PLIEGO DE PRESCRIPCIONES TÉCNICAS DEL SERVICIO DE EMISIÓN Y CUSTODIA DE CERTIFICADOS ELECTRÓNICOS DE ENRESA EXPTE Nº CO-SD-24-001	Clave: 000-ES-SD-0006 Páginas: 11

ÍNDICE

1 OBJETO

Este pliego establece las prescripciones técnicas requeridas para la prestación del servicio de emisión y custodia de certificados electrónicos de Enresa.

2 ALCANCE

Enresa, Empresa Nacional de Residuos Radiactivos, S.A. S.M.E., es la entidad integrada en el sector público institucional encargada de gestionar el servicio público esencial de gestión de los residuos radiactivos y el desmantelamiento y clausura de las centrales nucleares, tal y como establece el Real Decreto 102/2014, de 21 de febrero.

Desarrolla su actividad de acuerdo con lo previsto en el Plan General de Residuos Radiactivos (PGRR), que es revisado periódicamente por el Gobierno y establece las estrategias y líneas de actuación a llevar a cabo en cada momento por la compañía.

Parte de esta actividad se sustenta en procesos de negocio que son soportados por sistemas de información, en los que se necesita hacer uso de certificados electrónicos para funciones tales como:

- transmisiones de datos en el marco de interoperabilidad con terceros.
- firma de contenidos como herramienta para garantizar la autenticidad, integridad y no repudio.
- identificación digital de los empleados de Enresa en el ejercicio de sus funciones.
- representación digital de persona jurídica con otras administraciones o terceros.
- garantizar la seguridad en las comunicaciones de los sistemas y aplicaciones.

3 ACTIVIDADES

Las actividades a realizar en el servicio son las siguientes:

3.1 Emisión de certificados electrónicos

El contratista, conforme el REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (en adelante, reglamento eIDAS), proveerá a demanda de Enresa los siguientes tipos de certificados electrónicos:

- Certificado electrónico de persona física y pertenencia a entidad y/o certificado electrónico de representante de persona jurídica, que podrán ser según el criterio de Enresa:

- Cualificados, con funcionalidad de identificación y firma electrónica cualificada.
- No cualificados, con funcionalidad de identificación y firma electrónica avanzada.

Tendrán una validez máxima de 24 meses, y la renovación se realizará con un plazo mínimo de 30 días naturales antes de la fecha de caducidad del certificado.

Se estima la necesidad de disponer de 800 certificados electrónicos durante la ejecución del contrato, de los cuales se estiman 700 cualificados y 100 no cualificados, y se ejecutarán a demanda según las necesidades de Enresa, sin que Enresa quede obligada a la ejecución total de los mismos.

- Certificado cualificado de sello electrónico empresarial, para la actuación administrativa automatizada.

  Tendrán una validez máxima de 24 meses, y la renovación se realizará con un plazo mínimo de 30 días naturales antes de la fecha de caducidad del certificado.

  Se estima la necesidad de disponer de 2 certificados cualificados de sello electrónico empresarial durante la ejecución del contrato, y se ejecutarán a demanda según las necesidades de Enresa, sin que Enresa quede obligada a la ejecución total de los mismos.

- Certificados de servidor (SSL/TLS), para garantizar la seguridad en las comunicaciones de los sistemas y aplicaciones, que podrán ser a criterio de Enresa:
  - Para un solo dominio (Estándar).
  - Para subdominios ilimitados (Wildcard).

  El nivel de validación para estos certificados será OV (Organization Validation) o EV (Extended Validation).

  Tendrán una validez máxima de 13 meses, y la renovación se realizará con un plazo mínimo de 30 días naturales antes de la fecha de caducidad del certificado.

  Se estima la necesidad de disponer de 40 certificados de servidor durante la ejecución del contrato, de los cuales 36 serán de un sólo dominio y 4 de subdominios ilimitados, y se ejecutarán a demanda según las necesidades de Enresa, sin que Enresa quede obligada a la ejecución total de los mismos.

3.2 Autoridad de Registro

Para la gestión de los certificados de persona física y pertenencia a entidad y de representante de persona jurídica, Enresa actuará como autoridad de registro delegada por el contratista, quien deberá suministrar todos los medios necesarios para constituir y operar la autoridad de registro de Enresa, y en particular:

- Una aplicación de gestión que permita la realización de las tareas propias de una Autoridad de Registro por al menos cinco operadores de Enresa, y que permita las siguientes funcionalidades mínimas:
    - Autenticación mediante datos de contraste y/o certificado electrónico.
    - Gestión de usuarios y de las solicitudes de los certificados electrónicos de Enresa para todo el ciclo de vida de los mismos (emisión, renovación, revocación, etc).
    - Carga masiva de usuarios mediante CSV.
    - Aviso automático al usuario de la caducidad próxima del certificado.
    - Generación de informes por fechas del uso de certificados por estado (caducidad, generación, revocación, etc) o por validación.
- El material de formación y la documentación necesaria para acreditar a los operadores de la Autoridad de Registro en Enresa, y que puedan realizar sus funciones correctamente.

El contratista será responsable de gestionar con Enresa, anticipando a esta con el tiempo suficiente, todos los requisitos y procedimientos necesarios para dar cumplimiento en materia de normativa y control de auditorias respecto a la Autoridad de Registro delegada.

3.3 Custodia Centralizada de Certificados Cualificados

El contratista proporcionará un servicio de custodia centralizada y utilización de las claves privadas de los certificados electrónicos cualificados de Enresa de persona física y pertenencia a entidad y de representante de persona jurídica, integrado con el resto de los servicios de confianza que proporciona a Enresa, que permita realizar firmas cualificadas, con al menos las siguientes características:

- Un dispositivo seguro de creación y almacenamiento de claves mediante hardware criptográfico (HSM - Hardware Security Module).
- Un cliente-agente CSP (Crypto Service Provider) y licencias de uso durante la ejecución del contrato para todos los usuarios de Enresa, que permita el uso de los certificados electrónicos centralizados cualificados desde los equipos del usuario de manera análoga a como si los certificados estuvieran instalados en local. El CSP podrá ser distribuido mediante instalable MSI (Microsoft Installer) para versiones de 32 bits y 64 bits de Windows, o disponer de capacidades de despliegue y actualización mediante herramientas de despliegues centralizadas

y automáticas (como por ejemplo InTune), y deberá ser compatible con los navegadores Edge y Chrome.
- Integración con el Directorio Activo de Enresa (Microsoft Active Directory) para gestionar la autenticación de los titulares de los certificados.
- Posibilidad de habilitar mecanismos de segundo factor de autenticación basado en una clave temporal de un solo uso (OTP – One Time Password) recibida en al menos el dispositivo móvil y/o en el correo electrónico del firmante.

Para garantizar la seguridad y la trazabilidad de uso, los certificados cualificados custodiados mediante este servicio de custodia centralizada deberán generarse directamente a través del servicio, en la cuenta asociada de cada uno de los titulares o solicitantes del certificado. No se admitirán soluciones en las cuales la única alternativa sea la descarga previa del nuevo certificado en formato software y su posterior importación al servicio de custodia certificada.

3.4 Gestión y uso de Certificados Electrónicos

Para la gestión y uso de los certificados electrónicos cualificados de persona física y pertenencia a entidad y los de representante de persona jurídica, por parte de sus titulares, el contratista deberá proporcionar:

- Un portal web, con las siguientes características principales:
  - Accesible desde Internet, garantizando la seguridad en las comunicaciones.
  - Personalizado con la imagen corporativa de Enresa.
  - Integración con el directorio activo de Enresa (Microsoft Active Directory).
  - Incluirá al menos las siguientes funcionalidades para cada usuario:
    - Datos del titular.
    - Certificados electrónicos asociados.
    - Cambio de contraseña del certificado.
    - Opción de deshabilitar el certificado.
    - Opción de habilitar un segundo factor de autenticación. mediante clave temporal de un solo uso (OTP) para los procesos de firma del usuario.
    - Descarga de clave pública del certificado.
    - Reporte de auditoría del uso de los certificados por estado.
  - Posibilidad de disponer de una consola de administración y soporte del portal, con las siguientes funcionalidades:
    - Estadísticas de usuarios, certificados y firmas.
    - Reporte de información de usuarios y certificados asociados.
    - Configuración de permisos de usuarios, gestión de certificados, políticas de acceso y notificaciones.
    - Acceso a logs de auditoría y trazabilidad, para usuarios administradores, con al menos los siguientes datos: fecha y hora,

usuario, identificador del certificado, dirección IP o equipo desde el que se ha iniciado la operación, tipo de operación y resultado de la misma.

- Una sesión formativa para todo el personal de Enresa y creación de manuales de usuario final para el uso del portal web para la gestión de certificados y el proceso de firma.

4 REQUISITOS DEL SERVICIO

4.1.1 Prestador de Servicio de confianza cualificado

El contratista deberá acreditar en la reunión de lanzamiento del servicio y mantener durante toda la ejecución del contrato, ser un prestador de servicios de confianza cualificado, conforme el reglamento eIDAS, para ofrecer servicios de emisión de certificados cualificados de firma (QCert for Esig), y estar publicado en:

- La sede electrónica del Ministerio para la Transformación Digital y Función pública:

  https://sedeaplicaciones.minetur.gob.es/Prestadores/Inicio.aspx

- La lista de confianza de proveedores de servicios de certificación supervisados de los estados miembros de la Unión Europea:

  https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home

4.1.2 Soporte @firma

El contratista y todos los certificados emitidos en la prestación del servicio deberán estar incluidos en el Anexo – Proveedores de servicios de certificación de la plataforma @firma

https://sede.administracion.gob.es/PAG_Sede/LaSedePAG/SistemasFirmaAceptados.html

Este requisito deberá acreditarse en la reunión de lanzamiento del servicio y mantenerse durante toda la ejecución del contrato

4.1.3 Instalación y puesta en marcha del servicio

Serán responsabilidad del contratista la gestión de todas las tareas necesarias para el aprovisionamiento de todo el equipamiento técnico que se vaya a usar en la prestación

del servicio, así como para su instalación y puesta en marcha, incluyendo su configuración inicial.

4.1.4 Administración de la solución

El contratista realizará la configuración y administración de todas las soluciones hardware y software que emplee para la prestación del servicio objeto del contrato, considerando siempre que sea posible la aplicación de las mejoras prácticas sobre seguridad recogidas en las series de documentos "CCN-STIC" disponibles en la web del CERT del Centro Criptológico Nacional, adaptándose a las particularidades del contexto de Enresa.

4.1.5 Soporte y mantenimiento

El contratista proporcionará un servicio de soporte durante la ejecución del contrato, con capacidades para proporcionar soporte técnico y funcional a los operadores de la Autoridad de Registro, así como soporte técnico y de consultas relativas a la emisión de certificados, custodia centralizada de certificados cualificados, y gestión y uso de certificados electrónicos en Enresa.

El contratista proveerá una herramienta de gestión del servicio o ticketing, incluyendo todos los medios necesarios para su operación y sin que requiera ningún elemento adicional por parte de Enresa. Esta permitirá el tratamiento de todos las incidencias y peticiones relacionadas con el servicio.

Será responsabilidad del contratista el soporte y mantenimiento de todo el equipamiento o tecnología, tanto hardware como software y en cualquier modalidad de despliegue, que el contratista emplee para la prestación del servicio.

El servicio de soporte y mantenimiento se prestará conforme al horario enunciado en el apartado 6.2 "Horario de Prestación de los servicios".

4.1.6 Certificaciones

El contratista deberá aportar en la reunión de lanzamiento del servicio, como plazo máximo, y mantener durante la vigencia del contrato, las siguientes certificaciones:

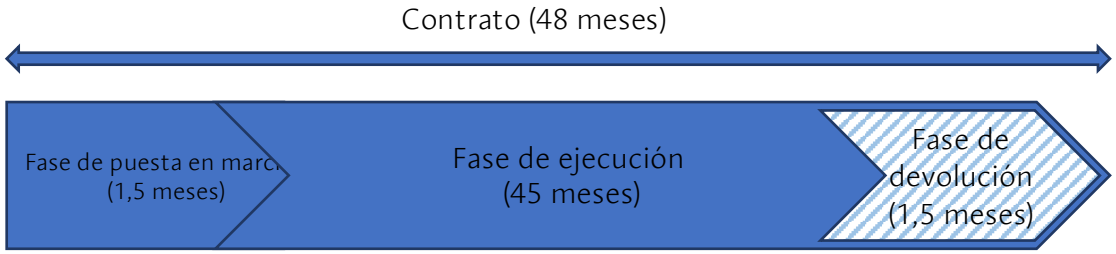
- Declaración o certificación de conformidad con el ENS nivel "medio" o superior, para los sistemas de información que dan soporte a la emisión y gestión de certificados digitales.

- Declaración o certificación de conformidad de la norma UNE-ISO/IEC 27001 – Seguridad de la información.

- Certificación de seguridad Common Criteria EAL4 o superior, o en su defecto certificación FIPS 140-2 o superior de NIST (National Institute of Standards and Technology) para el dispositivo seguro de creación y almacenamiento de claves mediante hardware criptográfico (HSM) que haga uso para el servicio de Custodia centralizada de certificados cualificados.

5 FASES DE PRESTACIÓN DEL SERVICIO

Para el correcto desarrollo de los servicios objeto del presente pliego se definen las siguientes fases de prestación del servicio: puesta en marcha, ejecución y devolución, que se definen a continuación.



5.1 Fase de puesta en marcha del servicio

La asunción y transición del servicio por parte del contratista **tendrá una duración máxima de 45 días naturales contados desde la fecha de formalización del contrato, finalizando en todo caso el 26 de Enero de 2025**.

El servicio durante esta fase será prestado por el anterior contratista, por lo que el nuevo contratista deberá convivir con él y realizar todas las actividades necesarias para implantar el servicio propuesto, sin pérdida de continuidad de los servicios que se prestan a Enresa.

El primer hito de esta fase será la reunión de lanzamiento, en los primeros 5 días hábiles tras el inicio del contrato, en la que se planificarán todos los trabajos para la implantación del servicio y que generará el siguiente entregable por parte del contratista:

- Presentación ejecutiva en formato PowerPoint del Plan de puesta en marcha del servicio, que contenga de manera específica la planificación de las actividades a realizar.

La finalización de la fase de puesta en marcha del servicio debe ser aceptada expresamente por Enresa, mediante un acta de aceptación firmada por las partes.

5.2 Fase de ejecución del servicio

Durante esta fase el contratista prestará el servicio con plena autonomía y responsabilidad conforme las actividades y requisitos establecidos.

La fase de ejecución del servicio por parte del contratista tendrá lugar desde la finalización de la fase anterior y hasta la finalización del contrato.

En esta fase el contratista deberá incluir, bien por sus propios medios o por terceros, la realización de las auditorías al servicio y a la autoridad de registro (RA) delegada en Enresa que legalmente sean necesarias.

5.3 Fase de devolución del servicio.

La fase de devolución del servicio tiene como objetivo garantizar la transferencia del conocimiento adquirido o generado durante la prestación del servicio por parte del contratista hacia Enresa, o hacia el nuevo contratista, sin que ello repercuta en una pérdida del control o del nivel de calidad del servicio.

En esta fase, el contratista estará obligado a devolver el control del servicio objeto de contratación, simultaneándose los trabajos de devolución con los de prestación del servicio regular, sin coste adicional.

El traspaso tendrá una duración máxima de 45 días naturales desde la notificación del inicio de esta fase y en todo caso durante el último mes y medio de contrato si se completa el tiempo de vigencia de este.

6 EQUIPO DE TRABAJO

El contratista designara:

- Un jefe de proyecto, que será el responsable de interlocución con Enresa y de la gestión del servicio, debe coordinar todas las actividades, los recursos humanos y la mejora en los procesos del servicio.
- Un responsable del servicio, cuya principal tarea será la interlocución y comunicación con el equipo directivo de Enresa.
- En aplicación del artículo 13 del Esquema Nacional de Seguridad, un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

El responsable del Servicio y el POC para la seguridad de la información, podrán ser la misma persona si el contratista así lo determina.

6.1 Lugar y prestación del servicio

Los trabajos se realizarán con carácter general en las instalaciones del contratista, si bien y conforme los requisitos establecidos en el pliego, el dispositivo seguro de creación y almacenamiento de claves mediante hardware criptográfico que se use para la custodia centralizada de certificados cualificados se podrá encontrar alojado en modalidad de cloud computing.

6.2 Horario de prestación de los servicios

El contratista deberá asegurar la disponibilidad del servicio para todas las actividades requeridas en el apartado 3 “Actividades” las 24 horas, los 7 días de la semana y los 365 días del año (modalidad 24x7), si bien el servicio de soporte y mantenimiento, requerido en el apartado 4.1.5 “Soporte y Mantenimiento”, se prestará dentro de la franja horaria de 9:00 a 17:00 de lunes a viernes (modalidad 8x5) en el uso horario peninsular de España, excepto para las incidencias clasificadas como de severidad **alta o crítica** que deberán prestarse en modalidad 24x7.

7 INFORMES

Con independencia de cualquier otro informe o entregable que se requiera en el ámbito de las actividades objeto del contrato, el contratista deberá presentar a lo largo de la fase de ejecución del servicio un informe mensual, que deberá ser enviado por el contratista al responsable del contrato designado por Enresa, y servirá como soporte para la facturación mensual, conteniendo al menos la siguiente información:

- Número de certificados electrónicos emitidos en el periodo de reporte.
- Número de certificados electrónicos emitidos acumulados durante la ejecución del servicio.
- Seguimiento de los Acuerdos de Nivel de Servicio.
- Seguimiento económico del contrato.
- Cualquier otro hito o hecho relevante que se haya producido durante el mes

8 PROPIEDAD INTELECTUAL

Durante la ejecución de los trabajos objeto del contrato el contratista se compromete, en todo momento, a facilitar a las personas designadas por la Dirección de Sistemas y Documentación de Enresa, la información y documentación que soliciten para tener pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

Toda la documentación generada durante la ejecución del contrato será propiedad exclusiva de Enresa, sin que el contratista pueda conservarla, ni obtener copia o facilitarla a terceros sin la autorización expresa y por escrito de Enresa.

9 SEGURIDAD

Enresa tiene establecida una Política de Seguridad que regula la gestión de la Seguridad de la Información en la organización, fundamentada en un Sistema de Gestión de la Seguridad de la Información (en adelante, SGSI), cuyo propósito es garantizar que los riesgos de la seguridad de la información son conocidos y gestionados por la organización, y en el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS).

Las medidas de seguridad a aplicar en los servicios objeto de este contrato y en los posibles sistemas de información desplegados serán las que correspondan del Anexo II del Esquema Nacional de Seguridad, en función de la categorización del sistema MEDIO, así como el Reglamento General de Protección de Datos (RGPD) y su normativa de desarrollo vigente, según la tipología de los datos e información gestionada.

El contratista dotará de todas las herramientas informáticas y de comunicaciones necesarias para el desarrollo de todas las actividades a todos los recursos asignados al servicio sean o no presenciales. Si se requiere acceso a los sistemas de información de Enresa, sólo está permitido previa solicitud y autorización por el Departamento de Sistemas y Tecnologías de la Información (DSTI), quien en función de las necesidades evaluará el método de acceso, que con carácter general exigirá un mecanismo de doble factor de autenticación para iniciar sesión en los sistemas.

Para los supuestos en los que se usen aplicaciones web para la prestación de las actividades del servicio, estás deberán implementar protocolos seguros cifrados de comunicación (https/ssl) asegurando la corrección de vulnerabilidades publicadas sobre los mismos.

El contratista, será responsable de que las soluciones y servicios que se presten a Enresa cumplen los requisitos de seguridad. Los daños y perjuicios causados a Enresa y a terceros, por las consecuencias derivadas en el entorno de la seguridad de los trabajos realizados en el ámbito de este contrato, serán responsabilidad del contratista.