PLIEGO DE CONDICIONES PARTICULARES. ABIERTO. LICITACIÓN ELECTRÓNICA.				
TITULO: CONTRATACIÓN PARA *ZIURTAPEN ETA ZERBITZU ENPRESA-EMPRESA DE CERTIFICACIÓN Y SERVICIOS, IZENPE S.A.* DEL SERVICIO DE EMISIÓN DE CERTIFICADOS SSL				SERVICIOS ☒ SUMINISTROS ☐ MIXTO ☐
Nº EXPEDIENTE	IZNP_S_003_2025	CPV	48825000-7	

Documento firmado digitalmente por:
IZASKUN URRESTARAZU AMUNDARAIN (24/07/2025 15:37 CEST), TONI SAEZ GONZALEZ (24/07/2025 15:38 CEST)

Contenido

1. OBJETO Y ALCANCE **¡Error! Marcador no definido.**
2. REQUISITOS DEL SERVICIOS 3
3. REQUISITOS FUNCIONALES 3
4. NIVELES DE SERVICIO (SLA) 4
5. PLAZO DE EJECUCIÓN 4

1. REQUISITOS DEL SERVICIOS

El servicio ha de contemplar la provisión de certificados SSL (DV, OV, Wildcard y EV) emitidos por una CA externa ya incluida en los Root Programs de los principales navegadores (Chrome, Mozilla, Safari, Edge).

El alcance incluye:

- Aprovisionamiento de una CA subordinada exclusiva a nombre de Izenpe que será la emisora de los certificados que solicite Izenpe.
- Api de servicios web para todas las funciones necesarias en el ciclo de vida de los certificados, como p ej para la Emisión, reemisión, renovación y revocación de certificados SSL.
- Cumplimiento normativo (CA/B Forum, ETSI/eIDAS, CCADB y root programas de los diferentes navegadores y sistemas operativos).
- Soporte técnico continuo durante la integración y operación del servicio.

2. REQUISITOS FUNCIONALES

- R1. Se generará una SUBCA a nombre de Izenpe firmada por la CA reconocida del prestador, que permita mantener el nombre de Izenpe como entidad emisora intermedia.
- R2. Tipos de certificados a emitir. El adjudicatario deberá permitir emitir como mínimo los siguientes tipos de certificados SSL:
    - SSL DV (Domain Validation) con uno o varios dominios.
    - SSL OV (Organization Validation) con uno o varios dominios.
    - SSL Wildcard DV y OV con uno o varios dominios.
    - Certificados Cualificados (EV).
- R3. Compatibilidad técnica. Los certificados deberán ser compatibles con todos los navegadores web (Chrome, Firefox, Safari, Edge) y sistemas operativos relevantes, incluyendo versiones móviles.
- R4. Alta disponibilidad de servicios validación (OCSP y/o CRL).
- R5. Los certificados deberán cumplir con los últimos perfiles técnicos definidos en los Baseline Requirements y políticas del CA/Browser Forum así como los root programs de los navegadores web, Sistemas Operativos (Mozilla, Google, Apple, Microsoft), incluyendo versiones móviles.
- R6. Soporte a automatización mediante protocolo ACME (RFC 8555) y, si aplica, ACME Renewal information (ARI).
- R7. El adjudicatario deberá proporcionar una API REST o SOAP que permita a Izenpe:
    - Solicitar, renovar y revocar certificados.

- Consultar estado de certificados y operaciones.
- Acceder a logs de actividad.
- Gestionar notificaciones de caducidad.

La API deberá estar disponible en entorno de pruebas y en entorno productivo, valorará positivamente la disponibilidad de SDKs o librerías en distintos lenguajes (Java, Python, .NET).

– R8. El adjudicatario debe estar acreditado como Qualified Trust Service Provider (QTSP) según eIDAS o normativa equivalente.

3. NIVELES DE SERVICIO (SLA)

El adjudicatario se compromete a los siguientes niveles de servicio:

- Disponibilidad mensual del servicio superior al 99,9%.
- Tiempo de emisión de certificados inferior a 30 minutos desde la solicitud válida.
- Disponibilidad de soporte técnico durante el horario laboral como mínimo, con resolución de incidencias críticas en menos de 4 horas.

4. PLAZO DE EJECUCIÓN

El servicio deberá estar completamente operativo y validado por Izenpe antes del 31 de diciembre de 2025, incluyendo la integración técnica, pruebas funcionales y generación de primeros certificados.

Técnico Responsable del Contrato: D. Toni Sáez González

Órgano de Contratación: Dª. Izaskun Urrestarazu Amundarain