Junta de Andalucía

Agencia Digital de Andalucía
Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa

SOLICITUD DE CERTIFICADO DE SELLO ELECTRÓNICO

1. DATOS DE LA PERSONA SOLICITANTE [1]

ÓRGANO SOLICITANTE: (máx. 64 caracteres)	NIF:
NOMBRE Y APELLIDOS RESPONSABLE:	NIF:
CARGO:	
NOMBRAMIENTO BOJA:	
CORREO ELECTRÓNICO:	TELÉFONO:
DIRECCIÓN POSTAL:	

2. DATOS DEL CERTIFICADO [2]

USO DEL CERTIFICADO:	
JUSTIFICACIÓN NECESIDAD DE FIRMA ELECTRÓNICA AUTOMATIZADA:	
NOMBRE Y APELLIDOS RESPONSABLE:	NIF:
PUESTO:	
NOMBRAMIENTO BOJA:	
CORREO ELECTRÓNICO:	TELÉFONO:
ÓRGANO RESPONSABLE EFECTOS IMPUGNACIÓN[3]:	

3. DATOS DEL RESPONSABLE TÉCNICO [4]

NOMBRE Y APELLIDOS:	NIF:
CORREO ELECTRÓNICO:	TELÉFONO:

4. LUGAR, FECHA Y FIRMA

SOLICITO la expedición del certificado de servidor seguro emitido por FNMT-RCM y declaro conocer y aceptar las Condiciones de utilización, así como lo dispuesto en la Declaración General de Prácticas de Servicios de Confianza y de Certificación electrónica del prestador. (5)

En , a de de

Firma electrónica del solicitante: [6][7]

NOTAS

(1) La persona solicitante debe ser el titular del órgano para el que se solicita la expedición del certificado. Los datos indicados en los campos Órgano solicitante y el NIF asociado se incluirán en el certificado emitido.

(2) Datos relacionados con la finalidad y uso que se hará del certificado, siendo el responsable la persona titular del Servicio de Informática correspondiente o la persona titular del centro directivo con competencias TIC, responsable de la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente conforme a lo especificado en el art. 41.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. El certificado emitido tendrá como asunto (CN) el nombre del órgano para el que se emite el certificado. Los certificados emitidos tendrán una vigencia de 3 años.

(3) Es necesario indicar el órgano responsable a efectos de impugnación conforme a lo indicado en el art. 41.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

(4) Persona encargada de las tareas técnicas relacionadas con la gestión técnica del certificado.

(5) 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 en las transacciones electrónicas en el mercado interior (eIDAS), establece un marco legal común para los prestadores de servicios de confianza cualificados a la hora de emitir certificados digitales de confianza.

Adicionalmente a las características generales establecidas en la CPS, cada tipo de certificado emitido por FNMT-RCM se describe en detalle en un documento denominado «Política de Certificación» (en inglés CP o Certificate Policy), que recoge las características particulares del mismo.

Existe una política de certificación por cada tipo de certificado emitido que se puede consultar en la siguiente dirección:

https://www.sede.fnmt.gob.es/normativa/declaracion-de-practicas-de-certificacion

(6) El formulario debe ser firmado electrónicamente por el solicitante indicado en el apartado 1 mediante la herramienta Port@firmas o Adobe Reader.

(7) Las solicitudes deben ser remitidas a través de la herramienta de gestión de incidencias NAOS, en el servicio "Administración Electrónica", componente "Gestión de certificados de servidor y sello electrónico". Deben ir acompañadas de un fichero de texto plano con el Certificate Signing Request (CSR). **Las claves deben generarse con algoritmo RSA de longitud 2048.**

Se recomienda para la generación de claves la herramienta proporcionada por el prestador

:https://www.cert.fnmt.es/componente/generacion-claves

Posteriormente se puede utilizar la misma herramienta para unir la clave privada generada y el certificado remitido por el prestador.