



**Mutua
Montañesa**
Mmuy fácil

Pliego Técnico

Servicio de Certificados Wildcard OV SSL



1. INTRODUCCIÓN	3
2. CERTIFICADOS SSL	4
2.1. OBJETO	4
2.2. ALCANCE	4
2.3. REQUISITOS TÉCNICOS.....	4
2.3.1. <i>Aspectos generales</i>	4
2.3.2. <i>Entidad emisora</i>	5



1. INTRODUCCIÓN

Mutua Montañesa requiere para su operativa el Servicio de certificación que se realizará a través de los siguientes productos:

- Certificados SSL wildcard

2. CERTIFICADOS SSL

Mutua Montañesa necesita contar con un servicio de certificados web, que se utilizan para establecer una conexión segura a los sitios y servicios web de la organización.

En la actualidad cuenta con un certificado OV wildcard para el dominio mutuamontanesa.es emitido por la entidad Entrust a través del proveedor Sistemas Informáticos Abiertos S.A.U

Los certificados SSL son un elemento imprescindible para garantizar la seguridad en el intercambio de información entre los sitios Web, siendo el medio que permite el cifrado de las comunicaciones entre ambos extremos, para garantizar su privacidad e integridad.

En la actualidad es necesario disponer de certificados web. Las páginas que no disponen de un certificado web se muestran como "no seguras" en los navegadores principales, como pueden ser Chrome o Firefox.

2.1. OBJETO

El objeto del presente procedimiento es establecer las condiciones técnicas que regirán la contratación Servicio de Certificados Wildcard OV SSL.

En este pliego técnico se recogen los requisitos mínimos tanto de la entrega inicial como de los pedidos posteriores, bajo demanda en función de las necesidades.

De manera general el servicio de referencia incluirá:

- El suministro de certificados web.
- El Portal de Gestión del Servicio.
- Contacto telefónico y/o por correo electrónico 24x7 con un asesor técnico personalizado nominal.

2.2. ALCANCE

Se estima el servicio para 4 años del certificado de la siguiente tipología y cantidad:

- 1 certificado Wildcard OV con el servicio del portal de gestión del mismo y un asesor técnico.

2.3. REQUISITOS TÉCNICOS

2.3.1. ASPECTOS GENERALES

Todos los requisitos enumerados son de cumplimiento obligatorio. Las ofertas que ofrezcan características que no se ajusten a estos requisitos no serán tomadas en consideración en el presente procedimiento de licitación.

Se debe disponer de un panel de gestión web de la entidad emisora en el que visualizar las unidades de certificado disponibles, así como descargar los certificados emitidos, CSR y certificados de CA.

El servicio debe permitir la validación/aprobación de dominios sobre los que se solicitarán los certificados necesarios. Esta prevalidación debe permitir la emisión más ágil, o incluso instantánea, de los certificados de los dominios preaprobados.

El servicio debe disponer de un asesor técnico personalizado, con contacto telefónico y/o por correo electrónico **en español**, así como disponer de soporte técnico 24x7.

Debe ser posible o bien solicitar al asesor la emisión de los certificados, enviando el correspondiente CSR o poder hacer la gestión directamente a través de la web de la entidad emisora. La emisión de certificados deberá ser automática o semiautomática en el caso de certificados de dominios previamente validados/aprobados.

Los certificados tendrán una duración mínima de 1 año, y se podrán renovar anualmente. En el caso de renovaciones, el año deberá ser adicional y empezar a contar a partir de la fecha de vencimiento del certificado en cuestión.

2.3.2. ENTIDAD EMISORA

Tanto si la oferta es presentada por la entidad emisora, como si es presentada a través de un partner, reseller o similar, todos los certificados deben ser de la misma entidad emisora de certificados, o de la misma marca.

Se requiere que la entidad emisora de certificados pueda emitir certificados del tipo QWAC (Qualified Website Authentication Certificate), en conformidad con el reglamento europeo eIDAS, por lo que será una información que deberá aportarse antes de la adjudicación.

El licitador debe indicar en su oferta la entidad emisora o marca que propone para los certificados, que se comprobará que se encuentra en alguno de los siguientes:

- Listado de QTSPs (Qualified Trust Service Providers) de España (<https://webgate.ec.europa.eu/tl-browser/#/tl/ES> // <https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/ES>) para el servicio **QWAC - Qualified certificate for website authentication.**
- Relación de prestadores de servicios electrónicos de confianza cualificados (<https://sedeaplicaciones.minetur.gob.es/Prestadores/>), en el apartado Servicios electrónicos de confianza cualificados Servicio de expedición de certificados electrónicos cualificados de autenticación de sitios web.

Se deberá poder preaprobar la validación del dominio mutuamontanesa.es de cara a agilizar la posterior emisión y renovación de certificados bajo ese nombre de dominio y los subdominios que de él se requiera

Adicionalmente la entidad emisora deberá cumplir con las siguientes características/servicios:

- Asistencia de expertos 24/7
- Licencias de servidor ilimitadas
- Garantía de devolución del dinero de 30 días
- Garantía de 1 000 000 \$ para certificados SSL
- Incluye el sello de confianza de de la entidad registradora
- Notificación de expiración.
- Certificados con cumplimiento X.509.
- Reediciones ilimitadas gratuitas, que se podrán realizar con o sin renovación de las claves.
- Certificados web compatibles con navegadores Internet Explorer, Firefox y Chrome sin requerir la instalación de certificados raíz adicionales.
- Portal de Gestión del Servicio directo de la Entidad Emisora, no se admitirá la gestión a través de un portal intermedio del partner.
 - El portal de gestión del servicio debe ser proporcionado dentro del portal de gestión de la entidad emisora, o de la empresa perteneciente a la marca de la entidad emisora, con las máximas medidas de seguridad.



- Se valorará que sea posible disponer de varios usuarios gestores.
-
- Soporte técnico, telefónico y/o por correo electrónico, 24x7.
- Asesor técnico personalizado en español que podrá formar parte de la organización de la entidad emisora o del reseller/partner que se presente a la licitación

2.3.2.1. Características específicas de certificados Wildcard

El certificado Wildcard ofertado deberá cumplir las siguientes características mínimas

- Certificados con validación de organización (OV), en los que se verifica la identidad de organización.
- Cifrado de 256 bits.
- Algoritmo SHA-2 de clave pública RSA (al menos, compatible con funciones hash: 256)
- Criptografía de clave pública ECC (al menos, compatible con funciones hash: 256)
- Compatible con cifrado de clave pública de 2048 bits o superior.
- Asegurar un dominio y todos sus subdominios de primer nivel. (mutuamontanesa.es y *.mutuamontanesa.es)