



Consorci
Administració Oberta
de Catalunya

PLIEGO DE PRESCRIPCIONES TÉCNICAS POR LA PRESTACIÓN DEL SERVICIO DE FIRMA REMOTA BASADA EN CERTIFICADOS CALIFICADOS DEL CONSORCI AOC. AOC 2014 17

*“Se trata de una traducción automatizada del catalán al castellano. En caso de
discrepancia, prevalece la versión en catalán”.*

Realizado por: Consorci AOC

Versión:1.1

Fecha: 2023

Archivo: PPT_SSR_2023_v.1.1.docx



LOCALRET

1	Índice	
2	OBJETO.....	6
3	ALCANCE	7
4	MARCO NORMATIVO.....	8
5	DESCRIPCIÓN DE LA SITUACIÓN ACTUAL.....	10
5.1	El servicio de certificación digital del Consorci AOC.....	10
5.1.1	Modelo de registro.....	11
5.2	Los servicios de identificación y firma electrónica	12
5.2.1	Bus de integración de mecanismos de identificación y firma electrónica (Servicio VALid).....	12
5.2.2	Firmador	12
5.2.3	Mecanismos de autenticación para trabajadores públicos	12
5.3	El servicio Firmador Centralizado	13
6	DESCRIPCIÓN DE LOS SERVICIOS OBJETO DEL CONTRATO	14
6.1	Obligaciones esenciales del contrato.....	14
6.2	Obligaciones relativas al proceso de registro	15
6.3	Catálogo de servicios objeto del contrato	16
6.3.1	Servicios a tanto alzado	16
6.3.2	Servicios a precio unitario y mantenimiento de aplicaciones informáticas	17
6.3.3	Gestión de las claves de entidad final y jerarquía.....	17
6.4	El Servicio de Firma Remota (SSR) del Consorci AOC.....	18
6.4.1	Servicio de firma electrónica en remoto para la ciudadanía	18
6.4.2	Servicio de firma electrónica en remoto para los empleados y trabajadores del sector público	19
6.4.3	Servicio de firma electrónica en remoto con certificados de sello electrónico calificado por el sector público	19
6.5	Aplicación PKI	20
6.5.1	Emisión de Listas de Revocación de Certificados (CRL).....	21
6.5.2	Servicio de Consulta de Estado de Certificados en Línea (OCSP)	21
6.6	Modelo de registro de servicios del Consorci AOC.....	22
6.6.1	Registro ámbito del empleado público y sellos electrónicos.....	22
6.6.2	Registro ámbito ciudadanía.....	24
6.7	Infraestructura tecnológica	24
6.7.1	Entornos	24
6.7.2	Centros de Procesamiento de Datos	25
6.7.3	Hardware y software dedicado.....	25
6.8	Gobernamiento de la Seguridad	26
6.8.1	Gestión de trazas	26

6.8.2	Comunicaciones seguras de acceso a las aplicaciones objeto de la licitación	26
6.8.3	Arquitectura, pruebas de recuperación de desastres y pruebas de recuperación de backups	26
6.8.4	Seguridad de las instalaciones desde las que se presta el servicio	26
6.8.5	Seguridad en el cloud.....	26
6.8.6	La gestión de la seguridad y el cumplimiento normativo	27
6.8.7	La gestión de la continuidad y la disponibilidad	29
6.8.8	Cese de la actividad	30
6.8.9	Auditorías en las Entidades de Registro vinculadas	30
6.8.10	Auditorías del Prestador de Servicios de Certificación Consorci AOC	30
6.9	El servicio de soporte	31
6.9.1	El servicio de Apoyo del Consorci AOC	31
6.9.2	Ámbitos de atención y apoyo a prestar por el adjudicatario:	31
6.9.3	Canales de entrada de peticiones	31
6.9.4	Horario de atención	31
6.10	Servicio de Mantenimiento Evolutivo	32
6.10.1	Metodología.....	32
6.10.2	Mantenimiento correctivo	36
6.10.3	Mantenimiento técnico - legal.....	36
6.10.4	Mantenimiento evolutivo.....	37
6.10.5	Tareas en el ámbito del mantenimiento evolutivo	37
6.11	Servicios organizativos y de cumplimiento	37
6.11.1	Servicios de formación	38
6.11.2	Servicios de facturación	39
7	Acuerdos de nivel de servicio	40
7.1	Modelo de medida del nivel de servicio	41
7.1.1	Indicadores	42
7.1.2	Fuentes de información para la obtención de los niveles de servicio	42
7.1.3	Aplicación de los acuerdos de nivel de servicio	43
7.2	ANS de Explotación del Servicio	43
7.2.1	ANS del Servicio de emisión o cambio de estado de certificados T-CAT	43
7.2.2	ANS de disponibilidad	44
7.2.3	ANS de capacidad	44
7.2.4	ANS de continuidad.....	45
7.2.5	ANS de calidad del servicio de emisión y gestión de certificados	46
7.2.6	ANS del Servicio de Apoyo	46
7.3	ANS de los Servicios de Programación	47
7.3.1	Acuerdos de nivel de servicio del desarrollo	47

7.3.2	Requerimientos de nivel de servicio en el mantenimiento correctivo y resolución de incidencias	47
7.3.3	Tiempo de respuesta en el mantenimiento evolutivo	48
7.3.4	Desviaciones en el mantenimiento evolutivo	48
8	FASES DE EJECUCIÓN DEL CONTRATO	49
8.1	Creación y explotación del servicio firma remota calificada basada en certificados calificados del Consorci AOC	50
8.2	Transición de la operación del servicio actual	50
8.3	Devolución del servicio.....	50
9	SEGUIMIENTO DEL SERVICIO	52
9.1	Gobernamiento y mejora del servicio.....	52
9.2	Estructura de responsabilidades del adjudicatario.....	52
9.3	Estructura de responsabilidades del Consorci AOC	55
9.4	Gestión de incidencias y problemas	56
9.5	Órganos de Gestión	56
9.5.1	Reuniones de dirección.....	56
9.5.2	Reuniones de seguimiento.....	57
9.6	Modelo de relación en la fase de Transición de la operación	58
9.6.1	Gobernamiento de la fase de transición de la operación.....	58
10	REFERENCIAS	60
11	Anexo - Situación actual	61
11.1	Catálogo actual de certificados del Consorci AOC	61
11.2	Situación actual de subsistemas y componentes del Servicio.....	62
11.3	El Servicio de Registro de certificados personales y de sello electrónico por el Sector Público (T-CAT)	63
11.3.1	Modelo de Registro T-CAT.....	63
11.3.2	Topología de la red de Entidades de Registro T-CAT	65
11.3.3	Roles del sistema de registro T-CAT	66
11.3.4	Diagrama de relaciones de los procedimientos de emisión.....	68
11.3.5	Gestión documental del Servicio de Certificación T-CAT	71
11.3.6	Tabla de relación entre roles e historias de usuario del componente ASCD	71
11.3.7	Historias de usuario de las operaciones de solicitud y gestión del ciclo de vida de los certificados dentro de EACAT	72
11.3.8	Otras operaciones	75
11.4	El servicio de Registro de certificados personales por Ciudadanía (idCAT)	75
11.4.1	La web del ciudadano	76
11.4.2	La Web de los Operadores de Registro	76
11.4.3	La Web de los Operadores de Certificación o de administración	76

11.4.4	Procedimiento de solicitud y emisión idCAT	77
11.4.5	Servicios para el uso de certificados de sello electrónico centralizados: el Servicio Firmador Centralizado	78
11.4.6	Activos de software, código y datos del servicio actual a disposición del adjudicatario	78
11.5	Servicios de auditoría de ER.....	79
11.6	Servicios evolutivos y de personalización de software actuales.....	79
11.7	ANS actual del servicio de certificación	80
11.8	Formación y divulgación.....	80

2 OBJETO

El Consorci Administració Oberta de Catalunya (Consorci AOC) es el órgano competente en relación a 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 Catalunya y con sus estatutos. De acuerdo con esta competencia, como Prestador de Servicios de Confianza, ofrece al conjunto de las Administraciones Públicas Catalanas servicios de emisión de certificados cualificados, tanto de persona física, para los empleados públicos y la ciudadanía, como de sellos electrónicos.

El objeto de este pliego es la contratación de un servicio tecnológico de firma y sello electrónicos remotos, en modalidad de Platform as a Service (PaaS), así como su operación, para dar cobertura a la firma electrónica de documentos, y que permita la custodia y el uso de sellos electrónicos en el ejercicio de la actuación administrativa automatizada, así como de certificados cualificados de empleado público y de la ciudadanía.

3 ALCANCE

El presente pliego tiene por objeto la contratación del servicio de custodia de certificados calificados de sello electrónico, empleado público y ciudadanía, como base para la prestación de un servicio de firma remota para el conjunto de las Administraciones Públicas Catalanas. El Consorci AOC requiere contratar la infraestructura, puesta en marcha y operación, así como el soporte necesario para lograr la calificación de los certificados custodiados, tanto de persona física como sellos electrónicos, de acuerdo con las condiciones fijadas en los pliegos de prescripciones técnicas y administrativos particulares que regulan esta licitación.

En concreto, el adjudicatario deberá poner en marcha y operar una infraestructura que permita:

- Custodiar y utilizar certificados de sello electrónico calificados de las Administraciones Públicas Catalanas, que sea integrable con sus aplicaciones a través de las soluciones comunes de firma electrónica del Consorci AOC, para su uso en el ámbito de la actuación administrativa automatizada.
- Un sistema de firma remota que permita custodiar y utilizar certificados cualificados de trabajador público y que se pueda integrar con las aplicaciones de las Administraciones Públicas Catalanas, a través de las soluciones comunes de firma electrónica que el Consorci AOC ofrece.
- Un sistema de firma remota que permita custodiar y utilizar certificados cualificados de persona física orientado a la ciudadanía, sea integrable con las aplicaciones de las Administraciones Públicas Catalanas a través del servicio VALid del Consorci AOC. Teniendo en cuenta el uso esporádico que suelen tener este tipo de certificados, el sistema deberá permitir la posibilidad de que éstos sean de un solo uso.

En todos estos casos, los sistemas contratados y operados por el adjudicatario serán los dispositivos calificados de creación de firma y sello electrónicos remotos que utilizarán los certificados calificados de empleado público y trabajador público (TCAT), los sellos electrónicos calificados y los certificados de persona física (idCAT) que el Consorci AOC emite como Prestador Calificado de Servicios de Confianza. Para facilitar esta emisión, la empresa adjudicataria del contrato objeto de este pliego operará dos raíces intermedias, una por ciudadanía y otra por sellos electrónicos y certificados de empleado y trabajador público.

Estamos ante un servicio de alta criticidad, con un consumo elevado y una gran cantidad de usuarios concurrentes, así como una importante dependencia estratégica con los servicios digitales de los entes y organismos públicos del 39; ámbito catalán.

4 MARCO NORMATIVO

El Artículo 7 de la Ley 29/2010, de 3 de agosto, del uso de los medios electrónicos en el sector público de Catalunya establece, entre otros, que la Administración de la Generalitat y los entes locales, sin perjuicio de otras fórmulas de colaboración, cooperan y colaboran, ordinaria y voluntariamente, por medio del Consorci Administració Oberta Electrónica de Catalunya, en la definición y ejecución de las estrategias comunes por la extensión de los medios electrónicos para garantizar la identidad y acreditar la voluntad en las actuaciones de los ciudadanos y el personal del sector público. Por otra parte, el mismo artículo estipula que la Agencia Catalana de Certificación, integrada actualmente en el Consorci AOC, presta servicios de firma electrónica al sector público de Catalunya para garantizar la confidencialidad, la integridad, la identidad y el no- rechazo a las comunicaciones electrónicas que llevan a cabo las entidades del sector público de Catalunya.

La prestación de los servicios de servicios de certificación, como servicio de confianza, queda regulada por el Capítulo III del Reglamento (UE) 910/2014 del Parlamento y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza por las transacciones electrónicas en el mercado interior y que deroga la Directiva 1999/93/CE (en adelante eIDAS). En cuanto a los certificados calificados de firma electrónica, en su Anexo II sobre los requisitos de los dispositivos calificados de firma electrónica, abre la puerta a que los prestadores calificados de servicios de confianza puedan gestionar las claves de firma en nombre del signatario cuando dice, en punto 4, que éstos sólo podrán duplicarlas con el objetivo de realizar una copia de seguridad.

Por su parte, la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, y que es de aplicación a los prestadores establecidos en el Estado Español, en su artículo 9 especifica que uno prestador no podrá “almacenar ni copiar, por sí mismo oa través de un tercero, los datos de creación de firma, sello o autenticación de sitio web de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del titular. En este caso, utilizarán sistemas y productos fiables, incluidos los canales de comunicación electrónica seguros, y se aplicarán procedimientos y mecanismos técnicos y organizativos y adecuados, para garantizar que el entorno sea fiable y se utilice bajo el control exclusivo del titular del certificado. Además, tendrán que custodiar y proteger los datos de creación de firma, sello o autenticación de sitio web ante cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.”

Con el objetivo de cumplir con los requisitos de seguridad establecidos, se han definido dos normas técnicas aplicables a las aplicaciones de firma en servidor, a los módulos de activación de firma ya los módulos criptográficos, que son respectivamente:

- CEN EN 419 241-1 Trustworthy Systems Supporting Server Signing; - Parte 1: General System Security Requirements
- CEN EN 419 241-1 Trustworthy Systems Supporting Server Signing; - Parte 2: Protection profile for QSCD for Server Signing
- CEN EN 419 221-5 Protection Profiles for TSP Cryptographic Modules - Parte 5: Cryptographic Module for Trust Services

Por otra parte, existen especificaciones técnicas que definen requisitos de seguridad para los prestamistas de servicios de confianza aplicables a la operación de dispositivos remotos de firma y sello electrónicos, así como un protocolo para su uso:

- ETSI TS 119 431-1 Electronic Firms and Infraestructuras (ESI); Policy and security requirements for trust service providers; Parte 1: TSP service components operating a remote QSCD / SCDev
- ETSI TS 119 431-2 Electronic Firms and Infraestructuras (ESI); Policy and security requirements for trust service providers; Parte 2: TSP service components supporting AdES digital signature creation

- ETSI TS 119 432 Electronic Firmas and Infraestructuras (ESI); Protocolos for remote digital signature creation

Por último, hay que tener en cuenta las normas europeas aprobadas para garantizar los requisitos que deben cumplir los prestadores calificados de servicios de confianza en general, y los que emiten certificados calificados de firma y sello electrónico, y que son:

- ETSI EN 319 401 Electronic Firmas and Infraestructuras (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411 Electronic Firmas and Infraestructuras (ESI); Policy and security requirements for Trust Service Providers issuing certificates
- ETSI EN 319 412 Electronic Firmas and Infraestructuras (ESI); Certificate Profiles

En cuanto a la prestación de servicios de certificación en el ámbito de las administraciones públicas, tratándose de servicios que trabajan con datos de carácter personal, será necesario tener en cuenta y cumplir con lo que establece Reglamento (UE) 2016/679, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales. Por otra parte, siendo el Consorci AOC parte del sector público de Catalunya, se requerirá que la empresa adjudicataria esté certificada en el Esquema Nacional de Seguridad, regulado actualmente por el Real Decreto 311/2022, de 3 de mayo.

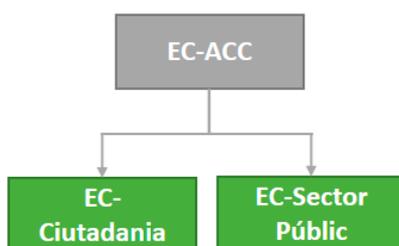
La normativa interna del Consorci AOC en materia de seguridad y del servicio objeto de licitación.

5 DESCRIPCIÓN DE LA SITUACIÓN ACTUAL

5.1 El servicio de certificación digital del Consorci AOC

El Consorci AOC es el prestador calificado de servicios de confianza de las Administraciones Públicas Catalanas, emitiendo certificados de sello electrónico, de empleado público y de persona física para la ciudadanía. Como tal, dispone de una jerarquía formada por una Entidad de Certificación raíz (root CA), que es la EC-ACC, y 2 Entidades de Certificación subordinadas y englobando de la siguiente forma los ámbitos de prestación de los servicios:

- **EC-SectorPublic:** que concentra la emisión de certificados por el Sector Público de Catalunya. Es la entidad subordinada que emite los certificados:
 - **TCAT y TCAT-P** como certificados calificados de firma calificada y firma avanzada respectivamente.
 - **TCAT de representante** de administración pública
 - **TCAT y T-CAT P de seudónimo**
 - **Certificados de sellos electrónico**
 - **Certificados de dispositivo Aplicación (CDA) y Sello Electrónico**
- **EC-Ciudadanía:** que emite certificados digitales a la ciudadanía conocidos como idCAT.



Actualmente, el Consorci AOC está ampliando esta jerarquía para incluir autoridades de certificación subordinadas por los siguientes ámbitos concretos:

- SubCA SECTOR PUBLIC Q (G3) A.1: para la emisión de certificados electrónicos calificados para el sector público de Catalunya, en sustitución del EC-SECTORPUBLIC.
- SubCA CIUDADANÍA Q (G3) A.2: para la emisión de certificados electrónicos calificados para ciudadanía, en sustitución de la EC-CIUDADANÍA.
- SubCA SECTOR PÚBLICO R Q (G3) A.3: para la emisión de certificados electrónicos calificados de firma remota para el sector público de Catalunya.
- SubCA CIUDADANÍA R Q (G3) A.4: para la emisión de certificados electrónicos calificados de firma remota para ciudadanía.
- SubCA Q TSA (G3) A.5: para la emisión de certificados electrónicos calificados para servicios de sellos de tiempo calificado.
- SubCA TSA noQ (G3) A.6: para la emisión de certificados electrónicos calificados para servicios de sellos de tiempo no calificado.
- SubCA noQ (G3) A.7: para la emisión de certificados electrónicos no calificados.

Con el objetivo de permitir al adjudicatario del contrato objeto de la presente licitación poder emitir certificados de firma y sello electrónico remotos, éste se encargará de la operación de las siguientes entidades subordinadas:

- SubCA SECTOR PÚBLICO R Q (G3) A.3.

- SubCA CIUDADANÍA R Q (G3) A.4.

Las claves privadas de estas subCAs se generaron en 2022 en una sesión auditada, se protegieron con unas tarjetas de Operación (OCS) en propiedad exclusiva del Consorci AOC y se mantienen sin operación desde ese momento hasta la adjudicación del contrato objeto de esa licitación.

La prestación de los servicios de certificación del Consorci AOC está regulado por un documento de Declaración de Prácticas, unas políticas de certificación, unos textos de divulgación y unos documentos de perfiles disponibles en <https://epsd.aoc.cat/regulacio>. El contenido final de este conjunto de documentos dependerá de la solución ofrecida por el adjudicatario, aunque estará basado en las best practices recomendadas por la norma aplicable. El Consorci AOC facilitará al adjudicatario la inclusión de sus propuestas de cambio en este conjunto documental para reflejar las características del servicio.

Se adjunta más detalle sobre la situación actual de los servicios ofrecidos por el Consorci AOC en el punto 11 ([Anexo I](#)) de este mismo documento

5.1.1 Modelo de registro

Sector Público

Para poder emitir certificados de empleado y trabajador público y sellos electrónicos para su personal, aplicaciones y servicios, las administraciones públicas catalanas se establecen como entidades suscriptoras del Servicio TCAT, desde donde se llevan a cabo las tareas de verificación de la identidad y registro previo. En concreto, las entidades suscriptoras verifican la identidad del sujeto de los certificados, gestionan su emisión y su entrega y custodia. En su caso, también gestionan su revocación o renovación.

Las personas operadoras de las entidades suscriptoras se identifican y solicitan la emisión de certificados a través de pantallas dispuestas al efecto en la plataforma EACAT, que enviará las peticiones al software de la Entidad de Certificación, encargada de su gestión y ejecución. El resto de las operaciones relativas al ciclo de vida de los certificados (petición, aprobación, entrega y revocación) se realizan a través de la aplicación web de registro de la Entidad de Certificación.

Las entidades suscriptoras del servicio TCAT actúan de acuerdo con el correspondiente documento de [condiciones específicas](#) disponible desde el sitio web del Consorci AOC.

Ciudadanía

Asimismo, el Consorci AOC dispone también de una red de Entidades de Registro distribuidas por todo el territorio que se encargan de identificar y registrar a las personas que piden un certificado de persona física idCAT de forma presencial. El portal de apoyo del Consorci AOC ofrece una [lista de las entidades](#) dónde se puede dirigir la ciudadanía a la hora obtener un certificado idCAT.

Como en el caso de las entidades suscriptoras del servicio TCAT, las entidades de registro idCAT operan con acuerdo en el correspondiente documento de [condiciones específicas](#). Sin embargo, en el caso de idCAT la aplicación web para gestionar las operaciones de una entidad de registro idCAT no está integrada en la plataforma EACAT, y el software de la Entidad de Certificación que las hace efectivas es también independiente.

Por su parte, el Consorci AOC pone a disposición de la ciudadanía un portal (<https://www.idcat.cat/>) desde donde se pueden pedir y descargar los certificados idCAT, así como gestionar el resto de las operaciones de su ciclo de vida.

Actualmente el Consorci AOC está desarrollando el sistema que permitirá emitir los certificados idCAT mediante un proceso de videoidentificación, cumpliendo con los requisitos

establecidos al efecto en la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos calificados.

5.2 Los servicios de identificación y firma electrónica

5.2.1 Bus de integración de mecanismos de identificación y firma electrónica (Servicio VALid)

Para facilitar al conjunto de las Administraciones Públicas Catalanas la integración de los sistemas de identificación y firma electrónica, el Consorci AOC pone a su disposición el servicio VALID como bus de integración de este tipo de mecanismos. Como servicio de identificación electrónica, VALID implementa es una implementación del protocolo o Auth 2.0 que incluye un servicio de consulta de los datos de la persona identificada. Actualmente los mecanismos de identificación electrónica que el servicio admite son:

- idCAT Móvil como mecanismo de autenticación basado en el envío de contraseñas desechables al teléfono móvil de las personas usuarias.
- Autenticación con certificados calificados
- Las credenciales admitidas por la plataforma CI@ve, incluyendo el acceso a los mecanismos de identificación notificados por los diferentes Estados miembros de la Unión Europea de acuerdo con lo especificado en el Capítulo II del ReldAS

5.2.2 Firmador

Por otra parte, el Consorci AOC ofrece un servicio para facilitar al conjunto de las aplicaciones web de las Administraciones Públicas Catalanas la funcionalidad de firma electrónica con certificados personales en local llamado Signador. Las aplicaciones que integran este servicio pueden redirigir la firma de documentos al servicio, que permitirá a los usuarios firmar con los certificados que gestionen en su máquina en local, ya sea utilizando el almacén de claves del navegador o el sistema operativo. La operación concreta de firma actualmente se puede llevar a cabo o bien utilizando una aplicación nativa instalable en el ordenador de las personas usuarias, o bien ejecutando un archivo de Java Web Start (jnlp).

5.2.3 Mecanismos de autenticación para trabajadores públicos

Por último, las aplicaciones de cada administración pública, como por ejemplo los gestores de expedientes y portafirmas, autentican la identidad de sus trabajadores públicos empleando sus propios sistemas. Por ejemplo, los trabajadores de la Generalitat de Catalunya autentican su identidad para acceder a las diferentes aplicaciones de negocio a través de una plataforma llamada GICAR.

Desde el Consorci AOC se dispone de un servicio de federación de estos mecanismos de autenticación, con el objetivo de poder dar un acceso unificado a servicios comunes a todas las administraciones.

5.3 El servicio Firmador Centralizado

Actualmente, el Consorci AOC ofrece al conjunto de Administraciones Públicas Catalanas un servicio, llamado Firmador Centralizado, como plataforma tecnológica de firma electrónica desatendida que da cobertura a la firma electrónica de documentos. Como servicio permite custodiar y utilizar sellos electrónicos en el ejercicio de la actuación administrativa automatizada.



Figura 1. Custodia de certificados de sello electrónicos

Cuando uno nos pide un sello electrónico de nivel medio en el Consorci AOC a través de una entidad suscriptora puede decidir que éste sea custodiado en exclusividad por el Consorci AOC y en aplicaciones (para uso propio y para herramientas de la AOC), tanto servicios que ofrece el propio Consorci AOC como externos, a su uso.

El servicio comprende las siguientes funcionalidades:

- Custodia de certificados de sello electrónico de nivel medio (o sustancial), emitidos por el Consorci AOC
- Soporte de los formatos de firma avanzada XML (XAdES), ASN.1 (CADES) y sobre PDF (PAdES).
- Creación de firmas electrónicas en formato avanzado a partir de las claves asociadas a los certificados electrónicos custodiados.
- Registro de todas las acciones realizadas en la plataforma por los usuarios de la misma para dejar constancia y traza de las mismas a efectos de auditoría ya instancia o requerimiento judicial.

6 DESCRIPCIÓN DE LOS SERVICIOS OBJETO DEL CONTRATO

6.1 Obligaciones esenciales del contrato

- [R1] El adjudicatario deberá proporcionar al Consorci AOC una infraestructura para hospedar las claves privadas de certificados de trabajador público, empleado público, ciudadanía y sello electrónico en remoto.
- [R2] Operar las Entidades de Certificación SubCA SECTOR PÚBLICO R Q (G3) A.3. y SubCA CIUDADANÍA R Q (G3) A.4 del Consorci AOC para emitir los certificados de firma electrónica de empleado público, sellos electrónicos y ciudadanía en remoto.
- [R3] Ofrecer al Consorci AOC y al conjunto de las administraciones Públicas Catalanas un servicio de firma electrónica remota que se pueda utilizar con certificados calificados de firma electrónica y sello electrónicos, y que sea integrable con las aplicaciones de las Administraciones Públicas Catalanas
- [R4] El adjudicatario queda obligado a la adecuación y plena conformidad de sus servicios al ReIDAS, ya las normas técnicas que, aprobadas para su aplicación, ya descritas en el [marco normativo](#) de este pliego. En este sentido, el contratista deberá obtener en su costa y en el menor espacio de tiempo posible, la evaluación periódica de la conformidad y cumplir con el resto de obligaciones correspondientes a su condición de prestador de servicios de confianza cualificado, así como asumir cualquier cambio que en cada momento exija el supervisor nacional o que se 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.
- [R5] Las claves de los certificados personales de firma y de sello electrónico calificados serán custodiadas y utilizadas en dispositivos certificados Common Criteria EAL 4+ con los perfiles de protección definidos por las normas CEN EN 419 241-2 y CEN EN 419 221-5 o similares y habrán de aparecer en la lista de dispositivos calificados de creación de firma y sello electrónicos que publica la Comisión Europea de acuerdo con los puntos 32 y 23 del artículo 3 del ReIDAS.
- [R6] La empresa adjudicataria deberá garantizar que los servicios de confianza digital cumplen con lo que indica la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, el 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, y sus normas técnicas y de seguridad de desarrollo, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, especialmente en lo que se refiere a la admisión e interoperabilidad de los certificados y los sistemas de firma o sello en el ámbito de las administraciones públicas. Asimismo, deberá cumplir con la Declaración de Prácticas de Certificación de la Entidad de Certificación del Consorci AOC y las Políticas de certificación correspondientes. Esta normativa es la aplicada en el momento de la redacción del pliego, pero puede verse modificada durante la ejecución.
- [R7] Facturar electrónicamente los importes de los certificados digitales en un plazo de 10 días laborales a contar desde el mes siguiente al de la emisión, de acuerdo con los requerimientos del Consorci AOC.
- [R8] Someterse y superar las auditorías periódicas establecidas en el ReIDAS y en la Ley 6/2020, de 11 de noviembre o en la normativa aplicada en cada momento.
- [R9] Emitir, entregar, administrar, revocar y renovar certificados cuando lo solicite la entidad de registro, en los casos excepcionales y por los motivos descritos en la a las respectivas Políticas de Certificación.

- [R10] Notificar al ente suscriptor en el caso de certificados de empleados públicos, o al titular del certificado, por el caso de los certificados de ciudadanos, como mínimo con 2 meses de antelación a la fecha de expiración del certificado, la posibilidad de renovarlos, así como revocación de los certificados cuando se produzcan.
- [R11] Comunicar a los terceros que lo soliciten el estado de los certificados, de acuerdo con lo que se establece en la Declaración de Prácticas de Certificación de la Entidad de Certificación del Consorci AOC para los diferentes servicios de verificación de certificado.
- [R12] Ofrecer un tercer nivel de soporte a los usuarios.
- [R13] Elaborar el material comunicativo y divulgativo necesario para la formación al personal de las Entidades de Registro que deba ejecutar las tareas, de acuerdo con los estándares del Consorci AOC. Este material divulgativo y formativo siempre deberá estar actualizado.
- [R14] Garantizar que las claves privadas de las Entidades de Certificación gestionadas por el adjudicatario no han sido comprometidas.
- [R15] Aplicar con una diligencia razonable para Disponer de mecanismos para garantizar que cada sistema de autenticación y firma suministrado en ejecución del servicio objeto de esta licitación cumpla con los requisitos de calidad y seguridad y la normativa de protección de datos.
- [R16] En cuanto a los usos de identificación y firma, los servicios objeto de este contrato se tendrán que integrar como proveedor de identidad y firma con el servicio VALid del Consorci AOC, en los términos que se describen en las Condiciones específicas del servicio. Para la funcionalidad de VALid de la generación de firmas, los servicios objeto del contrato se tendrán que ofrecer a través del elemento Firmador (<https://signador.aoc.cat/signador/init>). VALid y Firmador están ampliamente integrados con procesos de identificación y firma que ofrece el sector público de Catalunya y es estratégico poder ofrecer los servicios objeto de este contrato a través de los mismos.

6.2 Obligaciones relativas al proceso de registro

- [R17] El adjudicatario deberá registrar los datos de los entes y usuarios con el objetivo de gestionar las credenciales de acceso, de acuerdo con la normativa técnica y legislativa aplicable para poder ofrecer el servicio con el nivel de seguridad necesario.
- [R18] El adjudicatario será responsable de publicar y mantener un procedimiento y un mecanismo para el alta en el servicio donde figuren todos los participantes del servicio del ente solicitante con su rol y toda la documentación que sea necesaria para mantener el alta en el servicio. Para la primera alta, por ejemplo, podrá ser un formulario de alta en formato PDF que permita la inclusión como evidencia de la firma del solicitante del servicio. Los datos habrá que mantenerlos permanentemente actualizados. La documentación de las altas se mantendrá en un espacio seguro compartido con el Consorci AOC.
- [R19] En relación a los mecanismos de autorización de acceso, el adjudicatario podrá proponer varios en función del nivel de seguridad de la instancia a la que se accede (servicio calificado o no calificado) pero en ningún caso sin comprometer la seguridad del servicio. Para el acceso al entorno calificado se solicita que, como mínimo, la solución soporte mecanismos de autorización de acceso de servicios web estándar y con soporte a certificados (p.ej. JWT y API Key). Modalidades como la filtrada por IP origen y contraseña, aunque no permiten identificar unívocamente a una aplicación, deben permitirse en la fase inicial y por el servicio no cualificado. El adjudicatario tendrá que garantizar el cumplimiento de las normas técnicas de gestión de los secretos y, en particular, cumplimiento políticas de seguridad de AOC en relación a la gestión de éstos.
- [R20] Esta interfaz de acceso a los servicios deberá disponer de servicios para garantizar la continuidad del servicio y evitar ataques de denegación de servicio como se

- establece en el punto “6.8.6 La gestión de la seguridad y el cumplimiento normativo” y “6.8.7 La gestión de la continuidad y la disponibilidad” de este mismo documento. Adicionalmente, también deberá mantener el conteo y anotación del consumo de cada cliente para poder mantener un control y eventualmente, establecer cuotas de consumo o denegar el acceso al servicio por mal uso del mismo.
- [R21] Ofrecer y mantener una aplicación web desde la que las personas operadoras de las entidades suscriptoras TCAT puedan llevar a cabo las tareas relativas al ciclo de vida (emisión, y revocación) de los certificados en remoto de la SubCA SECTOR PÚBLICO R Q (G3) A. 3 , tanto empleado o trabajador público, como sellos electrónicos.
- [R22] Ofrecer APIs que permitan integrar la función de solicitud de certificados de todos los perfiles objeto de esta licitación.
- [R23] Emitir, entregar, administrar, revocar y renovar certificados en los casos y por los motivos descritos en la Declaración de Prácticas de Certificación de la Entidad de Certificación del Consorci AOC y la correspondiente Política de Certificación.
- [R24] Emitir un certificado para cada operador nombrado por el ente usuario después de la aprobación de la solicitud del certificado correspondiente, siempre que tenga la formación realizada y superada satisfactoriamente. Este certificado tiene una validez de un máximo de cuatro años.

6.3 Catálogo de servicios objeto del contrato

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

6.3.1 Servicios a tanto alzado

A lo largo de la fase inicial de transición de la operación del servicio, que se llevará a cabo durante el primero de ejecución del contrato (finaliza a finales de 2024), se incluyen todos los gastos generales necesarios para garantizar la puesta en marcha y buen funcionamiento del servicio.

Concretamente:

- La financiación de los gastos en hardware y software durante la fase de transición, prestación y devolución del servicio. Entre otros:
 - La provisión de dispositivos criptográficos HSM dedicados a la generación, custodia y uso de las claves de firma por los entornos de producción y contingencia, tal y como se especifica en el presente documento.
 - También las tarjetas de operación remota que sean necesarias para el cambio de titularidad de claves al adjudicatario.
 - La provisión de las herramientas de observación en tiempo real de los Acuerdos de Nivel de Servicio, detallados en el presente documento.
- Durante toda la vigencia del contrato, el mantenimiento y evolución de la solución de firma y sello electrónico remotos, interfaces y gestión de credenciales de acceso al servicio.
- Los gastos de funcionamiento ordinario, de gestión operativa y explotación del servicio, incluyendo específicamente la adecuación al marco normativo y técnico vigente en cada momento.
- El servicio de soporte de tercer nivel, de acuerdo con los acuerdos de nivel de servicio del Consorci AOC

- Adecuación de la documentación del servicio al marco normativo vigente en cada momento, así como las traducciones necesarias. La documentación del servicio incluye: manuales, material de soporte, procedimientos, etc.
- Las auditorías y otras evaluaciones periódicas a que deba someterse, en el ámbito de aplicación de este pliego.
- Los servicios “Servicios organizativos y de cumplimiento” descritos en el presente documento y que incluyen la emisión y control de las facturas enviadas a los organismos finales, de acuerdo con las directrices del Consorci AOC y el servicio de formación a operadores de registro.

Los siguientes servicios no son objeto de este contrato:

- El servicio de soporte de primer nivel.

6.3.2 Servicios a precio unitario y mantenimiento de aplicaciones informáticas

Una vez iniciada la fase de prestación del servicio, se considerará un coste unitario por su consumo bajo demanda, asociado a las modalidades indicadas a continuación.

Por los evolutivos que se requieran durante la ejecución del contrato, los servicios de programación tendrán un coste asociado.

Bajo estas categorías se incluye el siguiente catálogo de servicios con los precios y volumetrías previstas por año que se indican en el Pliego de Cláusulas Administrativas:

Concepto	Breve descripción
Emisión de certificado remoto para la ciudadanía	Emisión de certificado calificado en repositorio remoto no calificado para la ciudadanía
Emisión de certificado remoto Calificado por firma calificada por el sector público	Emisión de certificado personal cualificado con vigencia de 5 años en repositorio remoto calificado por el sector público.
Emisión de certificado personal remoto por el sector público	Emisión de certificado personal cualificado con vigencia de 5 años en repositorio remoto no calificado por el sector público.
Emisión de Sello Remoto por el sector público	Emisión de certificado de sello calificado con vigencia de 3 años en repositorio remoto no calificado por el sector público.
Servicios de programación	Precio/hora programador

6.3.3 Gestión de las claves de entidad final y jerarquía

[R25] Las claves de los certificados de entidad final del servicio de firma remota se generarán, utilizarán y custodiarán en dispositivos criptográficos (HSM) de acuerdo con la normativa aplicable y condiciones definidas en el presente pliego de

prescripciones técnicas. Los HSMs para alojar las llaves del SSR tendrán que ser provistos por el adjudicatario y dedicados al servicio del Consorci AOC. En el punto “6.4 El Servicio de Firma Remota (SSR) del Consorci AOC” se definen las condiciones en relación con los ámbitos, niveles de confianza, etc., requeridos para la prestación del servicio.

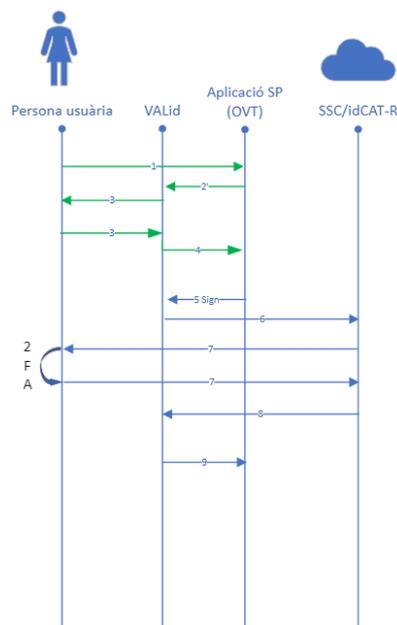
- [R26] Las claves de la jerarquía emisora de los certificados de entidad final se entregarán al adjudicatario durante la fase de transición. Se transferirán al adjudicatario mediante la entrega de los archivos de claves y los archivos del security world asociado. Se ampliará el conjunto de tarjetas de Operación de los dispositivos criptográficos y se entregarán al adjudicatario las tarjetas adicionales. El adjudicatario podrá proponer otras opciones de traspaso de la operación mientras ésta siga siendo segura y conforme al marco normativo. El adjudicatario las operará teniendo en las condiciones indicadas en el presente documento, y también se encargará de reconocer estas subCAs frente a terceras partes.

6.4 El Servicio de Firma Remota (SSR) del Consorci AOC

6.4.1 Servicio de firma electrónica en remoto para la ciudadanía

- [R27] Integrado con VALid como mecanismo de autenticación de la identidad de las personas usuarias.

Un ejemplo de funcionamiento del proceso de firma remota para la ciudadanía sería el mostrado por el siguiente esquema, donde “Aplicación SP” sería una carpeta ciudadana de un Ayuntamiento, por ejemplo:



- [R28] El adjudicatario ofrecerá una API para producir firmas electrónicas con los certificados generados que el Consorci AOC integrará con el servicio Firmador para ofrecer la funcionalidad de firma electrónica con certificado calificado.

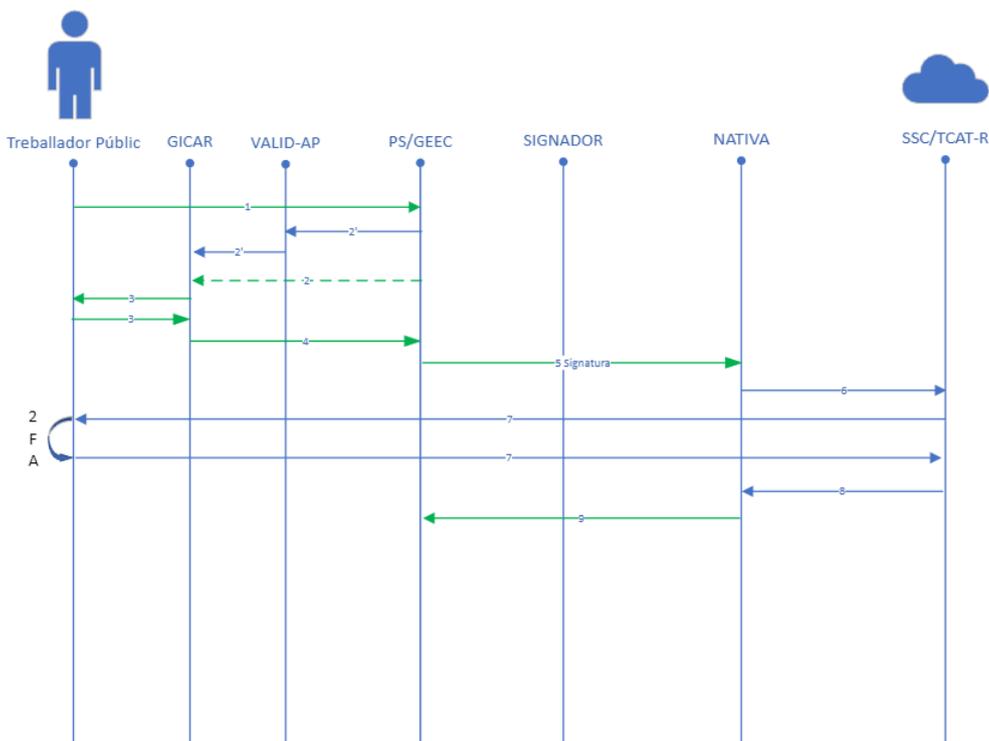
El proceso de registro y emisión de los certificados de firma electrónica en remoto para la ciudadanía será el mismo que se utiliza actualmente para la emisión de los certificados idCAT

en software. La emisión de los certificados se gestionará mediante las APIs que el adjudicatario proporcionará al efecto.

6.4.2 Servicio de firma electrónica en remoto para los empleados y trabajadores del sector público

- [R29] Por lo que respecta a los usos de identificación y firma, los servicios objeto de este contrato se tendrán que integrar, como proveedor de identidad y firma de las Administraciones Públicas Catalanas, a través de un servicio común ofrecido por el Consorci.
- [R30] En cuanto a las funcionalidades de generación de firma electrónica, los servicios objeto del contrato se tendrán que ofrecer a través del elemento Firmador (<https://signador.aoc.cat/signador/init>).

Ejemplo de funcionamiento, donde GICAR es un ejemplo de mecanismo de identificación de una administración, y “PS/GEEC” es una aplicación ejemplo que requiere que los usuarios firmen:



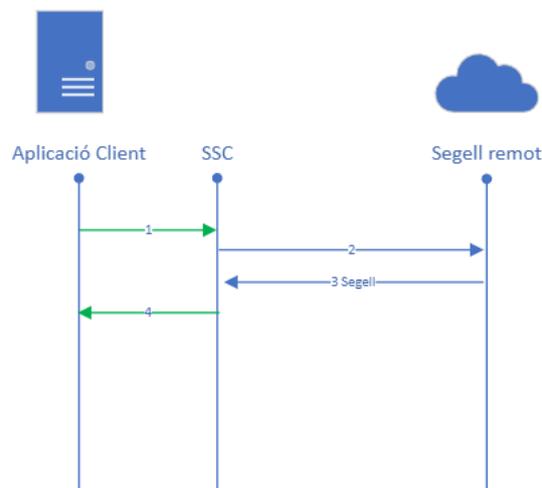
6.4.3 Servicio de firma electrónica en remoto con certificados de sello electrónico calificado por el sector público

- [R31] Ofrecer el servicio de custodia de certificados calificados de sello electrónico.
- [R32] Custodiar los certificados de sello electrónico que actualmente están hospedados en el servicio Firmador Centralizado del Consorci AOC descrito en el punto 4.3 de este documento.

- [R33] Ofrecer una API para integrar las funciones de sellado electrónico en los formatos calificados XAdES, CAdES y PAdES. Habrá que proporcionar un descriptor en WSDL para facilitar la integración de las aplicaciones que serán usuarias.
- [R34] El adjudicatario deberá prestar estas funcionalidades ajustándose al Acuerdo de Nivel de Servicio descrito en este pliego.
- [R35] Actualmente los sistemas y dispositivos de firma y sello electrónicos que el Consorci AOC ofrece trabajan con algoritmos de firma RSA y de resumen criptográfico SHA1, SHA256 y SHA512. En todo caso, el servicio de firma electrónica en remoto deberá trabajar con los algoritmos recomendados en la última versión de la especificación ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

Si es necesario cambiar la mensajería entera por algún motivo evolutivo, de seguridad, etc., será necesario planificarlo a lo largo del contrato. Si éste es el caso, el Consorci AOC definirá una mensajería propia, alineada con los estándares vigentes, para evitar cambios en futuros cambios de aplicaciones de firma.

Ejemplo de funcionamiento, donde “SSC” es el bus de integración de mecanismos de identificación que la AOC ofrece a las administraciones públicas catalanas, y que será el encargado de llamar, vía API, a las funciones de sellado electrónico que proporcionará el adjudicatario:



6.5 Aplicación PKI

- [R36] La aplicación de gestión de la infraestructura de clave pública (PKI) que el adjudicatario aporte para alojar y hacer uso de las claves de jerarquía, es necesario que esté certificada Common Criteria EAL 4+i esté configurada para aproximarse tanto como sea posible en la política de seguridad CIMC (Certificate Issuing and Management Components Protection Profile).
- [R37] La solución de infraestructura de clave pública (PKI) aportada por el adjudicatario deberá ser mantenida en términos de apoyo y actualizaciones de seguridad a lo largo de toda la vigencia del contrato. Adicionalmente, deberá permitir la devolución

del servicio a la finalización del contrato y no impedir que un futuro se requiriera transferir el servicio a un nuevo adjudicatario.

- [R38] 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 del software de la PKI empleado para la operación de las ECs que forman parte de la jerarquía de certificación del Consorci AOC.
- [R39] 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 requeridos en el apartado de ANS y según se definen a continuación.

6.5.1 Emisión de Listas de Revocación de Certificados (CRL)

- [R40] Para cada Entidad de Certificación (en adelante EC), el adjudicatario generará y alojará las correspondientes listas de revocación de certificados, de acuerdo con las condiciones (de periodicidad, vigencia, etc.) establecidas en la Declaración de Prácticas de Certificación, publicada en: <http://epsdc.aoc.cat/regulacio>. El Consorci AOC definirá con el adjudicatario un nombre DNS del dominio aoc.cat para el acceso al servicio.

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

- [R41] Para cada EC, el adjudicatario gestionará un servicio de respuestas OCSP. Este servicio NO podrá responder al estado desconocido (UNKNOWN) por los certificados que no haya emitido. El Consorci AOC definirá con el adjudicatario, un nombre DNS del dominio aoc.cat para el acceso al servicio.
- [R42] Transferencia de las claves de jerarquía: las claves privadas de las Entidades de Certificación objeto de esta licitación se generaron en 2022 en una sesión auditada y se han incluido en el alcance de auditoría EIDAS y, por tanto, en la Declaración de Prácticas de Certificación del Consorci AOC. Estas claves se generaron con tecnología Entrust de dispositivos HSMs modelo nCipher y se protegieron con unas tarjetas de operación (OCS) en una configuración 2/5 y con todas las tarjetas en propiedad exclusiva del Consorci AOC.
- [R43] Durante la fase de transición, el Consorci AOC ofrece la posibilidad de transferir al adjudicatario la custodia de estas claves mediante el procedimiento previsto por el fabricante de los dispositivos criptográficos donde se generaron las claves. Es decir, mediante la recuperación del Security World de AOC en los dispositivos criptográficos HSMs que provea y cambiando el conjunto OCS por un nuevo conjunto con titularidad de operadores que el adjudicatario defina.
- [R44] El adjudicatario podrá utilizar otros fabricantes de HSMs u otros mecanismos de transferencia siempre que no comprometan la seguridad de las claves ni las operaciones asociadas durante el proceso de la migración y usos posteriores.

6.6 Modelo de registro de servicios del Consorci AOC

- [R45] Por el cumplimiento de los puntos relativos al registro de datos de entes y roles del sistema, en las condiciones indicadas en el apartado “Obligaciones relativas al proceso de registro”, el adjudicatario deberá configurar los sistemas objeto del contrato con los roles del sistema del Servicio de Certificación Digital que opera el Consorci AOC.
- [R46] El Consorci AOC entregará al adjudicatario la información de entes y roles en vigor y que el adjudicatario tendrá que aplicar como configuración inicial del nuevo servicio que operará. Adicionalmente, las credenciales de operadores que se configurarán inicialmente en el sistema serán, por tanto, también las mismas que existen en la fase de transición. A partir de la primera sincronización, por cada cambio en los datos de los entes u operadores, el adjudicatario configurará las mismas en el sistema según los ANS existentes y relacionados a esta tarea.
- [R47] Los operadores de todo el sistema de registro actualmente operan con certificados no calificados EIDAS pero generados en tarjeta criptográfica. De esta forma se garantiza el acceso multifactor al sistema de registro. La provisión de estas tarjetas quedará fuera del alcance de este contrato.
- [R48] El cumplimiento de la gestión de las altas en relación con la auditoría externa EIDAS, recaerá en el sistema del adjudicatario, ya que es en este sistema donde se configuran los accesos a los servicios ofrecidos y los elementos aquí descritos sólo conforman el canal de entrada de las mismas hasta el adjudicatario.
- [R49] Por el cumplimiento de las obligaciones relativas al procedimiento administrativo de cualquiera de las solicitudes de datos del sistema o de emisión de certificados, el adjudicatario deberá registrar de entrada las peticiones a través del servicio de Registro Unificado (MUX) del Consorci AOC.
- [R50] Para el cumplimiento de las obligaciones relativas a la custodia electrónica segura de cualquiera de las solicitudes de datos del sistema o de emisión de certificados, el adjudicatario deberá integrar sus procesos con el servicio de custodia DESA'L del Consorci AOC.
- [R51] El adjudicatario tendrá que ofrecer y una aplicación para llevar a cabo la generación de las evidencias derivadas del ciclo de vida de los certificados objeto de este contrato, de acuerdo con los procedimientos y manuales del Consorci AOC. A modo de ejemplo, será necesario resolver la firma de múltiples operadores en la aprobación y generación de un certificado de empleado público. . El formato de evidencia generada debe permitir garantizar su retención, validación y consulta durante quince años desde la fecha de caducidad del certificado, o según el plazo normativo aplicable en cada momento durante la vigencia del contrato.
- [R52] El adjudicatario deberá ofrecer a través de una interfaz automática de software (API) el acceso a todos los datos y procesos de la entidad de registro. En concreto, debe permitir el acceso a los datos de usuarios, entes, roles, productos y también a los procesos de registro. El objetivo es garantizar el desacoplamiento de los componentes internos de las interfaces de usuario. También para facilitar la integración en otros sistemas que pueda desarrollar el Consorci AOC y que requieran datos del registro de certificados.

6.6.1 Registro ámbito del empleado público y sellos electrónicos

El Servicio de Certificación Digital T-CAT se compone de tres elementos principales:

- Conector AOC: canal de entrada para el alta de servicios y para la tramitación de solicitudes y modificación de datos de entes y roles en el servicio de forma digital, segura y con mecanismos para realizar el seguimiento del trámite.

- Solución web para la gestión de peticiones, emisión y ciclo de vida: para las operaciones de registro de datos de suscriptores, emisión de certificados, documentación y gestión del ciclo de vida del certificado digital por medios web y también mediante conectores automáticos.
- Solución web para gestionar entrega y códigos de activación: para hacer la entrega de los certificados de forma segura y enviando los códigos de activación por correo electrónico

El funcionamiento actual está expuesto con detalle en el anexo de este documento.

- [R53] El adjudicatario deberá gestionar las solicitudes de certificados recibidas por el Consorci AOC, a través de los diversos canales que éste ofrezca a sus entes usuarios.
- [R54] El adjudicatario deberá proveer una solución web que permita a los operadores gestionar las peticiones de los certificados, así como su ciclo de vida, una vez emitidos (revocación, consulta), de acuerdo con los procedimientos y experiencia de usuario del Consorci AOC.
- [R55] Esta solución web de gestión debe permitir la carga individual o masiva de peticiones de certificados, desde la propia web o vía “conector AOC”. Deberá disponer de opciones para recuperar datos del histórico de certificados.
- [R56] Disponer de un módulo de gestión de estados de los certificados (ciclo de vida). Este módulo debe poder ser utilizado vía web o bien conector automático. En este punto es importante destacar que la gestión de los certificados debe poder realizarse por parte de un operador y por parte del titular del certificado. En cuanto a la solución web para gestionar entregas y códigos de activación, el adjudicatario deberá proveer una solución web que permita a los responsables de los entes usuarios entregar los certificados a los titulares, así como la generación de los códigos de activación correspondientes, tantas veces como sea necesario, de acuerdo a los procedimientos y experiencia de usuario del Consorci AOC,
- [R57] En los componentes que interaccionan directamente con el usuario final, es necesario que éstos permitan la aceptación digital y generación de evidencia correspondiente por parte del usuario. Por ejemplo, la aceptación de las condiciones en la emisión del certificado en el momento de la entrega.
- [R58] Esta misma solución debe disponer de conectores de consulta de estado de certificados. En concreto, las consultas, a modo de informe, pueden ser sobre un certificado en particular o múltiples (p.e.: los asociados a una Entidad de Registro,) y pueden consumirse de forma síncrona o asíncrona (p.e. informes diarios).

6.6.1.1 ER vinculadas

- [R59] De acuerdo con lo expuesto hasta ahora, las ER vinculadas no deben tener necesidad de disponer de ningún hardware específico para hacer su función dentro del Servicio de Certificación Digital, a través de la solución web de gestión de entregas y códigos de activación.

6.6.1.2 L&ER centralizada del Consorci AOC

- [R60] El adjudicatario creará una ER en sus oficinas desde donde podrá ofrecer los servicios de acuerdo con las características de prestamista público que tiene el Consorci AOC. El Consorci AOC opera una ER que es la que centraliza las peticiones de certificados digitales de todos los entes que no están vinculados a otra ER o que, puntualmente, piden emisiones de envíos concretos de certificados, revocaciones de oficio, y la gestión de los operadores y roles en el sistema.

6.6.2 Registro ámbito ciudadanía

- [R61] El adjudicatario dispondrá de un sistema para emitir los certificados digitales en remoto para la ciudadanía, a partir del registro realizado mediante el sistema de videoidentificación provisto por el Consorci AOC.
- [R62] La solución se ocupará de gestionar el envío de las comunicaciones electrónicas necesarias al titular para la obtención del certificado, así como de ofrecerle el mecanismo que le permita firmar la evidencia correspondiente a la recepción del certificado.
- [R63] La responsabilidad del alojamiento y custodia de las evidencias de registro del proceso de obtención de los certificados recaerá en el adjudicatario de este contrato mientras no las deposite en los sistemas del Consorci AOC por custodia según el período normativo de retención.

6.7 Infraestructura tecnológica

6.7.1 Entornos

Para cumplir con los requisitos normativos, garantizando la disponibilidad y continuidad de los servicios prestados, el adjudicatario deberá desplegar la infraestructura en los siguientes entornos:

6.7.1.1 Producción

- [R64] 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.
- [R65] Los elementos de seguridad perimétricos deben garantizar el acceso controlado a los usuarios del sistema.

6.7.1.2 Contingencia

- [R66] 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.

6.7.1.3 Preproducción

- [R67] Despliegue de un entorno estable completo, destinado a las pruebas funcionales ya la realización de pruebas de rendimiento. Toda su actividad no tendrá impacto en el conjunto de datos reales ni afectará al rendimiento de los demás entornos.

6.7.1.4 Desarrollo

- [R68] 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.
- [R69] 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.

6.7.2 Centros de Procesamiento de Datos

- [R70] Dado que los custodios de las tarjetas de administración (ACS) de los dispositivos criptográficos (HSMs) en los que se alojarán las claves de las ECs del Consorci AOC serán personal vinculado al mismo Consorci AOC y, con el objetivo de minimizar los desplazamientos que estos tengan que realizar cada vez que sea necesario realizar una intervención sobre estos dispositivos, se requiere que el CPD principal (CPD-1) esté ubicado en el área metropolitana de Barcelona.
- [R71] La infraestructura técnica dentro del CPD principal 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 imponen las normas técnicas aplicables a los prestadores de servicios de confianza que emiten certificados calificados y ofrecen servicios de firma remota, ya especificadas en este pliego.
- [R72] En el CPD de contingencia (CPD-2), con requisitos de seguridad equivalentes a los del CPD principal, el adjudicatario deberá alojar los sistemas necesarios para garantizar la continuidad de todos los servicios objeto de este contrato en el entorno de Producción. Para los ANS de activación del Plan de Recuperación de Desastres (PRD), se requiere que este CPD esté también en la provincia de Barcelona ya una distancia de seguridad mínima de 15 kms del CPD principal (CPD-1). El Consorci AOC aceptará que el requisito de distancia sea superior, siempre dentro del territorio español, si el adjudicatario propone el uso de mecanismos de administración y operación de los dispositivos remotas que sean seguras, siempre de acuerdo con lo que indique el propio fabricante de los dispositivos criptográficos.
- [R73] El resto de capas de servicios tecnológicos pueden estar alojadas en la nube (cloud), si el proveedor lo considera. En este caso, deberá garantizar el cumplimiento de las obligaciones establecidas por el marco normativo del presente pliego, especialmente a lo especificado 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 lo que se refiere al tratamiento de datos personales, así como el Acuerdo de Nivel de Servicio requerido.

6.7.3 Hardware y software dedicado

- [R74] Las claves criptográficas de los usuarios del servicio de firma remota y de las EC's del Consorci AOC se tendrán que generar y mantener dentro de dispositivos criptográficos (HSMs) de uso exclusivo para el Consorci AOC. Las aplicaciones de generación y gestión de certificados, así como de firma electrónica remota también deben ser para uso dedicado a los servicios del Consorci AOC. La configuración será en alta disponibilidad para el entorno de producción y, si la capacidad lo permite, también para el de contingencia.
- [R75] 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 los dispositivos criptográficos del servicio, junto con los eventuales servicios de migración de claves 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, realizar su puesta en funcionamiento a lo largo de la ejecución del presente contrato y sus prórrogas.
- [R76] 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.

6.8 Gobierno de la Seguridad

6.8.1 Gestión de trazas

- [R77] El adjudicatario deberá cumplir con la norma de gestión de trazas vigente, y deberá asegurar que almacena todas las trazas que le aplican, de acuerdo con la clasificación de información según el Esquema Nacional de Seguridad ya los requisitos establecidos en las normas ETSI objeto de auditoría.
- [R78] Las trazas tendrán que ser accesibles en modo lectura y se asegurará el marcado de las trazas con requerimientos específicos de conservación según la legislación aplicable.
- [R79] El adjudicatario, teniendo en cuenta el nivel de clasificación de seguridad de la aplicación expuesto en el apartado “Clasificación de la información”, 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.
- [R80] El adjudicatario deberá llevar a cabo el retorno al Consorci AOC de los datos y trazas generadas como mucho en periodicidad anual.

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

- [R81] El adjudicatario tendrá que garantizar que todas las aplicaciones web objeto del contrato (tanto internet como intranet) utilicen canales de comunicación seguros HTTPS/TLS.

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

El adjudicatario deberá:

- [R82] Garantizar que el diseño de la arquitectura de la solución permite alcanzar los requerimientos de disponibilidad/continuidad requeridos.
- [R83] 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.

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

- [R84] 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.

6.8.5 Seguridad en el cloud

- [R85] En caso de que alguno de los servicios o herramientas de apoyo a la prestación del mismo 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.

6.8.6 La gestión de la seguridad y el cumplimiento normativo

- [R86] 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 en el alcance del servicio y que habrá que tener operativos para la puesta en marcha del mismo.

6.8.6.1 Clasificación de los sistemas de información

- [R87] El adjudicatario deberá tener en cuenta el nivel de seguridad de los sistemas de información objeto del contrato, según el análisis de riesgos realizado por el Consorci AOC con acuerdo a lo especificado en el Esquema Nacional de Seguridad, para aplicar correctamente el marco normativo y legal indicado anteriormente.

6.8.6.2 Cumplimiento normativo y legal

- [R88] 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 (ENS), el Reglamento General de Protección de datos (RGPD) y el Reglamento Europeo de identificación y servicios de confianza (eIDAS).
- [R89] El adjudicatario deberá incorporarse al modelo de cumplimiento normativo del Consorci AOC. En este modelo se integran las posibles auditorías que el Consorci AOC determine 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 que el Consorci AOC determine realizar 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.
- [R90] El adjudicatario deberá garantizar el acceso del personal autorizado del Consorci AOC a la información de seguridad (procedimientos, registro de incidentes, trazas, etc.). Toda la información de seguridad deberá estar siempre disponible para ese 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 requeridos.

6.8.6.3 Requisitos de protección de datos

- [R91] 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 ya la libre circulación de estos datos ya la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. En este sentido, 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).

- [R92] 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

6.8.6.4 Auditoría externa

- [R93] El adjudicatario tendrá que disponer de la certificación de cumplimiento, a partir del inicio de la fase de transición y hasta la finalización del contrato, 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 la consecución de este requerimiento:

- Esquema Nacional de Seguridad (ENS):
 - o 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 de ENS:

Sistema Servei de Certificació Digital						
Denominació de l'actiu essencial	C	I	D	A	T	DP
Subsistema repositori de jerarquia de claus de l'entorn principal	A	A	A	M	M	
Subsistema repositori de jerarquia de claus de l'entorn de contingència	A	A	A	M	M	
Subsistema d'emissió i revocació de certificats de l'entorn principal	M	M	A	M	B	M
Subsistema d'emissió i revocació de certificats de l'entorn de contingència	M	M	A	M	B	M
Subsistema d'Informació pública	B	B	A	M	M	
Subsistema repositori de claus remotes de l'entorn principal (SSR-QSCD)	A	A	A	M	A	M
Subsistema repositori de jerarquia de claus de l'entorn de contingència (SSR-QSCD)	A	A	A	M	A	M
Subsistema de suport	B	M	M	B	B	B
Subsistema serveis AOC (EACAT, MUX, DESAL, VO, VALID i Signador)	B	B	A	M	M	M
Valor màxim registrat	A	A	A	M	A	M
La valoració del subsistema es Alta (C=A, I=A, D=A, A=M, T=A, DP=M)						

- o RTO y RPO según definido en el punto “7.2.4ANS de continuidad”.
 - o Los subsistemas marcados en color verde, 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 también a lo largo de la vigencia del contrato.
- Accesibilidad:
 - o Cumplimiento normativo normas accesibilidad aplicables.
 - Plan de Seguridad del Consorci AOC:
 - o Política de seguridad y normas derivadas (ver punto “¡Error! No se encuentra el origen de la referencia. ¡Error! No se encuentra el origen de la referencia.”).
 - Acreditación voluntaria del PSC:

- Auditoría interna del % de certificados emitidos por parte del propio adjudicatario.
 - A nivel de trazas: de solicitud, aprobación, emisión, entrega.
 - A nivel de producto con certlint o herramientas equivalentes
- Auditorías periódicas de las Entidades de Registro.

6.8.7 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 frente a cualquier situación adversa, evitando un impacto significativo en la organización, con el objetivo de garantizar el Acuerdo de Nivel de Servicio (en adelante ANS) especificado en este pliego y cumplir con los requisitos a nivel normativo.

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 frente a 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)

[R94] El adjudicatario deberá entregar al Consorci AOC su política de continuidad.

[R95] El adjudicatario deberá documentar, desarrollar e implantar las medidas de disponibilidad necesarias para cubrir los indicadores de nivel de servicio de disponibilidad especificados en este pliego. Esta documentación deberá entregarse en el Consorci AOC.

[R96] El adjudicatario deberá implantar medidas sobre los activos implicados que le permitan elaborar y entregar al Consorci AOC un Plan de Continuidad y de Recuperación ante Desastres del servicio (en adelante, PRD) para garantizar los niveles de servicio establecidos en este pliego y que se derivan del documento de análisis de impacto de negocio (en inglés, Business Impact Analysis o BIA) elaborado por el Consorci AOC en relación con este servicio y de la normativa aplicable.

[R97] El adjudicatario deberá mantener actualizado el PRD frente a cambios propios o por causas de terceros.

[R98] El adjudicatario deberá proveer soluciones tecnológicas que permitan alcanzar los objetivos fijados en el PRD, siendo estas certificadas mediante pruebas de recuperación periódicas.

[R99] 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.

[R100] 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.

6.8.8 Cese de la actividad

- [R101] En caso de cese de la actividad por parte del Consorci AOC, el adjudicatario colaborará con el Consorci con las tareas descritas por éste en su Plan de Cese de la actividad. Estas tareas incluyen:
- La notificación a las personas y organizaciones usuarias del servicio, así como a los órganos supervisores y otras entidades implicadas.
 - La transferencia de sus obligaciones a otro eventual prestador de servicios de confianza para mantener el servicio durante el período de tiempo definido en el Plan.
 - La destrucción de las claves privadas, tanto de las entidades intermedias como de las entidades y usuarias del servicio, gestionadas por el adjudicatario.
 - En caso de cese de la actividad, el Consorci AOC revocará las autorizaciones al adjudicatario por en su nombre a la hora de prestar los servicios objeto de este pliego.

6.8.9 Auditorías en las Entidades de Registro vinculadas

- [R102] Tal y como se indica en el punto “11.5 Servicios de auditoría de ER”, el Consorci AOC lleva a cabo auditorías de control procedimental del cumplimiento de las funciones y responsabilidades ejercidas por las ER que hagan uso de los procesos y aplicaciones provistas por el adjudicatario en el marco de este contrato. En su caso, el adjudicatario deberá aplicar las medidas derivadas del resultado de las auditorías en las ER en sus procesos y aplicaciones.

6.8.10 Auditorías del Prestador de Servicios de Certificación Consorci AOC

- [R103] Tal y como se establece en las obligaciones esenciales del contrato, el adjudicatario queda obligado a la adecuación y plena conformidad de los servicios en el ámbito del presente contrato ReIDAS, ya las normas técnicas que aprobadas para su aplicación.
- [R104] 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.
- [R105] 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 por el Consorci AOC, dado que estos conceptos están incluidos en los servicios que prestará el adjudicatario.
- [R106] El ámbito de la auditoría externa incluirá las subCAs y perfiles que emita y opere el adjudicatario en el ámbito del presente contrato y, en ningún caso, otras subCAs o perfiles del resto de jerarquía de Certificación del Consorci AOC.
- [R107] El ámbito de auditoría también incluirá la aplicación de firma remota utilizada por el adjudicatario, dado que es un dispositivo calificado de firma electrónica remota.

6.9 El servicio de soporte

6.9.1 El servicio de Apoyo del Consorci AOC

Actualmente el servicio de soporte del Consorci AOC 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. Sus ANS están publicados en la web del Consorci AOC
- **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 apoyo ni en la web del Consorci AOC.
- **3er nivel:** Aquellas incidencias que no puedan ser resueltas en el nivel 2 se derivan al tercer nivel. En el caso del servicio objeto de este contrato, se requiere en la empresa adjudicataria la resolución de incidencias escaladas a este nivel.

6.9.2 Ámbitos de atención y apoyo a prestar por el adjudicatario:

[R108] El adjudicatario deberá ofrecer el servicio de soporte de tercer nivel al Consorci AOC.

[R109] También deberá realizar 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 apoyo y mejoren la percepción del servicio por parte de los usuarios.

6.9.3 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 (que 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 apoyo, en los casos que de la AOC se les solicite intervención para solventar alguna incidencia.

6.9.4 Horario de atención

[R110] 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 Catalunya. De forma ocasional podría ampliarse este horario por alguna campaña especial.

6.10 Servicio de Mantenimiento Evolutivo

[R111] Al tratarse de un servicio alojado por el adjudicatario, el mismo incluirá, dentro del precio de adjudicación del contrato, y durante toda la vigencia del mismo, un servicio de mantenimiento evolutivo para adecuaciones del servicio.

En este apartado se describe tanto la metodología como la dedicación que se va a destinar este servicio, así como la tipología de cambios y adecuaciones a aplicar.

El alcance de este mantenimiento serán las aplicaciones citadas en los requisitos objeto de esta licitación. El código de estos componentes se alojará en el gestor de código GIT del Consorci AOC para su mantenimiento y evolución a lo largo de toda la vigencia del contrato. Se excluye el código fuente y propiedad intelectual del producto comercial ya desarrollado que se aportará para ofrecer el servicio y del que únicamente se guardarán en el gestor de código las configuraciones y personalizaciones. Toda la gestión de estos cambios e intercambios de documentos relacionados se realizará a través de la herramienta JIRA del Consorci AOC.

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

- Antes de llevar a cabo una labor de evolutivo, la empresa adjudicataria llevará a cabo un análisis del impacto que ésta puede tener en materia de protección de datos de carácter personal y llevar a cabo un AARR
- 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 tique 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. Por lo 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.

Los acuerdos de nivel de servicio aplicables a las solicitudes de servicio de mantenimiento evolutivo serán los definidos por el ANS descrito en este pliego.

6.10.1 Metodología

La propuesta metodológica debe prever, como mínimo:

6.10.1.1 Toma de requerimientos

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

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

- Requisitos funcionales: tienen que ver con las funcionalidades que se desea incorporar o modificar en la aplicación.
- Requisitos técnicos: tienen que ver con posibles mejoras no funcionales de cariz tecnológico; por ejemplo, puede que la actualización de una versión determinada de una librería de un tercero. Otro caso, puede que una consulta en base de datos debe hacerse sobre una tecnología determinada (como podría ser mysql).
- Requisitos de calendario: tienen que ver con plazos de entrega del evolutivo.
- Requisitos de contexto: tienen que ver con la importancia que pueda tener el evolutivo, el posible impacto sobre los clientes, la prioridad del evolutivo respecto al resto de solicitudes en curso y/o previamente planificadas, etc.
- Requisitos de Seguridad: incorporar todos los controles de seguridad que, por el tipo de información tratada, debe incorporar el evolutivo.
- Medidas de privacidad, desde el diseño y por defecto, a implantar, en su caso, y en función del análisis de riesgos llevado a cabo por los derechos y libertades de los titulares de los datos

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

Para facilitar este trabajo se llevará a cabo las siguientes acciones:

- Se hará llegar al adjudicatario un documento, le llamaremos ficha de inicio de evolutivo, con una descripción lo más detallada posible del 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 requisitos", donde se recojan todos los requerimientos para abordar el evolutivo, agrupados según la tipología descrita anteriormente.
- El Consorci AOC revisará este documento y se gestionarán los cambios pertinentes hasta su formalización.

6.10.1.2 Fase de pre-análisis

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

En base al "Documento de requisitos", el adjudicatario procederá a realizar un pre-análisis de los cambios que implicaría realizar en la aplicación para conseguir el evolutivo deseado.

Del resultado de este ejercicio se realizará otro documento, "Documento de pre-análisis", 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 por la prestación del servicio necesario para realizar el evolutivo.
- Calendario con la planificación estimada del proyecto. A pesar de estar en una fase de pre-análisis, el adjudicatario tendrá que hacer el esfuerzo de elaborar un calendario, lo más esmerado 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.

6.10.1.3 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 pre-análisis antes de iniciar esta fase.

El adjudicatario deberá realizar un análisis exhaustivo, de al menos, los siguientes ítems:

- Análisis funcional y técnico
- Definición de las Interfaces de usuario
- Definición de las medidas de seguridad y medidas de privacidad desde el diseño y por defecto a implantar cuando proceda
- Descripción de pruebas de validación: es necesario describir las pruebas que se llevarán a cabo para 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 del evolutivo tienen el comportamiento esperado. Es necesario describir todas las pruebas funcionales que garanticen haber testeado todas las funcionalidades del evolutivo. También es necesario 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 realizar el evolutivo siguen funcionando correctamente.

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

6.10.1.4 Fase de diseño

El objetivo de la fase de diseño es detallar el diseño técnico que se utilizará para 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".

6.10.1.5 Fase de construcción del sistema

Las tareas que comportará esta fase son:

- Generación del código de los distintos componentes (p.e. clases): esto es programar/tocar todo el código necesario. Es necesario que todo el código esté comentado con detalle, por medio del “javadoc”.
- 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 solicitará un manual de usuario.
- Definición de la formación (si es necesario)

Como resultado del ejercicio anterior el adjudicatario elaborará un documento, le 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 con los requisitos de seguridad previo el paso a producción. En estos casos el adjudicatario deberá proveer de un usuario de prueba por 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. El código deberá estar comentado con detalle, por medio del “javadoc”.
- Entrega del compilable.
- “Guía de implantación del cambio”: este documento contendrá el detalle de todas y cada una de las instrucciones técnicas a ejecutar para implantar el evolutivo en cuestión.

6.10.1.6 Fase de implantación y aceptación

En base a las entregas de la fase anterior se procederá a realizar la implantación del evolutivo sobre los distintos 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 lo.

Por ejemplo, será necesario 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 realizada la ejecución del plan de pruebas con el 100% de las pruebas funcionando en el entorno de pre-producción y producción se dará el proyecto por cerrado. A partir de ese instante entrará en vigor el período 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 39; operación, y procedimental para que los nuevos desarrollos puedan ser ya objeto del servicio de soporte 24x7.

6.10.2 Mantenimiento correctivo

El software desplegado requerirá servicios de evolución y personalización. Estos servicios se dedican al mantenimiento evolutivo periódico ya la resolución de incidencias derivadas del día a día. Incluyen tareas como:

- Diagnóstico de problemas e incidencias.
- Tercer nivel de resolución de incidencias.
- Mejoras menores de gestión.
- Apoyo a la prestación y seguimiento del servicio.
- Apoyo a integraciones de clientes.
- 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.

6.10.3 Mantenimiento técnico - legal

El servicio de mantenimiento técnico-legal incluirá la actualización de la documentación jurídica vinculada a los servicios objeto de esa licitación. 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 **Error! No se encuentra el origen de la referencia.** del presente pliego. 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 organismos 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 a 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).

6.10.4 Mantenimiento evolutivo

El servicio de mantenimiento evolutivo incluirá aquellas modificaciones solicitadas por el Consorci AOC, al margen de las contempladas anteriormente en los puntos anteriores.

6.10.5 Tareas en el ámbito del mantenimiento evolutivo

Las tareas que se realizarán en el alcance de este Servicio de Mantenimiento Evolutivo se determinan en función de la demanda de los usuarios de los servicios, de los responsables de los mismos o de las diferentes incidencias que tienen lugar a lo largo de la duración del contrato y que generan necesidades de mejora. Para estimar las tareas y dedicaciones previstas y el presupuesto base de licitación se ha tenido en cuenta el uso actual del servicio de certificación digital del Consorci AOC y las necesidades detectadas en el momento de redactar este pliego.

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, han de estar previstas en el importe a tanto alzado del contrato.

6.11 Servicios organizativos y de cumplimiento

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

- Servicios jurídicos:
 - o 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.
 - o Informes ad hoc relativos a la prestación ordinaria del servicio.
- Apoyo a la operativa de las Entidades de Registro
 - o Gestión de la red de las ER's
 - o Gestión de la configuración de permisos en el 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.
- Experto en protección de datos que garantice que, en todo el ciclo de vida de los datos y para todas las actividades de tratamiento, se han adoptado las medidas de privacidad desde el diseño y por defecto, las medidas de seguridad necesarias en atención a los riesgos que puedan derivarse por los derechos y libertades de los titulares de los datos, así como su evaluación continuada y que en base al principio de responsabilidad proactiva se cumple. Se deberá disponer de la documentación acreditativa del citado cumplimiento.

Los servicios de cariz organizativo que intervienen en la prestación del servicio son los siguientes:

Implementación de los perfiles según los tipos de perfiles requeridos y propósitos y necesidades con OIDs definidos por los CAOC y propondrá las modificaciones en las DPC y PC y perfiles que serán aprobadas y publicadas por AOC, si procede.

En concreto, la definición de todos los perfiles y el reconocimiento con el ministerio durante la primera auditoría del servicio durante la fase de transición.

- Servicios jurídicos:
 - o Redacción y mantenimiento de la Documentación Jurídica (Declaraciones de prácticas, condiciones específicas de prestación del servicio, etc.) de forma coordinada con la Responsable de Asesoramiento Jurídico de Servicios del CAOC.
 - o Informes ad hoc relativos a la prestación ordinaria del servicio.
- Generación de informes sobre los datos de actividad del servicio e integración con el sistema de Business Intelligence del Consorci AOC.
- Facturación

Realizar los análisis de riesgos y disponer de la documentación acreditativa de las medidas aplicadas, para preservar los derechos y libertades de los titulares de los datos objeto de tratamiento. El Consorci AOC es el propietario de toda la documentación elaborada por el adjudicatario en lo referente al servicio prestado, y será el responsable de su validación y aprobación.

- [R112] Por su parte, el adjudicatario deberá mantener la documentación actualizada en el sistema de gestión documental que el Consorci AOC proporcione a 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 disponible en el repositorio de información que el Consorci AOC haya designado a tal efecto.
- [R113] 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.

6.11.1 Servicios de formación

- [R114] 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 realizarán utilizando la plataforma virtual del Consorci AOC, gestionada por el propio Consorci AOC, con los requerimientos de la plataforma.

- [R115] 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.

Por lo que respecta 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 soporte a las Entidades de Registro.

6.11.2 Servicios de facturación

- [R116] 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 y los mecanismos de reporting, su propuesta de coordinación con el Consorci AOC para que éste pueda realizar el seguimiento y el resto de las actividades relativas a la gestión de la facturación; incluyendo la coordinación para la gestión de los abonos.
- [R117] 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.
- [R118] 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 adecuado tratamiento para la anonimización. Se debe permitir identificar el pedido y cada elemento del mismo 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)
- [R119] El adjudicatario deberá realizar 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.

7 Acuerdos de nivel de servicio

El funcionamiento de los servicios objeto de este contrato 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 del Consorci AOC (publicadas en <https://www.aoc.cat/condicions-prestacio-serveis-aoc/>). Y los propios del servicio de certificación digital, también publicado en la web de la AOC

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

- ANS de Explotación del Servicio:
 - Indicadores de cumplimiento de los niveles de servicio recogidos en las Declaraciones de Prácticas de Certificación¹ que aplican a cada Entidad de Certificación en los siguientes ámbitos:
 - Publicación de información y directorio de certificados de las EC'
 - 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).
 - Alta de usuarios en el servicio en menos de 7 días
 - Disponibilidad del 99,9% del repositorio de publicación de información y directorio de certificados.
 - Acuerdos de nivel de servicios relativos a los procedimientos de identificación y autenticación previos a la realización de la firma remota.
 - ANS de emisión y gestión de los certificados:
 - Plazos de entrega en el servicio de emisión y renovación de certificados T-CAT por el sector público por ambos niveles (ordinario y urgente y casos especiales por elecciones u otras necesidades).
 - Plazos de emisión en el servicio de emisión y renovación de certificados idCAT por la ciudadanía.
 - Los plazos para los certificados con documentación adicional o no deben ser los mismos, de acuerdo con los publicados por parte del Consorci AOC
 - Plazos de modificación de las fichas de ente suscriptor, Entidad de Registro, alta de operadores, etc.
 - Observado con herramientas de observación o a partir de trazas del sistema de emisión.
 - ANS de disponibilidad:
 - Disponibilidad continua 24x7 de los servicios web
 - Nivel de disponibilidad superior al 99%.
 - Observado con splunk o herramienta equivalente.
 - ANS de capacidad:
 - En transacciones por segundo (tps) por los servicios web de firma remota, 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.

¹Las Declaraciones de Prácticas de Certificación de las ECs del Consorci AOC se encuentran publicadas en: <https://epsd.aoc.cat/regulacio>

- 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.
- ANS de Continuidad del Servicio: Indicadores relativos a la gestión del plan de contingencia, tal y como se describen en el apartado “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 documentación de las políticas, contratos de los certificados, etc.)

La medida de los ANS se realizará con herramientas de AOC y/o con herramientas provistas por el adjudicatario para la monitorización continua a partir de transacciones automáticas o interacciones humanas simuladas.

Los informes de Seguimiento requeridos 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.

7.1 Modelo de medida del nivel de servicio

Para disponer de la información necesaria para una gestión y gobierno homogéneos del Servicio, 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 la su mejora continua.

El Modelo de Medida del Nivel de Servicio estructura un conjunto de indicadores, organizados de forma jerárquica, que permiten medir los distintos 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 varios indicadores de rendimiento.
- Indicadores de rendimiento (IR). Agrupan distintos 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 distintos 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 provisionado, 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]), para alcanzar la medición del Indicador de Nivel de Servicio (NS).

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

7.1.1 Indicadores

Se definen indicadores mínimos para medir el nivel de servicio, de modo 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 a 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 medición, 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 grado del indicador de medida. Estos umbrales de grado pueden tener valores asociados de mejora en el tiempo.

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

7.1.2 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, frente a cualquier modificación de los indicadores y niveles de servicio con el objetivo de dar un mejor servicio; el Consorci AOC junto 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 comportar 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.

7.1.3 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 se le aplique. 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 realizarán 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 sucesivas revisiones se aplicarán 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 exista mutuo acuerdo entre el adjudicatario y el Consorci AOC.
- Por 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.).

7.2 ANS de Explotación del Servicio

Indicadores/valores de niveles de servicio recogidos en la futura Declaración de Prácticas de Sello de tiempo en los siguientes ámbitos derivados de las normas de negocio:

- Publicación de información y directorio de certificados de las Entidades de Certificación.
- 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.
- Emisión del resto de CRLs cada 24 h, máximo 7 días de vigencia
- Alta de usuarios en el servicio en menos de 7 días.
- Acuerdos de nivel de servicios relativos a los procedimientos de identificación y autenticación previos a la realización de firma remota.

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

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

El período 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.

Asimismo, 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.

La medida y obtención se realizará a través de herramientas de gestión de peticiones del Consorci AOC o, en su defecto, del adjudicatario. Éstas 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.

7.2.2 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 la categorización de los mismos en el Plan de continuidad del Consorci AOC, debe ser continuada 24x7 y con estos niveles de disponibilidad:

- Servicios de emisión/gestión de certificados: 99,9 %
 - Web operadores idCAT y T-CAT
 - Conectores de carga y consulta de peticiones (LDAP)
- Servicios de carga y uso de certificados remotos: 99,9%
 - Web gestión identidad remota.
 - Conectores de carga y uso del servicio.
- 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.

7.2.3 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 (LDAP): 5

- Servicios de carga y uso de certificados remotos (usuarios concurrentes):
 - Web gestión identidad remota: 5
 - Conectores de carga y uso del servicio: 5
- Servicios de validación (transacciones por segundo):
 - CRL:
 - Media día: 2
 - Picos máximos: 60
 - OCSP:
 - Media día: 45
 - Picos máximos: 200
 - Descarga de los certificados de jerarquía (Claves públicas):
 - Media día: 1
 - Picos máximos: 200

El tiempo de respuesta deberá estar por debajo del umbral de 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.

7.2.4 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 tal y como se describen en el documento de Análisis de Impacto en el negocio (en inglés BIA) en relación a los Servicios de emisión/gestión de certificados, los Servicios de Validación (OCSP y CRL) y la carga y uso:

- 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.
- Servicio de Firma Remota:

Paràmetres de continuïtat resultants del BIA			
Procés	RTO	RPO	MTPD
Càrrega de segells	4 dies	1 setmana	2 setmanes
Ús de segells	24 hores		
Càrrega de certificats personals	24 hores	24 hores	
Ús de certificats personals	4 hores		

Maximum Tolerable Period of Disruption (MTPD), por su acrónimo en inglés, que se define como el tiempo máximo que puede estar un proceso o servicio parado sin comportar un impacto catastrófico que provoque daños irreversibles en la organización.

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.

7.2.5 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 generados.
- Para 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 período objeto de seguimiento. Se propone utilizar la herramienta certlint (<https://github.com/awslabs/certlint>) para la comparación automática.

7.2.6 ANS del Servicio de Apoyo

El adjudicatario, en la prestación el servicio de apoyo de 3er 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 bloqueante (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 supondrá 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 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%

Por 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.

7.3 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 apartado 6.10.1 sobre la metodología de mantenimiento evolutivo.

7.3.1 Acuerdos de nivel de servicio del desarrollo

Los niveles mínimos de prestación del servicio tendrán que ser:

- La fecha de entrega planificada es de obligado cumplimiento una vez cerrada y acordada la orden de trabajo. Un mínimo del 95% de las peticiones acordadas con la dirección funcional del proyecto tendrán que 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 tendrán que superar el plan de pruebas de vulnerabilidades sin errores.
- Plan de pruebas sin errores. Un mínimo del 98% de los evolutivos entregados tendrán que superar el plan de pruebas ejecutado por personal del Consorci AOC sin errores.

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

7.3.2 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 fallos en el plazo.
 - Cálculo: $(A/B) \cdot 100$
 - A: Número total de incidencias resueltas sin error en el plazo
 - B: Total de incidencias resueltas en el plazo
- Periodicidad: Mensual

- El porcentaje de incidencias sin error en el plazo establecido deberá ser al menos 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.

7.3.3 Tiempo de respuesta en el mantenimiento evolutivo

En relación con el servicio de mantenimiento evolutivo, se definen los siguientes tiempos:

- 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 realizar la toma de requerimientos por indisponibilidad del adjudicatario se tendrán en cuenta para realizar el cálculo de los tiempos de toma de requerimientos.

- Tiempo pre-análisis: 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 pre-análisis”.

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 pre-análisis (en días)
Urgente	1	2
Normal	5	7
Baja	10	10

7.3.4 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 pre-análisis, 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 tanto, la fecha máxima permitida de entrega será el 15 de abril.

8 FASES DE EJECUCIÓN DEL CONTRATO

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

2024		2025	2026	2027
S1	S2			
Fase de transició de l'operació del Servei				
Fase de prestació del Servei				
				Fase de devolució del Servei

- 1) Transición de la operación del servicio: desde la firma del contrato hasta el 31 de diciembre de 2024. Esta fase se describe en detalle en el punto “8.2-Transición de la operación del servicio actual” del presente documento.
- 2) Prestación del servicio de firma remota: como máximo, a partir del 1 de septiembre de 2024 y hasta la finalización del contrato. Como puntos clave a tener en cuenta en este período, cabe mencionar:
 - a) Inicio de la prestación del servicio de firma remota no calificado, basada en certificados personales y certificados de sello electrónico, como máximo, a 1 de julio de 2024.
 - b) Como máximo doce meses después de la adjudicación del contrato, inicio de la prestación del servicio de firma remota calificada.
- 3) Adecuación del Servicio: desde la consecución de la autorización del supervisor nacional para el inicio del servicio de firma remota calificada y hasta la finalización del mismo, 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 detalladamente en el punto 8.3 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 y meta destacada.
- En su caso, anticipos o mejoras en el calendario de alguna fase.

8.1 Creación y explotación del servicio firma remota calificada basada en certificados calificados del Consorci AOC

El adjudicatario deberá crear, alojar, calificar y operar el servicio firma remota calificada basada en certificados calificados, cuya titularidad será del Consorci AOC, como Prestador de Servicios de Certificación para los entes del Sector Público de Catalunya de acuerdo con EIDAS.

Para la emisión y gestión de estado de los certificados del servicio, el Consorci AOC pondrá a disposición del adjudicatario unas claves de Autoridad de Certificación subordinada y una propuesta de perfiles de certificado, tal y como se expone el punto **Error! No se encuentra el origen de la referencia.** del presente pliego. El sistema que realizará las funciones de entidad de registro por estos certificados deberá gestionarlos el adjudicatario en el marco del presente contrato.

Para el uso de los certificados, el adjudicatario deberá proveer los mecanismos para la activación del servicio de acuerdo con el definido punto 6.4 El Servicio de Firma Remota (SSR) del Consorci AOC.

8.2 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 el servicio de firma remota del Consorci AOC, de forma que, a la finalización de esta fase, la prestación efectiva del servicio la lleve a cabo, a todos los efectos, el adjudicatario.

El calendario y metas de seguimiento específico según establece el punto “9.69.6 Modelo de relación en la fase de Transición de la operación” y “9.6.1 Gobierno de la fase de transición de la operación” serán:

- Por la fase de revisión de activos y documentación del servicio actual del Consorci AOC, el nuevo adjudicatario dispondrá de un plazo de 4 semanas.
- Para el inicio de la prestación del servicio de firma remota no calificado, el nuevo adjudicatario dispondrá de un plazo de 6 meses.
- Para el inicio de la prestación del servicio de firma remota calificado, el nuevo adjudicatario dispondrá de un plazo de 12 meses.
- Por el inicio de la auditoría de ENS y de calificación del servicio, 6 meses.

Durante la fase de Transición de la operación el adjudicatario deberá mantener el ANS de los servicios actuales por los servicios que se vayan transfiriendo.

8.3 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 desarrollos realizados por sus servicios dentro del marco del mismo. 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 aportada.

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 #39;ha amortizado durante el período 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.

El adjudicatario también deberá aportar la total colaboración que sea necesaria para la devolución o transferencia del servicio a la Administración o al prestamista 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 cuyo caso quedará automáticamente ampliado dicho plazo hasta la total finalización de la devolución o transferencia.

El adjudicatario es responsable de adoptar las medidas de seguridad necesarias para que los datos objeto de traspaso, hasta que no estén en poder del Consorci o el nuevo adjudicatario, se mantengan íntegros, exactos, disponibles, y se adopten las medidas de seguridad que determine el Consorci AOC

9 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.

9.1 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 “7Acuerdos de nivel de servicio” y que aplican a los diferentes ámbitos del gobernamiento del servicio objeto de esta licitación. Éstos 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 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 seguimiento de los ANS, la información (evidencias) con base a la que se hayan elaborado, para que el Consorci AOC pueda incorporarla 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.

A continuación, se presenta una estructuración de las funciones y responsabilidades que el Consorci AOC traslada al adjudicatario en el 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 el 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 contrato está sustentado 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.

9.2 Estructura de responsabilidades del adjudicatario

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

La estructura de responsabilidades y competencias mencionada se concreta en los siguientes roles, aunque una misma persona puede asumir más de uno.

Por parte del adjudicatario:

- **Responsable de cuenta:** Garantizar la existencia de los mecanismos de relación por parte del adjudicatario a la hora de llevar a cabo los acuerdos tomados con el Consorci AOC, será la figura de referencia en el marco del contrato y el último responsable de la prestación del conjunto de servicios y proyectos. Esta figura se

mantendrá durante toda la vida del contrato: en la gestión comercial, durante la provisión del servicio y hasta la devolución del mismo.

- **Responsable de servicios:** asignado por el proveedor, cuyas principales funciones 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, interpretando 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 los que debe relacionarse para mejorar el servicio de negocio final.
- **Responsable de Control de Gestión:** Proporcionará al Consorci AOC los informes de gestión acordados, tanto con indicadores económico-financieros como otros, y llevará a cabo el seguimiento del modelo económico acordado con el adjudicatario. 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 .
- **Responsable Jurídico:** Será el interlocutor principal con el Consorci AOC en materia jurídica por los servicios prestados por el adjudicatario.
- **Experto en protección de datos,** en caso de que no tenga obligación de disponer de Delegado de protección de datos con las atribuciones especificadas en el apartado 6.8.6.3 Requisitos de protección de datos.
- **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.
 - Tipificación 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:** Coordinará la aplicación de la arquitectura corporativa en los sistemas de información y servicios a construir o mantener por el proveedor.
- **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 (soporte) 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 y 2º nivel, del Consorci AOC; y también del 3er nivel, del adjudicatario) para todos los procesos.
- Asegurar una buena relación y coordinación entre los equipos bajo su responsabilidad a fin de cumplir las actividades asociadas a todos los procesos de gestión definidos, y con responsabilidad sobre el adjudicatario.
- **Responsable de Calidad:** Garantizará la existencia de un plan de calidad por los servicios y aplicaciones, así como su ejecución.
- **Responsable de Seguridad:** Será responsable de:
 - Actuar como enlace entre el adjudicatario y los distintos agentes implicados (Consorci AOC, Agencia de Ciberseguridad de Catalunya) 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 la Agencia de Ciberseguridad de Catalunya 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 al 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 en el Consorci AOC según los plazos marcados, de todo lo relacionado con la seguridad (incidentes, medidas correctoras, riesgos, nuevos proyectos, iniciativas, etc...).
 - 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 (URL, usuario de aplicación, logs, etc..))
- **Responsable de Continuidad:** Será el responsable de:
 - Garantizar y liderar en 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 al 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 despliegue 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 en el 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 por cada desarrollo (calidad, robustez, eficiencia, etc.)
 - Ejecución exhaustiva del plan de pruebas definido por el proyecto.
 - Colaboración puntual, si así se estima 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, por lo 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.

- **Técnico:** Para realizar tareas de puesta en marcha y operación del servicio.

El adjudicatario mantendrá una mesa actualizada con las personas que tendrán cada uno de estos roles.

9.3 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:** Presentará la planificación, alcance y metodología de ejecución de los distintos planes de transición del servicio. Impulsará y asegurará la ejecución de éstos según la dirección establecida por el Consorci AOC, de forma coordinada con los responsables del resto de proveedores del Consorci AOC. Informará del grado de avance, los riesgos y planes de mitigación correspondientes, asegurando 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.** Será el responsable de la prestación de los servicios de cara a la ciudadanía y entidades usuarias.
- **Jefe de Proyecto.** Será el coordinador por parte del Consorci AOC de las tareas técnicas relativas a la puesta en marcha y operación de los servicios objeto de este pliego de prescripciones técnicas.
- **Responsable de Asesoramiento Jurídico.** Se coordinará con el Responsable jurídico del adjudicatario para garantizar el cumplimiento normativo y regulación del servicio.
- **Responsable de Sistemas**
- **Representante de la Dirección** para garantizar la alineación del servicio con la estrategia y misión del Consorci AOC.
- **Persona Delegada de Protección de datos**

9.4 Gestión de incidencias y problemas

Se entiende por 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 este objetivo, la Gestión de Problemas llega hasta la causa a raíz de las incidencias y después 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 en el 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 los mismos 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

9.5 Órganos de Gestión

9.5.1 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.

9.5.2 Reuniones de seguimiento.

El gestor del servicio del adjudicatario y el Jefe del Servicio 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 #39; 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 realizará 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 realizará 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 “6.8.6 La gestión de la seguridad y el cumplimiento normativo”.
- Seguimiento de la continuidad y disponibilidad con la prescripción, seguimiento y verificación de los requisitos, acuerdos de nivel de servicio y condiciones definidas en la presente licitación.
- 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, a 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 que incluirá, 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 con arreglo al objeto y alcance del contrato.
- Mejoras aplicables en el servicio.
- Información de cumplimiento sobre los acuerdos de nivel de servicio establecidos.

Se utilizará una herramienta de gestión del Consorci AOC que debe permitir y facilitar la participación de los diferentes actores implicados en la ejecución del servicio. Esta herramienta es 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 distintos 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.

9.6 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 la fase 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	<ul style="list-style-type: none"> Establecimiento y seguimiento del plan global de transición.
Comité de Transición de la operación	<ul style="list-style-type: none"> Interlocución, a 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 en el inicio de la prestación del servicio, siendo revisable en función de los planes y proyectos de transición.

Dichos órganos de gestión podrán designar a los grupos de trabajo operativos que sean necesarios para desarrollar adecuadamente sus funciones.

9.6.1 Gobierno 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 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 despliegue de los diferentes planes, de acuerdo con el adjudicatario; con las necesidades y prioridades

del Consorci AOC, y con el impacto en el Servicio 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 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, quien 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 proponer y ejecutar los planes de mitigación correspondientes; que reportará al Responsable de transición. Éste 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 que establece el marco normativo aplicable y, en concreto, el punto "8.2 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 los hitos marcados 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.

10 REFERENCIAS

- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza por las transacciones electrónicas en el mercado interior y que deroga la Directiva 1999/93/CE.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de estos datos y que deroga la Directiva 95/46/CE.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- ETSI EN 319 401 - Electronic Firmas and Infraestructuras (ESI); General Policy Requirements for Trust Service Providers.
- CEN EN 419 241-1 Trustworthy Systems Supporting Server Signing; - Parte 1: General System Security Requirements
- CEN EN 419 241-1 Trustworthy Systems Supporting Server Signing; - Parte 2: Protection profile for QSCD for Server Signing
- CEN EN 419 221-5 Protection Profiles for TSP Cryptographic Modules - Parte 5: Cryptographic Module for Trust Services
- ETSI TS 119 431-1 Electronic Firmas and Infraestructuras (ESI); Policy and security requirements for trust service providers; Parte 1: TSP service components operating a remote QSCD / SCDev
- ETSI TS 119 431-2 Electronic Firmas and Infraestructuras (ESI); Policy and security requirements for trust service providers; Parte 2: TSP service components supporting AdES digital signature creation
- CEN EN 419 241-1 Trustworthy Systems Supporting Server Signing; - Parte 1: General System Security Requirements
- CEN EN 419 241-1 Trustworthy Systems Supporting Server Signing; - Parte 2: Protection profile for QSCD for Server Signing
- CEN EN 419 221-5 Protection Profiles for TSP Cryptographic Modules - Parte 5: Cryptographic Module for Trust Services
- ETSI TS 119 431-1 Electronic Firmas and Infraestructuras (ESI); Policy and security requirements for trust service providers; Parte 1: TSP service components operating a remote QSCD / SCDev
- ETSI TS 119 431-2 Electronic Firmas and Infraestructuras (ESI); Policy and security requirements for trust service providers; Parte 2: TSP service components supporting AdES digital signature creation
- RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

11 Anexo - Situación actual

11.1 Catálogo actual de certificados del Consorci AOC

El Consorci AOC ofrece únicamente certificados de firma personal y sellos electrónicos que corresponden a las tipologías de servicios de Reglamento EIDAS. A tal efecto, el [catálogo actual de certificados](#) que ofrece el Consorci AOC se puede consultar en la web del Consorci AOC. Se adjunta una tabla resumen:

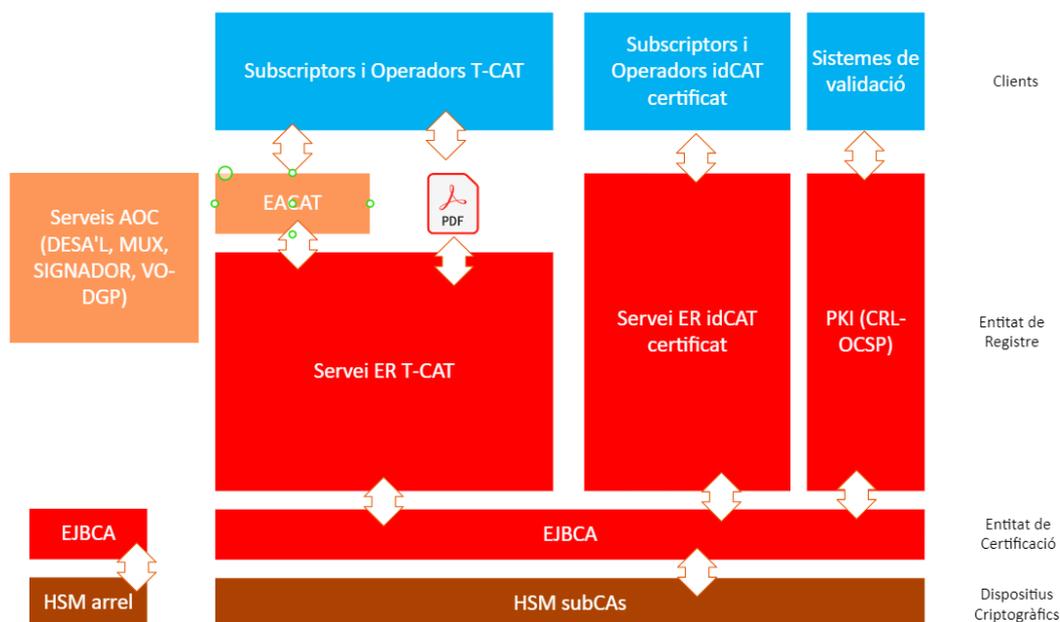
Certificados	Producto	Acrónimos nuevos	Duración	Soporte
idCAT: ciudadano	idCAT	CPISA2_idcat	4 años	software
T-CAT: Certificados electrónicos calificados de empleado público	T-CAT	CPI-1+CPSQ-1	4 años	tarjeta
	T-CAT P	CPISA-1	4 años	software
T-CAT: Certificados electrónicos calificados de trabajador público	T-CAT	CPISQ-3	4 años	tarjeta
	T-CAT P	CPISA-3	4 años	software
T-CAT: Certificados electrónicos calificados para el personal de la administración pública	T-CAT Representante	CPRISQ-1	4 años	tarjeta
	T-CAT Seudónimo	CPPI1+CPPSQ-1	4 años	tarjeta
T-CAT: Certificados la administración pública Certificados electrónicos calificados de sello electrónico de la	Sello nivel medio	CDA-1_SGNM	3 años	software

administración pública				
T-CAT: Certificados aplicación	Dispositivo aplicación	CDA-1	3 años	software

El detalle concreto de cada perfil de certificado, así como el propósito y modalidades de provisión y soporte, se pueden consultar en los documentos vigentes de perfiles, políticas y declaración de prácticas ubicadas en la web de regulación del servicio en <https://epsco.aoc.cat/regulacio>.

11.2 Situación actual de subsistemas y componentes del Servicio

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

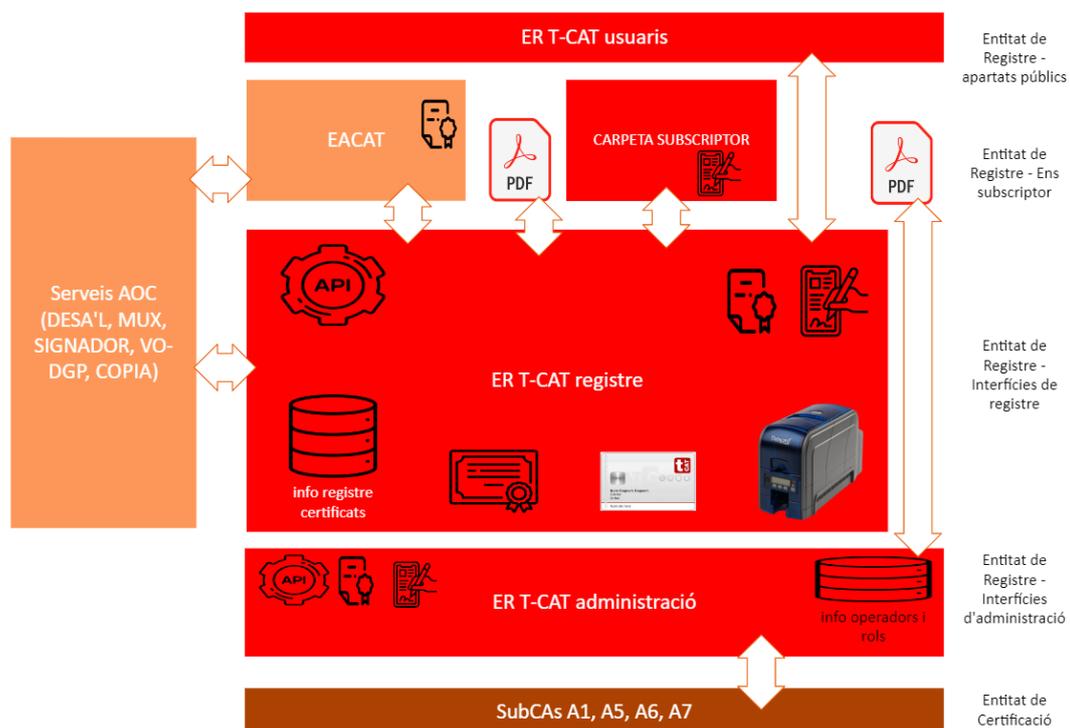


- En azul oscuro se muestran clientes agrupados por operadores del sistema de portales o como clientes y/o suscriptores.
- En rojo se muestran los componentes del SCD, ya sean productos comerciales o desarrollados a medida:
 - Servicio ER-T-CAT: portal, conectores y software de la Entidad de Registro 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 (FIRMADOR), servicio de digitalización (COPIA), acceso a datos de la DGP (VO-DGP), etc.

11.3 El Servicio de Registro de certificados personales y de sello electrónico por el Sector Público (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 Public. Como perfiles de certificado se incluyen los certificados de firma electrónica y de sello electrónico.



11.3.1 Modelo de Registro T-CAT

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 ello, existen 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 tanto, se utiliza por todos los entes 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 del 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 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 del 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 unas ochenta entidades que desempeñan el rol de Entidad de Registro de la SCD T-CAT.
 - a. Módulo peticionario: módulo de carga de peticiones en el sistema de registro. Dispone de un canal de entrada web y de un canal de entrada automático vía conectora 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 esa petición de certificado pasa directamente a estar lista por 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 via 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 entes 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 llama 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 Entidad.
 - 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. Por último, 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.
 - g. También en este módulo se implementa la Cesión de certificados entre EERR que se define en el punto "11.3.4.3 Módulo de cesión de certificados".

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

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

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

11.3.2.1 Nos suscriptores o Entidades de Registro Virtuales o vinculadas

En el entorno T-CAT, los Entes suscriptores o ERs 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 utilizan el ASCD de EACAT para la certificación de datos de certificados T-CAT y la entrega de los certificados T-CAT con la carpeta del suscriptor.

El número de Entes suscriptores o ERs Virtuales o vinculadas (entes dados de alta en el sistema) actualmente es de 2.482.

11.3.2.2 ERs Colaboradoras

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

El número de ERs Colaboradoras es de 68 entidades de registro, de las cuales algunas tienen varios puntos de atención. El número total de operadores de las ERs T-CAT es de aproximadamente: 747.

11.3.2.3 L&ER centralizada del Consorci AOC

El Consorci AOC opera una ER que es la que centraliza las peticiones de certificados digitales de todos los entes que no están vinculados a una ER Colaboradora o que, puntualmente, piden emisiones de envíos concretos de certificados.

11.3.3 Roles del sistema de registro T-CAT

11.3.3.1 Roles del ASCD y Carpeta del Suscriptor

Estos roles corresponden a los componentes de ASCD y Carpeta del suscriptor descritos anteriormente. Están definidos en la web del Consorci AOC y se replican aquí por mejor referencia.

- Responsable del servicio. Personas con un rol de gestión y no un perfil de elevado grado de responsabilidad, éstos 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 para garantizar la continuidad del servicio.
- Certificador de datos. Personas que se responsabilicen 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.
- Solicitante de certificados personales. Personas con autoridad dentro del ente para solicitar la emisión, renovación y revocación de certificados personales o de entidad (p. ej. el alcalde, teniente de alcalde o un concejal en el ayuntamiento, o el director 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.
- Solicitante de certificados de aplicación. Personas con autoridad dentro del ente para solicitar la emisión, renovación y revocación de certificados de dispositivo (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.

- Editor de solicitudes. Personas que pueden cumplimentar, aunque no firmar, solicitudes de emisión, renovación y revocación de certificados digitales a través del EACAT, de forma que queden preparadas para la firma de un usuario con el rol de solicitud licitante 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.

NOTA: los roles solicitante y certificador son incompatibles, siendo recomendable que haya un mínimo de dos personas en cada rol.

Estos roles son informados en el Servicio de Certificación Digital del Consorci AOC a través de la Ficha de Ente Suscriptor. Esta ficha también incorpora los datos oficiales del Ente en cuestión que, como solicitante de certificados T-CAT, constarán en los certificados que solicite. La ficha debe actualizarse cada dos años y se envía a través de un trámite ofrecido por el servicio EACAT. Se adjunta un anexo de muestra en el presente pliego de prescripciones técnicas y un [enlace](#) a un vídeo explicativo del proceso.

11.3.3.2 Roles web Operadores / Entidad de registro de SCD

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:

- Peticionario: persona encargada de introducir los datos de las solicitudes de certificados en la aplicación de petición de certificados. Se debe tener en cuenta que cuando una petición entra por la EACAT este rol desaparece y queda para casos de extraordinarios (nuevos entes o entes no dados de alta en el EACAT o problemas técnicos que impidan hacer uso de la plataforma.)
- Aprobador: persona encargada de revisar los datos de las solicitudes introducidas por el petionario y aprobar (validar) o denegar (devolver al petionario) la petición en consecuencia. En el caso de peticiones introducidas por la EACAT, no se tratará de una tarea de revisión del trabajo del petionario, que no existe, pero si será necesario comprobar que no existen errores evidentes, pruebas de los entes que solicitan certificados, etc.
- Generador: persona encargada de generar los certificados una vez aprobadas las peticiones
- Gestor de certificados: persona encargada de habilitar y revocar los certificados digitales durante su ciclo de vida (la suspensión es sólo telefónica). Debe tenerse en cuenta que, cuando una petición entra por la EACAT este rol desaparece y queda para casos de emergencia (en que no sea posible utilizar la EACAT).

- 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 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.
- Responsable de seguridad física: las funciones del responsable de seguridad física consisten en coordinar, controlar y revisar el conjunto de medidas contenidas en la política de seguridad y las normas y procedimientos de seguridad relacionados con los aspectos físicos. Es decir, todo lo referente al control de acceso a la sala de operaciones, la detección y extinción de incendios, la protección de la información y material a nivel físico, etc. Este rol queda englobado en el responsable de la Entidad de Registro T-CAT.
- Responsable de seguridad lógica: las funciones del responsable de seguridad lógica consisten en coordinar, controlar y revisar el conjunto de medidas contenidas en la política de seguridad y las normas y procedimientos de seguridad relacionados con los aspectos lógicos de la Entidad de Registro. Es decir, todo lo referente a la seguridad informática (control de acceso a la red, políticas de instalación de software, configuración de los equipos, etc.). Este rol queda englobado en el Responsable de la Entidad de Registro T-CAT.
- Archivero: el archivero o persona que este designe se encargará de organizar, clasificar, describir y velar por la salvaguarda de la documentación que se genere fruto de la emisión y gestión de los certificados de acuerdo con el sistema de gestión documental de su organismo, o en su ausencia, según las directrices que establezca el archivero del Consorci AOC. Este rol queda englobado en el Responsable de la Entidad de Registro T-CAT.

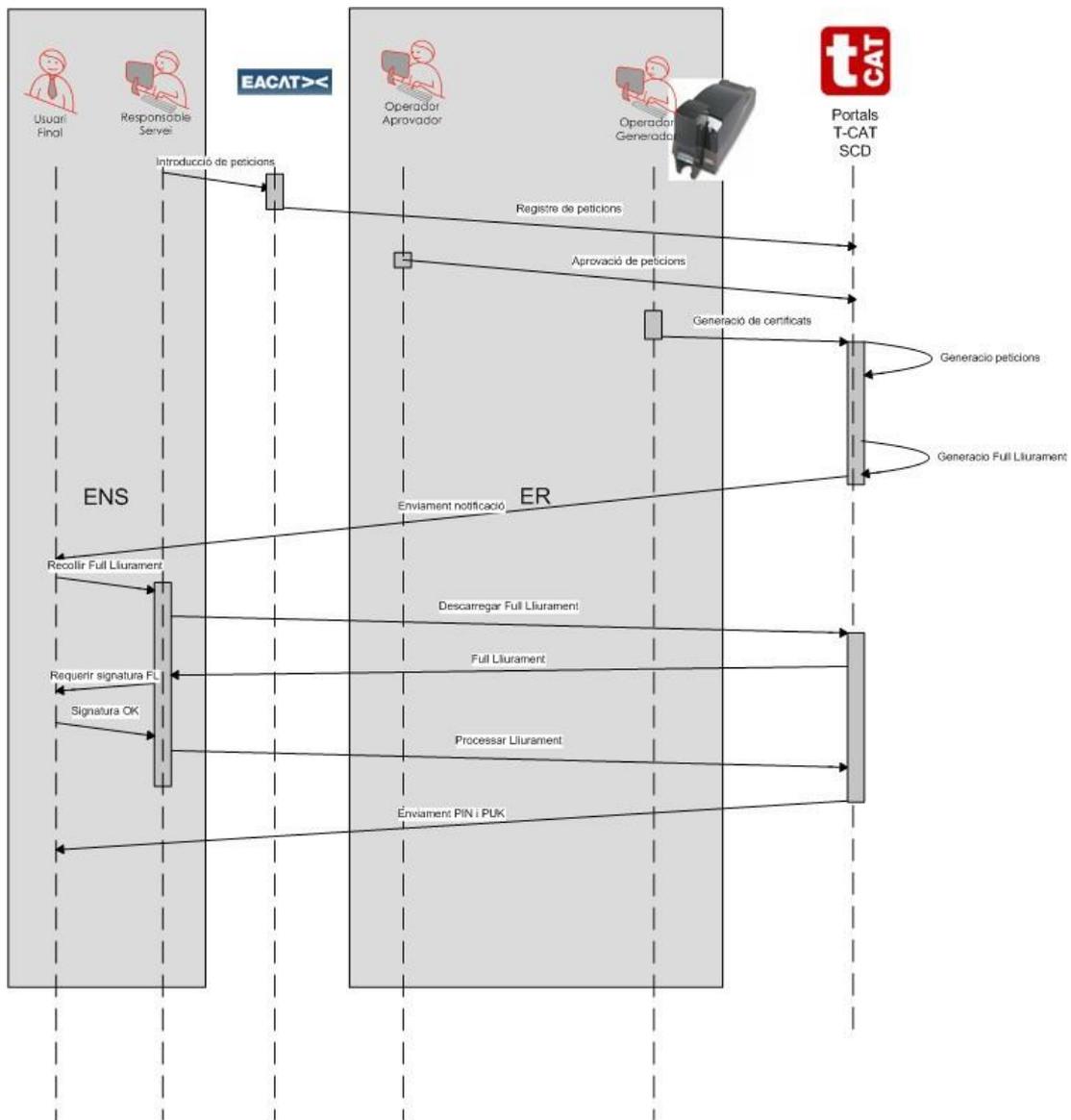
Estos roles son informados en el Servicio de Certificación Digital del Consorci AOC a través de la Ficha de Entidad de Registro. La ficha debe actualizarse cada dos años y se envía a través de un trámite ofrecido por el servicio EACAT. Se adjunta un anexo de muestra en el presente pliego de prescripciones técnicas.

11.3.4 Diagrama de relaciones de los procedimientos de emisión

Mediante los siguientes diagramas de relaciones, se ilustran los procesos de emisión de certificados digitales en soporte tarjeta y software. Los esquemas muestran los roles que intervienen a lo largo del proceso.

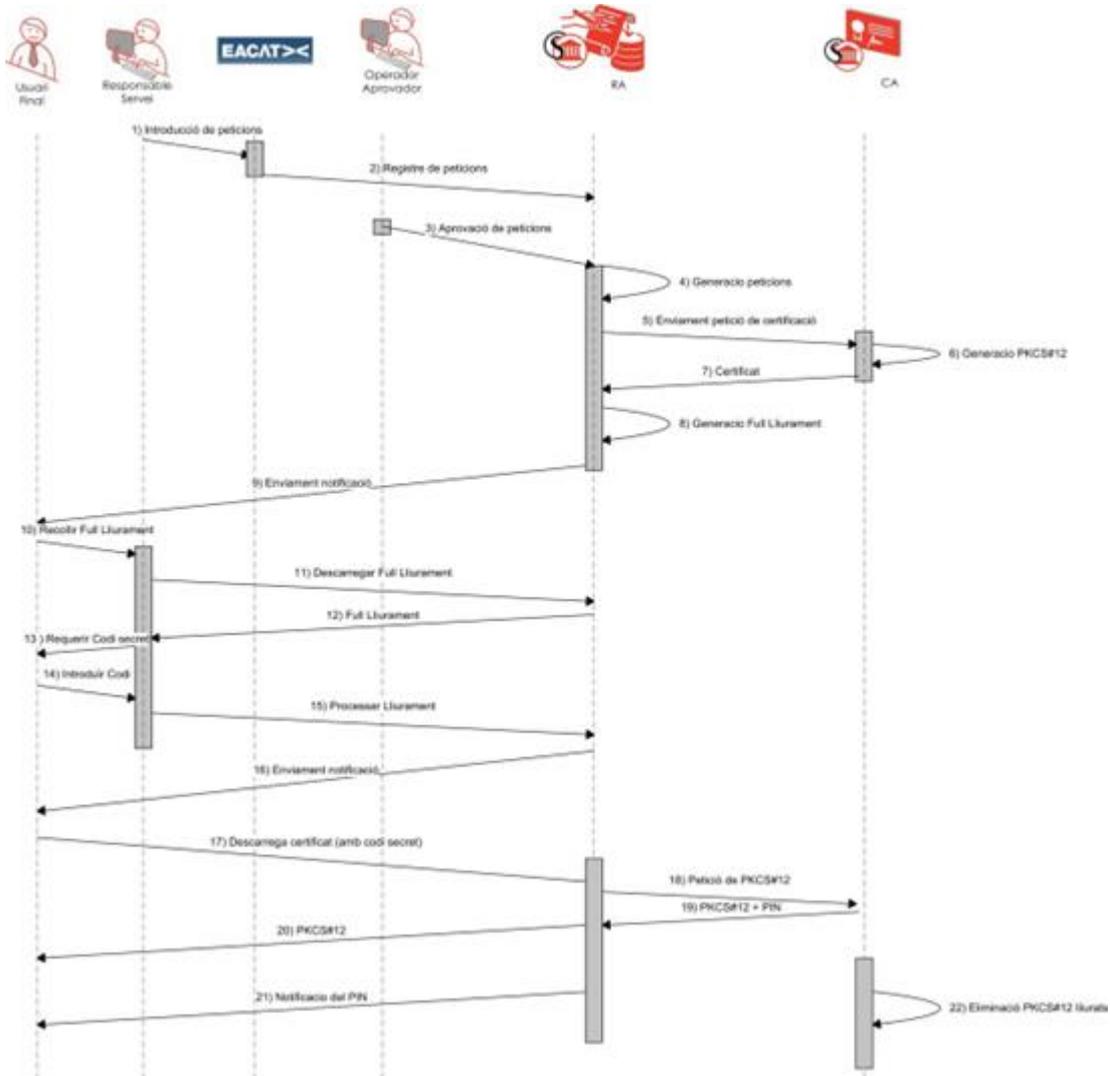
11.3.4.1 Procedimiento T-CAT

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/PUK enviados por correo-e :



11.3.4.2 T-CAT-P (Software)

El siguiente diagrama de flujo representa el procedimiento de emisión estándar de un certificado T-CATP en software con la solicitud a través de EACAT, con personación física del usuario final ante el responsable de servicio por el “entrega” de la tarjeta, firma del contrato y envío del PIN y PUK por correo-e:



11.3.4.3 Mòdul de cesió de certificats

Este mòdul de la Carpeta del Suscriptor incorpora la possibilitat de delegar en el Consorci AOC la descàrrega de les claus, en format pkcs#12, per als tipus de certificat de Sello electrònic de nivell mitjà.

Actualment les claus es generen en l'entitat de certificació, es associen a un certificat del perfil de sello de nivell mitjà i es importen en el servei de firma centralitzada per al seu ús per part dels clients tal i com es descriu a continuació en el punt "11.4.5 Serveis per al ús de certificats de sello electrònic centralitzats: el Servei Firmador Centralitzat".

Los operadors del sistema amb rol "depositario" són els responsables de descarregar aquests certificats i carregar-los en el servei de firma centralitzada en l'almacén corresponent de cada entitat, identificat amb el codi INE10 (etiqueta DEPOSITARIO de la missatgeria del servei). Els codis INE10 identifiquen internament al Consorci AOC i en l'àmbit de tots els serveis que ofereix, cada entitat usuària dels serveis. En el moment de la càrrega es informa l'etiqueta (etiqueta ROL de la missatgeria del servei) que s'utilitzarà per invocar el servei.

11.3.5 Gestión documental del Servicio de Certificación T-CAT

El software del 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 para la gestión de la documentación derivada del trámite.

El gestor documental se utiliza también para generar las comunicaciones de finalización o rechazo de la tramitación solicitada, a fin de informar a los solicitantes del trámite de su estado. Hay que recordar que se asigna un número de registro de entrada desde el módulo ASCD de EACAT y éste es el número que se utiliza para realizar 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 en el 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 del ER vinculada durante el período legalmente exigido.

11.3.6 Tabla de relación entre roles e historias de usuario del componente ASCD

En la siguiente tabla se muestran los roles con las operaciones que pueden realizar en el módulo ASCD de EACAT y que están al alcance de este contrato:

Operación	Responsable Servicio (RE)	Certificador de Datos (CD)	Solicitando certificados personales (SCP)	Solicitando certificados aplicación (SCA)	Editor de solicitudes (ES)
Solicitud y renovación certificados personales			X		
Solicitud y renovación de certificados de aplicación				X	
Solicitud de certificados de seudónimo o representante			X		
Solicitud de revocaciones			X	X	
Solicitud y renovación de certificados de operador			X		
Revocación de certificados de operador			X		

Validación de solicitud de certificados		X			
Autenticación y Autorización	X	X	X	X	X
Consulta de solicitudes	X	X			
Firma Digital	X	X	X	X	

11.3.7 Historias de usuario de las operaciones de solicitud y gestión del ciclo de vida de los certificados dentro de EACAT

11.3.7.1 Solicitud y renovación de certificados personales

Objetivo

Es posible realizar la solicitud para la generación o renovación de un certificado digital de tipo personal.

Precondiciones

Los usuarios requeridos tendrán que tener los roles correspondientes a EACAT.

Procedimiento

El solicitante accede a la página correspondiente para iniciar el proceso, donde le aparece un asistente web con varios pasos a seguir.

En el primer paso dentro del proceso se le pide al usuario establecer la siguiente información:

- Entidad de Registro destinataria
- Tipo de certificado a realizar (Lista)
- Prioridad de la petición (Ordinaria o Urgente)
- Comentario

En el siguiente paso, se introduce la información correspondiente al certificado, es posible añadir varios certificados en la misma solicitud (formando un envío):

- Nombre*

- Primer Apellido*
- Segundo Apellido
- NIF/NIE*
- Correo electrónico*
- Unidad Orgánica
- Usuario Ms Windows
- Número de #39; expediente
- Expediente de facturación

Al avanzar, aparece un formulario en el que aparecen los datos del RE, permitiendo modificar la información correspondiente a:

- Nombre
- Dirección
- Código Postal
- Localidad

Seleccionamos la opción de Enviar a Firmar, que muestra un mensaje de confirmación indicando que la petición quedará pendiente de firma, mostrándose también un formulario de resumen con los datos que se han registrado para la solicitud. En este punto seleccionamos la opción de Firmar, que realiza una firma digital asociada a la solicitud.

L'operación finaliza y se muestra un mensaje indicando que el proceso ha finalizado correctamente, enviando un correo electrónico al usuario certificador con el resumen de la operación.

11.3.7.2 Solicitud y renovación de certificados de aplicación

Proceso similar al de solicitud y renovación de certificados personales

11.3.7.3 Solicitud de certificados de seudónimo o representante

Proceso realizado 100% a través de formulario PDF

11.3.7.4 Solicitud de revocaciones

Proceso similar al de solicitud y renovación de certificados

11.3.7.5 Solicitud y renovación de certificados de operador

Proceso realizado 100% a través de formulario PDF

11.3.7.6 Revocación de certificados de ' operador

Proceso realizado 100% a través de formulario PDF

11.3.7.7 Validación de solicitud de certificados

Objetivo

Como certificador es posible realizar la validación de una solicitud de certificados realizada por un solicitante.

Precondiciones

Existe una solicitud de certificados personales registrada correctamente y pendiente de validación.

El usuario que realiza la operación debe estar asignado como certificador dentro del Ente.

Procedimiento

El certificador hace login en la aplicación y selecciona la opción de ver las solicitudes de certificados, y se muestra una tabla con la lista de solicitudes. En la tabla se muestra el Tipo de la Solicitud, la Fecha, el Tipo del certificado y el número de certificados asociados a la solicitud (envío). Para las solicitudes pendientes, tiene la opción de firma.

El certificador selecciona de la lista una solicitud para firmar, y se muestra un formulario con el resumen de los certificados solicitados asociados, donde tiene la opción de realizar la firma, realizando una firma digital de los datos y confirmando la validación de la solicitud.

La operación finaliza y se muestra un mensaje indicando que el proceso ha finalizado correctamente, enviando un correo electrónico al solicitante que realizó la solicitud con el resumen de la operación.

11.3.8 Otras operaciones

11.3.8.1 Autenticación y Autorización

La Autenticación y Autorización se hace en base a los datos de usuarios y roles, respectivamente, que han sido informadas en las fichas de ENS mencionadas anteriormente y que se han configurado en la base de datos de usuarios y roles dentro del propio EACAT.

11.3.8.2 Consulta de solicitudes

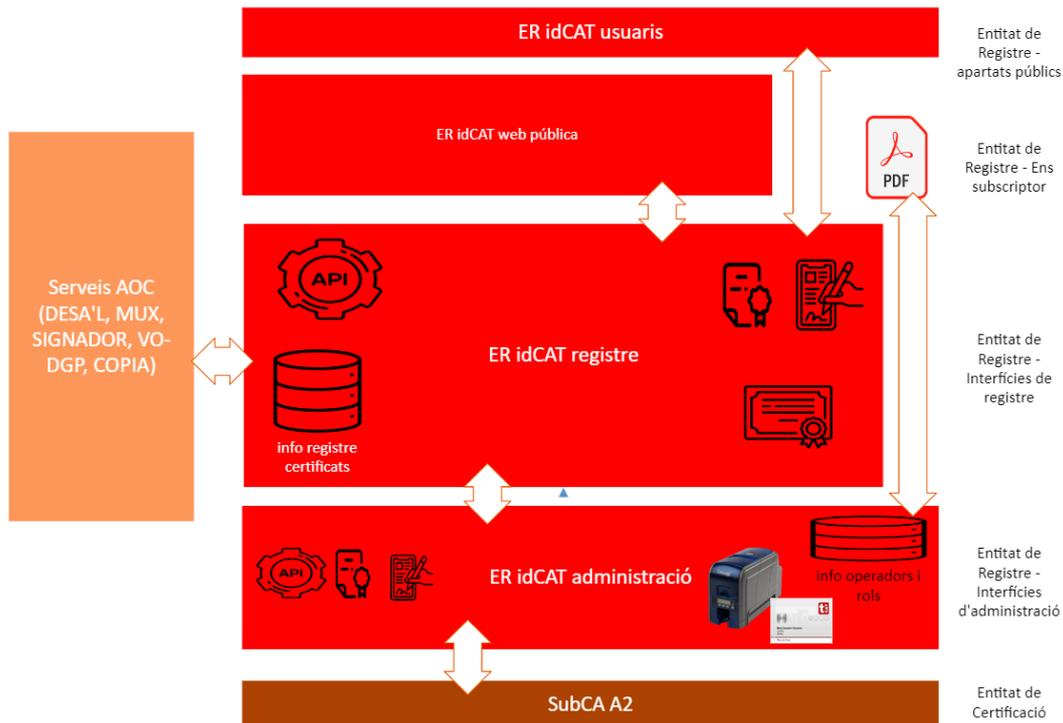
La consulta de solicitudes se realiza a través de la consulta de las trazas de envío de los envíos de solicitudes de certificados desde el componente ASCD de EACAT hacia la ER a través de su conector web.

11.3.8.3 Firma Digital

La firma digital de las evidencias se realiza mediante el componente Firmador de AOC. Las solicitudes de certificados personales incluyen dos firmas (de los roles solicitante y certificador) y las de certificados de sello una única firma (del rol SCD).

11.4 El servicio de Registro de certificados personales por Ciudadanía (idCAT)

Por su parte, los operadores de las ERs idCAT trabajan utilizando una única aplicación que es la 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:



11.4.1 La web del ciudadano

Desde donde se puede realizar 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.

11.4.2 La Web de los Operadores de Registro

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 realiza 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 Oberta del Consorci AOC, modalidad DGP) para que se pueda emitir el certificado y la generación de la documentación.

11.4.3 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.

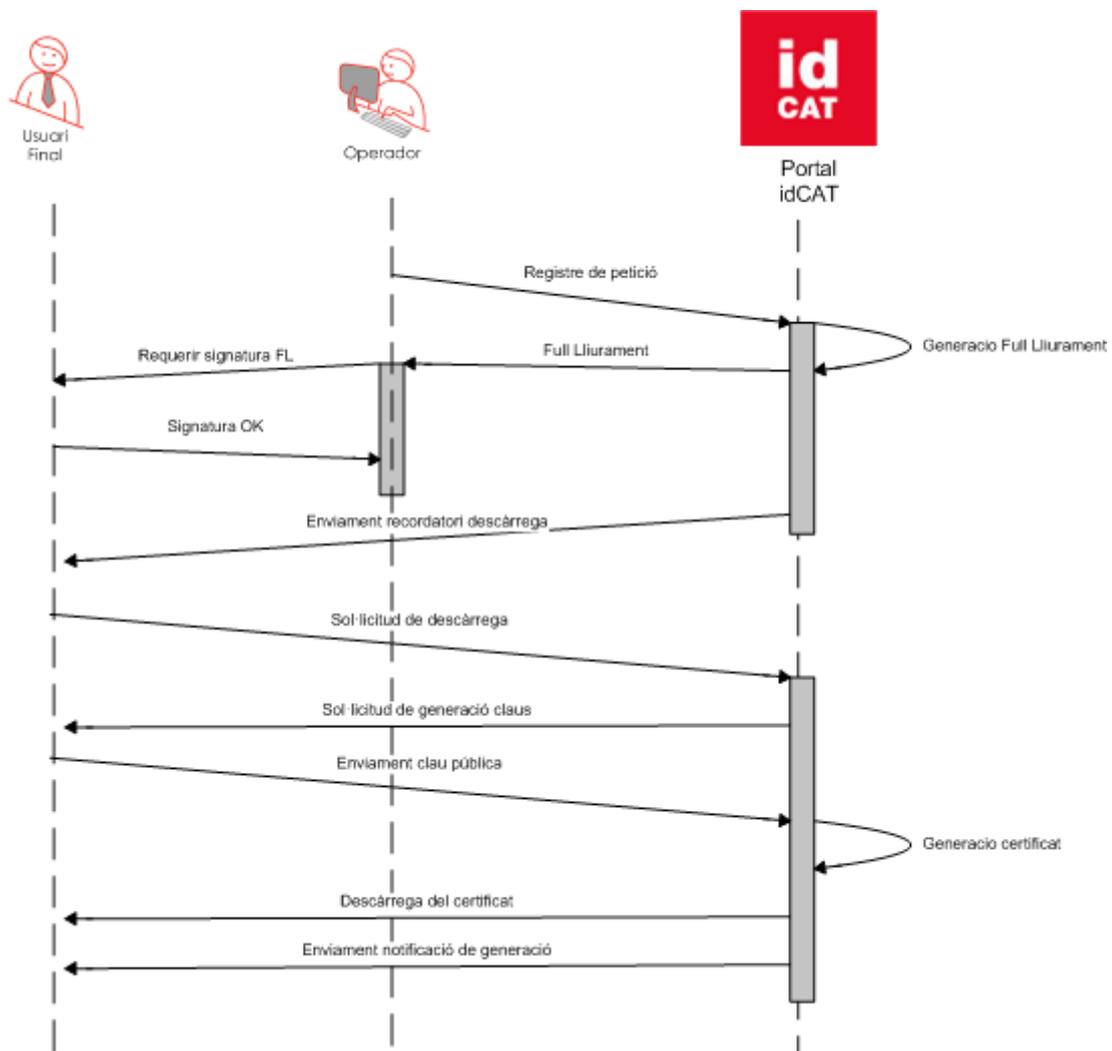
Dimensiones ER idCAT:

- Número de ERs: 372
- Número de operadores de las ERs idCAT: 3.566

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

11.4.4 Procedimiento de solicitud y emisión idCAT

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.

11.4.4.1 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 en el suscriptor del certificado. En ambos casos, esta documentación en papel es custodiada por el archivero del ER vinculada durante el período legalmente exigido.

11.4.5 Servicios para el uso de certificados de sello electrónico centralizados: el Servicio Firmador Centralizado

Servicio de custodia centralizada de certificados digitales de sello electrónico, integrado con la PKI para la provisión de certificados digitales, que realiza una custodia centralizada y segura, y que se integra con herramientas que permiten el uso de las claves allí almacenadas por parte de los usuarios titular o de aplicaciones que estén expresamente autorizadas a su uso. En el servicio se custodian sellos electrónicos de dos modalidades previstas en el procedimiento de solicitud actual (consultar [aquí](#)) y que son “Cedit en exclusividad por uso de los servicios AOC” o bien “Cedit en exclusividad por uso de herramientas propias”.

La integración con el servicio se realiza mediante webservice XML con autenticación de cliente con certificado digital, cifrado de transporte HTTPS y TLS 1.2. La autorización es mediante el certificado digital de autenticación y las etiquetas Rol y Depositari indicadas en el mensaje. El servicio permite realizar firmas en formato PDF con envío del documento entero, XML attached o detached. El formato predeterminado de hash es SHA2. La documentación de integración del servicio, con más detalle técnico de lo aquí expuesto, se puede consultar [aquí](#).

En relación con las volumetrías, el servicio aloja actualmente más de 1400 claves de todos los organismos de la administración pública catalana, y se realizan un volumen de 5 millones de firmas mensuales con picos de 600 transacciones por minuto.

11.4.6 Activos de software, código y datos del servicio actual a disposición del adjudicatario

A continuación, se enumeran los activos de software, código y datos del servicio actual que se pondrán a disposición del adjudicatario para conseguir los objetivos por la prestación de los servicios objeto del contrato. En el apartado “6 DESCRIPCIÓN DE LOS SERVICIOS OBJETO DEL CONTRATO” y sus subapartados, se definen las condiciones para el traspaso, puesta en marcha, uso, mantenimiento, mejora y retorno de estos activos por parte del adjudicatario.

Las claves de las entidades subordinadas a utilizar por estos servicios y que se han mencionado en el punto “5.1 El servicio de certificación digital del Consorci AOC”. Las claves se generaron en dispositivos del fabricante ENTRUST, modelo XC Connect. El security world

que las aloja es de nueva creación en 2022 y está protegido por un conjunto de tarjetas ACS en configuración 3 de 8 y OCS de 2 de 5. Las tarjetas son del tipo que permiten operación remota.

El servicio de firmador centralizado de sellos se ofrece a través de infraestructura propia del Consorci AOC y con el producto TrustedX eSignature bajo el licenciamiento vigente del fabricante ENTRUST. El Consorci AOC dispone de los descriptores del servicio web de la mensajería de integración, las claves y configuración (relación ROL+DIPOSITARI) del servicio, así como los formularios de alta en el mismo.

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 distintos componentes enumerados en el punto "11.2 Situación actual de subsistemas y componentes del Servicio". También las fichas de alta de los ENS y ER con su información verificada y los operadores y roles que las componen.

En relación a los servicios de identificación y firma de VALid y Firmador, el Consorci AOC lleva a cabo el ciclo de vida de gestión del software completo, así como la explotación y soporte.

11.5 Servicios de auditoría de ER

El Consorci AOC lleva a cabo las auditorías de las entidades de registro para garantizar que su funcionamiento se ajusta a los procedimientos, funciones y responsabilidades que se transfieren mediante las condiciones específicas del servicio.

El objetivo de realizar auditorías en los entes suscriptor y en las Entidades de Registro IDCAT y T-CAT es supervisar y controlar que todo el procedimiento de emisión y gestión de los certificados digitales IDCAT y T-CAT se realiza de forma correcta y cumple con los procedimientos operativos que el Consorci AOC proporciona a las ERs.

En el momento de licitación de este contrato, este servicio está adjudicado a un proveedor externo a través del contrato "AOC-2020-53". El pliego técnico con los detalles de auditoría que lo rigen se pueden consultar aquí: <https://contractaciopublica.cat/ca/detall-publicacio/a1fd1b13-5185-2ac8-80e5-efe217cfb5c5/60315938>

Las auditorías pueden ser presenciales o virtuales y siguen un procedimiento que el Consorci AOC establece y que se puede consultar en el pliego técnico del mencionado contrato con el nombre "ER_idCAT_T-CAT_procediment_auditoria.pdf".

A principios de cada año el Consorci AOC acordará con el adjudicatario la selección de las ERs que tendrán que auditarse durante ese año, en base a los criterios descritos en el citado documento; y con el objetivo de que todas las ERs se sometan, como mínimo, a una auditoría cada 3 años. También se acordará la planificación de las correspondientes auditorías.

11.6 Servicios evolutivos y de personalización de software actuales

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

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

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

11.7 ANS actual del servicio de certificación

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.

Asimismo, 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

11.8 Formación y divulgación

El servicio de certificación digital lleva a cabo acciones de formación y divulgación dirigidas a usuarios finales, entes suscriptores y los operadores y técnicos de las Entidades de Registro idCAT y T-CAT.

Durante 2022 se realizaron 45 actividades formativas, que suponen más de 1000 horas de cursos on line horas de formación impartida, durante las cuales se formaron más de 400 asistentes.

Por lo que respecta al servicio de formación, se realizan estas sesiones con estos formatos:

- Talleres de formación presencial T-CAT anuales en el aula de formación del Consorci AOC (y con el apoyo del servicio de formación de la AOC):
- 4 formaciones virtuales a operadores de ER T-CAT al año
- Curso virtual para usuarios finales de Usos del certificado digital T-CAT, abierto y autodirigido
- 17 ediciones del curso virtual para operadores de ER idCAT tutorizado

El 5% de estas acciones formativas se llevaron a cabo de forma presencial y el 95% restante fueron formaciones a distancia.

En relación con la divulgación, ésta se realiza principalmente a través de la plataforma de formación del Consorci AOC.

