La Entidad de Registro está alineada con el plan de continuidad de la AOC		OBL	no evaluado	
	2.2.		Formación y repaso de conocimientos			
	1	Todos los operadores han realizado el curso formativo de operador de entidad de registro T-CAT de Consorcio AOC.		OBL	no evaluado	
	2	El responsable del servicio muestra conocimiento del procedimiento aprobado para guardar la documentación en el archivo de gestión en forma de expediente.		OBL	no evaluado	
	3	Se dispone de una ficha personal actualizada con la formación recibida del personal involucrado.		OBL	no evaluado	

4	**Todo el personal (temporal o fijo) dispone de su descripción del puesto de trabajo donde consta la sensibilización de posición en función de los derechos y nivel de acceso, formación y sensibilización.**	**OBL**	no evaluado	
5	**La Entidad de Registro tiene descritas sanciones disciplinarias por aquellos trabajadores que incumplan las políticas o procedimientos establecidos.**	**OBL**	no evaluado	
6	**La Entidad de Registro dispone de procedimientos y procesos de gestión alineados con los de seguridad de la información.**	**OBL**	no evaluado	
7	**Todos los operadores deben estar libres de conflictos de intereses que puedan perjudicar la imparcialidad de las operaciones del servicio.**	**OBL**	no evaluado	
8	**El personal no tendrá acceso a las funciones de operador del sistema hasta que se hayan cumplido todos los controles necesarios.**	**OBL**	no evaluado	
9	**Todos los operadores muestran conocimiento del procedimiento para registrar y comunicar incidentes de seguridad de la información.**	**OBL**	no evaluado	
10	**Todos los operadores han recibido una formación sobre actualizaciones sobre nuevas amenazas y prácticas de seguridad actuales en los últimos 12 meses.**	**OBL**	no evaluado	
3.1.	seguridad física			
1	**La sala de operaciones debe disponer de un sistema electrónico de apertura o, como mínimo, de una puerta con llave. En caso de que esto no fuera posible, la LRA debe estar ubicada en un lugar reservado donde sólo tenga acceso el personal del ER y en ningún caso personal ajeno al Nos suscriptor.**	OPT	no evaluado	
2	**La Entidad de Registro almacena las tarjetas vírgenes en una ubicación con acceso restringido.**	**OBL**	no evaluado	
3	**El siguiente material se custodia en el interior de la sala de operaciones: PC, impresora de tarjetas, caja fuerte, stock de tarjetas generadas y la documentación de procesos y sistemas.**	**OBL**	no evaluado	
4	**Los componentes críticos para la prestación del servicio están localizados en un perímetro de seguridad protegido físicamente contra la intrusión y se controla el acceso a través de un perímetro de seguridad y alarma.**	**OBL**	no evaluado	
5	**La Entidad de Registro realiza prueba de penetración a las infraestructuras y la registra.**	**OBL**	no evaluado	
6	**La entidad tiene implementados controles para evitar el compromiso o robo de información y de las instalaciones de procesados de la información.**	**OBL**	no evaluado	
3.2	seguridad lógica			
1	**La Entidad de Registro dispone de un sistema antimalware instalado, está activo y actualizado (al menos de forma diaria).**	**OBL**	no evaluado	
2	**La Entidad de Registro dispone de políticas de acceso, calidad de contraseñas y salvapantallas**	**OBL**	no evaluado	
3	**La Entidad de Registro dispone de un SAI con una autonomía suficiente para finalizar un trámite en condiciones seguras.**	OPT	no evaluado	

REQUISITOS DE SEGURIDAD		4	**En la LRA no se ha detectado ningún software instalado sin la aprobación deL Consorcio AOC**	**OBL**	no evaluado	
		5	**En la LRA no se ha detectado ningún software instalado que permita acceder de forma remota.**	**OBL**	no evaluado	
		6	**La entidad de registro únicamente utiliza la LRA para realizar tareas relacionadas con el servicio de certificación T-CAT.**	OPT	no evaluado	
		7	**Todas las informaciones se tratarán de manera segura según su clasificación de riesgo.**	**OBL**	no evaluado	
		8	**La Entidad de Registro se protege contra la obsolescencia y el deteriomentdurante el tiempo en que deban conservar los registros.**	**OBL**	no evaluado	
		9	**El acceso a la información ya las funciones del sistema de aplicación están restringidos de acuerdo con la política de acceso.**	**OBL**	no evaluado	
		10	**Los despliegues de seguridad que están disponibles, se aplican en un tiempo razonable.**	**OBL**	no evaluado	
		11	**La Entidad de Registro se somete a simulacros de vulnerabilidades periódicos en direcciones IP publicadas, privadas y sistemas y registra las pruebas realizadas.**	**OBL**	no evaluado	
		12	**El personal de la Entidad de Registro identifica y autentica antes de utilizar aplicaciones críticas relacionadas con el servicio.**	**OBL**	no evaluado	
	3.3		Seguridad del personal			
		1	**Los operadores custodian con diligencia sus tarjetas de operador, así como el PIN y el PUK.**	**OBL**	no evaluado	
		2	**En caso de participación de personal externo, estos han firmado una cláusula de confidencialidad con la Entidad de Registro**	**OBL**	no evaluado	
		3	**En el caso de los operadores que han causado baja, el responsable del servicio ha procedido a comunicarlo a Consorcio AOC y se ha revocado el certificado del operador en cuestión.**	**OBL**	no evaluado	
		4	**Los operadores no tienen acceso a las funciones de confianza (trusted functions) hasta que no se cumplen todos los requisitos.**	**OBL**	no evaluado	
	3.4		Seguridad del archivo			
		1	**La entidad de registro dispone de procedimiento de archivo.**	OPT	no evaluado	
		2	**Las tarjetas inutilizadas se garantiza la destrucción.**	OPT	no evaluado	
		3	**Existe un protocolo o política de borrado seguro de datos confidenciales en dispositivos para evitar el acceso no autorizado**	**OBL**	no evaluado	

Resumen de evaluación

	cumple	no cumple	no aplica
controles obligatorios	0	0	0
controles optativos	0	0	0

evaluación: **APTA**

0

PLAN DE ACCIÓN	Id. control	Descripción del control	Id. acción	acción	responsable	plazo Resolución

OBSERVACIONES DEL ENTE	
	Primero. **Segundo.** **Tercero.**

Barcelona, día, mes año

Responsable del servicio

Auditor Consorcio AOC:

Consorci
Administració Oberta
de Catalunya

Informe de auditoría de Entidad de Registro idCAT

datos Generales	
Entidad de Registro	
Responsable del servicio	
auditor AOC	
fecha auditoría	

áreas	Id. control		control	tipo Control	valoración	Evidencia / Observación
REQUISITOS DE GESTIÓN DOCUMENTAL Y ARCHIVO	1.1.		Tramitación de los expedientes			
		1	**Metodología de archivo y trazabilidad**	**OBL**	no evaluado	
		2	**El contenido de los expedientes es el adecuado (Solicitud de emisión, acuse de recibo de correos y copia de la hoja de entrega y aceptación de certificados firmada por el titular, en los casos en que se haya tramitado en papel).**	**OBL**	no evaluado	
		3	**La información de los expedientes seleccionados se corresponde con la información de los certificados emitidos.**	**OBL**	no evaluado	
		4	**Los expedientes están impresos con papel que cumple la Norma UNE-EN ISO 9706: 1999.**	OPT	no evaluado	
	1.2.		Archivo de gestión			
		1	**Los archivadores y / o armarios de gestión permanecen cerrados con llave cuando el personal del servicio no está presente.**	**OBL**	no evaluado	
		2	**El acceso a los archivadores sólo se permite al personal autorizado.**	**OBL**	no evaluado	
	1.3.		Transferencia al archivo central			
		1	**Existe un procedimiento de transferencia de expedientes que define la periodicidad, el responsable y el modo de envío físico al archivo central.**	OPT	no evaluado	
	1.4.		archivo Central			
		1	**Los controles de seguridad física del archivo son adecuados.**	**OBL**	no evaluado	
		2	**Metodología de archivo y trazabilidad**	**OBL**	no evaluado	

REQUISITOS OPERATIVOS	2.1.		documentación Requerida			
	1	Disponen de una ficha de suscriptor actualizada y ha sido enviada en los últimos 2 años		OBL	no evaluado	
	2	Disponen de una ficha de entidad de registro actualizada y ha sido enviada en los últimos 2 años		OBL	no evaluado	
	3	Disponen de términos y condiciones donde constan:	Las obligaciones de los suscriptores, periodo de tiempo de archivo de logs, marco legal y compromiso sobre disponibilidad	OBL	no evaluado	
	4	Disponen de términos y condiciones donde constan:	Procedimiento de quejas y resolución de conflictos	OBL	no evaluado	
	5	La entidad informa previamente a los suscriptores y partes interesadas sobre los términos y condiciones antes de iniciar la relación contractual		OBL	no evaluado	
	6	Los términos y condiciones se encuentran disponibles en medios no perecederos con un lenguaje comprensible y se pueden transmitir electrónicamente.		OBL	no evaluado	
	7	Los servicios deben ser accesibles a todos los solicitantes		OBL	no evaluado	
	8	Disponen de políticas y procedimientos para la resolución de conflictos o reclamaciones de clientes u otras partes interesadas		OBL	no evaluado	
	9	Se dispone de la Ficha de identidad y se ha revisado el cumplimiento		OBL	no evaluado	
	10	Disponen de un procedimiento de gestión de incidentes		OBL	no evaluado	
	11	Disponen de un procedimiento de cumplimiento legal y normativo (compliance)		OBL	no evaluado	
	12	Mantener un listado actualizado de activos de información con la asignación de la clasificación correspondiente con la evaluación de riesgos realizada.		OBL	no evaluado	
	13	Se dispone de un procedimiento y registro de gestión de cambios para versiones, modificaciones y desarrollos.		OBL	no evaluado	
	14	Existe un procedimiento de reinicio y recuperación del sistema en caso de fallo ..		OBL	no evaluado	
	15	La Entidad de Registro está alineada con el plan de continuidad de la AOC		OBL	no evaluado	
	2.2.		Formación y repaso de conocimientos			
	1	Todos los operadores han realizado el curso formativo de operador de entidad de registro idCAT de Consorcio AOC.		OBL	no evaluado	
	2	El responsable del servicio muestra conocimiento del procedimiento aprobado para guardar la documentación en el archivo de gestión en forma de expediente.		OBL	no evaluado	
	3	Se dispone de una ficha personal actualizada con la formación recibida del personal involucrado.		OBL	no evaluado	

		4	**Todo el personal (temporal o fijo) dispone de su descripción del puesto de trabajo donde consta la sensibilización de posición en función de los derechos y nivel de acceso, formación y sensibilización.**	**OBL**	no evaluado	
		5	**La Entidad de Registro tiene descritas sanciones disciplinarias por aquellos trabajadores que incumplan las políticas o procedimientos establecidos.**	**OBL**	no evaluado	
		6	**La Entidad de Registro dispone de procedimientos y procesos de gestión alineados con los de seguridad de la información.**	**OBL**	no evaluado	
		7	**Todos los operadores deben estar libres de conflictos de intereses que puedan perjudicar la imparcialidad de las operaciones del servicio.**	**OBL**	no evaluado	
		8	**El personal no tendrá acceso a las funciones de operador del sistema hasta que se hayan cumplido todos los controles necesarios.**	**OBL**	no evaluado	
		9	**Todos los operadores muestran conocimiento del procedimiento para registrar y comunicar incidentes de seguridad de la información.**	**OBL**	no evaluado	
		10	**Todos los operadores han recibido una formación sobre actualizaciones sobre nuevas amenazas y prácticas de seguridad actuales en los últimos 12 meses.**	**OBL**	no evaluado	
	3.1.		seguridad física			
		1	**La sala de operaciones debe disponer de un sistema electrónico de apertura o, como mínimo, de una puerta con llave. En caso de que esto no fuera posible, la LRA debe estar ubicada en un lugar reservado donde sólo tenga acceso el personal del ER y en ningún caso personal ajeno al Nos suscriptor.**	OPT	no evaluado	
		2	**La Entidad de Registro almacena las tarjetas vírgenes en una ubicación con acceso restringido.**	**OBL**	no evaluado	
		3	**El siguiente material se custodia en el interior de la sala de operaciones: PC, impresora de tarjetas, caja fuerte, stock de tarjetas generadas y la documentación de procesos y sistemas.**	**OBL**	no evaluado	
		4	**Los componentes críticos para la prestación del servicio están localizados en un perímetro de seguridad protegido físicamente contra la intrusión y se controla el acceso a través de un perímetro de seguridad y alarma.**	**OBL**	no evaluado	
		5	**La Entidad de Registro realiza prueba de penetración a las infraestructuras y la registra.**	**OBL**	no evaluado	
		6	**La entidad tiene implementados controles para evitar el compromiso o robo de información y de las instalaciones de procesados de la información.**	**OBL**	no evaluado	
	3.2		seguridad lógica			
		1	**La Entidad de Registro dispone de un sistema antimalware instalado, está activo y actualizado (al menos de forma diaria).**	**OBL**	no evaluado	
		2	**La Entidad de Registro dispone de políticas de acceso, calidad de contraseñas y salvapantallas**	**OBL**	no evaluado	
URIDAD		3	**La Entidad de Registro dispone de un SAI con una autonomía suficiente para finalizar un trámite en condiciones seguras.**	OPT	no evaluado	

REQUISITOS DE SEGU						
	4	**Todas las informaciones se tratarán de manera segura según su clasificación de riesgo.**	**OBL**	no evaluado	
	5	**La Entidad de Registro se protege contra la obsolescencia y el deterioment durante el tiempo en que deban conservar los registros.**	**OBL**	no evaluado	
	6	**El acceso a la información ya las funciones del sistema de aplicación están restringidos de acuerdo con la política de acceso.**	**OBL**	no evaluado	
	7	**Los despliegues de seguridad que están disponibles, se aplican en un tiempo razonable.**	**OBL**	no evaluado	
	8	**La Entidad de Registro se somete a simulacros de vulnerabilidades periódicos en direcciones IP publicadas, privadas y sistemas y registra las pruebas realizadas.**	**OBL**	no evaluado	
	9	**El personal de la Entidad de Registro identifica y autentica antes de utilizar aplicaciones críticas relacionadas con el servicio.**	**OBL**	no evaluado	
3.3		Seguridad del personal			
	1	**Los operadores custodian con diligencia sus tarjetas de operador, así como el PIN y el PUK.**	**OBL**	no evaluado	
	2	**En caso de participación de personal externo, estos han firmado una cláusula de confidencialidad con la Entidad de Registro**	**OBL**	no evaluado	
	3	**En el caso de los operadores que han causado baja, el responsable del servicio ha procedido a comunicarlo a Consorcio AOC y se ha revocado el certificado del operador en cuestión.**	**OBL**	no evaluado	
	4	**Los operadores no tienen acceso a las funciones de confianza (trusted functions) hasta que no se cumplen todos los requisitos.**	**OBL**	no evaluado	
3.4		Seguridad del archivo			
	1	**La entidad de registro dispone de procedimiento de archivo.**	OPT	no evaluado	
	2	**Las tarjetas inutilizadas se garantiza la destrucción.**	OPT	no evaluado	
	3	**Existe un protocolo o política de borrado seguro de datos confidenciales en dispositivos para evitar el acceso no autorizado**	**OBL**	no evaluado	

Resumen de evaluación

	cumple	no cumple	no aplica
controles obligatorios	0	0	0
controles optativos	0	0	0

evaluación: **APTA**

0

N DE ACCIÓN	Id. control	Descripción del control	Id. acción	acción	responsable	plazo Resolución

PLA						

OBSERVACIONES DEL ENTE	
	Primero. **Segundo.** **Tercero.**

Barcelona, día, mes año

Responsable del servicio

Auditor Consorcio AOC:

Consorci
Administració Oberta
de Catalunya

FORMULARIO DE AUTOEVALUACIÓN DE ENTIDAD DE REGISTRO

Entidad de Registro:

fecha:

1.1. Tramitación de los expedientes

1.1.1. Hay una metodología de archivo y trazabilidad?	SI	NO
En caso afirmativo, indicar documento.		
1.1.2. El expediente de Solicitud de emisión tiene acuse de recibo, una copia de la hoja de entrega, y aceptación de certificados firmada por el titular?		
1.1.3. La información de los expedientes seleccionados se corresponde con la información de los certificará emitidos.	SI	NO
1.1.4. Los expedientes impresos con papel cumplen la Norma Une-EN ISO-9076?	SI	NO

1.2. Archivo de Gestión

1.2.1. Se cierran con llave los archivadores y / o armarios de gestión cuando el personal de servicio no está presente?	SI	NO
1.2.2. El personal autorizado es el único que puede acceder a los archivadores?	SI	NO

1.3. Transferencia al archivo central

1.3.1. Existe un procedimiento de transferencia de expedientes que define la periodicidad, el responsable y el modo de envío físico al archivo central? *	SI	NO
* En el caso de que la respuesta sea NO, indicar cuáles de los requerimientos no se cumplen		

1.4. archivo Central

1.4.1. Los controles de seguridad física del archivo son adecuados?	SI	NO
1.4.2. Hay una metodología de archivo y una trazabilidad?	SI	NO

2.1. documentación Requerida

2.1.1. Se dispone de una ficha de suscriptor actualizada y ha sido enviada en los últimos 2 años? *	SI	NO
* En caso de que la respuesta sea no, indicar por qué		
2.1.2. Se dispone de una ficha de entidad de registro actualizada y ha sido enviada los últimos 2 años? *	SI	NO
* En caso de que la respuesta sea no, indicar por qué		
2.1.3. Se dispone de términos y condiciones donde constan:		
a) Las obligaciones de los suscriptores.	SI	NO
b) El periodo de tiempo de archivo de logs.	SI	NO
c) Marco Legal.	SI	NO
d) Compromiso sobre disponibilidad.	SI	NO
2.1.4. Se dispone de términos y condiciones donde consta un procedimiento de quejas y resolución de conflictos?	SI	NO
2.1.5. La entidad informa previamente a los suscriptores y partes interesadas sobre los términos y condiciones antes de iniciar la relación contractual.	SI	NO
2.1.6. Los términos y condiciones se encuentran disponibles en medios no perecederos con un lenguaje comprensible y se pueden transmitir electrónicamente.	SI	NO

2.1.7. Los servicios son accesibles a todos los solicitantes.	SI	NO
2.1.8. Se dispone de políticas y procedimientos para la resolución de conflictos o reclamaciones de clientes u otras partes interesadas? *	SI	NO
* En caso afirmativo, indicar procedimientos.		
2.1.9. Se dispone de una Ficha de identidad y se ha revisado el cumplimiento	SI	NO
2.1.10. Se dispone de un procedimiento de gestión de incidentes?	SI	NO
2.1.11. Se dispone de un procedimiento de cumplimiento legal y formativo (compliance)?	SI	NO
2.1.12. Se mantiene un listado de activos actualizado con la asignación de clasificación de información correspondiente y una evaluación de riesgos de los mismos?	SI	NO
2.1.13. Se dispone de un procedimiento y registro de gestión de cambios para versiones, modificaciones y desarrollos?	SI	NO
* En caso afirmativo, indicar procedimiento.		
2.1.14. Existe un procedimiento de reinicio y recuperación del sistema en caso de fallo? *	SI	NO
* En caso afirmativo, indicar procedimiento.		
2.1.15. La Entidad de Registro está alineada con el plan de continuidad de la AOC?	SI	NO

2.2. Formación y repaso de conocimientos

2.2.1. Han realizado todos los operadores el curso formativo de operador de entidad de registro T-CAT de Consorcio AOC?	SI	NO
2.2.2. El responsable del servicio muestra conocimiento del procedimiento aprobado para guardar la documentación en el archivo de gestión en forma de expediente?	SI	NO

2.2.3. Se dispone de una ficha personal actualizada con la formación recibida del personal involucrado?	SI	NO
2.2.4. Dispone todo el personal (temporero o fijo) de su descripción del puesto de trabajo donde consta la sensibilización de posición en función de los derechos, nivel de acceso y formación?	SI	NO
2.2.5. Dispone la Entidad de Registro de descripciones de las sanciones disciplinarias para aquellos trabajadores que incumplan las políticas o procedimientos establecidos?	SI	NO
2.2.6. Dispone La Entidad de Registro de procedimientos y procesos de gestión alineados con los de seguridad de la información?	SI	NO
* En caso afirmativo, indicar procedimiento.		
2.2.7. Están todos los operadores libres de conflictos de intereses que puedan perjudicar la imparcialidad de las operaciones del servicio?	SI	NO
2.2.8. Tiene el personal acceso a las funciones de operador del sistema antes de que se completen todos los controles necesarios?	SI	NO
2.2.9. Muestran todos los operadores conocimiento del procedimiento para registrar y comunicar incidentes de Seguridad de la Información?	SI	NO
2.2.10. Han recibido todos los operadores una formación sobre actualizaciones sobre nuevas amenazas y prácticas de seguridad actuales en los últimos 12 meses?	SI	NO

3.1. seguridad física

3.1.1. Dispone la sala de operaciones de un sistema electrónico de apertura o, como mínimo, de una puerta con llave? *	SI	NO
* En caso de que la respuesta sea NO, indicar de qué se dispone.		
3.1.2. Almacena la Entidad de Registro las tarjetas vírgenes en una ubicación con acceso restringido?	SI	NO
3.1.3. Se custodia el siguiente material en el interior?		
a) PC	SI	NO
b) Impresora de tarjetas	SI	NO

c) Caja Fuerte	SI	NO
d) Stock de Tarjetas generadas	SI	NO
e) Documentación de Procesos y Sistemas	SI	NO
3.1.4. Están los componentes críticos para la prestación del servicio localizados en un perímetro de seguridad protegido físicamente contra la intrusión y se controla el acceso a través de un perímetro de seguridad y alarma? *	SI	NO
* En caso de que la respuesta sea NO, describir las medidas de seguridad de que se dispone		
3.1.5. La Entidad de Registro realiza y registra pruebas de penetración a las infraestructuras?	SI	NO
3.1.6. La entidad tiene implementados controles para evitar el compromiso o robo de información y de las instalaciones de procesados de la información?	SI	NO

3.2. seguridad Lógica

3.2.1. Dispone la Entidad de Registro de un sistema antimalware instalado?	SI	NO
a) Está activo?	SI	NO
b) Se actualiza al menos de forma diaria?	SI	NO
3.2.2. Dispone la Entidad de Registro de políticas de acceso, calidad de contraseñas y salvapantallas?	SI	NO
3.2.3. Dispone la Entidad de Registro de un SAI con una autonomía suficiente para finalizar un trámite en condiciones seguras?	SI	NO
3.2.4. En la LRA ha detectado software instalado sin la aprobación del Consorcio AOC	SI	NO
3.2.5. En la LRA ha detectado software instalado que permita acceder de forma remota.	SI	NO
3.2.6. La Entidad de registro utiliza la LRA únicamente para realizar tareas relacionadas con el servicio de certificación T-CAT? *	SI	NO

* En caso de que la respuesta sea NO, describir qué otras tareas realiza con la LRA		
3.2.7. Se tratan de manera segura según su clasificación de riesgo todas las informaciones?	SI	NO
3.2.8. Se protege la Entidad de Registro contra la obsolescencia y el deterioro durante el tiempo en que deban conservar los registros?	SI	NO
3.2.9. Están el acceso a la información ya las funciones del sistema de aplicación restringidas de acuerdo con la política de acceso?	SI	NO
3.2.10. Se aplican en un tiempo razonable los despliegues de seguridad disponibles?	SI	NO
3.2.11. Se plantea la Entidad de Registro a simulacros de vulnerabilidad periódicos en direcciones IP publicadas, privadas y sistemas y registra se pruebas realizadas?	SI	NO
3.2.12. El personal de la Entidad de Registro identifica y autentica antes de utilizar aplicaciones críticas relacionadas con el servicio?	SI	NO

3.3. Seguridad del Personal

3.3.1. Los operadores custodian con diligencia sus tarjetas de operador, así como el PIN y el PUK?	SI	NO
3.3.2. En caso de participación de personal externo, estos firman una cláusula de confidencialidad con la Entidad de Registro?	SI	NO
3.3.3. En el caso de los operadores que han causado baja, el responsable del servicio ha procedido a comunicarlo a Consorcio AOC y se ha revocado el certificado del operador en cuestión?	SI	NO
3.3.4. Los operadores tienen acceso a las funciones de confianza (trusted functions) antes de que se cumplen todos los requisitos?	SI	NO

3.4. Seguridad del archivo

3.4.1. La entidad de registro dispone de procedimiento de archivo?	SI	NO
3.4.2. Se garantiza la destrucción de las tarjetas inutilizadas?	SI	NO
3.4.3. Existe un protocolo o política de borrado seguro de datos confidenciales en dispositivos para evitar el acceso no autorizado?	SI	NO

Firmamos la presente declaración a fecha del documento.

FORMULARIO DE AUTOEVALUACIÓN DE ENTIDAD DE REGISTRO

Nombre de la persona que firma:

Lugar de trabajo de la persona que firma:

Consorci
Administració Oberta
de Catalunya

Auditorías relacionadas con SCD:

- ER T-CAT
- ER idCAT
- ER de identidades (Organismos suscriptores)

Generalitat de Catalunya

LOCALRET

Realizado por:
versión:
fecha: 09/07/2024
archivo: D1153 Auditoría de conformitat.doc

Index

1 Objeto y alcance

El objeto de este documento es desarrollar los requisitos de las Auditorías relacionadas con los organismos que ejecutando parte Servicio de Certificación Digital concretamente en los ámbitos de:

- **Entidades de registro T-CAT**: Es un organismo o departamento que colabora con el Consorcio AOC en la emisión de certificados digitales en las administraciones públicas catalanas.
- **Entidades de Registro idCAT** : Es un organismo o departamento que colabora con el AOC, en el registro de las identidades digitales para la ciudadanía, concretamente para emitir y gestionar certificados idCAT i idCAT en móvil
- **Entidades de registro u organismos suscriptores:** es un ente o departamento que colabora con el Consorcio AOC en los trámites de identificación, registro y autenticación para la emisión de certificados digitales, siguiendo los procedimientos y las relaciones con los titulares de los certificados.

2 Programación de auditorías

2.1 Frecuencia de auditoría de conformidad

El Consorcio AOC, como prestador de servicios de certificación, tiene la obligación de realizar periódicamente una auditoría de conformidad a sus Entidades de Registro y organismo suscriptor para probar que cumple con los requisitos de seguridad, archivo y operacionales marcados en la documentación del servicio.

Se procederá a un muestreo que permita de forma bianual la revisión de la totalidad de las entidades que han hecho uso del servicio SCD.

La ejecución de estas auditorías se realizará de manera virtual o presencial según programación anual. Auditará presencialmente las Entidades de Registro T-CAT y idCAT que por criterios de volumen de emisiones, incidencias u otros factores que lo requieren.

2.2 Estudio inicial del entorno a auditar

Para materializar las auditorías habrá que realizar una serie de tareas previas:

- Revisión de la documentación actual
    - Comprobar que existe la ficha o alta del servicio al día
    - Número de certificados emitidos
    - Fecha de la última auditoría y resultados (en el caso de que haya)
    - Revisión de cualquier cambio que haya podido afectar al servicio.
    - Revisión y selección de los certificados a auditar
    - Revisión de los posibles datos erróneos en los datos de los titulares de los certificados.
    - Listado de incidencias sufridas
    - Listado del personal que participa en los procesos del Servicio de Certificación Digital
    - Verificación de la existencia de un archivo central donde permanezcan archivados los documentos relacionados con el SCD y control de la documentación y registros.
    - Informe de revisión por la dirección, donde se especifique lo siguiente:
        - Resultados de auditorías internas y externas
        - Retroalimentación de partes interesadas
        - Retroalimentación del mecanismo para mantener la imparcialidad
        - Estado de las acciones preventivas y correctivas
        - Acciones de seguimiento provenientes de revisiones previas por parte de la dirección
        - Cumplimiento de objetivos
        - Cambios que podrían afectar al sistema de gestión
        - Quejas y apelaciones
        - Acciones y decisiones relativas a:
            - Mejora de la eficacia del sistema de gestión y de sus procesos
            - Mejora del organismo de certificación en relación al cumplimiento de norma
            - La necesidad de recursos

2.3 Plan de auditorías

Anualmente la AOC procederá a una programación de entidades a auditar que contemplará los requerimientos legales y el muestreo definido en el punto 2.1.

Posteriormente se ejecutará un plan de auditoría donde se informará a los centros seleccionados.

Este plan de auditoría deberá incluir los siguientes puntos:

- Objetivo y alcance
- Criterios de auditoría
- equipo auditor
- Documentos de referencia
- Agenda con tiempo de inicio o duración
- Temas de confidencialidad
- Riesgos de la auditoría
- Instrucciones de resolución y seguimiento

Se deberá comunicar con anterioridad 30 días en el centro.

3 Ejecución de auditorías

3.1 Relación de elementos objeto de auditoría

- Términos y condiciones: Poner a disposición de los suscriptores, las entidades de registro y partes interesadas los términos y condiciones de cada uno de los servicios prestados. Estos términos y condiciones especificarán:
  - Las obligaciones del suscriptor y las entidades de registro, si hay,
  - El período de tiempo que se guardan los logs del servicio de confianza
  - Las limitaciones de responsabilidad
  - Marco legal aplicable
  - Procedimiento de quejas y resolución de conflictos
  - Información de contacto del servicio de confianza
  - Compromiso sobre la disponibilidad

  Hay que informar a los suscriptores, las entidades de registro ya las partes interesadas de los términos y condiciones antes de iniciar la relación contractual. Además, estos términos y condiciones deben estar disponibles a través de medios de comunicación no perecederos, con un lenguaje sencillo y que se puedan transmitir electrónicamente.
- Operación y gestión del servicio
  - Los servicios deben ser accesibles a todos los solicitantes, cuyas actividades están dentro de su campo de operación declarado y que aceptan cumplir con sus obligaciones especificadas en los términos y condiciones del servicio.
  - Disponer de políticas y procedimientos para la resolución de conflictos o reclamaciones de clientes u otras partes interesadas
  - Contrato en vigor con la AOC.
- Recursos humanos involucrados: El ente debe asegurarse de que el personal que da el servicio es responsable y da confianza al servicio dado.

- El personal estará calificado para hacer el trabajo encomendado y habrá recibido formación sobre seguridad y protección de datos personales adecuadas al servicio ofrecido y el lugar de trabajo.
- Se dispondrá de una ficha de personal actualizada con la formación recibida (conocimiento, experiencia y calificaciones) o experiencia en el puesto de trabajo que se irá actualizando cada año, en función de actualizaciones sobre nuevas amenazas o nuevas prácticas de seguridad.
- Se describirán sanciones disciplinarias por aquellos trabajadores que incumplan las políticas o procedimientos establecidos.
- Las funciones de seguridad y las responsabilidades estarán descritas claramente en la descripción de los puestos de trabajo que estarán disponibles para todo el personal implicado. Las funciones de confianza, de las que depende la seguridad de la operación del servicio, deben estar claramente identificadas. Las funciones de confianza serán nombradas por la dirección y serán aceptadas por la dirección y por la persona implicada.
- Todo el personal (temporal o fijo) dispondrá de su descripción del puesto de trabajo donde constará la sensibilidad de posición en función del derechos y nivel de acceso, formación y sensibilización.
- Se dispondrá de procedimientos y procesos de gestión alineados con los de seguridad de la información.
- Todo el personal con funciones de confianza deben estar libres de conflictos de intereses que puedan perjudicar la imparcialidad de las operaciones del servicio.
- Las funciones de confianza incluyen:
    - Operador del sistema: Responsable para operar el sistema de confianza en el día a día. Autorizado para realizar la copia de seguridad.
- El personal no tendrá acceso a las funciones de confianza hasta que se hayan cumplido todos los controles necesarios.

- Gestión de activos: El ente deberá asegurarse del nivel apropiado de protección de los activos, incluyendo los activos de información.
    - Mantener un listado actualizado de activos de información con la asignación de la clasificación correspondiente con la evaluación de riesgos realizada.
    - Todos los materiales se tratarán de manera segura según su clasificación de riesgo. Los materiales que contengan datos sensibles se destruirán de forma segura cuando ya no sean necesarios.
- Control de acceso digital: El acceso al sistema estará limitado al personal autorizado.
    - El acceso a la información ya las funciones del sistema de aplicación deben estar restringidos de acuerdo con la política de acceso.
    - El personal del ente debe identificarse y autenticarse antes de utilizar aplicaciones críticas relacionadas con el servicio.
    - El personal del ente es responsable de sus actividades.

  - Debe existir un protocolo o política de borrado seguro de datos confidenciales en dispositivos para evitar el acceso no autorizado.

- Control de acceso físico: Se debe controlar el acceso físico a los componentes del sistema del ente, cuya seguridad es crítica para la provisión del servicio de confianza y minimizar los riesgos relacionados con la seguridad física.
  - Acceso físico limitado a los componentes del sistema del ente que son críticos para la prestación del servicio.
  - Se deben implementar controles para evitar la pérdida, daño o compromiso de activos e interrupción de las actividades
  - Se deben implementar controles para evitar el compromiso o robo de información y de las instalaciones de procesados de la información.
  - Los componentes que son críticos para la prestación del servicio deben estar localizados en un perímetro de seguridad protegido físicamente contra la intrusión y se debe controlar el acceso a través de un perímetro de seguridad y alarma.
- Seguridad operacional: El ente debe utilizar sistemas de confianza y productos protegidos contra modificaciones y debe asegurarse de la seguridad técnica y fiabilidad de los procesos realizados por ellos.
  - Hay que aplicar un procedimiento y registro de gestión de cambios para versiones, modificaciones y correcciones de software.
  - La integridad de los sistemas del organismo deben estar protegidos contra virus, software malicioso y software no autorizado.
  - Los materiales utilizados en los sistemas del ente deben gestionar de manera segura para proteger -los de daños, robos, accesos no autorizados y obsolescencia.
  - Se deben proteger contra la obsolescencia y el deterioro, los materiales utilizados durante el tiempo en que se hayan de conservar los registros.
  - Se deben implementar y establecer los procedimientos para las funciones administrativas y de confianza que impactan en la provisión de los servicios.
  - El organismo ha de aplicar procedimientos para asegurarse de lo siguiente:
    - Los despliegues de seguridad que están disponibles se aplican en un tiempo razonable.
    - No se aplican despliegues de seguridad que introducen vulnerabilidades o inestabilidades mayores que los beneficios que puedan aportar.
    - Se documentan las razones por las que no de aplicado un despliegue de seguridad.
- Seguridad de las redes: El ente debe proteger su red y sus sistemas de los ataques.
    - El organismo mantendrá todos los sistemas que son críticos para la operación del ente en una o más zonas seguras.
    - El ente debe someterse o realizar un escáner de vulnerabilidad periódico en direcciones IP publicadas y privadas identificadas por el ente y registrar pruebas que cada persona o entidad realizaba cada escaneo de vulnerabilidad con las habilidades, las

herramientas, la competencia, el código ético y la independencia necesario para proporcionar un informe fiable.

- El ente debe someterse a una prueba de penetración en sus sistemas en la instalación y después de la infraestructura o las actualizaciones o modificaciones de las aplicaciones que determine el ente como significativas. El ente registrará pruebas que cada prueba de penetración fue realizada por una persona o entidad con las habilidades, las herramientas, la competencia, el código ético y la independencia necesarias para proporcionar un informe fiable.

- Gestión de incidentes: Se debe controlar la actividad del sistema relacionada con el acceso a los sistemas informáticos, el uso de sistemas informáticos y las solicitudes de servicio.
    - Las actividades de seguimiento deberían tener en cuenta la sensibilidad de cualquier información recogida o analizada
    - Las actividades anormales del sistema que indican una posible vulneración de seguridad, incluida la intrusión en la red del ente, han de detectar e informar como alarmas.
    - Los sistemas de TI del ente deben supervisar los siguientes eventos:
        - Puesta en marcha y apagado de las funciones de registro; y
        - Disponibilidad y utilización de los servicios necesarios con la red del ente.
    - El ente debe actuar de manera oportuna y coordinada para responder rápidamente a incidentes y limitar el impacto de las violaciones de la seguridad. El ente designará personal de rol de confianza para hacer un seguimiento de las alertas de eventos de seguridad potencialmente críticos y garantizar que se registren incidentes relevantes de acuerdo con los procedimientos del ente.
    - El ente debe establecer procedimientos para notificar a las partes apropiadas de acuerdo con las normas reguladoras aplicables de cualquier incumplimiento de la seguridad o pérdida de integridad que tenga un impacto significativo en el servicio de confianza prestado y en los datos personales mantenidas en él, dentro de las 24 horas posteriores al momento en que se identifica el incumplimiento.
    - Cuando el incumplimiento de la seguridad o pérdida de integridad pueda afectar negativamente a una persona física o jurídica a la que se ha prestado el servicio fiduciario, el ente también notificará a la persona física o jurídica el incumplimiento de la seguridad o la pérdida de integridad sin demora indebida.
    - Se deben controlar los sistemas del ente, incluida la supervisión o la revisión periódica de los registros de auditoría para identificar evidencias de actividad maliciosa que implican mecanismos automáticos para procesar los registros de auditoría y personal de alertas de posibles eventos de seguridad críticos.
    - El ente abordará cualquier vulnerabilidad crítica que no se haya tratado previamente por el mismo, dentro del plazo de 48 horas

después de su descubrimiento. Si esto es efectivo en función del efecto en términos de costes, el ente ha de crear e implementar un plan para mitigar la vulnerabilidad o documentará la base por la que la vulnerabilidad no hay que ser tratada.

- Se deben utilizar los procedimientos de información y respuesta de los incidentes de manera que se minimice el daño causado por incidentes de seguridad y mal funcionamiento.

- Alineación con el Plan de continuidad de negocio de la AOC: El ente debe tener definido y mantener un plan de continuidad que promulgará en caso de desastre.
- Cumplimiento legal y normativo: El ente debe asegurarse de que opera dentro del marco legal aplicable.
  - Procedimiento de cumplimiento de marco legal donde se pueda demostrar cómo se gestiona el marco legal.
  - El ente debe asegurarse de que los servicios son accesibles a personas con discapacidad.
  - Cumplimiento del marco legal vigente en protección de datos personales. Adecuación al nuevo Reglamento Europeo de Protección de Datos.
- Gestión de la identificación:
- Gestión del cambio: Procedimiento transversal donde se planifiquen los cambios, se registren y se lleve un seguimiento.

3.2 Pautas de la auditoría virtual

Mirar los anexos específicos para cada ente.

- Hacer muestreo de los certificados personales generados. establecer un valor no superior al 10% o un mínimo de 10 certificados.
- Hacer un muestreo de los certificados de dispositivo y aplicación generados (casos de ER T-CAT y organismo suscriptor), no superior al 10% o un mínimo de 10 certificados.
- Enviar un correo al responsable del Servicio del ente con el informe de auditoría para llenar y firmar y con los nombres de los titulares de las hojas de entrega solicitados. Será necesario que organismo envíen esta documentación escaneada al correo electrónico indicado.
- La auditora deberá comprobar que los datos del certificado generado son las mismas que el certificado solicitado o que el DNI. En los casos de hoja de entrega de T-CAT se comprobará mediante la aplicación que la hoja de entrega no se ha impreso en el momento de la auditoría si no cuando se realizó el certificado
- Comprobar la seguridad del tratamiento de datos personales en cumplimiento de la legislación vigente.

3.3 Pautas de la auditoría presencial

Mirar los anexos específicos para cada ente.

- Concertar la visita para la realización de la auditoría con el responsable del Servicio, solicitando la participación de todos los roles implicados.
- Hacer un muestreo de los certificados personales generados, entre un 5% y un 10% del total.
- Hacer un muestreo de los certificados de dispositivo y aplicación generados (casos de ER T-CAT y organismo suscriptor), entre un 6% y un 10%.
- Solicitar al responsable del servicio la documentación del muestreo para analizar.
- La auditora deberá comprobar que los datos del certificado generado son las mismas que el certificado solicitado o que el DNI u otros documentos identificativos. En los casos de hoja de entrega de T-CAT se comprobará que están debidamente archivados.
- Comprobar la seguridad del tratamiento de datos personales en cumplimiento de la legislación vigente.

3.4 Elaboración de los informes de auditoría

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

1.- Completar cheking de seguimiento.
2.- Realización del informe indicando cuales son las no conformidades encontradas y las evidencias que lo demuestran.
3.- Creación de las fichas con los planes de acción para corregir los errores. Hay que crear una ficha para problema encontrado.
4.- Enviar el informe
5.- Comunicar a la ER u organismo suscriptor, las debilidades significativas y las recomendaciones oportunas.
6.- Indicar al ER u organismo suscriptor como se actuará desde el Consorcio AOC para realizar el seguimiento de las recomendaciones.

3.5 Acciones a emprender como resultado de una falta de conformidad

Los informes de resultados de las auditorías serán entregados por el Consorcio AOC, en un plazo máximo de 25 días después de la ejecución de la auditoría, para su evaluación y gestión diligente.
En caso de una no conformidad en términos de protección de datos personales, se deberá informar a al Delegado de Protección de Datos por que informe a la AGPD.
Para otros no conformidades, se deberá describir las actuaciones a realizar para subsanar la no conformidad, marcar un responsable y un plazo de resolución coherente.

3.6 Finalización de auditoría

A la recepción de las correcciones, El auditor evaluará la conformidad de las acciones ejecutadas para garantizar la corrección de las desviaciones.

Se deberá tener especial cuidado por:

1- Establecer medidas para controlar el progreso de las no conformidades graves.
2- Realizar las revocaciones de oficio los certificados emitidos de manera errónea. (Enviando mail al suscriptor).
3- En caso de que el ER idCAT no haga lo recoge los DNI s deberán enviar el correo de plantilla para que el suscriptor lo lleve a la ER. En caso de que no lo lleve en 90 días, el Consorcio AOC procederá a la revocación de oficio de aquel certificado.

Una vez evaluado el auditor considerará cerrado el proceso de auditoría.

4 normativa aplicable

- UNE-EN-ISO 19011: 2011 Directrices para la auditoría de los sistemas de gestión.
- UNE-EN-ISO / IEC 17065: 2012 Evaluación de la Conformidad. Requisitos para organismos que certifican productos, procesos y servicios.
- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93 / CE.
- DIRECTIVA (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión
- ETSI EN 319 401 Electronic Signatures and Infraestructuras (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 403 Electronic Signatures and Infraestructuras (ESI); Trust Service Provider Conformity Assessment-Requirements for Conformity assessment bodies assessing Trust Services Providers
- Y toda la relacionada con la prestación de servicios de certificación

5 Relación de registros

Plantilla de correo electrónico con la planificación de la auditoría

Modelo de informe de auditoría

checking de auditoría

Consorci
Administració Oberta
de Catalunya

INFORME DE AUDITORÍA DE CONFORMIDAD

ENTIDAD DE REGISTRO

fecha

1. DATOS DE LA ORGANIZACIÓN

NOMBRE:

DIRECCIÓN:

RESPONSABLE:

OBJETO:

FECHA DE REALIZACIÓN:

DIRECCIONES DE LA ORGANIZACIÓN:

2. ALCANCE DE LA AUDITORÍA

Sedes:

3. APLICABILIDAD

4. EQUIPO AUDITOR

AUDITOR CAP:
AUDITOR:

5. DOCUMENTACIÓN DE REFERENCIA

6. MUESTRA AUDITADA

total personal		**grado de confianza**	**%**
personal auditado			
Tipo de certificados		**grado de confianza**	**%**
tipo auditadas			

7. NO CONFORMIDADES

DESCRIPCIÓN DE LA NO CONFORMIDAD	área afectada

8. OBSERVACIONES

DESCRIPCIÓN DE LAS OBSERVACIONES

9. OPORTUNIDADES DE MEJORA APORTADAS POR EL AUDITOR

DESCRIPCIÓN DE LAS PROPUESTAS DE MEJORA

10. RESULTADO

1. La organización se quedará con una copia del informe.
2. Las no conformidades han sido aclaradas y entendidas.
3. Teniendo en cuenta las no conformidades constatadas e indicadas en este informe, la entidad de registro se compromete a presentar acciones correctivas.
4. El equipo auditor informa que esta auditoría se ha realizado a través de un muestreo por lo que pueden existir otras no conformidades no identificadas en este informe.
5. Las no conformidades se refieren a incumplimientos de los requisitos de la Regulación eIDAS a través de las normas ETSI.
6. OPINIÓN DEL AUDITOR: La auditora considera adecuada la situación actual.

11. MODIFICACIONES DEL ALCANCE

No constan modificaciones al alcance.

lugar:
fecha:

Firma / s Auditor / es

Firma del representante de la organización

ANNEXO VOLUMETRIAS DE EMISIÓN DE CERTIFICADOS

	ANY									
TIPUS DE CERTIFICAT	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**
Certificats personal T-CAT	16.805	18.967	20.793	19.766	28.338	17.534	16.259	17.646	21.026	36.378
Certificat personal T-CAT urgents	792	1.179	1.320	1.692	1.851	1.389	1.240	1.806	1.695	3.723
T-CAT P	285	1.171	1.461	2.990	5.162	5.588	9.962	12.045	15.099	37.027
TCAT P urgent	9	56	81	142	206	371	1.256	751	628	3.363
TCAT P classe 2	0	2	3	3	12	0	5	28	12	47
TCAT P classe 2 urgent	0	0	0	0	0	0	2	0	2	2
certificat operador idcat	436	483	406	490	504	570	610	720	750	789
certificat operador T-CAT	143	137	151	101	141	75	67	85	11	97
Certificat classe 2	4.409	7.001	4.140	4.098	505	20	37	23	58	169
Certificat operador Classe 2	32	15	15	7	44	14	34	40	32	24
Certificat idCAT	34.424	33.076	52.099	69.588	88.225	109.552	191.360	298.600	277.562	321.311
certificat seu electrònica (*)	66	51	47	59	118	no aplica	no aplica	no aplica	no aplica	no aplica
certificat seu electrònica urgent (*)	11	13	15	13	41	no aplica	no aplica	no aplica	no aplica	no aplica
certificat CDS (*)	739	902	1.017	991	1.227	no aplica	no aplica	no aplica	no aplica	no aplica
certificat CDS urgent (*)	51	59	65	33	39	no aplica	no aplica	no aplica	no aplica	no aplica
certificat EV (*)	33	27	32	47	56	no aplica	no aplica	no aplica	no aplica	no aplica
certificat EV urgent (*)	1	2	6	8	6	no aplica	no aplica	no aplica	no aplica	no aplica
Certificat CDA	133	144	181	277	249	137	223	294	248	136
Certificat CDA urgent	5	13	25	33	25	17	29	43	53	19
Certificat CDANM	386	616	555	661	845	948	770	753	958	838

Certificat CDANM urgent	38	66	65	82	75	77	29	33	75	77
Certificat pseudònim	0	0	0	0	119	178	180	319	773	1.661
Certificat pseudònim urgent	0	0	0	0	0	0	0	0	0	0
Certificat representant	0	0	0	0	21	75	82	39	68	250
Certificat representant urgent	0	0	0	0	0	0	0	0	0	0

(*) los certifcados marcados salen del catalogo en el 2018
(**) tener en cuenta la variabilitad de los años electorales

ANNEXO Entitats de Registre T-CAT

Consorci AOC

Diputació de Tarragona

Ajuntament de Castelldefels

Ajuntament de Girona

Ajuntament de Lleida

Ajuntament de Vilanova i la Geltrú

Consell Comarcal de l'Alt Penedés

Consell Comarcal de l'Alt Urgell

Consell Comarcal del Baix Ebre

Consell Comarcal de la Conca de Barberà

Consell Comarcal de la Garrotxa

Consell Comarcal d'Osona

Consell Comarcal del Pallars Sobirà

Consell Comarcal de la Ribera d'Ebre

Consell Comarcal del Ripollés

Consell Comarcal del Segrià

Consell Comarcal de la Selva

Consell Comarcal del Tarragonés

Consell Comarcal de la Terra Alta

Organisme de Gestió Tributària de la DIBA

Consell Comarcal del Pla de l'Estany

Ajuntament de Sant Feliu de Llobregat

Ajuntament de Mollet del Vallés

Consell Comarcal del Baix Camp

Consell Comarcal de la Segarra

Consell Comarcal de l'Alt Camp

Ajuntament de Tarragona

Ajuntament de Reus

Ajuntament de Manresa

Ajuntament de Badalona

Consell Comarcal del Maresme

Consell Comarcal del Vallés Oriental

Consell Comarcal de l'Anoia

Consell Comarcal del Pla d'Urgell

Consell Comarcal de la Noguera

Consell Comarcal del Berguedà

Consell Comarcal del Baix Empordà

Consell Comarcal del Pallars Jussà

Consell Comarcal de l'Urgell

Consell Comarcal del Vallés Occidental

Consell Comarcal del Garraf

Consell Comarcal del Montsià

Ajuntament de Sabadell

Consell Comarcal de l'Alt Empordà

Consell Comarcal de l'Alta Ribagorça

Consell Comarcal del Priorat

Consell Comarcal del Baix Penedès

Consell Comarcal de les Garrigues

Conselh Generau d'Aran

Consell Comarcal del Solsonés

Consell Comarcal del Bages

Consell Comarcal de la Cerdanya

Consell Comarcal del Gironés

Ajuntament de Cerdanyola del Vallés

Ajuntament de Mataró

Ajuntament de Cornellà de Llobregat

Consell Comarcal del Baix Llobregat

CTTI

Autoritat Catalana de Protecció de Dades

CESICAT

Mossos d'Esquadra

UPC

Universitat de Lleida

Universitat Pompeu Fabra

Universitat de Barcelona

Universitat Rovira i Virgili

Parlament de Catalunya

Consell Comarcal del Moianès

(*) listado es de junio de 2024 y puede variar a lo largo del tiempo pot variar al llarg del temps.

ANNEXO Entitats de Registre idCAT

Ajuntament de Castell-Platja d'Aro
Ajuntament de Pallejà
Ajuntament de Sabadell. SAC Despatx Lluch
Ajuntament de la Cellera de Ter
Ajuntament de Manlleu - Oficines centrals
Ajuntament de Mataró
Ajuntament de Mataró
Ajuntament de Mataró
Ajuntament de Mataró
Ajuntament de Palafolls
Ajuntament de Sils
Consell Comarcal del Pla de l'Estany
Departament de Cultura- Palau Marc
Institut Municipal d'Hisenda
OAC de la Generalitat de Catalunya a la Cerdanya
OAC de la Generalitat de Catalunya a Lleida
OFICINA D'ATENCIÓ A LES EMPRESES (OAEM)
Oficina d'Atenció al Ciutadà - Districte de Nou Barris
Oficina d'Atenció Ciutadana - Districte de Ciutat Vella
Oficina d'Atenció Ciutadana - Districte de Gràcia
Oficina d'Atenció Ciutadana - Districte de l'Eixample
Oficina d'Atenció Ciutadana - Districte de Les Corts
Oficina d'Atenció Ciutadana - Districte de Sant Martí
Oficina d'Atenció Ciutadana - Districte de Sarrià-Sant Gervasi
Oficina d'Atenció Ciutadana - Districte d'Horta- Guinardó
Sant Andreu, Oficina d'Atenció al Ciutadà - Districte de
TRESORERIA MUNICIPAL
Ajuntament de Mataró
Oficina d'Atenció Ciutadana - Districte de Sants- Montjuïc
Oficina d'Atenció Ciutadana - Plaça Sant Miquel
OFICINA D'ATENCIÓ CIUTADANA MONUMENTAL
Ajuntament de Sant Adrià de Besòs
Ajuntament de Barberà del Vallès
Ajuntament de Sant Cugat del Vallès
Ajuntament de Vilablareix
Cateb - Oficina Vilafranca
Cateb - Oficina Barcelona
Cateb - Oficina Terrassa
Cateb - Oficina Mataró - Cateb
Cateb - Oficina Manresa
Cateb - Oficina Granollers

Cateb - Oficina Vic
UAB - Arxiu General i Registre
Ajuntament de Badalona
Ajuntament de Begues
Ajuntament de Calonge de Segarra
Ajuntament de Castelló d'Empúries
Ajuntament de Sant Celoni
Ajuntament d'El Bruc
Consell Comarcal del Moianès
Garraf, Consell Comarcal del
OAC de la Delegació del Govern a Lleida
Propietat Forestal, Centre de la
Torelló-Torelló Jove, Ajuntament de
Ajuntament de Castelldefels
Calonge, Ajuntament de
Centre Municipal d'Informació Juvenil
Oficina Municipal d'Atenció Ciutadana
Ajuntament de Santa Coloma de Gramenet
Ajuntament de Gurb
Ajuntament de Montblanc
Ajuntament de Vidreres
Ajuntament de Quart
Ajuntament de Palau-saverdera
Ajuntament de Tossa de Mar
Ajuntament Vilanova del Camí
Ajuntament de Vilafranca del Penedès
Ajuntament de Sitges
Ajuntament de Sitges
Ajuntament de Sitges
Ajuntament de Sant Andreu de Llavaneres
Ajuntament del Papiol
Ajuntament d'Olivella
Ajuntament de Sitges
Ajuntament de Sabadell. SAC Est
Ajuntament de Sabadell. SAC Oest
Ajuntament de Monistrol de Montserrat
Ajuntament de Sant Pere de Vilamajor
Ajuntament de Subirats
Ajuntament de Tremp
Ajuntament de Torelló
Ajuntament de Gavà

Ajuntament de l'Ametlla de Mar
Ajuntament de Lloret de Mar - El Puntet
Ajuntament del Pla de Santa Maria
Montsià, Consell Comarcal del
Universitat Pompeu Fabra
Universitat Pompeu Fabra
Universitat Pompeu Fabra
BASE. Oficina Altafulla
BASE. Oficina Amposta
BASE. Oficina Calafell
BASE. Oficina Creixell
BASE. Oficina de Cunit
BASE. Oficina de Deltebre
BASE. Oficina del Vendrell
BASE. Oficina Falset
BASE. Oficina Gandesa
BASE. Oficina Hospitalet de l'Infant i Vandellòs
BASE. Oficina La Canonja
BASE. Oficina La Sénia
BASE. Oficina Miami platja
BASE. Oficina Montblanc
BASE. Oficina Mont-roig del Camp
BASE. Oficina Móra d'Ebre
BASE. Oficina Reus
BASE. Oficina Riudoms
BASE. Oficina Roda de Berà
BASE. Oficina Sant Carles de la Ràpita
BASE. Oficina Torredembarra
BASE. Oficina Tortosa
BASE. Oficina Ulldecona
BASE. Oficina Valls
BASE. Oficina Vila-seca
Ajuntament de Lloret de Mar - Biblioteca Municipal de Lloret
Institut Municipal d'Informàtica
Ajuntament de Sant Esteve Sesrovires
Ajuntament de Figueres
Ajuntament de Celrà
Ajuntament de Reus
Ajuntament de Salou
Ajuntament d'Arenys de Mar
Ajuntament de Sant Quirze del Vallès
Ajuntament de les Preses
Ajuntament de Bigues i Riells
Ajuntament de Sant Llorenç Savall
Ajuntament de Vilobí d'Onyar
Consell Comarcal de les Garrigues

Ajuntament de Sant Feliu de Llobregat
Ajuntament d'Olot

Ajuntament d'Aitona

Ajuntament de Balaguer
Ajuntament de Bell-lloc d'Urgell
Ajuntament de Cerdanyola del Vallès
Ajuntament de l'Escala
Ajuntament de Pineda de Mar
Ajuntament d'Hostalric
Consell Comarcal de la Garrotxa
Consell Comarcal de la Segarra
Consell Comarcal de l'Alta Ribagorça
Consell Comarcal del Berguedà
Priorat, Consell Comarcal del
Ajuntament de Gelida
Ajuntament de Vilanova i la Geltrú
Ajuntament de Llinars del Vallès

UAB - Campus de Sabadell

Ajuntament de Sant Llorenç d'Hortons
Ajuntament de Centelles
Fundació Universitària Balmes. Universitat de Vic-UCC
OAIC - Centre Cívic Onyar
OAIC - Centre Cívic Pla de Palau
OAIC - Centre Cívic Pont Major
OAIC - Centre Cívic Sant Narcís
OAIC - Centre Cívic Santa Eugènia
OAIC - Llar d'avis de Taialà
OAIC - Plaça del Vi, 1
Ajuntament de Cornellà de Llobregat
Ajuntament de Salt
Ajuntament d'Esparreguera
Ajuntament de l'Hospitalet de Llobregat
Ajuntament de Calafell
Consell Comarcal del Ripollès
Ajuntament de Sabadell. SAC Nord
Ajuntament de Sabadell. SAC Sud
Consell Comarcal del Pla d'Urgell
Ajuntament de Dosrius
Ajuntament de Calaf
Ajuntament de Corbera de Llobregat
Oficina d'Atenció Ciutadana (OAC) dels Serveis Territorials d'Empresa i Treball a Tarragona

Oficina d'Atenció Ciutadana (OAC) d'Empresa i Treball

Departament de Cultura - ST Girona Casa Solterra
Departament de Cultura - ST Lleida
Departament de Cultura- ST Catalunya Central
Departament de Cultura- ST Terres de l'Ebre

Departament de Cultura - ST Tarragona
Oficina d'Atenció Ciutadana (OAC) dels Serveis Territorials d'Empresa i Treball a Lleida
Ajuntament de Sant Martí de tous
Ajuntament de Calella
Ajuntament de les Masies de Voltregà
Ajuntament d'Arbúcies
Ajuntament de Castellterçol
Ajuntament de Fogars de la Selva
Ajuntament de la Garriga
Ajuntament de Massanes
Ajuntament de Sant Andreu de la Barca
Ajuntament de Teià
Ajuntament de Torroella de Montgrí
BASE. Oficina Alcanar
Conselh Generau d'Aran
Consell Comarcal de la Cerdanya
Consell Comarcal de l'Alt Urgell
Consell Comarcal del Baix Penedès
Ajuntament de Polinyà
Ajuntament de Palamós
Consell Comarcal del Segrià
Ajuntament de Sant Feliu de Guíxols
BASE. Oficina Tarragona
Consell Comarcal de la Noguera
Consell Comarcal d'Osona
Institut Municipal d'Ocupació
Oficina de Gestió i Atenció Tributària
Ajuntament de Cubelles
Ajuntament de Terrassa - Oficina d'Atenció Ciutadana de Plaça Didó - OAC1
Ajuntament de Terrassa - Oficina d'Atenció Ciutadana del Districte 2 - OAC2
Ajuntament de Terrassa - Oficina d'Atenció Ciutadana del Districte 3 - OAC3
Ajuntament de Terrassa - Oficina d'Atenció Ciutadana del Districte 4 - OAC4
Ajuntament de Terrassa - Oficina d'Atenció Ciutadana del Districte 5 - OAC5
Ajuntament de Terrassa - Oficina d'Atenció Ciutadana del Districte 6 - OAC6
Ajuntament de Terrassa - Oficina d'Atenció Ciutadana del Districte 7 - OAC7
Ajuntament de Vilassar de Dalt
Ajuntament de Lloret de Mar
Ajuntament de Mollet del Vallès
Ajuntament de Moià
Ajuntament de Sant Joan de les Abadesses
Consell Comarcal del Pallars Sobirà
Ajuntament de Molins de Rei
OAC de la Generalitat de Catalunya a Barcelona

Ajuntament de Canet de Mar
Ajuntament de Canyelles
Ajuntament de Collbató
Ajuntament de Palau-solità i Plegamans
Ajuntament de Santa Eulàlia de Ronçana
Ajuntament de Sentmenat
Ajuntament de Mediona
Ajuntament de Sant Pol de Mar

Taxi, Institut Metropolità del
Ajuntament de Tàrrega

Punt d'informació del Departament de Territori
Ajuntament d'Esplugues de Llobregat
Ajuntament de Ripollet
Ajuntament de Masquefa - CTC - MASQUEFA
Consell Comarcal de l'Alt Camp
Ajuntament d'Òdena
Ajuntament de Sant Vicenç dels Horts. SIAC
Oficina d'Atenció Ciutadana a Tarragona
Oficina d'Atenció Ciutadana del Departament de Treball Afers Socials i Famílies a les Terres de l'Ebre
Oficina d'Atenció Ciutadana del Departament de Treball Afers Socials i Famílies a Lleida
Consell Comarcal de la Terra Alta
Ajuntament de Breda
Departament d'Acció Exterior i Unió Europea
Ajuntament d'Almacelles
Consell Comarcal del Baix Camp
Ajuntament de Berga
Ajuntament de Tordera
Ajuntament de Torelló - La Carrera
Ajuntament de Granollers
Ajuntament de Carme
Ajuntament del Morell
Ajuntament de Viladasens
Ajuntament de Castellfollit de la Roca
Ajuntament de Prats de Lluçanès
Ajuntament de Blanes
Ajuntament de Palafrugell
Ajuntament de Sant Pere de Ribes
Ajuntament de Sant Pere de Ribes
Ajuntament de Rubí-RAMBLETA
Ajuntament del Masnou
Ajuntament de Caldes de Montbui
Ajuntament de l'Ametlla del Vallès
Ajuntament de Lliçà d'Amunt

Ajuntament de Lliçà de Vall
Ajuntament de Llagostera
Ajuntament de Riudellots de la Selva
Consell Comarcal de la Ribera d'Ebre
Ajuntament d'Alcanar
Consell Comarcal del Solsonès
Ajuntament de Viladecavalls
Ajuntament de Castellbisbal
Sant Sadurní d'Anoia, Ajuntament de
Ajuntament de la Llagosta
Ajuntament de Navàs
Ajuntament de Sant Joan Despí
Ajuntament d'Olesa de Montserrat
Ajuntament de Montornès del Vallès
Consell Comarcal de l'Alt Penedès

Ajuntament de Torelló - La Cooperativa

Oficina d'Afers Socials i Famílies de Barcelona - Sants / Eixample
Ajuntament de Vic - ER idCAT de la Biblioteca
Ajuntament de Vic - ER idCAT de la Plaça Major

Ajuntament del Vendrell

Ajuntament de Sant Hilari Sacalm
Ajuntament d'Albatàrrec
Ajuntament de Castellolí
Ajuntament de Parets del Vallès
OAC SAV
Ajuntament de Cabrils
Ajuntament de Santpedor
Ajuntament de Cardedeu
Ajuntament de Guissona

Ajuntament de Malgrat de Mar

Ajuntament de Polinyà - Centre de Serveis a l'Empresa i l'Emprenedoria
Ajuntament de Polinyà - El Roure
Ajuntament de Santa Perpètua de Mogoda
Ajuntament de Vilassar de Mar
Consell Comarcal de l'Urgell
Consell Comarcal del Maresme
Ajuntament de Montcada i Reixac
Ajuntament de Valls
Ajuntament de Castellet i la Gornal
Ajuntament de Sant Feliu de Buixalleu
Ajuntament de Premià de Dalt
Oficina d'Atenció Ciutadana del Districte Administratiu
Ajuntament de Santa Bàrbara
Ajuntament del Prat de Llobregat
OAC Aragó - Departament de Territori

OAC Casa Gasset (Tarragona)- Departament de Territori
OAC Clot de les Monges (Lleida)
Ajuntament de Viladecans
Ajuntament de Santa Cristina d'Aro
Ajuntament de Matadepera
Ajuntament de la Torre de Claramunt
Ajuntament de Camprodon
Ajuntament de Mont-roig del Camp
Ajuntament de Salomó
Ajuntament de Cambrils
Ajuntament d'Argentona
Ajuntament de Constantí

L'Aleixar, Ajuntament de

Ajuntament dels Hostalets de Pierola
Ajuntament de Sant Feliu de Codines
Consell Comarcal del Tarragonès
Ajuntament d'Arenys de Munt
Delegació Territorial del Govern a les Terres de l'Ebre
Universitat de Barcelona
Ajuntament de Campllong
Ajuntament de Rubí-Narcís Menard
Ajuntament d'Alella
Ajuntament de Montmeló
Ajuntament de Roses
Ajuntament de les Franqueses del Vallès
Ajuntament de Riells i Viabrea
Consell Comarcal de la Selva
Consell Comarcal del Baix Empordà
Ajuntament de les Borges del Camp
OAC de la Generalitat de Catalunya a Tarragona
Ajuntament de La Bisbal del Penedès
Ajuntament de Badia del Vallès
Ajuntament de Mieres
Consell Comarcal de l'Anoia
Ajuntament de Premià de Mar
Ajuntament de Brunyola i Sant Martí Sapresa
Ajuntament de Manresa
Ajuntament de Sant Hipòlit de Voltregà
Ajuntament de Castellar del Vallès
Ajuntament de Sant Boi de Llobregat
Ajuntament de la Tallada d'Empordà
Consell Comarcal de la Conca de Barberà
Ajuntament de Canet d'Adri
Ajuntament d'Anglès

Delegació del Govern de la Generalitat de Catalunya a Mèxic i a l'Amèrica Central
Delegació del Govern de la Generalitat de Catalunya a Alemanya
Delegació del Govern de la Generalitat al Con Sud
Consell Comarcal del Baix Llobregat
Consell Comarcal del Vallés Oriental
Ajuntament dels Alamús
OAC de la Delegació Territorial del Govern a Girona
Baix Ebre, Consell Comarcal del
Oficina d'Atenció Ciutadana del Departament de Treball Afers Socials i Famílies
Ajuntament de Martorell
Ajuntament de Sant Vicenç de Castellet
Oficina d'Atenció Ciutadana de Barcelona

Ajuntament de la Llacuna

OAC de la Delegacio de Govern de Tarragona
Oficina d'Atenció Ciutadana de la Cerdanya
Treball, Afers Socials i Famílies - OAC Albareda, Departament de

(*) este listado es junio de 2024 y puede variar a lo largo del tiempo.

Nos titular de la ER T-CAT	núm ER s	impresión pin desde la LRA	recuperación de pin desde la carpeta del suscriptor	tipo Tarjeta	Diseño del plástico	grabación con lector externo (no impresora de tarjetas)	aprobador + generador	otras personalizaciones
Badalona, Ayuntamiento de	1	opcionalmente	SI	propia	T-CAT BADALONA	SI	NO	no aplica
Castelldefels, Ayuntamiento de	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Cornellà de Llobregat, Ayuntamiento de	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Manresa, Ayuntamiento	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Mataró, Ayuntamiento de	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Mollet del Vallés, Ayuntamiento	1	opcionalmente	SI	propia	T-CAT Mollet	SI	NO	no aplica
Sabadell, Ayuntamiento de	1	opcionalmente	SI	propia	no aplica	SI	NO	no aplica
Sant Feliu de Llobregat, Ayuntamiento	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Cerdanyola del Vallès. Ayuntamiento de	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Politécnica de Cataluña, Universtitat	17 + 1	opcionalmente	SI	bancaria	no aplica	SI	SI	no aplica
Pompeu Fabra, Universidad	8	opcionalmente	SI	bancaria	no aplica	SI	SI	no aplica
Lleida, Universidad de	2	opcionalmente	SI	bancaria	no aplica	SI	SI	no aplica
Universidad Rovira i Virgili	25	opcionalmente	SI	bancaria	no aplica	SI	SI	no aplica
Girona, Ayuntamiento de	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	SI	no aplica
Barcelona, Universidad de	25	opcionalmente	SI	bancaria	no aplica	SI	SI	no aplica
Lleida, Ayuntamiento de	1	opcionalmente	SI	propia	no aplica	SI	NO	no aplica
Reus, Ayuntamiento	1	opcionalmente	SI	propia	T-CAT FOTO	NO	NO	no aplica
Tarragona, Ayuntamiento	1	opcionalmente	SI	propia	T-CAT ESTANDAR	NO	NO	no aplica
CTTI	1	opcionalmente	SI	propia	no aplica	SI	NO	no aplica
Catalana de la Protección de Datos, Agencia	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Parlamento	1	opcionalmente	SI	propia	T-CAT PARLAMENTO	NO	NO	no aplica
ORGT de la DIBA	1	opcionalmente	SI	propia	T-CAT ORGT	NO	NO	no aplica
Tarragona, Diputación de	1	opcionalmente	SI	propia	T-CAT ESTANDAR	NO	NO	no aplica
Alt Camp, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Alt Empordà, Consejo Comarcal	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Alt Penedès, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Alt Urgell, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Alta Ribagorça, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Anoia, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Bages, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Baix Camp, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Bajo Ebro, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Baix Empordà, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Barcelona, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Baix Penedès, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Berguedà, Consejo Comarcal de	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Cerdanya, Consejo Comarcal de la	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Conca de Barberà, Consejo Comarcal de la	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Garraf, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Garrigues, Consejo Comarcal de las	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Garrotxa, Consejo Comarcal de la	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Gironès, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Maresme, Consejo Comarcal	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Montsià, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Noguera, Consejo Comarcal de la	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Osona, Consejo Comarcal de	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Pallars Jussà, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Pallars Sobirà, Consejo Comarcal de	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Plan del Urgell, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Pla de l'Estany, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Priorat, Consejo Comarcal	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Ribera de Ebro, Consejo Comarcal de la	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica

Ripollès, Consejo Comarcal de	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Segarra, Consejo Comarcal de la	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Segrià, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Selva, Consejo Comarcal de la	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Solsonès, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Tarragonès, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Terra Alta, Consejo Comarcal de la	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Urgell, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Aran, Consejo General de Aran	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Moianès, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Barcelona, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
Valles Oriental, Consejo Comarcal del	1	opcionalmente	SI	T-CAT	T-CAT ESTANDAR	NO	NO	no aplica
AOC	2	opcionalmente	SI	T-CAT	todos	NO	NO	no aplica
CESICAT	1	opcionalmente	SI	propia	no aplica	SI	NO	no aplica

Consorci
Administració Oberta
de Catalunya

Descripción funcional de la plataforma SCD T-CAT

Generalitat
de Catalunya

LOCALRET

Realizado por: AOC
versión:
fecha: 9/7/2024
archivo: Anexo 7 -
Descripcio_plataforma_SCD.docx

Index

1 Definiciones y acrónimos

1.1 definiciones

DISPOSITIVO: Soporte donde se graban los certificados emitidos, por ejemplo, una tarjeta criptográfica específica, un archivo PKCS # 12 en un directorio, o una memoria USB. El sistema debe utilizar los diferentes dispositivos físicos vía interfaz PKCS # 11.

ORGANISMO. Organismo con usuarios que necesitan y utilizan los certificados emitidos. Normalmente será el valor del campo O del certificado. Está ligado a un código de entes que es la base para los filtros de visibilidad de datos que utiliza el sistema a partir del rol de cada operador.

ENTIDAD DE REGISTRO. Oficina donde hay operadores del sistema. Una Entidad de Registro puede peticionar o ver certificados de uno o varios entes sobre los que está autorizado. Al mismo tiempo, puede tramitar certificados de una o varias Entidades de Certificación y de uno o varios perfiles de certificado de cada Entidad de Certificación. Cada Entidad de certificación tiene un tipo especial de Entidad de Registro (código 000) que puede tratar certificados de cualquier ente.

LOTE. Conjunto de peticiones de certificación agrupadas bajo un mismo identificador y que permite realizar operaciones globales para todos sus elementos.

OPERADOR. Persona o software, identificado mediante un certificado digital, que puede acceder al sistema del SCD y realizar las funciones definidas por sus roles.

PERFIL DE CERTIFICADO. Certificado o conjunto de certificados que emite el sistema. En la definición del perfil se podrán especificar cosas como: certificados a emitir (por ejemplo firma y cifrado), datos necesarios para el certificado, datos de gestión (direcciones, etc), datos para la personalización gráfica del soporte (fotografía, diseño, etc .), reglas de unicidad que aplican a los certificados, etc.
En caso de que un perfil genere más de un certificado, el sistema permitirá realizar las operaciones del ciclo de vida (revocación, suspensión, consulta, etc) de manera conjunta y transparente desde el punto de vista de los operadores.
El sistema dispone de diferentes Entidades de Certificación que al mismo tiempo emiten diferentes perfiles cada una. Dentro del concepto perfil Cada perfil se puede generar sobre uno o varios dispositivos diferentes.

POSEEDOR DE CLAVES. Usuario titular del certificado y que será el responsable de su uso.

RESPONSABLE DE SERVICIO. Es el interlocutor y gestor principal ante el servicio por un ente.

ROL. Propiedad asociada a un Operador y que define las operaciones que puede hacer. Un operador puede tener más de un rol, siempre que éstos no sean incompatibles.

SISTEMA ONLINE. Parte del sistema de SCD que permite generar certificados de manera completa a partir de los datos de la petición.

SISTEMA LOTES. Parte del sistema de SCD que permite generar los archivos a partir del envío de información en forma de Lot al fabricante de tarjetas, En este esquema las tareas logísticas quedan repartidas entre el fabricante de tarjetas y la AOC. Este sistema sólo es

aplicable a un conjunto reducido de certificados y perfiles, siempre en soporte tarjeta criptográfica.

1.2 acrónimos

CRL. Lista de certificados revocados (Certificate revocación List)

EC. Entidad de Certificación

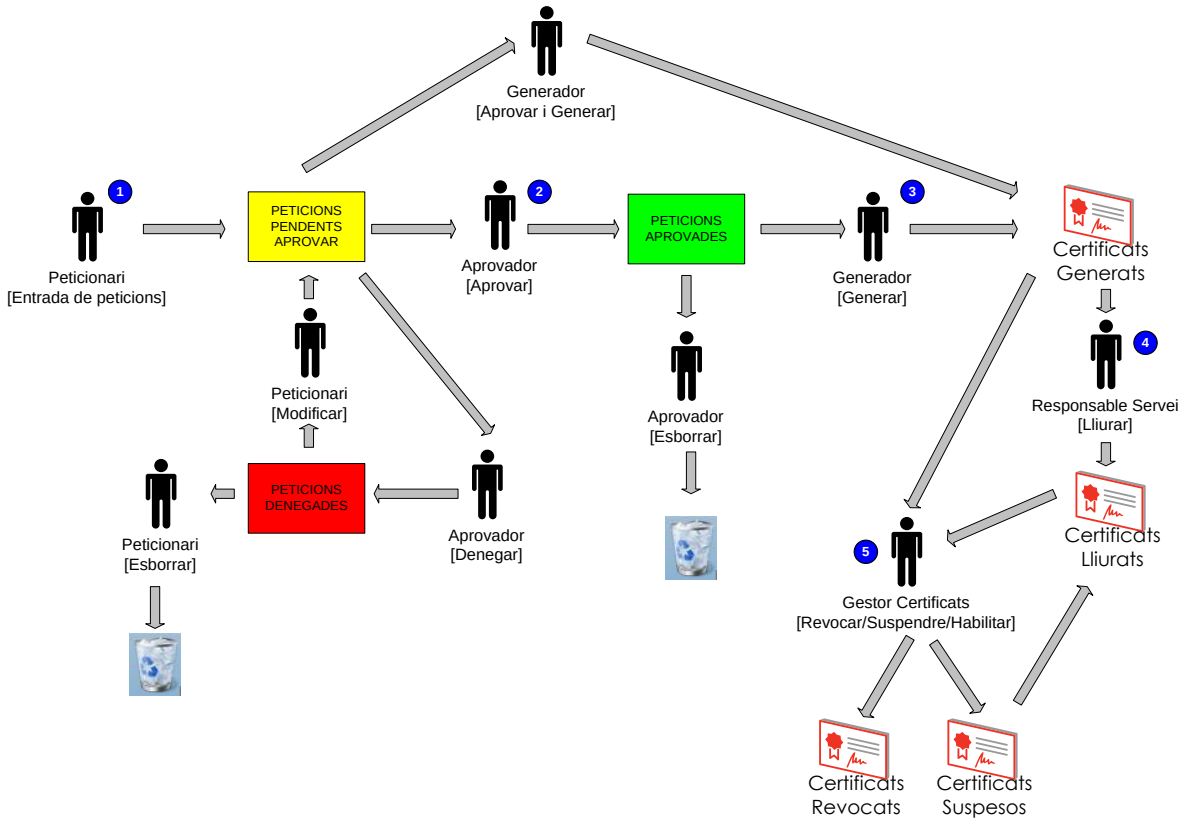
ER. Entidad de Registro

ERV. Entidad de Registro Virtual

SCD. Servicio de Certificación Digital

2 Descripción general de los procesos de certificación.

Para entender el funcionamiento del sistema, después se detalla cuál es el flujo de la información dentro del SCD. La siguiente figura muestra este flujo en función de su orden cronológico más natural dentro del sistema que conforma el Web de Operadores de la Entidad de registro y la Carpeta del suscriptor (ver punto 6.4.4 del Pliego de Prescripciones Técnicas, PPT en adelante). A continuación se describen cada uno de los pasos y una breve descripción de los procesos más importantes asociados a cada uno de ellos.



Dentro del sistema pueden existir algunas excepciones al flujo general mostrado en función de requerimientos adicionales que pueden aplicarse a un perfil de certificado, a una Entidad de certificación o una Entidad de registro.

2.1 Fase 1. Introducción de peticiones.

En estos no se realiza la 'grabación' de los datos de la petición de certificación en la base de datos del SCD. Esta acción se puede realizar de diferentes maneras en función de si el certificado será generado por el sistema ONLINE o por el sistema de LOTES. Estos dos entornos tienen pequeñas diferencias de funcionamiento.

sistema ONLINE

Durante este proceso se realizan las operaciones de validación de los datos (longitud, DNI, valores limitados por listas, etc) y las validaciones de unicidad. Si la petición se introduce correctamente en el sistema, esta queda en estado PENDIENTE.

También existe un estado borrador que permite al operador tener las peticiones en borrador y que sólo son visibles sólo para él mismo.

Destacar que el valor del campo organismo (normalmente trasladado al campo O del certificado) está limitado por la lista de entes asociados a la ER que opera el peticionario.

sistema LOTES

Cuando se introducen las diferentes peticiones, se realizan las operaciones de validación de los datos (longitud, DNI, valores limitados por listas, etc). En este punto las peticiones las podríamos considerar que están en estado DRAFT ya que sólo son visibles para el propio operador.
Es en el momento que se ejecuta la acción de CERRAR LOT, que es verifica la unicidad y las peticiones (englobadas dentro del LOT) quedan en estado PENDIENTE DE APROBAR.

2.2 Fase 2. Aprobación de peticiones.

En esta fase, se permite a los operadores, aprobar o denegar las peticiones. Como en el caso anterior, hay pequeñas diferencias entre el sistema ONLINE y el sistema de LOTES.

sistema ONLINE

Se permiten las operaciones de APROBAR, DENEGAR y BORRAR para cada una de las peticiones que están en estado PENDIENTE DE APROBAR. Hay que realizar la firma digital para cada petición que quedará registrada al sistema.

sistema LOTES

Es permiten las operaciones de APROBAR y DENEGAR a nivel del LOTE que se ha creado en el paso anterior. Hay que realizar una firma digital para cada lote que quedará registrada al sistema.

2.3 Fase 3. Generación

En esta fase es el momento en que se generan los certificados. Como en los casos anteriores hay diferencias entre el sistema ONLINE y el sistema de LOTES:

sistema ONLINE

Mediante la aplicación del módulo generador, se recuperan las peticiones pendientes de generar y el sistema gestiona los elementos necesarios para su generación en el correspondiente soporte (tarjetas, impresoras, lectores, etc.). En este paso se genera la documentación relacionada a cada certificado:

- Hoja de entrega
- Sobre ciego, con PIN y PUK, por los perfiles en tarjeta y en formato certificado o PKCS # 12 para el resto de perfiles. Este elemento se continúa generando pero su impresión ya no se realiza. El envío lo hace el sistema por correo electrónico una vez entregado el certificado.

También realiza la publicación de la hoja de entrega y los códigos PIN y PUK en el servidor de la Entidad de Registro (ER o RA, adelante en inglés, Registration Authority) para poder realizar el envío de manera automática.

sistema LOTES

Mediante la aplicación del módulo generador, se recuperan los lotes aprobados pendientes de generar y el sistema genera los archivos que hay que enviar al servicio externo de generación de tarjetas. Una vez hecho este flujo, queda bajo la responsabilidad del generador de las tarjetas de generar la documentación asociada y la logística de su entrega.

Esta operativa sólo está disponible en los entornos de la web de Operadores de la entidad de registro ubicados en las oficinas del Consorcio AOC.

2.4 Fase 4. Entrega

Una vez generados los certificados estos deben ser entregados a sus destinatarios.

En la operativa inicial del servicio SCD T-CAT (hasta el 2009) esta fase era 'externa' al servicio del SCD T-CAT y constaba de las siguientes operaciones:

- Envío de las tarjetas al responsable del servicio o de los certificados / PKCS # 12 por correo de forma manual.
- Envío de las hojas de entrega al responsable del servicio.
- Envío de los sobres de PIN y PUK al poseedor de las llaves.
- Recepción de la copia de la hoja de entrega, debidamente firmada por el poseedor de claves, por parte del Consorcio AOC y cierre del expediente asociado a GEDA-e.

A partir del 2009 y para minimizar el uso del papel en los anteriores pasos, se define el flujo de la siguiente manera que se materializa en la llamada Carpeta del Suscriptor:

- Envío de las tarjetas al responsable del servicio. En el caso de los certificados / PKCS # 12 el propio responsable del servicio podrá realizar la descarga de los mismos a través del portal del servicio SCD T-CAT.

- El Responsable del Servicio recibe las tarjetas, accede a la web del SCD T-CAT con su certificado y realiza las siguientes operaciones:
    - Marca en la web del SCD T-CAT que ha recibido los certificados. [Esta operación conlleva la realización de una firma digital]
    - Descarga las hojas de entrega
    - Libra tarjetas o PKCS # 12 / certificados (previa descarga de los archivos) y hace firmar la hoja de entrega al poseedor de las llaves y los custodia. Marca en la web del SCD T-CAT que ha entregado los certificados. [Esta operación conlleva la realización de una firma digital por parte del operador que la realiza]
    - El sistema, una vez detecta que los certificados han sido entregados, envía el PIN / PUK (o palabra de paso del PKCS # 12) por correo electrónico firmado al poseedor de las llaves, indicado en la petición. Será responsabilidad del ente si se utiliza una misma dirección por diferentes peticiones.

2.5 Fase 5. Ciclo de vida

Aparte del ciclo de generación descrito en los pasos anteriores. El sistema permite la gestión del estado de los certificados.
A través del portal del SCD, por los roles 'Gestores' podrán realizar el cambio de estado de los certificados asociados a su ER.

Estas operaciones conllevan también la realización de una firma digital que quedará registrada al sistema.

3 Roles del sistema

A continuación se detallan cada uno de los roles de los sistema SCD y que están ligados a las operaciones que podrán realizar y en qué fase del flujo definido en el capítulo anterior.

La gestión de los operadores y sus roles se realiza por parte de un Administrador a partir de las credenciales de certificados en tarjeta criptográfica, excepto en los casos indicados expresamente.

3.1 peticionario

Rol de operador encargado de entrar las solicitudes de certificados.
También podrá importar archivos en formato texto que permite la introducción masiva de peticiones. Esta opción se puede definir por cada operador.

opciones Menú

- introducir peticiones
- Buscar peticiones

permisos especiales

- Puede importar peticiones en archivo

Tipo de certificados válidos para ser utilizados por este rol

- CIPISR emitidos por diversas EC's
- CDA's emitidos por diversas EC's. Este son para las aplicaciones que utilizan el conector y, por tanto, tendrán activado el permiso para importar peticiones a nivel de archivo.

3.2 peticionario Lotes

Rol de operador encargado de la gestión de lotes de peticiones para ser enviadas a un proveedor externo. Se trata de un rol reservado a personal del Consorcio AOC. Todos los filtros y el control de unicidad de las peticiones se ejecutan en esta fase.

opciones Menú

- nuevo Lote
- gestionar Lotes
- gestionar plantillas

Tipo de certificados válidos para ser utilizados por este rol

- CIPISR emitidos por diversas EC's.

3.3 aprobador

Rol de operador encargado de aprobar las solicitudes existentes y de dejarlas disponibles para generar el certificado.

opciones Menú

- Buscar peticiones

Tipo de certificados válidos para ser utilizados por este rol

- CIPISR emitidos por diversas ecs.

3.4 aprobador Lotes

Rol de operador encargado de la aprobación de los lotes de los lotes generados por el peticionario de lotes. Se trata de un rol reservado a personal del Consorcio AOC.
En caso de denegación, podrá indicar las peticiones con errores y consignar comentarios adicionales.

opciones Menú

- gestionar Lotes

Tipo de certificados válidos para ser utilizados por este rol

- CIPISR emitidos por diversas EC's.

3.5 Generador

Rol de operador encargado de generar los certificados a partir de solicitudes previamente aprobadas.
Se podrá activar la posibilidad de realizar las operaciones de aprobación y generación de manera unitaria.

Tipo de certificados válidos para ser utilizados por este rol

- CIPISR emitidos por diversas EC's.

Adicionalmente a la gestión realizada desde el portal del SCD, estos operadores deben gestionarse en una segunda capa dentro del entorno de la aplicación PKI, definiéndolos como Registration Officer.

3.6 Generador Lotes

Rol de operador encargado de generar la información para el envío a un proveedor a partir de los lotes previamente aprobados.

Tipo de certificados válidos para ser utilizados por este rol

- CIPISR emitidos por diversas ecs.

Adicionalmente a la gestión realizada desde el portal del SCD, estos operadores deben gestionarse en una segunda capa dentro del entorno de la aplicación PKI, definiéndolos como Registration Officer.

3.7 gestor Certificados

Rol de operador encargado de efectuar diferentes operaciones correspondientes al ciclo de vida de los certificados existentes (suspender, habilitar y revocar).

opciones Menú

- Buscar
- búsqueda avanzada

permisos especiales

- Operaciones permitidas. Revocar, suspender, habilitar
- Revocación automática. (Revocación a través de un conector)

Tipo de certificados válidos para ser utilizados por este rol

- CIPISR emitidos por diversas ecs.

3.8 Responsable del servicio de la Entidad de Registro T-CAT

Operador al cargo de una y sólo una Entidad de Registro que tiene privilegios para ver el estado de las peticiones de la ER y obtener informes de actividad de la misma.

opciones Menú

- estado peticiones
- informes

Tipo de certificados válidos para ser utilizados por este rol

- CIPISR emitidos por diversas EC's.

3.9 Responsable del servicio de la Entidad de Registro Virtual

Usuario interlocutor y gestor principal de cada ente ante el servicio. Será encargado de la fase de entrega y también podrá obtener informes de actividad de su ente. Un usuario puede ser responsable de más de un ente.

opciones Menú

- Informes de servicio
- Gestión de Entrega y PIN's
- Seguimiento de las peticiones propias (estado de tramitación)

Tipo de certificados válidos para ser utilizados por este rol

- Certificados personales, normalmente CPISR

Gestión de los operadores

En este caso la gestión, y debido al gran número de potenciales operadores se realiza de manera externa al sistema. El servicio del SCD T-CAT es, por tanto, autogestionado gracias a las consultas hechas al repositorio de usuarios y permisos (roles) de EACAT, ya disponible en los sistemas del Consorcio AOC.

Los datos disponibles son:

- Descripción del ente
- Datos del responsable de servicio (y los correspondientes suplentes)
    - Nombre y apellidos
    - correo electrónico
    - DNI del responsable

El algoritmo de decisión durante la autenticación del operador será el siguiente:

A.- Obtener el certificado CPISR utilizado en la conexión SSL
B.- Obtención del DNI contenido dentro del certificado CPISR
C.- Obtención de la lista de entes habilitados para el DNI obtenido

3.10 administrador

Operador con máximos privilegios, entre ellos el de crear otros operadores y concederles los permisos adecuados, y mantener los ficheros maestros de Entidades de Registro, organismo, perfiles y dispositivos. Restringido a operadores del Consorcio AOC.

opciones Menú

- operadores
- Entidad de Registro
- Lista de entes
- gestión entrega
- gestión DNS

Tipo de certificados válidos para ser utilizados por este rol

- CIPISR emitidos por diversas ecs.

Gestión de los operadores

Estos operadores se basan en una lista de confianza (ACL firmada digitalmente) configurada en la herramienta y gestionada manualmente. Hay que comunicar los números de serie de los certificados para que la pueda configurar.

3.11 depositario AOC

Operador con permisos para efectuar la entrega y la descarga de certificados cedidos por los entes a la AOC.

opciones Menú

- Búsqueda / Descarga

Tipo de certificados válidos para ser utilizados por este rol

- CIPISR emitidos por diversas ecs.

3.12 Compatibilidad entre roles

A continuación se muestra una tabla indicando los roles que son compatibles para un mismo operador:

	peticionario	peticionario Lotes	aprobador	aprobador Lotes	Generador	Generador Lotes	gestor Certificados	Responsable del servicio de la Entidad de Registro T-CAT	Responsable del servicio de la Entidad de Registro Virtual	administrador
peticionario on line		SI	NO	NO	SI	SI	SI	SI	NO	SI
peticionario Lotes			NO	NO	SI	SI	SI	SI	NO	SI
aprobador on line				SI	SI * / No	SI * / NO	SI	SI	NO	SI
aprobador Lotes					SI * / No	SI * / No	SI	SI	NO	SI
Generador on line						SI	SI	SI	NO	SI
Generador Lotes							SI	SI	NO	SI
gestor Certificados								SI	NO	SI
Responsable del servicio de la Entidad de Registro T-CAT									NO	SI
Responsable del servicio de la Entidad de Registro Virtual										SI
administrador										

*** Sí, sólo en caso de que hayan fusionado aprobador + generador.**

4 Módulos funcionales de la infraestructura

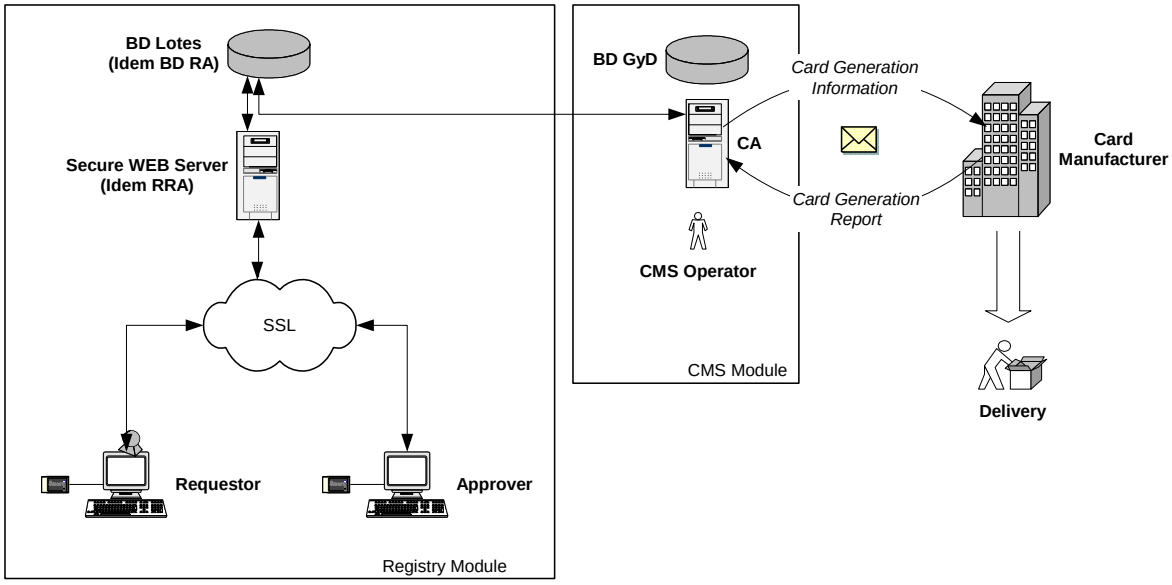
A continuación se describe con más detalle diferentes módulos del sistema. Estos aportan funcionalidades que aplican a partes del flujo descrito en capítulos anteriores y también operaciones enumeradas en la definición de los roles del sistema.

Esta descripción más detallada debe permitir tener una visión más exacta de su función, funcionalidad y por tanto impacto sobre el sistema global.

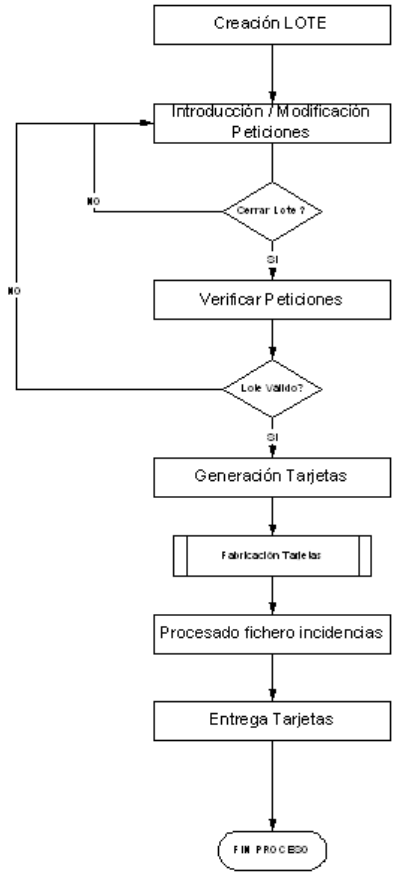
4.1 Sistema de emisión por lotes

Este módulo permite la gestión de las peticiones y agrupaciones de éstas (LOTES) que permiten la generación de las tarjetas de manera masiva y directa en las instalaciones del proveedor de las tarjetas GiD.

La arquitectura de esta parte dentro del sistema de certificación está descrita la siguiente figura.



A continuación se muestra el flujo de los datos en este circuito de certificación.



Como se puede observar en las anteriores figuras, a parte de la interfaz WEB para la introducción y aprobación de datos hay una pieza para la gestión del ciclo entre el Consorcio AOC y GyD, CMS Module. Este módulo permite realizar las operaciones a partir de los datos y que interaccionan tan con la fábrica de tarjetas (GyD) como con la entidad de certificación.

Las operaciones para cada fase del proceso, identificadas también con su rol son:

rol Peticionario

- → Creación / gestión de lotes de peticiones
- → Introducción de los datos de las peticiones de manera
  - → manual
  - → Importación de archivo
  - → Recuperación de peticiones con incidencias
  - → Importación a partir de la base de datos del sistema ONLINE
- → Exportación de peticiones hacia el sistema ONLINE
- → Creación / gestión de lotes de plantillas de datos
- → Visualización de las peticiones una vez emitido el lote

rol aprobador

- → Vista / aprobación / denegación de lotes de peticiones

→ Cambio de estado de un lote en proceso de producción.

Rol Generador (aplicación módulo generador)

→ Generación del fichero .req con los datos de las tarjetas a generar
→ Tratamiento del fichero .ret con las claves públicas, generación de los certificados y generación del archivo .batch que ya contiene los certificados y los PKCS # 12 de cifrado.
→ Tratamiento del fichero de incidencias .inc que cierra el ciclo con el fabricante de las tarjetas.

A continuación se detallan otros aspectos a tener en cuenta de este módulo.

4.1.1 Acceso al sistema

Para acceder al módulo necesario disponer de:

- Certificado de operador reconocido con rol PETICIONARIO o aprobadores
- Conexión al servidor WEB interno (Importante: módulo no accesible desde Internet)
- Navegador Chrome + JAVA
- Sólo disponible actualmente para la entidad EC-Sector público

4.1.2 Estados de los lotes

A continuación es describen los diferentes estados que puede tener un lote.

código Estado	***estado***	***Descripción***	**Quién puede operarlo?**
100	abierto	Lote creado y disponible para la modificación e introducción de peticiones	PETICIONARIO
200	cerrado	Lote preparado para su aprobación	aprobador
300	aprobado	Lote preparado para su generación a partir de la ER	GENERADOR o aprobador
400	emitido	Lote en proceso de fabricación	GENERADOR o aprobador
500	recibo	Lote finalizado. Se puede proceder a la entrega de las tarjetas.	PETICIONARIO (lectura)

4.1.3 Estados de las peticiones.

A continuación es describen los diferentes estados que puede tener una petición dentro de un lote. Este estado cambio de manera automática al realizar algún paso del flujo del sistema.

código Estado	*estado*	*Descripción*
0	VALID	Petición introducida por el peticionario. Es marca como válida pero no asegura que contenga los datos necesarios.
1	VERIFIED	Petición verificada por el aprobador
2	INVALID	Petición invalidada por el aprobador
3	ISSUED	Petición correcta pendiente de entrega de la tarjeta
4	DELIVERED	Petición correcta y entregada al poseedor
5	ERROR	Petición que ha causado error durante la fabricación de la tarjeta
6	RE-ISSUED	Petición que ha causado error y posteriormente se ha recuperado para su reemisión.

4.1.4 rol Peticionario

4.1.4.1 funcionalidad generales

- Cada peticionario gestiona sus lotes y plantillas de lotes, por lo tanto los peticionarios no comparten en ningún caso la información contenida en el lote. El sistema actual, no permite pues, que un peticionario pueda ver lotes de otro peticionario sea cual sea el estado del mismo.
- Todas las operaciones se realizan a nivel de lote y por tanto el primero que tiene que hacer el peticionario es acceder / crear un lote.
- Sólo se pueden introducir las peticiones que están soportadas dentro del sistema de lotes. Actualmente tenemos las siguientes políticas: CPISR-1 y CPISRC-1.

4.1.4.2 Plantillas de lote

- Las plantillas de lote definen un conjunto de datos prefijadas que se utilizarán por defecto si durante la introducción / importación de la petición éstas no están definidas.
- Se permiten las operaciones de ALTA, MODIFICACIÓN y BAJA de las plantillas.
- Las plantillas se visualizan a partir del dato introducida en el campo NOMBRE.
- Las plantillas son exclusivas de cada usuario.

4.1.4.3 Gestión manual de peticiones

- El formulario de visualización de datos es fijo para todos los tipos de certificado
- En la operación de alta llenan los campos con el valor de la plantilla relacionada al lote
- Es realizan validaciones de los datos a nivel de Javascript en determinados campos
- Si falta un dato obligatorio hay que llenarla para seguir adelante
- Al visualizar una petición la podremos MODIFICAR o BORRAR

4.1.4.4 Importación de peticiones a partir del sistema ONLINE

- El buscador de peticiones contra el sistema de certificación ONLINE con el mismo look que tienen los buscadores de los aprobadores actuales, incluyendo el ID_TRAMESA
- Si se importa una petición en estado aprobado, la información de esta aprobación (firma) es pierde.
- El módulo que permite importar las peticiones del módulo ONLINE al módulo de lotes es el Módulo Peticionario del sistema de LOTES.
- Para hacer la importación el sistema permite buscar peticiones en cualquier estado, es decir pendientes de aprobar, aprobadas y denegadas
- Una petición importada al sistema de lotes desaparece del sistema ONLINE para siempre (hay por temas de unicidad)
- La función de importación ejecuta la misma validación de datos que se aplica actualmente a la importación de datos a partir de archivo plano.

4.1.4.5 Importación de peticiones a partir de fichero

- Es mantiene la posibilidad de importar peticiones a partir del fichero generado con ACCES (sortida_lot.txt)
- El formato de este archivo está definido en el documento 'Formato de importación peticiones para sistema LOTS_v1.4.doc' situado en el directorio M: \ NouPrometeo \ Departamentos \ Tecnica \ Documentacio_PKI_CATCERT \ LOTES \
- El sistema de importación tiene en cuenta los valores de la plantilla asociada por los campos no definidos en el archivo
- Es realizan una serie de validaciones antes de aceptar cada registro

4.1.4.6 Recuperación de peticiones erróneas

- El sistema permite importar también peticiones erróneas de otros lotes en estado RECIBO.
- Al realizar esta operación la petición origen queda en estado Re-issued
- Esta operación afecta a todos los lotes en estado recibido

4.1.4.7 Exportación de peticiones al sistema ONLINE

- Cuando visualizamos la lista de peticiones de un lote es permite la exportación de las mismas
- La exportación inserta al sistema ONLINE la petición con los datos de peticionario del operador que está operando
- Las peticiones quedan por defecto en estado pendiente de aprobar

4.1.4.8 Cierre del LOTE

- El peticionario 'ordena' la generación de un lote a partir de su cierre
- En la operación de cierre es verifica la unicidad de las peticiones introducidas tanto contra la mesa certificados como el sistema ONLINE.
- Es valida que dentro del lote no existan dos peticiones con el mismo DNI. Esta restricción está originada por el procedimiento de generación que utiliza GyD.

4.1.5 rol aprobador

- Se pueden visualizar los lotes en estado CERRADO y EMES
- Por defecto es visualizan los lotes de los últimos 3 meses
- Sobre los lotes en estado cerrado pueden Aprobar o rechazar el Lote
- A nivel de petición podemos asignar una razón de denegación por cada petición
- La aprobación implica la realización de una firma digital
- Los datos firmados son un resumen de las peticiones del lote
- Sobre un lote en estado emitido podemos volverlo a estado ABIERTO. Esta operación sólo es para casos excepcionales de error durante la generación del archivo .ret con la aplicación de gestión de Lotes

4.2 Gestión de diseños / personalizaciones de tarjetas

Este módulo permite la gestión de los diferentes tipos de tarjeta física y que pueden contener en su chip certificados de políticas diferentes.
Así, por ejemplo, un certificado de tipo CPISR-1 podrá generarse en diferentes tipos de plástico en función del ente final donde estarán destinadas.
También se puede gestionar a nivel de permisos del operador qué diseños de tarjetas puede generar una determinada Entidad de registro

4.2.1 requerimientos

A continuación se enumeran una lista de requerimientos que soporta el nuevo módulo

- Sistema para gestionar de manera más eficiente los posibles diseños de tarjetas diferentes presentes en la plataforma de certificación.
- Sobre una misma política de certificado (por ejemplo CPISR) pueden aplicar N diseños de tarjeta
- El diseño es elegido por el peticionario a partir de un desplegable en el momento de introducir los datos de la petición
- Los diseños disponibles para una política será la intersección entre los diseños ligados al perfil y diseño permitidos ala ER del peticionario (entidad de registro asociada).
- Desde el módulo de administración se configuran los diseños ligados a cada ER

4.2.2 Solución técnica y funcionamiento

A continuación se describe la solución técnica que se ha implementado para alcanzar los requerimientos descritos.
Esta aproximación a la implementación permite entender de una manera más clara los pasos que hay que hacer en el momento que se quiere añadir o modificar los datos ligados a un determinado diseño.

4.2.3 Ficheros de mapeo y diseño

Cada diseño está formado por dos ficheros de definición:

1. **Archivo de diseño físico:** Contiene las características físicas del diseño tales como:
    a. Número y posición de las líneas de impresión que van tan al anverso como el reverso.
    b. Tamaño de la letra de cada línea
    c. Alineación de las líneas
    d. Posición de las imágenes o logos
    e. Presencia de datos la banda magnética
2. **Archivo de mapeo de datos** Principalmente contiene toda la lógica necesaria para 'ligar' los datos del formulario con las líneas físicas definidas en el archivo de diseño físico. Dentro de este archivo se pueden:

    a. Incluir nuevos campos que aparecerán en el formulario y que nos permitirán pedir al operador datos que sólo se usan para imprimir, por ejemplo una fotografía.
    b. Fijar el vínculo entre datos del formulario y el diseño físico pueden incorporar, por ejemplo, partes fijas de texto.
    c. Opcionalmente se pueden volver a definir campos del formulario que ya están definidos a nivel de archivo de política para hacerlos más restrictivos (por ejemplo es limita el campo de la organización a un desplegable de 1 solo valor)

4.2.4 Archivo de política

Dentro de este archivo se definen los siguientes datos:

1. Datos relativos al certificados y datos de gestión.
2. Aparece un campo dentro del archivo de política, card_design, y que se define del tipo lista con un conjunto de valores igual a la lista de DISEÑOS disponibles para esta política. Por ejemplo para CPISR_1 de SAFP tenemos

```
spec_card_design <<<! spec_EOF
        label = Tipo de tarjeta
        type = INFO
        values = MAP_CATCERT_BASIC, MAP_JUSTICIA_BASIC, MAP_CAC_BASIC
        default_selected = MAP_CATCERT_BASIC
        filter_variable = op_design_list
spec_EOF
```

Con estas definiciones se consigue poder reaprovechar el mismo archivo de política aunque este pueda generar en tarjetas tan diferentes como la de por defecto.

4.2.5 Configuración a la entidad de registro. WEB Administración

Dentro del perfil del er se puede:

1. Configurar por cada entidad de registro el conjunto de diseños que puede generar de la lista de diseños disponibles.
2. Los operadores tendrán ligada su configuración a su entidad de registro en la que pertenecen.

4.2.6 funcionamiento

Cuando un operador (peticionario) es conecta al servicio:

→ se obtiene de la sede perfil la lista de diseños permitidos para su entidad de registro.
→al seleccionar una política se hace la intersección entre la lista de diseños del operador y la lista de diseños de la política. Si el resultado es> 1 aparece un desplegable para seleccionar el tipo de tarjeta. Si el resultado es 1 se pasa automáticamente al siguiente paso.
→ Es genera el formulario a partir de los datos del archivo de política más los datos adicionales definidas dentro del archivo de mapeo.

4.2.7 Pasos para incorporar un nuevo diseño

De manera resumida, la incorporación de un nuevo diseño conlleva los siguientes pasos:

1. Crear el archivo de definición físico
2. Crear el archivo de mapeo
3. Modificar los archivos de políticas que aplica el nuevo diseño
4. Modificar el archivo de definición de plantillas para incorporar el nuevo diseño
5. Modificar el archivo de configuración de la parte de administración
6. Entrar a nivel de administración y activar el nuevo perfil a las entidades de registro correspondientes.

4.3 Sincronización de la lista de entes

Cada operador que accede al sistema SCD, aparte de determinadas excepciones, no podrá ver, por ejemplo, todos los certificados de la EC. El sistema filtrará los entes en función del perfil del operador. Estos filtros de datos tienen efectos prácticos sobre todo en dos punto del flujo:

Petición de certificados. El filtro limitará el conjunto de valores válidos en el campo Organización de los formularios. No se permitirá la introducción de valores libres para el campo organización.

Gestión de certificados. El filtro limitará el conjunto de certificados que podrá ver el operador y, por tanto, gestionar su estado.

El sistema realizará la siguiente secuencia para establecer a qué nos puede acceder el operador.

1. Obtener la ER en la que pertenece el operador
    - Acceder a las propiedades de la ER y obtener la lista de de entes asociados
2. Aplicar a los filtros de búsqueda la lista obtenida en el punto anterior

La anterior secuencia no se aplica a los siguientes roles que tienen una visión global de todas las peticiones:

- peticionario Lotes
- aprobador Lotes
- Generador Lotes

Tampoco se aplica a todos los operadores de la ER con código 000.

el rol **Responsable del servicio de la Entidad de Registro Virtual** tiene un comportamiento especial ya que sólo podrá ver las peticiones o certificados asociados a su ente.

El sistema genera la tabla de entes dentro de su base de datos a partir de una sincronización entre el entorno PKI y el entorno donde está el maestro de terceros (EACAT).

Esta sincronización se realiza mediante una tarea programada en el entorno de la PKI con las siguientes características:

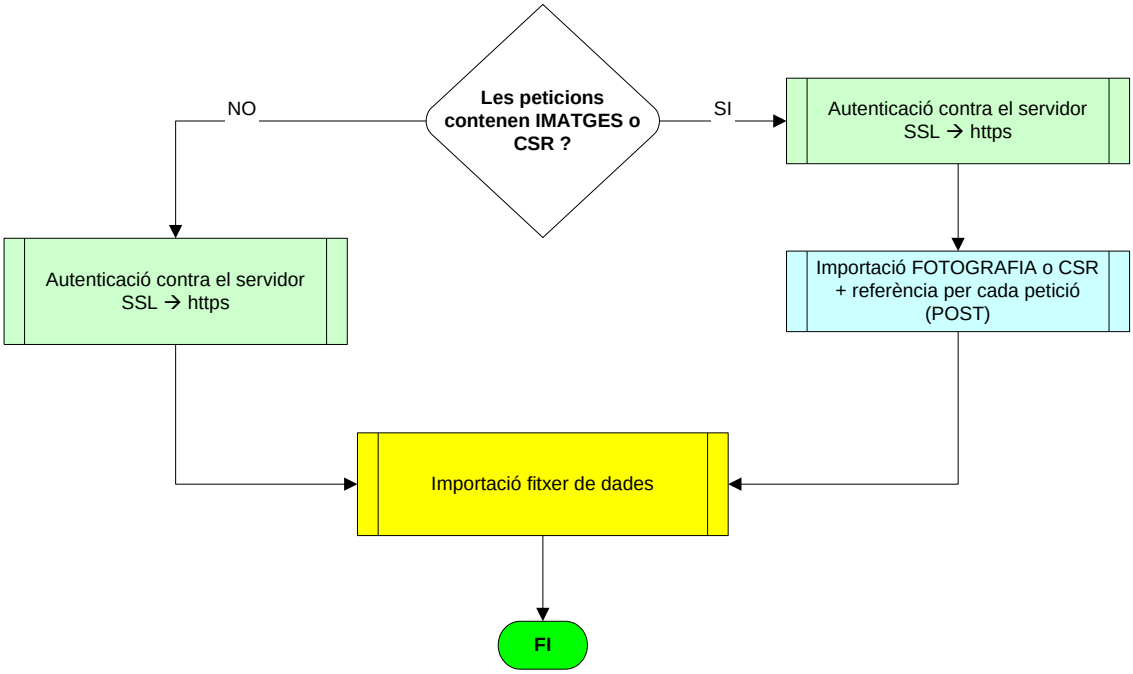
- Se ejecuta cada 30 minutos
- Actualizar los datos de los entes y también de los responsables titulares y suplentes asociados a cada uno de ellos.
- Una vez finalizada la sincronización borra los registros que ya no han sido sincronizados (se trata de una baja).
- En cada ejecución genera trazas e informes en formato CSV con los siguientes elementos:
    - Organismos con descripción demasiado larga y que por tanto no son válidos para la generación de certificados (actualmente fijado en 57 caracteres)
    - Lista de certificados huérfanos de la BD de la CA. Son aquellos que tienen asociado un CODI_ENS que no existe en el maestro. Estos certificados sólo pueden ser operados por operador asociados a la ER con código 000.
    - Por defecto los entes nuevos asocian a la ER 000
    - Los entes se pueden separar por EC en función de un campo del sistema de Terceros.

4.4 Interfaces para operaciones automáticas

4.4.1 Introducción de datos

El proceso de entrada de una petición en la plataforma de certificación puede llevarse a cabo por medio de un operador (persona humana) de la entidad de certificación o por medio de un proceso automático (una máquina / programa). A continuación se describe el módulo que permite la recepción peticiones automáticas.

Técnicamente se trata de un CGI disponible dentro del portal del servicio SCD (https con autenticación de cliente). Para realizar una petición el cliente requiere disponer de un certificado de aplicación (CDA).
La petición será un POST de los datos de la petición siguiendo un formato determinado. En función del tipo de certificado que se quiera peticionar el número de campos requeridos y el formato de los datos variará.
Si la petición contiene algún campo de datos que puede ser de gran tamaño, por ejemplo fotografías y / o peticiones de certificado (CSR) se deberá realizar la importación en dos



pasos. La primera consistirá en la importación de la fotografía o CSR junto con una referencia y el segundo paso importa el resto de datos de la petición.
A continuación se muestra una figura con el flujo de la importación de una petición.

Por otra parte el cliente puede solicitar tres acciones diferentes asociadas a una petición:

- **ALTA**: Permite entrar una petición nueva dentro de la plataforma.
- **MODIFICACIÓN**Modifica alguna de los datos asociados con alguna petición ya existente. El campo que se utiliza para identificar la petición es el documento de identificación (NIF, NIE, etc.) junto con el tipo del certificado de la petición.
- **BAJA**: Permite eliminar alguna petición ya existente en la plataforma. El campo que se utiliza para identificar la petición es el documento de identificación (NIF, NIE, etc.) junto con el tipo del certificado de la petición.

Aparte de las operaciones, el módulo tiene dos modos de funcionar

- En modo Normal.
- En modo Transacción.

A continuación es describen de manera funcional los dos modos.

Importación de peticiones en modo NORMAL

En este modo las peticiones son introducidas de manera unitaria al sistema y no conllevan la realización de tareas adicionales a las definidas en el procedimiento general.
Así en un fichero con diferentes peticiones, el resultado de la importación puede ser satisfactorio para algunos de los registros y errónea por otra parte.
Por otra parte en este caso se hará uso de algunos de los campos del archivo de importación ligados a la importación en modo transacción. Estos parámetros son:

- ID_TRAMESA - identificador de envío
- CODI_ENS - Código del ente

Importación de peticiones en modo TRANSACCIÓN

En este modo las peticiones son introducidas de manera conjunta (transaccional) al sistema y comportan la realización de tareas adicionales a las definidas en el procedimiento general.
Así en un fichero con diferentes peticiones, si el resultado de la importación de un registro es erróneo, ninguna de las peticiones será importada dentro del sistema.
En este modo y de manera adicional al procedimiento estándar de importación definido anteriormente, se realizan las siguientes acciones.

1. Si la importación es correcto se crea un registro en la tabla de ENVÍOS
2. Se tratan los nuevos datos ID_TRAMESA y CODI_ENS.
3. Se valida que el valor de ID_TRAMESA es igual en todo el archivo
4. También es genera de forma automática el dato POS_TRAMESA como la posición de la petición dentro envío (calculada automáticamente de1 a N)

4.4.2 Integración del módulo

URL de servicio

En función de la entidad de certificación por la que se quiera cargar una petición deberá usar una url u otra. Actualmente, los servicios de registro automático que están operativos para las siguientes Ecs y en las siguientes urls:
https://scd.aoc.cat/connectors

Donde IDCA puede tener los siguientes valores:

- EC_AL
- EC_SAFP

Si queremos realizar la importación en modo transacción habrá que añadir a las anteriores URLs & importMode = TRANS.

Para la importación de objetos del tipo fotografía o CSR habrá que utilizar la misma URL.

Será en función de otros parámetros enviados a esta URL que el sistema realizará una operación u otra.

Hay que hacer notar que desde el módulo peticionario de cada EC también se permite la importación de los archivos de texto que contienen las peticiones. Para acceder a esta URL

habrá una tarjeta de operador habilitada al sistema, con rol Peticionario y el permiso específico para importar peticiones.

pasos integración

La aplicación tendrá que hacer un post a la dirección indicada en el punto anterior con las siguientes variables:

- **importPet.** Debe contener el archivo de texto en el formato definido y coherente con el siguiente parámetro.
- **operationType.** Puede tener dos valores:
  - **ENROLL_DATA.**Para operaciones de introducción de peticiones. En este caso importPet debe ser este formato0
  - **ENROLL_OBJ.**Para operaciones de introducción de fotografías o csrss. En este caso importPet debe ser este formato0

Para hacer este post será necesario establecer una conexión SSL con el servidor y autenticarse con el certificado CDA proporcionado.

Urls de pruebas
Para poder probar si el desarrollo de la parte cliente funciona disponemos de URLs en el entorno de preproducción.
Las URLs de preproducción son las mismas de producción cambiando https://scd.preproduccio.aoc.cat/.

4.4.3 Formato general de los archivos de importación

En los siguientes apartados se muestra el formato y campos que deben contener las peticiones de manera general para todos los tipos de certificados. A partir de estas pautas generales habrá acabar 'de generar el archivo en función del tipo de certificado que queremos peticionar. La documentación asociada a cada tipo de certificado se puede obtener directamente del sistema (verObtener archivos de ejemplo para cada tipo de certificado).

Formado por el archivo de importación de fotografías o peticiones de certificación CSR

El formato del archivo de importación de datos tipo Petición de certificación (CSR) o fotografías es el siguiente:

Línea 1, Valor fijo
`IDENTIFICADOR | VALOR`
Líneas de peticiones
`<REFERENCIA> | <VALOR>`
Dónde
→ REFERENCIA es el un identificador alfanumérico libre de longitud máxima 10.
→ VALOR es la petición de certificación o la fotografía en formato textual BASE64 sin saltos de línea.

IMPORTANTE. Aunque el valor de origen ya esté en base64, SIEMPRE hay que aplicar la transformación del valor en base64 sin saltos de línea

ejemplo

```
IDENTIFICADOR | VALOR
00A123ASER | TUlJQ0R6Q0NBWGlnQXdJQkFnSUJBRE ..... EVWa2IrSmZkWDBSUk5vRHEvMExSNUNnMlQ4
```

Formado por el archivo de importación de peticiones

El formato del archivo de importación de peticiones es autodefinido, es decir en el primer registro define los campos que incorpora la petición. Así el formato del archivo será el siguiente:

línea 1
DEFINICIÓN | OPERACION | ESTADO | OPERADOR | ID_TRAMESA | CODI_ENS | <Lista de campos separados por |>

Líneas de peticiones
<ID_POLITICA> | <OPERACIÓN> | <ESTADO> | <OPERADOR> | <ID_TRAMESA> | <CODI_ENS> << Valores>

Dónde
→Lista de campos es el listado de campos de la petición. Esta lista depende del tipo de certificado. La propia aplicación permitirá la generación y descarga de ficheros de ejemplo para cada tipo de política que tenga permitida el operador.
→ID_POLITICA es el código que identifica la política. Por ejemplo CPISR_1, CESR_1, CDS_1, etc.
→OPERACION es la operación que queremos realizar sobre la petición. Los valores posibles son

- **ALTA**. nueva petición
- **MOD**. Modificación de peticiones. En caso de no existir se comporta igual que la operación ALTA
- **BAJA**. borrar petición

→ESTADO es el estado en que quedará la petición en la base de datos. Los valores posibles son:

- **PENDIENTE**. Peticiones en estado Pendiente de aprobar
- **APROBADA**. Peticiones en estado aprobado.
- **BORRADOR**. Peticiones en estado borrador

→OPERADOR es el código de operador que se insertará en la base de datos. Este valor permite gestionar el flujo de las peticiones dentro del sistema de registro de la entidad de certificación (códigos de ER) será la AOC quien dará los códigos en función de la naturaleza de la aplicación de importación de peticiones. El código del OPERADOR se fija tan al campo codipeticionari como codiaprovador al realizar importaciones con el código especificado en el archivo.
→ID_TRAMESA. [OPCIONAL] Es el código del envío. Su formato es del estilo 3bc3755b-1101-4ccf-b3a8-8955bccpf690
→CODI_ENS. [OPCIONAL] Es el código del ente. Su formato es del estilo 800600000.

ejemplo

```
DEFINICIÓN | OPERACION | ESTADO | OPERADOR | cn | CN2 | doc_type | doc_num | ea | user_upn | categoría | cargo | huevo | o | cif_org | resp_nom | resp_nif | resp_ea | resp_address | resp_cp | resp_pob | foto
CPISR_1 | ALTA | PENDIENTE | 0001001 | José | Catalán Pujol | NIF / NIE | 91554344B | estu1234@urv.es | W2000 @ dominio | TU -Titulares de universidad | cargo | departamento | URV | 11223344E | José Morey Gualta | 98786545Q | jmorei@urv.es | c / paseo la golondrina, 25 | 43001 | Tarragona | ref_foto
```

Como podemos ver en el ejemplo anterior el valor de la columna foto es el valor de la referencia utilizada en el paso anterior.

4.4.4 Obtener archivos de ejemplo para cada tipo de certificado

El sistema permite obtener la lista de campos de un tipo de certificado así como un archivo de ejemplo para la importación de una petición hay que seguir los siguientes pasos:

1. Acceder con un certificado de operador o el propio certificado CDA en la URL del servicio.
2. El sistema tiene una opción para acceder a una página con la lista de los tipos de certificados disponibles para el operador.
3. En este momento se generan ficheros de ejemplo para cada combinación de política y diseño de tarjeta disponible, permitiendo la descarga del mismo.

4.4.5 Interpretación de los mensajes de salida:

Se devuelve información sobre el estado de finalización de la carga de cada petición de archivo de entrada. Se identifica cada petición de entrada con el número de línea que ocupaba en el fichero de entrada acompañado de un mensaje de estado de finalización que puede ser "OK" o "ERROR". En el caso de "ERROR", acompaña un pequeño texto descriptivo del error y, en algunos casos, se muestra el valor que ha originado el mensaje de error.
Las peticiones con indicador de estado de finalización "OK" habrán sido cargadas correctamente dentro del sistema. Junto con el identificador OK, aparece un ID, se trata del identificador único de la petición en la base de datos enrollar. Las aplicaciones no deben hacer uso de este ID.
Las peticiones con indicador de estado de finalización "ERROR" no habrán sido cargadas en el sistema ya que no cumplían alguna de las restricciones de formato de los campos o de archivo requeridas para ese perfil. El mensaje que acompañará este indicador aportará información respecto del origen del error.

Ejemplo de salida

1.ERROR | El código de país del pasaporte / DNI foráneo no es válido (AA). Consulte la lista de códigos de país válidos.
2. OK | A13423BEF67
3.ERROR | El campo Pasaporte / DNI foráneo no puede ser nulo
4.ERROR | El campo Pasaporte / DNI foráneo = ES-123456789566546546546546546540987654321098765432 1 supera la longitud máxima 15
5.ERROR | Formato de Pasaporte / DNI foráneo incorrecto (ES11SFA54321).
6.ERROR | El código de país del pasaporte / DNI foráneo no es válido (AA). Consulte la lista de códigos de país válidos.
7. OK | F1323EA90A
8.ERROR | El campo Pasaporte / DNI foráneo = ES-123456789546546546540987654321098765432 1 supera la longitud máxima 15
9.ERROR | El campo Pasaporte / DNI foráneo no puede ser nulo
10.ERROR | Formato de Pasaporte / DNI foráneo incorrecto (ES11SFA54321).

4.4.6 Revocación de certificados

Los requerimientos del módulo de revocación automática son:

- Posibilidad de revocar certificados de a partir de una llamada automática al sistema, sin necesidad de operar la consulta avanzada
- El proceso remoto autenticará al sistema mediante el uso del protocolo SSL y presentando un certificado del tipo CDA
- El certificado CDA estará habilitado al sistema de consulta avanzada con rol Gestor y activando la opción de 'Revocación automática'.
- Los certificados que sobre los que podrá operar un CDA en concreto estarán limitados a los entes que tenga relacionado este certificado, a partir de la ER asignada.
- Las operaciones de cambio de estado desde la WEB dejan un rastro firmada de la operación dentro del sistema. En el caso del conector, esta traza será firmada por el certificado interno.
- Existe un modo de funcionamiento, orientado al uso desde EACAT, que permite realizar las operaciones de forma TRANSACCIONAL. Sólo se realiza la operación si todos los registros del archivo de entrada son correctos.
- El uso del modo TRANSACCIONAL conlleva la creación automática de un registro de ENVÍO dentro del sistema. Este hecho no tiene ninguna implicación directa sobre las operaciones de revocación.
- Se podrá indicar en la petición si se quieren revocar también los certificados relacionados al indicado. Es considera un certificado relacionado lo
    - tiene el mismo código de suspensión
    - está emitido en un tiempo cercano
- El registro de la tabla de envíos contiene los siguientes datos
    → Número de envío -> generado aleatoriamente
    → Fecha de recepción y finalización coinciden
    →Datos del operador. Se obtienen del CDA que envía el archivo a la consulta avanzada
    → Tipo ENVÍO código 200

4.4.6.1 funcionamiento

El flujo del módulo de revocación es el siguiente:

→ Obtener datos del certificado SSL (CDA)
→Consultar el ROL del certificado al sistema. Tiene que ser Administrador o Revocación automática '
→ Cargar el archivo de peticiones con nombre revocationFile
→ Por cada línea del archivo
    → Verificar que no se trata de un número de serie repetido dentro del archivo
    → Verificación del código de razón existe en la configuración
    →Verificar la existencia del número de serie. (Aquí se aplica el filtro de ER si procede) y si está indicado en el parámetro correspondiente obtener los certificados relacionados.
    → Verificar que el certificado (y los relacionados) no está caducado
    → Verificar que la acción requerida no sea incompatible con el estado actual del certificado
→ Realizar las operaciones de revocación en un solo lote de revocación y generar la traza firmada.

→ generar salida

4.4.6.2 Integración con el módulo

URLs de servicios y requerimientos

la URL del módulo de revocación en su modo de funcionamiento NORMAL será:
https://scd.aoc.cat/connectors/connector.ws?idCA= <valor>

Donde IDCA puede tener los siguientes valores:

- EC_AL
- EC_SAFP

la URL del módulo de revocación en su modo de funcionamiento TRANSACCIONAL será:
https://scd.aoc.cat/connectors/connector.ws?idCA=<valor>&importMode=TRANS

La aplicación que acceda dispondrá de un certificado de tipo CDA y las correspondientes claves para su verificación y también para verificar el certificado del servidor https://scd.aoc.cat.

pasos integración

La aplicación tendrá que hacer un post a la dirección indicada en el punto anterior con las siguientes variables:

- **revocationFile.**Debe contener el archivo de texto de las peticiones de revocación.
- **operationType.** Valor fijo a REVOKE

Para hacer este post será necesario establecer una conexión SSL con el servidor y autenticarse con el certificado CDA proporcionado.

Formato de archivo de peticiones

El archivo de texto que contiene las peticiones tendrá el siguiente formato:
línea 1
SERIAL | ACCION | RAO | MODE | CIF
Líneas de peticiones
NUMERO_DE_SERIE | OPERACION | RAZÓN | MODE | CIF

Dónde
→NUMERO_DE_SERIE. Número de serie del certificado, sin espacios y en mayúsculas
→OPERACION. Operación a realizar sobre los certificados. Las operaciones posibles son REVOCAR, SUSPENDER o HABILITAR.
→RAZÓN. Razón asociada a la acción. Ver por las posibles combinaciones.
→MODE. Indica si se quiere actuar sobre los certificados relacionados o no. Hay dos valores posibles:
000 - Aplica sólo al certificado indicado
001 - Aplica el certificado indicado y sus relacionados si existen
→CIF. Valor del CIF del ente del certificado.
El archivo podrá contener N registros con números de serie distintos.

ejemplo
SERIAL | ACCION | RAO | MODE | CIF
44918ADC7106693643B409DEDB1ED9BF | SUSPENDER | S01 | 001 | A12345678
7AAEBD0D2D5DE71843B409DE61FA71FC | REVOCAR | R01 | 001 | A12245678

761E3D8A562C6A2F437DDEA9302C75EA | REVOCAR | R02 | 000 | A12343278
18C410A5F42376CC43B415F2C304AF4C | HABILITAR | H01 | 001 | A11115678

Formato de archivo de respuesta

La respuesta de la operación POST, devuelve una página text / html que contendrá unos registros por cada uno de los registros del archivo de entrada con el siguiente formato.

NUMERO_REGISTRE | RESULTADO | CODI_ERROR | DESCRIPCIO_ERROR

Dónde
→NUMERO_REGISTRE. Número de registro relacionado con el archivo de entrada. Comienza por 0.
→RESULTADO. Resultado de la operación. Los resultados posibles son OK o ERROR.
→CODI_ERROR. Código de error producido. Ver por las posibles combinaciones.
→DESCRIPCIÓ_ERROR. Descripción del error.

ejemplo

0 | ERROR | E12 | El certificado con número de serie 44918ADC7106693643B409DEDB1ED9BF no existe
1 | OK |
2 | OK |
3 | ERROR | E15 |

4.4.6.3 Relación de razones de revocación y referencia de errores

Razones de Revocación
La siguiente tabla contiene las diferentes razones de revocación en función de la operación requerida.

ACCIÓN	CÓDIGO RAZÓN	Descripción
HABILITAR	**H01**	habilitar certificado
SUSPENDER	**S01**	Sospecha de que el certificado contiene datos incorrectos
	S02	Sospecha de pérdida del dispositivo criptográfico o del certificado
	S03	Sospecha de uso o acceso a la clave privada del certificado por parte de un tercero
	S99	otros
REVOCAR	**R01**	Compromiso de la información contenida en el certificado
	R02	Compromiso de la seguridad de la clave o del certificado
	R03	Compromiso del dispositivo criptográfico
	R04	Motivos referentes al suscriptor o al poseedor de claves
	R99	otros

4.4.6.4 Relación de errores

La siguiente tabla resume los posibles errores que se pueden producir al utilizar el módulo de revocación automática.

CODI_ERROR	Descripción
ERRORES GENERALES	
E00	Error inesperado del sistema. La descripción proporciona el error de bajo nivel.
E01	Certificado CDA no dispone de permisos para utilizar el servicio
ERRORES PARA REGISTRO	
E10	El número de serie está repetido dentro del archivo
E11	Error al realizar la consulta del número de serie dentro la BD La descripción proporciona el error de bajo nivel.
E12	El certificado especificado no existe, o el usuario no tiene permisos sobre él, o el CIF indicado no es correcto
E13	El certificado especificado está caducado. No se puede realizar ninguna operación sobre él.
E14	El certificado especificado es válido y por tanto no se puede habilitar.
E15	El certificado especificado está suspendido y por tanto no se puede suspender
E16	El certificado especificado está revocado. No se puede realizar ninguna operación sobre él.
E17	La razón especificada no está definida
E18	La razón y la acción no son coherentes

4.5 Sincronización de operadores

Para tener una capa más de seguridad, el sistema permite la definición de las relaciones entre operadores con rol aprobador y operadores con rol generador.

Cuando un aprobador y un generador están relacionado significa que el generador podrá procesar y por tan generar los certificados de las peticiones aprobadas por el rol aprobador.

Esta relación se define en el portal SCD por parte de los operadores Administradores. Aparte de esta configuración hecha a nivel del portal, la relación implica que el generador, cuando opera con la aplicación del módulo generador, verifica las firmas realizadas en la operación de aprobación por parte del operador.

Para poder hacer esta validación hay que construir para cada generador el conjunto de confianza de los aprobadores relacionados para poder hacer la verificación de la firma.

4.6 Generación de documentación

A continuación se describen los diferentes aspectos que permiten la gestión y generación de la documentación necesaria durante los procesos de generación de los certificados digitales.

4.6.1 requerimientos

Dentro de la gestión de documentos se cumplen los siguientes requerimientos.

- La documentación se genera a partir de una serie de documentos base
- El procedimiento de personalización se realiza a partir de la sustitución de cadenas concretas de texto que están dentro del documento.
- El sistema permite definir qué documentos se generan por cada tipo de certificado. Los tipos de documentos definidos son:
    - **FL** - Hoja de entrega
    - **CL** - Carta de lote
    - **PIN_PUK_TEMPLATE**
- El sistema permite definir qué grupos de documento, en función de la política, se envían a cada ER en función de su código de ER.
- El proceso de sustitución se realiza en dos puntos
    - En el proceso de generación de los documentos que se envían a una ER. En este punto se realizan las sustituciones de los datos fijos que dependen de la ER.
    - En el proceso de generación de los certificados. En este punto, ya partir de los documentos que se reciben dela CA, Se realizan las sustituciones de los datos que dependen de la petición de certificación que estamos generando.

4.6.2 Elementos técnicos del módulo

Existirán tantos archivos como plantillas de documentos diferente. En una primera versión tenemos la siguiente lista:

- CATCERT_CDS-CDA-CDSDC-CDP_CL.rtf
- CATCERT_CDS-CDP-CDA-CDSDC_FL.rtf
- CATCERT_CPISR-CPISRC-CESR_AL.rtf
- CATCERT_CPISR-CPISRC-CESR_CL.rtf
- CATCERT_CPISR-CPISRC-CESR_CP.rtf
- CATCERT_CPISR-CPISRC-CESR_FL.rtf
- CATCERT_PIN_PUK_TEMPLATE.rtf
- GENERIC_CDS-CDA-CDP-CDSDC_CL.rtf
- GENERIC_CDS-CDP-CDA-CDSDC_FL.rtf
- GENERIC_CPISR-CPISRC-CESR_AL.rtf
- GENERIC_CPISR-CPISRC-CESR_CL.rtf
- GENERIC_CPISR-CPISRC-CESR_CP.rtf
- GENERIC_CPISR-CPISRC-CESR_FL.rtf
- GENERIC_PIN_PUK_TEMPLATE.rtf

Donde los archivos que empezamos con CATCERT_ * pertenecen a las plantillas utilizadas para la ER del Consorcio AOC (código 000) y los archivos que empiezan por GENERIC_ * pertenecen a las plantillas utilizadas por el resto de ER.

Estos documentos pueden ser diferentes para cada EC.

Por otra parte, existe un archivo por cada ER (xxx.txt). El contenido de este archivo incluye:

AMBIT_DESC = Descripción de la ER
AMBIT_ADRESS = Dirección postal
AMBIT_POB = Población
AMBIT_CP = Código Postal
AMBIT_RESP = Nombre y apellidos del responsable
AMBIT_TEL = Teléfono de contacto
AMBIT_CIF = CIF de la ER

AMBIT_GRUP = Nombre del grupo de documentos (por ejemplo GENERIC o CATCERT)

Dentro del mismo directorio también existirá un fichero de definición (GRUP_NOM_GRUP.config) por cada etiqueta diferente que pueda haber dentro de los campos AMBIT_GRUP los anteriores ficheros.

Estos archivos contienen los siguientes parámetros.
LLISTA_POLITIQUES= Listado de las políticas que pueden generar las ERs de este grupo. También hay que añadir el elemento PIN_PUK si la ER puede generar tarjetas.

Por ejemplo:
LLISTA_POLITIQUES = CDA_1, CDS_1, CDP_1, CDSDC_1, CESR_1, CPISR_1_O, CPISRC_1_O, PIN_PUK

Para cada elemento de la lista anterior tenemos dos parámetros.

itemLlista_DOCS = Lista de identificadores de documentos que puede generar esta política.
itemLlista _DESC = Descripción de la política que se utilizará en los documentos.

Por ejemplo:
CPISR_1_DOCS = FL_CARD, CL_CARD, AL_CARD, CP_CARD
CPISR_1_DESC = CPISR + CPX

Finalmente el archivo contiene la definición de cada uno de identificadores de los ficheros de las variables xxx_DOCS. Esta definición contiene los siguientes campos.

DOC_BASE = Nombre de la plantilla
DOC_SUBST = Conjunto de sustituciones a realizar antes de generar el código para la ER relacionada.

Por ejemplo:

```
FL_CARD_DEFINICIO <<<! EOF_definicioDoc - $
        DOC_BASE = GENERIC_CPISR-CPISRC-CESR_FL.rtf
        DOC_SUBST <<<! EOF_docSubst - $
                doc = $ {subst: $$ nombre_: $ {escapecolon: $ {AMBIT_DESC}}: $ {doc}}
                doc = $ {subst: $$ ADRESS_ER: $ {escapecolon: $ {AMBIT_ADRESS}}: $ {doc}}
                doc = $ {subst: $$ CP_ER: $ {escapecolon: $ {AMBIT_CP}}: $ {doc}}
                doc = $ {subst: $$ POB_ER: $ {escapecolon: $ {AMBIT_POB}}: $ {doc}}
                doc = $ {subst: $$ TIPUS_CERT: $ {escapecolon: $ {$ {politicaItem} _DESC}}: $ {doc}}
        EOF_docSubst
EOF_definicioDoc
```

Una vez situados todos los elementos, se realizan los siguientes pasos a partir del código de la ER (xxx.txt).

a. Cargar el archivo xxx.txt
b. Obtener el parámetro AMBIT_GRUP y cargar el archivo relacionado GRUP_xxxxxx.config
c. Para cada elemento de la lista LLISTA_POLITIQUES obtener la lista de documentos asociados (itemLlista_DOCS) y generar a partir de los documentos base (DOC_BASE) realizando las sustituciones definidas (DOCS_SUBST).
d. Finalmente lo pone dentro del conjunto de scripts que se enviarán al software de la ER con el nombre de la política y tipo de documento adecuado.

Al finalizar esta fase los documentos están personalizados con los datos que no dependen de la generación del certificado correspondiente. Para el resto de la personalización del

documento hay que definirlo en el archivo de política, situados tanto en la máquina del portal del SCD.

Será necesario, en cada caso, realizar las asignaciones correspondientes a todas las variables de los documentos.
Estas asignaciones se realizan dentro de las definiciones como por ejemplo.

```
$ {PolicyId} _FL <<<! EOF - $
        doc = $ {subst: $$ resp_nom: $ {escapecolon: $ {resp_nom}}: $ {doc}}
        doc = $ {subst: $$ resp_nif: $ {resp_nif}: $ {doc}}
        doc = $ {subst: $$ nombre: $ {escapecolon: $ {cn} $ {CN2}}: $ {doc}}
        doc = $ {subst: $$ tipus_doc: $ {doc_type}: $ {doc}}
        doc = $ {subst: $$ doc_num: $ {doc_num}: $ {doc}}
        doc = $ {subst: $$ email: $ {ea}: $ {doc}}
        doc = $ {subst: $$ org: $ {escapecolon: $ {o}}: $ {doc}}
        doc = $ {subst: $$ huevo: $ {escapecolon: $ {huevo}}: $ {doc}}
        doc = $ {subst: $$ cif_org: $ {cif_org}: $ {doc}}
        doc = $ {subst: $$ pob: $ {escapecolon: $ {resp_pob}}: $ {doc}}
        doc = $ {subst: $$ fecha: $ {fecha}: $ {doc}}
        doc = $ {subst: $$ SN1: $ {serial1}: $ {doc}}
        doc = $ {subst: $$ SN2: $ {serial2}: $ {doc}}
        doc = $ {subst: $$ notafter1: $ {notafter1}: $ {doc}}
        doc = $ {subst: $$ notafter2: $ {notafter2}: $ {doc}}
        doc = $ {subst: $$ notbefore1: $ {notbefore1}: $ {doc}}
        doc = $ {subst: $$ notbefore2: $ {notbefore2}: $ {doc}}
        doc = $ {subst: $$ policy1: $ {policy1}: $ {doc}}
        doc = $ {subst: $$ policy2: $ {policy2}: $ {doc}}
        doc = $ {subst: $$ idsusp: $ {idsusp_clear}: $ {doc}}
EOF
```

Estas definiciones pueden depender de cada tipo de certificado y qué datos tenemos disponibles. Lo que hay que verificar es que todas las variables definidas en la plantilla son sustituidas por algún valor.

Finalmente y durante el proceso de generación del certificado, la aplicación del módulo generador, generará el documento definitivo a partir del documento base que recibe de la CA y sustituido el valor de las variables en minúscula siguiendo las reglas definidas dentro del archivo de política.

4.7 Notificaciones del sistema

A continuación se describen todas las comunicaciones que el sistema del SCD necesario que envíe. Para cada una de ellas se describe en las mismas características:

- Emisor [from]
- Destinatarios [To]
- Acción que la desencadena
- Descripción del contenido
- Hay que firmar y / o cifrar
- Otras consideraciones

4.7.1 Comunicación de Nueva Petición

emisor: scd@aoc.cat
destinatariosTodos los aprobadores relacionados de la ER en la que pertenece el peticionario + Responsable del ER
acción: Introducción de peticiones por parte de los peticionarios
contenido: Identificadores / datos de las peticiones introducidas

firmado: No
otras consideraciones:
Las peticiones introducidas al sistema de forma masiva no generan esta notificación.

4.7.2 Comunicación de Aprobación

emisor: scd@aoc.cat
destinatariosTodos los generadores relacionados de la ER en la que pertenece el aprobador + Responsable de la ER
acción: Aprobación de peticiones por parte de los aprobadores
contenido: Identificadores / datos de las peticiones introducidas
firmado: No
otras consideraciones:
No es necesario enviar ninguna comunicación si la aprobación se hace desde la aplicación del módulo generador.

4.7.3 Comunicación de Denegación

emisor: scd@aoc.cat
destinatarios: Peticionario que ha introducido la petición
acción: Denegación de peticiones por parte de los aprobadores
contenido: Identificadores / datos de las peticiones denegada
firmado: No
otras consideraciones:
Si la petición es introducida de manera automática se debe asegurar que la dirección que contiene el CDA utilizado es real y accesible para los operadores.

4.7.4 Comunicación de Cambio de estado

emisor: scd@aoc.cat
destinatarios: Poseedor de claves
acción: Revocaciones / suspensiones / habilitaciones de certificados por parte de los gestores de certificados
contenido: Identificadores / datos del certificado afectado
firmado: Sí
otras consideraciones:
Para evitar el envío de correos electrónicos en caso de errores en la generación, etc. sólo se aplicará a los certificados con sido entregado. Hay que tener en cuenta que tampoco afecta a los certificados esclavos.

4.7.5 Comunicación de PIN & PUK

emisor: scd@aoc.cat
destinatarios: Poseedor de claves
acción: Se ha marcado como entregado el certificado por parte del Administrador de la ERV
contenido: Identificadores / datos del certificado afectado, PIN y PUK en caso de tarjetas o contraseña de PKCS # 12 en otros casos.
firmado: Sí
otras consideraciones:

Sólo si están entregados
No afecta a los certificados esclavos

4.7.6 Recordatorio de Aprobación

emisor: scd@aoc.cat
destinatarios: Aprobador relacionados a las peticiones que están pendientes de aprobar
acción: Proceso que mire si las peticiones pendientes de aprobar superan el límite de tiempo configurado. Este tiempo tendrá un orden de magnitud de días.
contenido: Identificadores / datos de las peticiones.
firmado: No
otras consideraciones:
Se consideran 3 recordatorios, a los 3, 5 y 15 días.

4.7.7 Recordatorio de eliminación

emisor: scd@aoc.cat
destinatarios: Aprobador relacionados a las peticiones que están pendientes de aprobar. Solicitante de la petición
acción: Proceso que mire si las peticiones superan el límite de 90 días desde la última acción dentro del sistema.
contenido: Identificadores / datos de las peticiones.
firmado: No
otras consideraciones:
Debe existir la posibilidad de des-habilitar esta opción ya que hay ECS que tienen muchas peticiones precargadas y que son correctos.

4.7.8 Recordatorio de Generación

emisor: scd@aoc.cat
destinatarios: Generadores relacionados a las peticiones que están pendientes de generar
acción: Proceso que mire si las peticiones pendientes de generar superan el límite de tiempo configurado. Este tiempo tendrá un orden de magnitud de días.
contenido: Identificadores / datos de las peticiones.
firmado: No
otras consideraciones:

4.7.9 Recordatorio de Entrega

emisor: scd@aoc.cat
destinatarios: Administrador del ERV relacionados a los certificados pendientes de entregar
acción: Proceso que mire los certificados pendientes de entregar y que superan el límite superan el límite de tiempo configurado. Este tiempo tendrá un orden de magnitud de días.
contenido: Identificadores / datos de las peticiones.
firmado: No
otras consideraciones:
Se consideran 3 recordatorios, a los 3, 5 y 15 días después de la generación.

4.7.10 Recordatorio de Renovación - 60 días

emisor: scd@aoc.cat
destinatarios: Poseedor de claves y / o responsable de servicio de la ERV
acción: Proceso que mire si los certificados generados en estado válido y que caducan durante los próximos 60 días
contenido: Identificadores / datos de los certificados
firmado: Sí
otras consideraciones:
- El cuerpo del mensaje es diferente por el Administrador de servicio de la ERV y poseedor

4.7.11 Recordatorio de Renovación - 30 días

emisor: scd@aoc.cat
destinatarios: Poseedor de claves y / o responsable de servicio de la ERV
acción: Proceso que mire si los certificados generados en estado válido y que caducan durante los próximos 30 días. No se enviará si entre el de 60 días y este se ha renovado o revocado el certificado.
contenido: Identificadores / datos de los certificados
firmado: Sí
otras consideraciones:
- El cuerpo del mensaje es diferente por el Administrador de servicio de la ERV y poseedor

4.8 Generación de informes ONLINE

Desde el portal del SCD, los operadores con rol adecuado podrán obtener, en formato .csv, determinados informes sobre los certificados de sus entes asociados. Este informes, una vez solicitados por parte del operador, se generan en segundo plano. Una vez generados el sistema notifica al operador que puede acceder al mismo portal del SCD para proceder a su descarga.
Las características de estos informes son las siguientes:

1. informes disponibles
    a. Extracción global de certificados
    b. Informe de certificados válidos
    c. Informe de certificados revocados
    d. Informe de certificados suspendidos
    e. Informe de certificados que caducan en los próximos 2 meses
2. Los datos de los informes obtenidos son por EC y contienen los datos de los entes que tiene asociado el operador, sólo los operadores de la ER con código 000 obtienen informes que contienen la totalidad de certificados de la EC
3. El período de generación en segundo plano es un máximo de 24 horas
4. Los informes se entregan en formato .csv comprimidos en zip
5. Cada informe se puede pedir un máximo de una vez al día
6. Los operadores disponen del histórico de informes solicitados y generados

4.9 Generación de informes BACKOFFICE

El sistema genera informes en formato CSV, periódicamente y de manera automática. Los informes que generados son los siguientes:

extracción DWH

Periodicidad: Semanal
Destino: DWH AOC
Datos: extracción global, todas las EC
Formatos: .csv y .rar

extracción UPC

Periodicidad: Diaria
Destino: UPC, descarga WEB (autenticación con certificado)
Datos: Certificados de EC-UR con Organización igual a Universidad Politécnica de Cataluña ',' Universidad Politécnica de Cataluña ',' UPC ',' UPCnet '. EC-UR
Formatos: .csv y .rar

extracción UB

Periodicidad: Diaria
Destino: UB, descarga WEB (autenticación con certificado)
Datos: Certificados de EC-UR con código de ente igual a CINV00247. EC-UR
Formatos: .csv y .rar

extracción URV

Periodicidad: Diaria
Destino: URV, descarga WEB (autenticación con certificado)
Datos: Todos los certificados de EC-URV y todos los certificados de EC-UR con código de ente igual a CINV00215.
Formatos: .csv y .rar

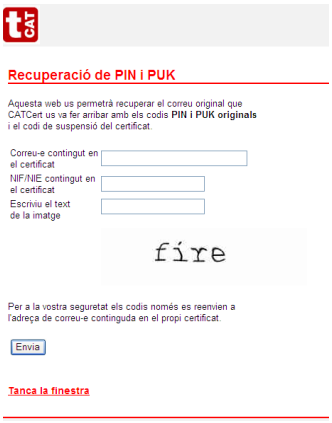
4.10 Recuperación de PIN / PUK

Esta parte del portal SCD permite recuperar los códigos PIN y PUK originales de las tarjetas emitidas con posterioridad de la primera mitad del año 2009.

Se trata de una parte del portal SCD que no requiere autenticación con certificado digital y que permite a los poseedores de las claves recibir en el correo electrónico contenido en el certificado y sólo en esta dirección los códigos originales que se fijaron en el momento de la generación de los certificados.
También se permite la recuperación de las palabras de paso de los archivos PKCS # 12, por certificados emitidos en este soporte.

Los datos necesarios para poder activar este reenvío son:

- DNI / NIF
- correo electrónico
- Código de suspensión, disponible en el documento de aceptación de los certificados
- código CAPTCHA



4.11 Certificados T-CATP

El sistema permite la generación de certificados personales en soporte software (PKCS # 12). Estos certificados por su naturaleza conllevan una serie de modificaciones y adaptaciones a los flujos estándares definidos en la plataforma.

A continuación se detallan las características del tipo de certificado T-CAT P:

1. Es un certificado personal, con usos de autenticación, firma y cifrado
2. El tamaño de las claves es de 2048 bits o superior
3. El par de claves es generado por la Entidad de certificación
4. La Entidad de certificación elimina la clave privada, una vez haya sido entregada al usuario
5. El formato de entrega es un archivo PKCS # 12
6. La EC cifra las claves privadas generadas con una llave de ofuscación custodiada por un HSM, para evitar que sean recuperables directamente de la base de datos
7. El destino de las claves, especificado en el momento de la aplicación, puede tener tres valores:
    a. **usuario**. El propio usuario se descargará el certificado y recibirá la palabra de paso para la instalación del PKCS # 12
    b. **aplicación**. Un sistema automatizado se descargará los PKCS # 12 y los habilitará para su uso en una plataforma de firma centralizada externa del Consorcio AOC. El usuario recibirá la contraseña del PKCS # 12 que le permitirá la activación de la clave en la plataforma mencionada.

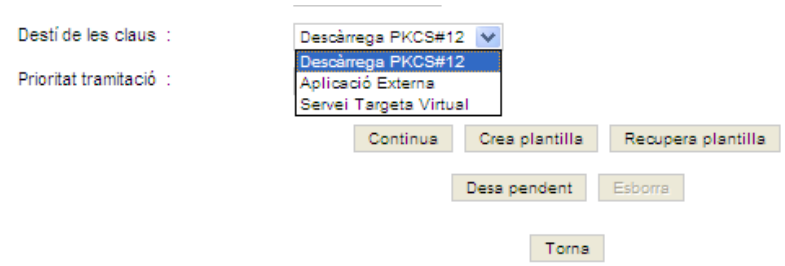
A continuación se describen los cambios en los flujos estándar.

4.11.1 petición

Los procesos de petición de un certificado tipo T-CAT P son los mismos que se siguen actualmente con los certificados T-CAT. Por lo tanto el origen de la petición puede ser:

- Desde EACAT
- Desde los propios formularios del servicio SCD

En el proceso de petición se deberá informar, a parte de los datos del poseedor de las llaves, el destino de las claves.



4.11.2 aprobación

El proceso de aprobación de un certificado tipo T-CAT P es el mismo que se sigue actualmente con los certificados T-CAT, por tanto se realizará desde los propios formularios del servicio.

4.11.3 generación

Una vez aprobados los certificados, éstos se generan de la siguiente manera.
Un proceso programado, residente en la propia EC, accede a la base de datos y selecciona los certificados tipo T-CAT P en estado aprobado y, por tanto, pendientes de generar. En este momento el sistema hace las siguientes acciones:

- La EC genera un par de claves y el correspondiente certificado.
- Genera un PKCS # 12 con una contraseña aleatoria que también guarda.
- El PKCS # 12 y su contraseña se guardan en una tabla de la base de datos [TCATP_DATA] cifrada con una clave del HSM. Esta tabla no es propia del producto de PKI.
- Se genera la hoja de entrega y se publica al servicio SCD
- Se envía un correo electrónico al poseedor del certificado indicando que se ha generado un certificado a su nombre. NO se anexa la hoja de entrega.
- Se deja disponible a los responsables del servicio del ente al que pertenece el poseedor el certificado para proceder a su entrega

Este proceso se ejecuta cada 2 minutos. Este intervalo de tiempo se puede configurar mediante uno de los parámetros del sistema.

4.11.4 entrega

La entrega se basa en diferentes pasos:

A. El poseedor se persona ante el responsable de servicio.
B. El responsable accede a la carpeta del suscriptor y descarga la hoja de entrega.
C. El poseedor firma la hoja de entrega.
D. En caso de que el destino de las claves sea el usuario o el servicio de tarjeta virtual, el poseedor introduce un Código personal que sólo conoce él y que necesitará en el momento de la descarga o activación de la tarjeta virtual. Este código deberá tener como máximo 8 caracteres (mínimo 1 carácter) entre números y / o letras. En el otro caso, donde el destino es la aplicación externa este código no es necesario.
E. El responsable marca la entrega del certificado a la aplicación.
F. En este momento el sistema guarda en la base de datos junto con el PKCS # 12 ofuscado, el PIN del PKCS # 12 generado por el sistema también ofuscado con la misma clave que custodia un HSM y, por último, el HASH del Código de descarga personal que conoce sólo el usuario. En este mismo punto, se habilita la descarga del PKCS # 12 o la activación del servicio de tarjeta virtual.

4.11.5 Descarga

Este procedimiento, ejecutado por parte del usuario, sólo aplica si el destino de las claves es PKCS # 12. El procedimiento es el siguiente:

A. El poseedor, ya en su puesto de trabajo, accede a la página de descarga / activación de T-CAT P (URL con SSL pero sin autenticación).
B. Introduce su correo-e contenido en el certificado, el NIF / NIE contenido en el certificado, el Código de suspensión (se encuentra dentro la hoja de entrega) y el Código de descarga personal. El sistema le devuelve el fichero PKCS # 12.
C. Posteriormente, el usuario recibirá por correo electrónico el PIN del archivo PKCS # 12.
D. El sistema controla el número de descargas y el período de tiempo en que se pueden realizar. Se configura con una posible descarga durante los 10 días posteriores a la activación de la propia. Como excepción, y para evitar posibles incidencias, los 5 minutos siguientes al momento en que el usuario efectúa la primera descarga están exentos de la limitación de número de descargas. Es decir, se podrá pulsar el botón de descarga tantas veces como se necesite sin que ningún error aparezca. Las situaciones que se quieren evitar son por ejemplo que el usuario haga "Abrir" en vez de "Guardar" en el diálogo y vuelva a empezar para poder guardar el PKCS # 12, o

que guarde el PKCS # 12 pero no recuerde dónde y quiera volver a guardarlo en un lugar específico.

En esta etapa se definen dos periodos de retención: el de entrega y el de descarga.

- Por un lado, el periodo de retención de entrega del PKCS # 12 es de 30 días desde la generación. Es decir, si no se entrega en este periodo el PKCS # 12 y la palabra de paso se borra de la base de datos.
- Por otra parte, el periodo de retención de descarga del PKCS # 12 es de 10 días, máximo de tiempo que puede transcurrir entre que el responsable del servicio marca como entregado la hoja de entrega y que el usuario poseedor descarga el PKCS # 12. Sin embargo, si esta condición no se cumple el PKCS # 12 y la palabra de paso se borra de la base de datos.

En ambos casos, el certificado es revocado antes de borrar el PKCS # 12 de la base de datos. Para evitar que el PKCS # 12 se borre de la base de datos para el desempeño de estos dos periodos y tener que volver generar una nueva petición, se envían correos-e recordatorios tanto al responsable de servicio durante la etapa de entrega como al usuario en periodo de descarga. En concreto se envían dos recordatorios de entrega (el día 7 y el día 21 desde la generación) y dos recordatorios de descarga (el día 3 y el día 7 desde la entrega).

En caso de olvidar o perder el correo-e con el PIN del PKCS # 12, el usuario tendrá la opción de recuperación de éste a través de un formulario web.

4.12 Administración del sistema

A continuación es información sobre las opciones de administración del sistema, que se pueden realizar desde el portal del servicio SCD.

Los operadores con este rol están configurados en una ACL a partir de su número de serie de su certificado. Un operador con este rol puede administrar cualquiera de las ecs del sistema, excepto EC-CIUDADANÍA que tiene su propia gestión en la capa RA.

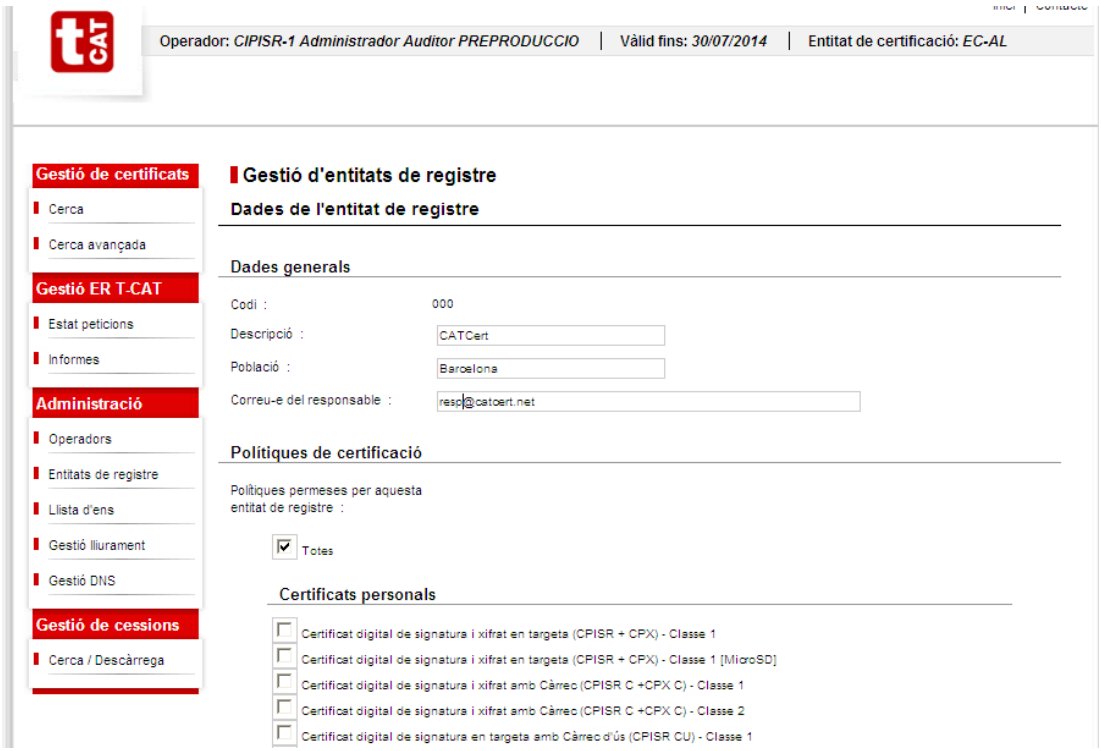
Aparte de conocer la operativa de esta parte también puede ayudar a tener un acercamiento a las tareas de administración necesarios para gestionar el correcto funcionamiento de la infraestructura.

4.12.1 Gestión de ER

Permite la gestión de los datos relacionados con cada ER.

El operador puede realizar las siguientes operaciones sobre las ER de cada EC.

- Buscar
- Alta (una nueva ER requiere también de otros procedimientos técnicos, jurídicos y logísticos)
- baja
- modificación
- Fijar los siguientes parámetros para cada entidad de registro
    - código
    - Descripción
    - Lista de correos-e de responsables relacionados a esta ER
    - Lista de políticas disponibles para esta ER
    - Lista de diseños de tarjeta disponibles para esta ER
    - Lista de organismos a aplicar en el filtro de los operadores de la ER



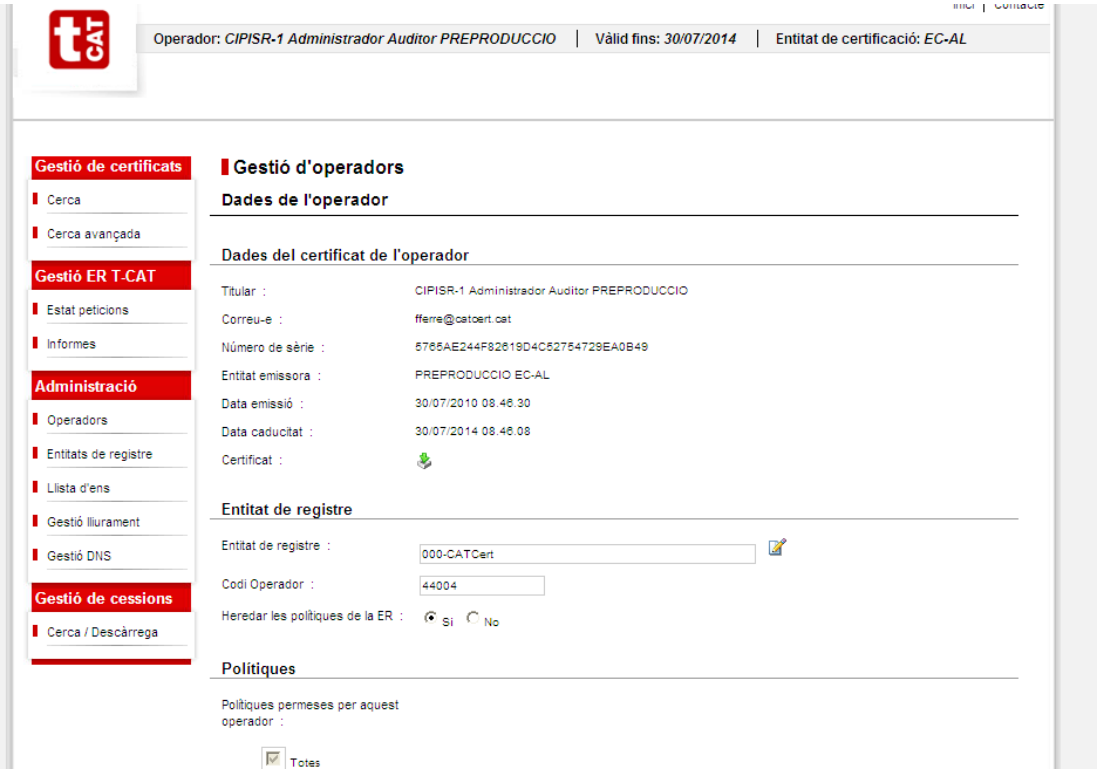
4.12.2 Gestión de operadores

Permite la gestión de los operadores, los roles, sus datos, la relación con las ERs, etc.

El operador puede realizar las siguientes operaciones durante la gestión de operadores.

- Buscar
- Alta. Para dar de alta operador hará falta tener disponible el archivo .crt que contiene el certificado de autenticación (normalmente CIPISR) del mismo
- baja
- modificación
- Fijar los siguientes parámetros para cada entidad de registro
    - código operador
    - Correo electrónico. Se obtiene el Email del operador a partir de los datos del certificado
    - ER a la que pertenece, sólo puede ser una.
    - Rol del operador
        - introducir peticiones
        - aprobar peticiones
        - Gestionar certificados (Suspender / habilitar o Revocar / Suspender / habilitar)
        - Generar certificados. Estos roles también precisan, por seguridad, de configuración adicional directamente a la aplicación de PKI.
        - Administrador ERV T-CAT
        - depositario AOC
    - permisos especiales
        - importar peticiones
        - revocación automática
        - Acceso al sistema de Lotes

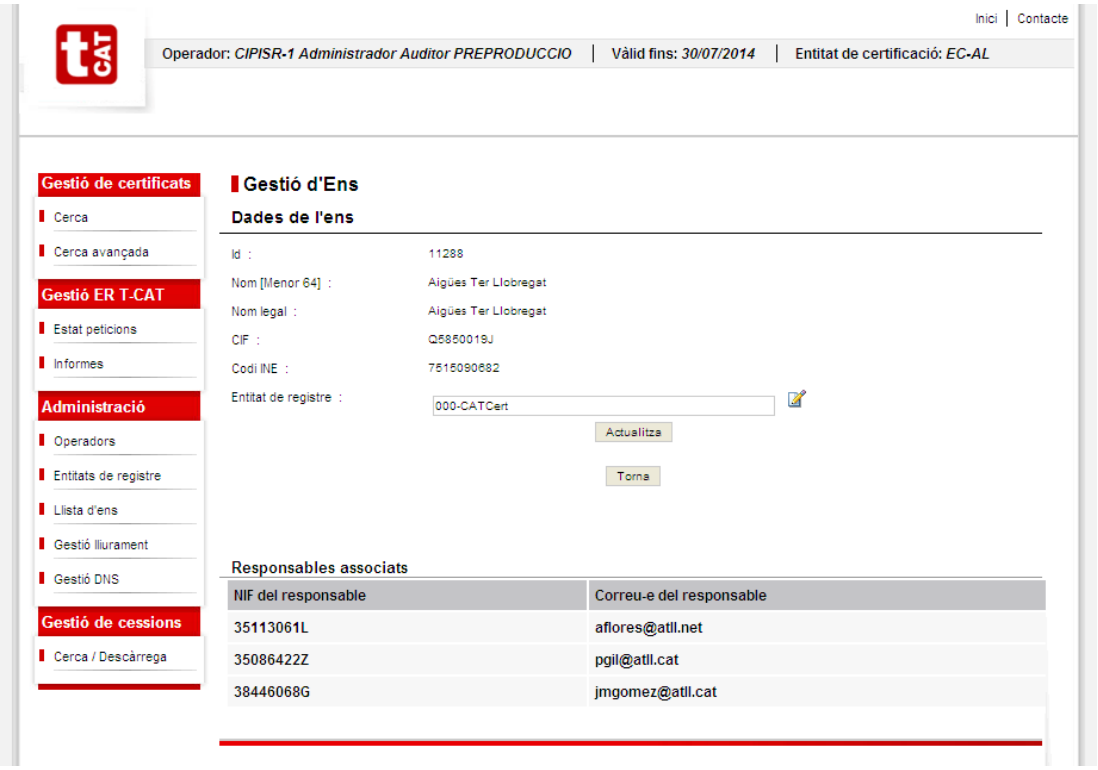
- Lista de políticas disponibles para este operador. Se pueden heredar de la configuración de la ER
- Lista de correo-e de operadores. Aplica a notificaciones entre operadores peticionarios, aprobadores y generadores.
- Operadores relacionados. Aplica a rol aprobador y generador y fija la lista de aprobadores aceptados por cada generador.



4.12.3 Lista de entes

Permite la gestión de los entes por cada EC. En este caso la fuente es externa y sólo se permite la asignación de cada ente a una ER determinada. Si su ER es la que tiene código 000, no hay que hacer nada.
El operador puede realizar las siguientes operaciones durante la gestión de entes.

- Buscar
- Visualización de responsables asignados
- Fijar los siguientes parámetros para cada entidad de registro
  - ER asignada

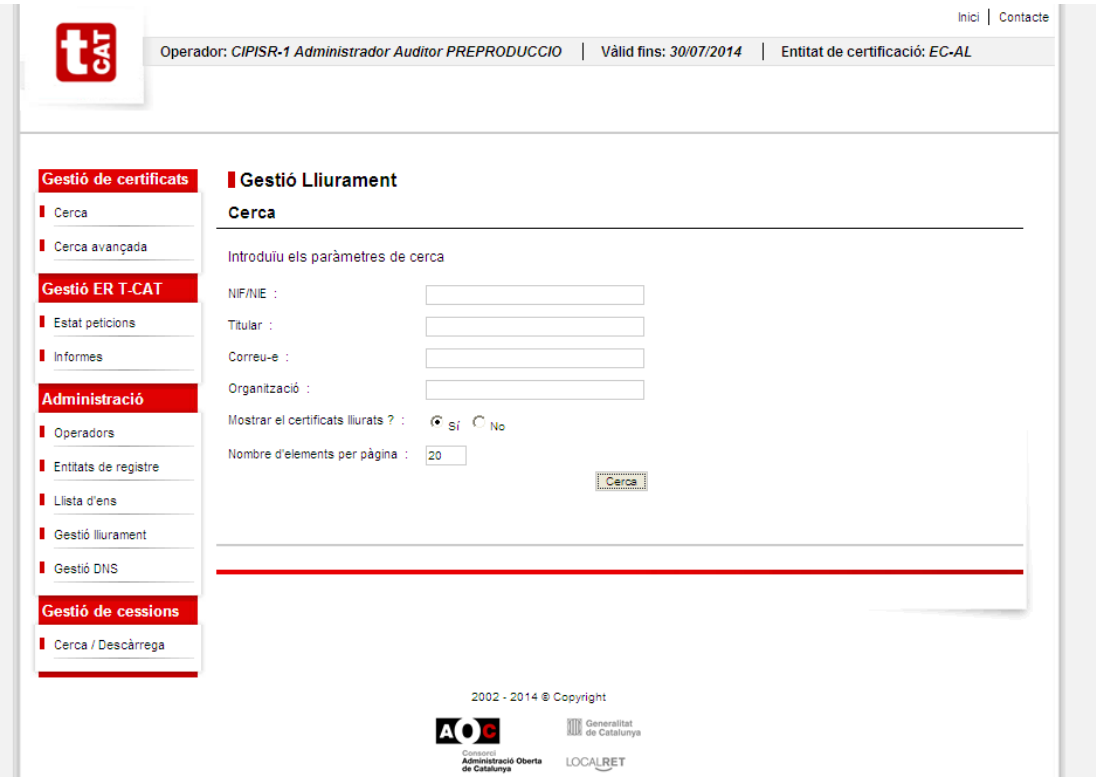


4.12.4 gestión Entrega

Permite la visualización del estado de entrega de cualquier certificado del sistema. Se trata de una opción utilizada sobre todo para la gestión de incidencias debidas al proceso de entrega que deben hacer el responsable de servicio de cada ente.

El operador puede realizar las siguientes operaciones:

- Buscar
- Vista de certificados
- Visualizar la documentación
- Activar el envío del PIN / PUK o contraseña del PKCS # 12 según corresponda

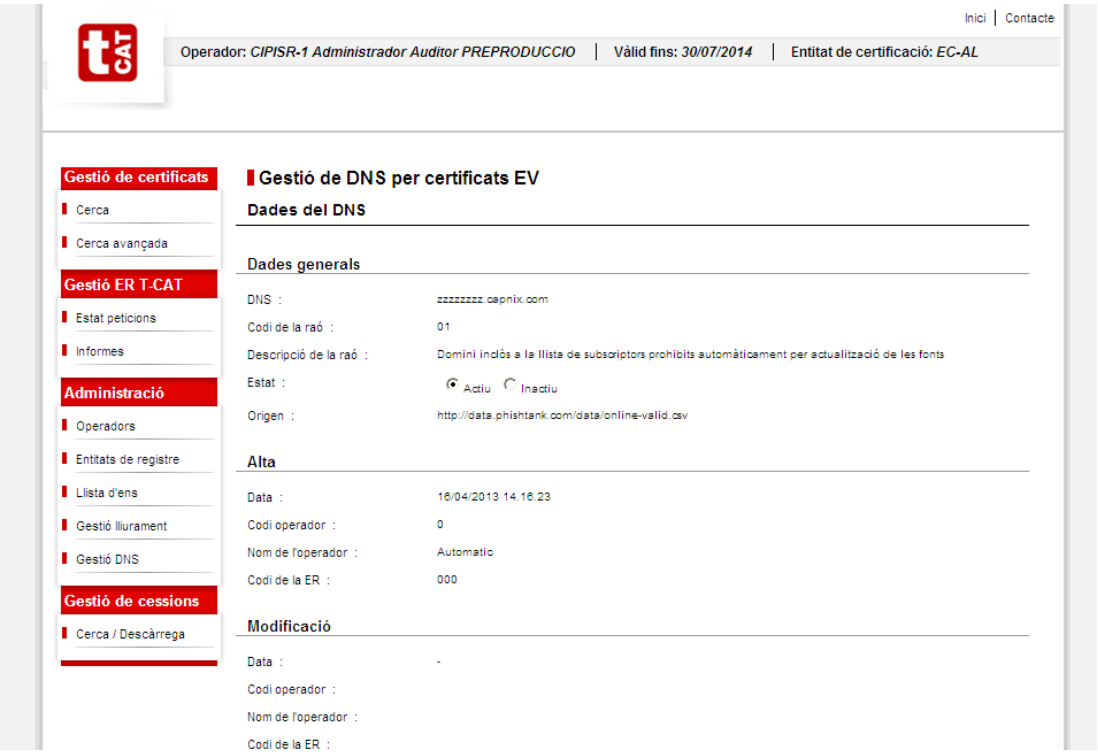


4.12.5 gestión DNS

Permite la gestión manual de la lista de dominios utilizados como lista de validación al emitir certificados para uso en servidores WEB (ver Elementos para la emisión de certificados de servidor WEB (EV)).

El operador puede realizar las siguientes operaciones:

- Buscar
- alta
- Vista de DNS y sus datos
- Fijar el estado en la lista (Activo o Inactivo)



4.13 Módulo de cesión

Este módulo incorpora la posibilidad de delegar en un tercero la descarga de las claves, para los tipos de certificado de Sello electrónico y CDA. Esto hace más eficiente y seguro la gestión de estos tipos de certificados cuando estos son utilizados para servicios y aplicaciones de la propia AOC.

En este caso, se indicará en la petición del certificado, que éste está cedido a la AOC. Estos certificados modificarán parte de su flujo estándar con los siguientes cambios:

- Cuando se genera el certificado, el suscriptor podrá ver el certificado en la lista pero no puede descargar la clave privada
- El Consorcio AOC tiene una opción dentro de la carpeta del suscriptor para descargar todas las claves privadas cedidas, así como sol • licitar el correspondiente PIN (una opción en la que sólo tendrá acceso quien Operaciones determine - operador con rol 'Depositario AOC').
- En las opciones disponibles para el responsable de servicios se deshabilita la posibilidad de descarga del P12 para los certificados de este tipo. El responsable continúa haciendo el acto de 'entrega' pero este no implica ni que pueda descargar el P12 ni tampoco que el sistema envíe el PIN. Para hacer este acto debe haber firmado el nuevo "hoja de entrega" de cesión / depósito.
- La gestión del ciclo de vida del certificado (emisión, revocación, suspensión, etc ..) sigue siendo responsabilidad plena del ente titular.
- El sistema garantiza que no se ha bajado nunca el p12 desde el ente que lo solicita, evitando copias.

El operador con rol Depositario AOC puede realizar las siguientes operaciones:

- Buscar

- Entrega y Descarga de certificados. Como consecuencia recibirá el correo electrónico con la palabra de paso para su utilización / instalación.

4.14 Elementos para la emisión de certificados de servidor WEB (EV)

Para cumplir los requerimientos operacionales para la emisión de certificados de servidor web con características de Extended Validation (EV) se incorporan funcionalidades adicionales en la fase de registro de este tipo de certificados. A continuación se detallan los componentes relacionados.

4.14.1 Verificación de dominios declarados como phishing.

Este módulo permite la gestión y bloqueo de todos los nombres de dominio que estén asociados a listas de dominios declarados como phishing (phishing). En el ramo de la informática, la pesca electrónica (o phishing en inglés) es un fraude que acontece a través de correo electrónico o mensajería instantánea en el que se piden datos sobre las tarjetas de crédito, contraseñas, claves bancarias u otros tipos de información. Los mensajes emprenden todo tipo de argumentos relacionados con la seguridad de la entidad para justificar la necesidad de introducir los datos de acceso.
Por lo tanto, para evitar este tipo de fraude electrónico, se pone a disposición este nuevo módulo para proteger a los certificados electrónicos de esta peligrosidad.

Esta validación se activará por las políticas de certificados EV y adicionalmente también a otras políticas de emisión de certificados de servidor donde se quiera controlar este aspecto. En concreto, este módulo está activado por los perfiles CDS-1 EV, CDS-1 SENA y CDS-1 SenM, los cuales, disponen de un campo de nombre de dominio.

Los requerimientos que soporta el módulo son:

- Sistema para gestionar dominios incluidos en listas phishing
- Descarga periódica de una fuente oficial
- Poder revocar un certificado indicando que el motivo es que el dominio está incluido en las listas phishing con actualización automática en la base de datos

A continuación es la solución técnica implementada al sistema para alcanzar los requerimientos descritos:

- Tarea programada que descarga diaria de una lista pública de dominios afectados por la pesca electrónica, ubicada en http://data.phistank.com/data/online-valid.csv
- También se ponen en esta lista los 1000 primeros registros de la lista Alexa, ya que potencialmente son los más demandados para poder hacer una suplantación de identidad.
- Estos datos se insertan en una tabla de la base de datos (EV_PHISHING_DATA) visible para toda la jerarquía del Consorcio AOC
- Al peticionar algún del tipo de certificado afectado, el sistema hace la comprobación dentro de la tabla que contiene la lista y si la petición contiene un dominio inválido, este avisa y no deja continuar. Los campos comprobados son el CN y el CN opcional, tanto el DNS incluido en el archivo CSR (P10) como el campo DNS incluido por formulario.

- Se emiten, de forma periódica, dos informes de auditoría que contienen la siguiente información:
    - Certificados emitidos los perfiles CDS-1, CDS-1 SENA, CDS-1 SenM) que contengan DNS incluidos en la lista de nombres de dominio conflictivos.
    - Weblog con la lista de acciones relacionadas con peticiones, emisiones y revocaciones que se haya realizado una comprobación de DNS en dispondremos de información respecto a peticiones bloqueadas por nombres de dominio phishing.
- Debido a la validación diaria de todos los dominios vigentes con la lista actualizada, se enviará un correo electrónico con los dominios afectados para servicio pueda evaluar su revocación.
- Al revocar un certificado, con el motivo de dominio catalogado como phishing, éste será incluido en la tabla de la base de datos mencionada, donde estará la lista negra de DNS referentes a phishing.

La tabla que contiene la lista de dominios declarados como phishing se llena normalmente a través de la tarea automática con los datos procedentes de listas de phishingTank (http://www.phishtank.com/), Sitio web responsable de recopilar todos los DNS que propician la pesca electrónica, pero adicionalmente los operadores con rol Administrador disponen de un opción para poder añadir elementos de manera manual.

4.14.2 Verificación del formato FQDN en dominios web

Este módulo permite la validación del nombre de dominio completo FQDN (Fully Qualified Domain Name) en todas las políticas que impliquen un servicio con conexión SSL. En este caso, los perfiles afectados son CDS-1, CDS-1 EV, CDSCD-1, CDS-1 SENA y CDS-1 SenM.

Un FQDN (Fully Qualified Domain Name) es un nombre que incluye el nombre del ordenador y el nombre de dominio asociado a este equipo. Por ejemplo, dado el nombre de ordenador «serv1» y el nombre de dominio «bar.com», el FQDN será «serv1.bar.com». Por lo tanto, un FQDN asociado a serv1 podría ser «post.serv1.bar.com».

Las validaciones realizadas son las siguientes:

- La longitud máxima permitida para un FQDN es de 255 caracteres (bytes), con una restricción adicional de 63 bytes por etiqueta dentro de un nombre de dominio. Las etiquetas FQDN se restringen a un juego de caracteres limitado: letras AZ de ASCII, los dígitos, y el carácter «-», y no distinguen mayúsculas de minúsculas.
- El campo CN no puede contener ningún IP, número o palabra que contenga 'localhost'.
- Que la estructura del campo sea del tipo XXX (todos los puntos sobrantes se eliminarán)
- La sintaxis de los nombres de dominio se discute en varios RFCs (RFC 1035, RFC 1123 y RFC 2181). Actualmente, se han añadido algunas letras acentuadas «ä, ö, ü, é, à, è ...» como caracteres permitidos para las etiquetas.

Diariamente, se ejecuta una tarea para validar, sobre los certificados ya generados, que contengan un nombre de dominio completo válido. Esta tarea, genera un informe de auditoría que contiene los datos de los certificados que no contengan un FQDN correcto.

En la fase de peticionario, éste hará la comprobación del campo CN y CN opcional, de forma automática y advirtiendo al usuario de que no puede seguir adelante si no se cumplen los requerimientos estándares de un FQDN válido.

5 otros módulos

A continuación se describen otros módulos (más tecnológicos) que aportan a la infraestructura el cumplimiento de más requerimientos.

5.1 Control de unicidad

El control de unicidad evita la generación de dos certificados válidos del mismo tipo al mismo titular.

Este módulo cumple los siguientes requerimientos.

- La regla de unicidad, conjunto de datos que configuran el valor que no puede repetirse, es configura para cada perfil en el fichero de política correspondiente.
- El sistema controla la unicidad en dos fases, la de peticionario y finalmente a la de generación.
- El sistema permite configurar el periodo de tiempo llamado de renovación que permite saltarse la regla de unicidad. Actualmente fijado en dos meses.
- El control en la fase de petición se realiza tanto en el sistema ONLINE como en el sistema de LOTES. En esta fase también se controla que no haya unicidad entre peticiones de certificación pendientes de generar, con el mismo criterio.
- En caso de encontrarse un certificado que cumpla la unicidad informa al operador que no se puede realizar la operación y se devuelve el número de serie del certificado que la provoca.
- Adicionalmente, en la fase de petición, también se indica al operador, en este caso en modo informativo, si hay certificados o peticiones dentro del sistema con el mismo código de documento, normalmente DNI.

5.2 Módulo de paso de certificados suspendidos a revocados

El módulo pasa de manera automática los certificados suspendidos que lleven más de 120 días en este estado a revocados. El valor de 120 días está especificado en las prácticas de certificación pero dentro del sistema se puede configurar.

Este módulo cumple los siguientes requerimientos.

- Es una tarea de sistema configurada por cada EC
- Técnicamente se desarrollado como un flujo de trabajo de la aplicación PKI.

5.3 Interfaz de conexión para la EC-CIUDADANÍA

A continuación se describe la mensajería que implementa la EC-CIUDADANÍA (flujo de trabajo de la aplicación PKI) para su conexión entre la capa RA (aplicación externa a la PKI) y la instancia de la aplicación PKI.
La comunicación entre estos dos elementos se realiza mediante un canal seguro SSL autenticando la RA con un certificado digital.

5.3.1 Petición de certificados

petición

<Soapenv: Envelope xmlns: soapenv = "http://schemas.xmlsoap.org/soap/envelope/" xmlns: key = "http://www.safelayer.com/namespaces/keyoneca">
<Soapenv: Header />
<Soapenv: Body>
<Key: idc_issuercertProcedureRequest>
<Key: subject> {dn} </ key: subject>
<Key: policy> {policy} </ key: policy>
<Key: request> {pkcs10} </ key: request>
<Key: email> {email} </ key: email>
<Key: dirName> 2.5.4.5 = {dni} </ key: dirName>
<Key: citizenship> ES </ key: citizenship>
<Key: residence> ES </ key: residence>
<Key: name> {nom_cognoms} </ key: name>
<Key: idNumber> {dni} </ key: idNumber>
</ Key: idc_issuercertProcedureRequest>
</ Soapenv: Body>
</ Soapenv: Envelope>

respuesta

<Env: Envelope env: encodingStyle = "http://schemas.xmlsoap.org/soap/encoding/" xmlns: env = "http://schemas.xmlsoap.org/soap/envelope/">
<Env: Body>
<Koca: idc_issuercertProcedureResponse xmlns: Koca = "http://www.safelayer.com/namespaces/keyoneca">
<Koca: p7> PKCS # 7 en base 64 </ Koca: p7>
<Koca: cierto> CERT en base 64 </ Koca: cierto>
<Koca: n_serie> {SerialNumber} </ Koca: n_serie>
</ Koca: idc_issuercertProcedureResponse>
</ Env: Body>
</ Env: Envelope>

respuesta Error

<Env: Envelope env: encodingStyle = "http://schemas.xmlsoap.org/soap/encoding/" xmlns: env = "http://schemas.xmlsoap.org/soap/envelope/">
<Env: Body>
<Env: Fault>
<Faultcode> env: Cliente </ faultcode>
<Faultstring> ERROR - IDCAT_E7002

Causa: Error de unicidad en la CA

Detalles: Número de serie del certificado vigente: 7091B9493C0A5B1052C1791D71A6EA58 Fecha de expiración del certificado vigente: 30/12/2017 14:46:03 </ faultstring>
</ Env: Fault>
</ Env: Body>
</ Env: Envelope>

5.3.2 Revocación de certificados

petición

<Soapenv: Envelope xmlns: soapenv = "http://schemas.xmlsoap.org/soap/envelope/" xmlns: key = "http://www.safelayer.com/namespaces/keyoneca">
<Soapenv: Header />
<Soapenv: Body>
<Key: idc_revokecertProcedureRequest>
<Key: SerialNumber> {SerialNumber} </ key: SerialNumber>
<Key: reason> unspecified </ key: reason>
</ Key: idc_revokecertProcedureRequest>
</ Soapenv: Body>
</ Soapenv: Envelope>

respuesta

<Env: Envelope env: encodingStyle = "http://schemas.xmlsoap.org/soap/encoding/" xmlns: env = "http://schemas.xmlsoap.org/soap/envelope/">
<Env: Body>
<Koca: idc_revokecertProcedureResponse xmlns: Koca = "http://www.safelayer.com/namespaces/keyoneca" />
</ Env: Body>
</ Env: Envelope>

respuesta Error

<Env: Envelope env: encodingStyle = "http://schemas.xmlsoap.org/soap/encoding/" xmlns: env = "http://schemas.xmlsoap.org/soap/envelope/">
<Env: Body>
<Env: Fault>
<Faultcode> env: Cliente </ faultcode>
<Faultstring> ERROR - IDCAT_E7302

Causa: no puede modificarse el estado del certificado Porque ya está revocado.

Detalles: Número de serie: 0x0C95DB60830EEC2B533D418565679D7A </ faultstring>
</ Env: Fault>
</ Env: Body>
</ Env: Envelope>

5.3.3 Suspensión de certificados

petición

<Soapenv: Envelope xmlns: soapenv = "http://schemas.xmlsoap.org/soap/envelope/" xmlns: key = "http://www.safelayer.com/namespaces/keyoneca">
<Soapenv: Header />
<Soapenv: Body>
<Key: idc_suspendcertProcedureRequest>
<Key: SerialNumber> {SerialNumber} </ key: SerialNumber>
</ Key: idc_suspendcertProcedureRequest>
</ Soapenv: Body>
</ Soapenv: Envelope>

respuesta

<Env: Envelope env: encodingStyle = "http://schemas.xmlsoap.org/soap/encoding/" xmlns: env = "http://schemas.xmlsoap.org/soap/envelope/">
<Env: Body>
<Koca: idc_suspendcertProcedureResponse xmlns: Koca = "http://www.safelayer.com/namespaces/keyoneca" />
</ Env: Body>
</ Env: Envelope>

respuesta Error

<Env: Envelope env: encodingStyle = "http://schemas.xmlsoap.org/soap/encoding/" xmlns: env = "http://schemas.xmlsoap.org/soap/envelope/">
<Env: Body>
<Env: Fault>
<Faultcode> env: Cliente </ faultcode>
<Faultstring> ERROR - IDCAT_E7102

Causa: ERROR - StoresEvent_RecordNotFound </ faultstring>
</ Env: Fault>
</ Env: Body>
</ Env: Envelope>

5.3.4 Habilitación de certificados

petición

<Soapenv: Envelope xmlns: soapenv = "http://schemas.xmlsoap.org/soap/envelope/" xmlns: key = "http://www.safelayer.com/namespaces/keyoneca">
<Soapenv: Header />
<Soapenv: Body>
<Key: idc_activatecertProcedureRequest>
<Key: SerialNumber> {SerialNumber} </ key: SerialNumber>
</ Key: idc_activatecertProcedureRequest>
</ Soapenv: Body>
</ Soapenv: Envelope>

respuesta

<Env: Envelope env: encodingStyle = "http://schemas.xmlsoap.org/soap/encoding/" xmlns: env = "http://schemas.xmlsoap.org/soap/envelope/">
<Env: Body>

<Koca: idc_activatecertProcedureResponse xmlns: Koca = "http://www.safelayer.com/namespaces/keyoneca" />
</ Env: Body>
</ Env: Envelope>

respuesta error

<Env: Envelope env: encodingStyle = "http://schemas.xmlsoap.org/soap/encoding/" xmlns: env = "http://schemas.xmlsoap.org/soap/envelope/">
<Env: Body>
<Env: Fault>
<Faultcode> env: Cliente </ faultcode>
<Faultstring> ERROR - IDCAT_E7202

Causa: no puede modificarse el estado del certificado Porque ya está revocado.

Detalles: Número de serie: 0x0C95DB60830EEC2B533D418565679D7A </ faultstring>
</ Env: Fault>
</ Env: Body>
</ Env: Envelope>

5.4 Generación y publicación de CRLs

El sistema genera CRLs de duración 7 días con los certificados revocados y suspendidos. Cada EC genera un mínimo de una CRL cada 24 horas.

Una vez generadas se publican de manera automática, a través de una conexión segura SSH, a tres servidores externos.

Estas tareas las realiza la aplicación PKI mediante automatismos.

5.5 Servicio de validación OCSP

La infraestructura dispone de servicio de validación a través del protocolo OCSP.

El origen de los datos de revocación son las CRLs generadas por la EC y publicadas en servidores externos.

El sistema verifica la existencia de nuevas CRLs cada minuto y deja de responder si la disponibilidad de las CRLs supera un tiempo de 5 minutos.

Adicionalmente al comportamiento estándar el servicio OCSP tiene dos funcionalidades adicionales que se describen a continuación.

5.5.1 Clave para cada EC

Por cada EC configurada al servicio OCSP, se dispone de una llave con usos de firma de respuestas OCSP emitida por esta EC.

Esto permite, que en un único servicio (URL, https://ocsp.catcert.cat) Se pueda dar servicio a todas las Ecs de la infraestructura y dar respuestas firmadas con una llave de la misma jerarquía que el certificado que colamos validar. Este aspecto es especialmente importante

para ser interoperable con la validación de los certificados SSL que realiza el navegador Firefox.

5.5.2 auditoría

Para obtener datos de auditoría de las peticiones recibidas por el servicio, existe una tarea en segundo plano, que se ejecuta cada noche y que, a partir de los rastros del servicio, genera en la base de datos una tabla de auditoría. A partir de esta tabla el sistema genera los siguientes informes que son utilizados a modo de auditoría.

Los informes generados son:

- OCSP - PETICIONES PARA EC, MES y AÑO
- OCSP - PETICIONES POR MES Y TIPO DEL AÑO EN CURSO
- OCSP - RANKING DE PETICIONES POR DIA MAS ACTUAL
- OCSP - PETICIONES PARA EC, POLITICA, MES y AÑO

Ejemplo de OCSP - PETICIONES POR MES Y TIPO DEL AÑO EN CURSO (datos reales)

AÑO	MES	TIPO	NUMERO_PETICIONS	AVG_PETICIONS_DIA
2012	6	OCSP	3974190	132473
2012	7	OCSP	3100344	100011
2012	8	OCSP	1953499	63016
2012	9	OCSP	4032410	134414
2012	10	OCSP	5078318	163817
2012	11	OCSP	4958461	165282
2012	12	OCSP	4137535	133469
2013	1	OCSP	4867867	157028
2013	2	OCSP	4661009	166465
2013	3	OCSP	4899335	158043
2013	4	OCSP	4992197	166407
2013	5	OCSP	5292794	170735
2013	6	OCSP	4937539	164585
2013	7	OCSP	4164789	134348
2013	8	OCSP	2173591	70116
2013	9	OCSP	4401772	146726
2013	10	OCSP	5459965	176128
2013	11	OCSP	4646048	154868
2013	12	OCSP	4259595	137406
2014	1	OCSP	4554034	146904
2014	2	OCSP	4596994	164178
2014	3	OCSP	5268504	169952
2014	4	OCSP	2197	2197

Fecha generación: 04/01/2014 02:42:14

Maquinari físic

CA Root: HP Model 290 G1 amb HSM USB Edge	SW Linux, EJBCA, MySQL
CA Root CONT: HP Model 290 G1 amb HSM USB Edge	SW Linux, EJBCA, MySQL

Dispositius criptogràfics (HSM)

HSM-PKI-PRO-1	HSM Connect XC, NCIPHER	NH2089	EC2A-03E0-D947	46-SC0577	HSM de PKI	
HSM-PKI-PRO-2	HSM Connect XC, NCIPHER	NH2089	ED16-05E0-D947	46-SC4384	HSM de PKI	
CA Root: HP Model 290 G1 amb HSM USB Edge	HSM USB Edge	HSM			Linux	EJBCA, MYSQL
CA Root CONT: HP Model 290 G1 amb HSM USB Edge	HSM USB Edge	HSM			Linux	EJBCA, MYSQL

Codi Font en PHP de IDCAT (GIT)
Dump de BD Mysql IDCAT
Codi Font en PHP de OSIRIS (GIT)
Dump de BD Mysql OSIRIS
Impressores
Stock targetes
Stock de material d'oficina: sobres, cartes, cintes d'impressora
Procediment intern de gestió de sol·licituds
Targetes d'Operacions (revocació)
Indicadors de volumetries dels serveis
PCs per les ER

nos	CP	población	CIF	Id. equipo	código Ámbito	Descripción	marca	modelo
Ayuntamiento de Castelldefels	8860	Castelldefels	P0805500F	ER-001	101	CPU Estación RRA	HP	DC5100 / P5 650 SFF
						Monitor Estación RRA	HP	L1702
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	SP55
						Impresora láser para PINs y PUKs	HP	Laserjet 1320n
						Windows 7 64 bits		
Ayuntamiento de Girona	17004	Girona	P1708500B	ER-002	102	CPU Estación RRA	HP	DC5100 / P5 650 SFF
						Monitor Estación RRA	HP	L1702
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP60Plus
						Impresora láser para PINs y PUKs	HP	Laserjet 1320n
						Windows XP		
Ayuntamiento de Lleida	25007	Lleida	P2515100B	ER-003	103	CPU Estación RRA	HP	DC5100 / P5 650 SFF
						Monitor Estación RRA	HP	L1940G
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	SP55 PLUS
						Impresora láser para PINs y PUKs	HP	Laserjet 1320n
						Windows XP		
Ayuntamiento de Rubí	8191	Rubí	P0818300F	BAJA	104	CPU Estación RRA	HP	DC5100 / P5 650 SFF
						Monitor Estación RRA	HP	L1702
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	SP55
						Impresora láser para PINs y PUKs	HP	Laserjet 1320n
Ayuntamiento de Terrassa	8221	Terrassa	P0827900B	BAJA	105	CPU Estación RRA	HP	DC5100 / P5 650 SFF
						Monitor Estación RRA	HP	L1702
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	SP55
						Impresora láser para PINs y PUKs	HP	Laserjet 1320n
Ayuntamiento de Vilanova y la Geltrú	8800	Vilanova y la Geltrú	P0830800I	ER-006	106	CPU Estación RRA	HP	DC5100 / P5 650 SFF
						Monitor Estación RRA	HP	L1702
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	SP55
						Impresora láser para PINs y PUKs	HP	Laserjet 1320n
						Windows XP		
Consejo Comarcal del Alt Penedès	8720	Vilafranca del Penedès	P5800013D	ER-007	107	CPU Estación RRA	HP	Compaq 8000 ELITE
						Monitor Estación RRA	HP	LE 1901W
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP40 PLUS
						Impresora láser para PINs y PUKs	HP	Laserjet P2055d
						Windows 7 32 bit		
Consejo Comarcal del Alt Urgell	25700	La Seu d'Urgell	P7500006G	ER-008	108	CPU Estación RRA	HP	HP Compaq 8000 Elite
						Monitor Estación RRA	HP	L1702
						Lector de Tarjetas	Bit4id	MINILECTOR
						Impresora de tarjetas	DATACARD	CD800
						Windows 7 32 bit		
						Impresora láser para PINs y PUKs	HP	Laserjet 1320n
Consejo Comarcal del Baix Ebre	43500	Tortosa	P9300004J	ER-009	109	CPU Estación RRA	HP	Compaq 8000 ELITE
						Monitor Estación RRA	HP	LE1901W
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP40 PLUS
						Windows 7 32 bit		
						Impresora láser para PINs y PUKs	HP	Laserjet P2055d
Consejo Comarcal de la Conca de Barberà	43400	Montblanc	P9300007C	ER-009	110	CPU Estación RRA	HP	Compaq 8000 ELITE
						Monitor Estación RRA	HP	L1702
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CD800
						Windows 7 32 bit		
						Impresora láser para PINs y PUKs	HP	Laserjet 1320n
Consejo Comarcal de la Garrotxa	17800	Olot	P6700007E	ER-011	111	CPU Estación RRA	HP	Compaq 8000 ELITE
						Monitor Estación RRA	HP	LE1901W
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP40 PLUS
						Windows 7 32 bit		
						Impresora láser para PINs y PUKs	HP	Laserjet P2055d
Consejo Comarcal de Osona	8500	Vic	P5800015I	ER-012	112	CPU Estación RRA	HP	Compaq 8000 ELITE
						Monitor Estación RRA	HP	LE 1901W
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP40 PLUS
						Windows 7 32 bit		
						Impresora láser para PINs y PUKs	HP	Laserjet P2055d
Consejo Comarcal del Pallars Sobirà	25560	suerte	P7500010I	ER-013	113	CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1702
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP60
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 1320n
Consejo Comarcal de la Ribera d'Ebre	43740	Mora de Ebro	P9300011E	ER-014	114	CPU Estación RRA	HP	HP Compaq 8000 Elite
						Monitor Estación RRA	HP	LE1901W
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP40 PLUS
						Windwos 7 32 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet P2055d
Consejo Comarcal del Ripollès	17500	Ripoll	P6700004B	ER-015	115	CPU Estación RRA	HP	Compaq 8000 ELITE
						Monitor Estación RRA	HP	LE1901W
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CD800
						Windows 7 32 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet P2055d
	25007	Lleida	P7500008C			CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1702

Consejo Comarcal del Segrià				ER-016	116	Lector de Tarjetas	Bit4id	MINILECTOR
						Impresora de tarjetas	DATACARD	CD800
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 1320n
Consejo Comarcal de la Selva	17430	Santa Coloma de Farners	P6700002F	ER-017	117	CPU Estación RRA	HP	Compaq 8000 ELITE
						Monitor Estación RRA	HP	LE1901W
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP40 PLUS
						Windows 7 32 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet P2055d
Consejo Comarcal del Tarragonès	43003	Tarragona	P9300002D	ER-018	118	CPU Estación RRA	HP	Compaq 8000 ELITE
						Monitor Estación RRA	HP	LE1901W
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP40 PLUS
						Windows 7 32 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet P2055d
Consejo Comarcal de la Terra Alta	43780	Gandesa	P9300010G	ER-019	119	CPU Estación RRA	HP	HP Compaq 8000 Elite
						Monitor Estación RRA	HP	L1702
						Lector de Tarjetas	Bit4id	MINILECTOR
						Impresora de tarjetas	DATACARD	CD800
						Windows 7 32 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 1320n
Consejo Comarcal del Pla de l'Estany	17820	Banyoles	P6700010I	ER-020	121	CPU Estación RRA	HP	HP Compaq 8000 Elite
						Monitor Estación RRA	HP	LE1901W
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP40 PLUS
						Windows 7 32 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet P2055d
CATCert (1)		Barcelona		ER-000	000	CPU Estación RRA		
						Monitor Estación RRA		
						Lector de Tarjetas		
						Impresora de tarjetas		
						Impresora láser para PINs y PUKs		
Ayuntamiento de Santa Coloma de Gramanet	8921	Santa Coloma de Gramenet	A60517018	BAJA	122	CPU Estación RRA	HP	DC5100 / P5 650 SFF
						Monitor Estación RRA	HP	L1702
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	SP55
						Impresora láser para PINs y PUKs	HP	Laserjet 1320n
Departamento de Justicia	8010	Barcelona	S0811001G	ER-025	301	CPU Estación RRA	HP	DC5100 / P5 650 SFF
						Monitor Estación RRA	HP	L1702
						Lector de Tarjetas	C3PO	TLTC4USB
						Impresora de tarjetas	DATACARD	CP60 Plus
						Impresora láser para PINs y PUKs	HP	Laserjet 1320n
ORGT	8028	Barcelona	P5800016G	ER-026	120	CPU Estación RRA	HP	
						Monitor Estación RRA	HP	L1740
						Lector de Tarjetas		Integrado al teclado
						Impresora de tarjetas	DATACARD	CP 40 plus
						Window 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 14250 DTN
CATCert (material)		Barcelona		ER-027		CPU Estación RRA		
						Monitor Estación RRA		
						Lector de Tarjetas		
						Impresora de tarjetas		
						Impresora láser para PINs y PUKs		
Firmaprofesional	8173	Sant Cugat del Vallès		ER-028	000	CPU Estación RRA	HP	DC8000
						Monitor Estación RRA	HP	LE1901W
						Lector de Tarjetas		
						Impresora de tarjetas	DATACARD	CD800
						Impresora láser para PINs y PUKs		
Ayuntamiento de Sant Feliu de Llobregat	8980	Sant Feliu de Llobregat	P0821000G	ER-029	123	CPU Estación RRA	HP	DC7700 SFF
						Monitor Estación RRA	HP	L1740
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP 60 plus
						Windows 7		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Ayuntamiento de Mollet del Vallès	8100	Mollet del Vallès	P0812300B	ER-031	124	CPU Estación RRA	HP	DC7700 SFF
						Monitor Estación RRA	HP	L1740
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP40
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Consejo Comarcal del Baix Camp	43202	Reus	P9300003B	ER-032	125	CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1750
						Lector de Tarjetas	Bit4id	MINILECTOR
						Impresora de tarjetas	DATACARD	CD800
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Consejo Comarcal de la Segarra	25200	Cervera	P7500007E	ER-033	126	CPU Estación RRA	HP	Compaq Elite 8000
						Monitor Estación RRA	HP	LE1901W
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP 40 plus
						Windows 7 32 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
Consejo Comarcal del Alt Camp	43800	Valls	P9300005G	ER-034	127	CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1750
						Lector de Tarjetas	Bit4id	MINILECTOR
						Impresora de tarjetas	DATACARD	CP60
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Ayuntamiento de Manresa	8241	Manresa	P0811200E	ER-037	130	CPU Estación RRA	HP	DC7700 SFF
						Monitor Estación RRA	HP	L1740
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	SP55
						Windows XP		

						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Ayuntamiento de Badalona	8911	Badalona	P0801500J	ER-038	131	CPU Estación RRA	HP	DC7800 SFF
						Monitor Estación RRA	HP	L1750
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CP60
						Windows XP		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
CATCert (desarrollo D.Cos)				LRA-39	0	CPU Estación RRA	HP	DC7700 SFF
						Monitor Estación RRA	HP	L1740
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	SP55
Consejo Comarcal del Maresme	8301	Mataró	P5800008D	ER-040	132	CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1740
						Lector de Tarjetas	Bit4id	MINILECTOR
						Impresora de tarjetas	DATACARD	CD800
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Ayuntamiento de Reus	43201	Reus	P4312500D	ER-041	129	CPU Estación RRA	HP	DC7800 SFF
						Monitor Estación RRA	HP	L1750
						Lector de Tarjetas	C3PO	LTC31
						Impresora de tarjetas	DATACARD	CP60
						Windows 7		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Consejo Comarcal del Vallès Oriental	8401	Granollers	P5800010J	ER-042	133	CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1750
						Lector de Tarjetas	Bit4id	MINILECTOR
						Impresora de tarjetas	DATACARD	CD800
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Consejo Comarcal del Anoia	8700	Igualada	P5800006H	ER-043	134	CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1740
						Lector de Tarjetas	Bit4id	MINILECTOR
						Impresora de tarjetas	DATACARD	CD800
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Consejo Comarcal del Pla d'Urgell	25230	Mollerussa	P7500012E	ER-044	135	CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1740
						Lector de Tarjetas	Bit4id	MINILECTOR
						Impresora de tarjetas	DATACARD	CD800
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Ayuntamiento de Tarragona	43003	Tarragona	P4315000B	ER-045	128	CPU Estación RRA	HP	DC7800 SFF
						Monitor Estación RRA	HP	L1750
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP60 PLUS
						Windows XP		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Consejo Comarcal de la Noguera	25600	Balaguer	P7500005I	ER-046	136	CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1750
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CP60
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Consejo comarcal del Berguedà	8600	Berga	P0800015J	ER-047	137	CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1750
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CP60
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Consejo comarcal del Baix Empordà	17100	La Bisbal del Empordà	P6700009A	ER-048	138	CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1740
						Lector de Tarjetas	Bit4id	LTC31
						Impresora de tarjetas	DATACARD	CP60
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Consejo comarcal del Pallars Jussà	25620	Tremp	P7500014A	ER-049	139	CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1750
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CP60
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Consejo comarcal del Urgell	25300	Tàrrega	P7500003D	ER-050	140	CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1750
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CD800
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Consejo Comarcal del Vallès Occidental	8227	Terrassa	P5800007F	ER-051	141	CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1750
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CD800
						Windows 7 64 bits		
						CPU Estación RRA	HP	DC7800 SFF
Consejo Comarcal del Montsià	43870	Amposta	P9300008A	ER-052	143	CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1750
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CD800
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
CTTI	8908	Hospitalet de Llobregat	Q5856338H	ER-053	302	CPU Estación RRA	HP	DC7800 SFF
						Monitor Estación RRA	HP	L1750
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CP60
						Windows 7 32 bits		
						Impresora láser para PINs y PUKs	HP	

Parlamento	8003	Barcelona	Q5856081D	ER-054	000	CPU Estación RRA	HP	DC5100 / P5 650 SFF
						Monitor Estación RRA	HP	L1702
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	ImageCard Select PS
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
Diputación de Tarragona	43003	Tarragona	P9300002D	ER-055	100	CPU Estación RRA	HP	dc7900 COMPAQ
						Monitor Estación RRA	HP	L1702
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP40
						Windows Vista 32 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2010
Consejo Comarcal del Alt Empordà	17600	Figueres	P6700008C	ER-056	145	CPU Estación RRA	HP	G280 G1
						Monitor Estación RRA	HP	LE1901W
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CD800
						Windows 7 64 bits		
						CPU Estación RRA	HP	Laserjet 2055d
Consejo Comarcal del Garraf	8800	Vilanova y la Geltrú	P5800020I	ER-057	142	CPU Estación RRA	HP	HP 280 G1
						Monitor Estación RRA	HP	L1750
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CP60
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
Ayuntamiento de Sabadell	8201	Sabadell	P0818600I	ER-059	144	CPU Estación RRA	DELL	Optiplex X755
						Monitor Estación RRA	DELL	
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CP60
						Windows XP		
						Impresora láser para PINs y PUKs	HP	Laserjet 1320n
Consejo General de Aran	25530	Vielha	P7500011G	ER-060	150	CPU Estación RRA	HP	G280 G1
						Monitor Estación RRA	HP	LA1951G
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CP 60 plus
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
Consejo Comarcal de las Garrigues	25400	Les Borges Blanques	P7500004B	ER-061	149	CPU Estación RRA	HP	G280 G1
						Monitor Estación RRA	HP	LA1951G
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CP 60 plus
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
Consejo comercal del Priorat	43730	Falset	P9300009L	ER-062	147	CPU Estación RRA	HP	G280 G1
						Monitor Estación RRA	**HP**	LA1951G
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CP 60 plus
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
Consejo Comarcal del Solsonès	25280	Solsona	P7500009A	ER-063	151	CPU Estación RRA	HP	G280 G1
						Monitor Estación RRA	HP	LA1951G
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CP 60 plus
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
Consejo Comarcal de la Alta Ribagorça	25550	El Pont de Suert	P7500013C	ER-064	146	CPU Estación RRA	HP	dc7900 SFF
						Monitor Estación RRA	HP	LA1951G
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CD800
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
Consejo Comarcal del Baix Penedès	43700	el vendrell	P9300006E	ER-065	148	CPU Estación RRA	HP	dc7900 SFF
						Monitor Estación RRA	HP	LA1951G
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CP 60 plus
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
Consejo Comarcal del Bages	8241	Manresa	P5800009B	ER-066	152	CPU Estación RRA	HP	dc7900 SFF
						Monitor Estación RRA	HP	LA1951G
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CP 60 plus
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
CATCert LRA PRODUCCIÓN		Barcelona		ER-067		CPU Estación RRA	HP	DC7700 SFF
						Monitor Estación RRA	HP	L1940
						Lector de Tarjetas	C3PO	LTC-31
						Impresora de tarjetas	DATACARD	CD800
						Impresora láser para PINs y PUKs	HP	Laserjet 2015d
CESCA (CSUCA)	8034	Barcelona		no tiene ID	000	CPU Estación RRA	HP	D530
						Monitor Estación RRA	Phillips	107511
						Lector de Tarjetas	Cherry	ACR38
						Impresora de tarjetas	DATACARD	CP40 +
						Impresora láser para PINs y PUKs	HP	LJ P2015d
Consejo Comarcal de la Cerdanya	17520	Puigcerdà	P1700016G	ER-068	**153**	CPU Estación RRA	HP	dc7900 SFF
						Monitor Estación RRA	HP	LA1951G
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CP40 +
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
Agencia Catalana de la Protección de Datos	8018	Barcelona	P5800009B	ER-069	303	CPU Estación RRA	HP	dc7900 SFF
						Monitor Estación RRA	HP	LA1951G
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	Fargo	CP60Plus
						Windows 7		
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
						CPU Estación RRA	HP	G280 G1
						Monitor Estación RRA	HP	LA1951G

Consejo Comarcal del Gironès	17003	Girona	P6700003D	ER-070	154	Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	Datacard	CD800
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
Agjuntament de Cerdanyola del Vallès	8290	Cerdanvola del Vallès	P0826600I	ER-071	155	CPU Estación RRA	HP	dc7900 SFF
						Monitor Estación RRA	HP	LA1951G
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	Datacard	CP40 +
						Windows 7		
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
Ayuntamiento de Mataró	8006	Mataró	P0812000H	ER-072	156	CPU Estación RRA	HP	dc7900 SFF
						Monitor Estación RRA	HP	LA1951G
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	Datacard	CP40 +
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
Ayuntamiento de Cornellà de Llobregat	8940	Cornellà de Llobregat	P0807200A	ER-073	157	CPU Estación RRA	HP	dc7900 SFF
						Monitor Estación RRA	HP	LA1951G
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	Datacard	CP60
						Windows Vista 32 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
Departamento de Agricultura	8007	Barcelona	S0811001G	ER-074	304	CPU Estación RRA	HP	dc7900
						Monitor Estación RRA	HP	LE1901W
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	Datacard	CP40 +
						Windows Vista 32 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
Consejo Comarcal del Baix Llobregat	08890	Sant Feliu de Llobregat	P5800011H	ER-075	158	CPU Estación RRA	HP	Compaq dc7900
						Monitor Estación RRA	HP	LE 1901W
						Lector de Tarjetas	Bit4id	ACR38
						Impresora de tarjetas	DATACARD	CP40 PLUS
						Windows 7 64 bits		
						Impresora láser para PINs y PUKs	HP	Laserjet P2055d
Firmaprofesional	8173	Sant Cugat del Vallès		ER-076	0	CPU Estación RRA	HP	Compaq 8000 ELITE
						Monitor Estación RRA		
						Lector de Tarjetas		
						Impresora de tarjetas	Datacard	CP60
						Impresora láser para PINs y PUKs	HP	Laserjet 2055d
Firmaprofesional	8173	Sant Cugat del Vallès		ER-077	0	CPU Estación RRA	HP	Compaq 8000 ELITE
						Monitor Estación RRA	HP	
						Lector de Tarjetas		
						Impresora de tarjetas	Datacard	CD800
						Impresora láser para PINs y PUKs		
Firmaprofesional	8173	Sant Cugat del Vallès		ER-078	0	CPU Estación RRA	HP	Compaq 8000 ELITE
						Monitor Estación RRA	HP	LE1901w
						Lector de Tarjetas		
						Impresora de tarjetas	Datacard	CD800
						Impresora láser para PINs y PUKs		
Consejo Comarcal del Moianès	8180	Moià	P0800317J	ER-079	0	CPU Estación RRA	HP	G280 G1
						Monitor Estación RRA	HP	LE1901w
						Lector de Tarjetas		
						Impresora de tarjetas	Datacard	CD800