INFORMACIÓN ADICIONAL AL CONTENIDO DEL PLIEGO TÉCNICO PARA LA RENOVACIÓN DE CERTIFICADO WILDCARD SSL (EXPTE. CG-2025/5101/0032)

1. Reconocimiento por el Ministerio de Industria

La entidad que emita los certificados SSL (es decir, el Prestador de Servicios Electrónicos de Confianza) debe estar registrada y supervisada por el Ministerio de Asuntos Económicos y Transformación Digital.
El Prestador de Servicios deberá estar incluido en la "Lista de confianza de prestadores cualificados de servicios electrónicos de confianza" (TSL), que incluye a aquellos que proporcionan servicios cualificados y están establecidos y supervisados en España, a la que pueda accederse desde la siguiente URL:

https://sede.serviciosmin.gob.es/prestadores/paginas/inicio.aspx

2. Uso de ECMS para la gestión de certificados

Los certificados SSL deberán utilizar un ECMS para su gestión al ser recomendable su utilización para disponer de ventajas como mejorar el control de acceso y la auditoría de los certificados o la automatización de su ciclo de vida.

3. Validación pública del Certificado y del Dominio

El certificado SSL deberá haber sido emitido por una Autoridad de Certificación (CA) reconocida globalmente, la cual forme parte de una cadena de confianza aceptada por navegadores, sistemas operativos y dispositivos móviles. De esta forma el certificado será válido y confiable para cualquier usuario que acceda al sitio web sin que aparezcan advertencias de seguridad.
Que el dominio esté validado públicamente significa que el proceso de emisión del certificado incluya una verificación pública de la propiedad del dominio. En la práctica existen tres niveles de validación: DV (Domain Validation), OV (Organization Validation) y EV (Extended Validation).

El certificado debe ser debe ser aceptado por cualquier navegador sin mostrar advertencias de seguridad.

4. Validez del Certificado

El certificado solicitado tendrá una validez inicial de un año y deberá renovarse cada año hasta finalizar el contrato, ya que la duración de 1 año es una limitación temporal impuesta de facto por navegadores como Google Chrome, Mozilla Firefox, Apple Safari y Microsoft Edge.

5. Acreditación de la capacidad para el suministro

Para acreditar la capacidad de emitir certificados SSL como revendedor o proveedor del servicio, es suficiente presentar un contrato con la Autoridad de Certificación con la que se trabaje, adjuntando adicionalmente el Certificado de Partner (siempre y cuando la entidad emisora otorgue esta certificación como partner).

6. Condiciones de soporte

- En ningún caso se accederá directamente a los sistemas de Cesma.
- Proporcionar indicaciones sobre cómo instalar el certificado SSL en diferentes servidores y entornos.
- Recibir notificaciones previas a la expiración del certificado con cierto tiempo de margen.
- Apoyo por si surge alguna incidencia en las renovaciones de los certificados o durante algún proceso de revocación que deba ser llevado a cabo.
- Asistencia en la validación del Dominio y resolución de problemas si la CA rechazara la solicitud.

Ceuta 6 de febrero 2025

Departamento informática Cesma.

75165480P ROCIO SEVILLA (C:G11901808)

Firmado digitalmente por 75165480P ROCIO SEVILLA (C:G11901808)
Fecha: 2025.02.06 11:16:18 +01'00'