

SOLICITUD EN LA PLATAFORMA @FIRMA DE LA ADMINISTRACIÓN PÚBLICA DE LA JUNTA DE ANDALUCÍA

TIPO SOLICITUD: ALTA BAJA MODIFICACIÓN
ENTORNO: PRUEBAS PRODUCCIÓN

1 DATOS DE LA PERSONA SOLICITANTE	
APELLIDOS Y NOMBRE	DNI
TELÉFONO	CORREO ELECTRÓNICO
CONSEJERÍA/AGENCIA/ORGANISMO	

2 DATOS DE LA APLICACIÓN	
NOMBRE/IDENTIFICADOR	
DESCRIPCIÓN DE LA APLICACIÓN	
EN CASO DE QUE LA APLICACIÓN ACCEDA DESDE FUERA DE LA RCJA, INDICAR IP DE ACCESO: (sólo entorno de pruebas)	
APELLIDOS Y NOMBRE DEL RESPONSABLE TÉCNICO DE LA APLICACIÓN ⁽¹⁾	
TELÉFONO DE CONTACTO DEL RESPONSABLE TÉCNICO	CORREO DEL RESPONSABLE TÉCNICO
SELLADO DE TIEMPO <input type="checkbox"/> Con sello de tiempo ⁽²⁾ <input type="checkbox"/> Sin sello de tiempo	TIPO APLICACIÓN <input type="checkbox"/> Nuevo desarrollo <input type="checkbox"/> Ya existente
TIPO DE AUTORIZACIÓN DE ACCESO A LOS SERVICIOS WEB: <input type="checkbox"/> Mediante usuario/contraseña <input type="checkbox"/> Mediante certificado electrónico ⁽³⁾	Fecha prevista de puesta en producción: Volumen aproximado de accesos/día:

3 TIPOS DE SERVICIO DE @FIRMA SOLICITADOS	
Módulo de autenticación: <input type="checkbox"/> Fachada de autenticación por ticket ⁽⁴⁾ <input type="checkbox"/> Autenticación basada en el cliente de firma ⁽⁵⁾	Módulo de validación: ⁽⁶⁾ <input type="checkbox"/> Validación de firmas <input type="checkbox"/> Validación de certificados <input type="checkbox"/> Actualización de firmas
Módulo de firma: <input type="checkbox"/> Firma delegada ⁽⁷⁾	

4 DECLARACIÓN Y SOLICITUD
<p>La persona firmante DECLARA que son ciertos cuantos datos figuran en este formulario, que se han atendido y atenderán las guías y directrices en materia de certificados electrónicos y firma electrónica, en particular en lo relativo a la no utilización de componentes que no forman parte de la plataforma, de servicios obsoletos, de custodia de ficheros en la plataforma o cuya desaparición esté prevista para futuras versiones, y a formatos de firma electrónica, que los ficheros a firmar no contendrán contenido dinámico que afecte a su validez y que pudiese modificar el resultado de la firma a lo largo del tiempo, que no se remitirán ficheros de contenido a la plataforma aunque no se custodien en la misma o estén incluidos en las firmas electrónicas, que se han realizado las pruebas de carga precisas para garantizar un correcto y satisfactorio funcionamiento, y SOLICITA el alta/baja/modificación de la aplicación, en el ámbito y alcance definidos para la identificación y firma electrónica mediante certificados electrónicos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica y la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración.</p> <p>En a de de</p> <p>(Sello) EL/LA (cargo)</p> <p>Fdo.:</p>

(1) Personal del servicio o unidad con competencias TIC de la Consejería o entidad.
(2) Restringido a aplicaciones, servicios, sistemas, etc. a los que no les corresponda una categorización de nivel alto para la dimensión de seguridad de trazabilidad y la medida 5.7.5 del Anexo II del Esquema Nacional de Seguridad. La aplicación deberá realizar una operación dssAfirmaUpgrade de actualización de firma y verificar su correcta realización.
(3) Una vez aceptada la solicitud se le requerirá que aporte el certificado de componente o servidor. Para el entorno de producción deberá utilizarse un certificado emitido para este propósito y emitido por FNMT-RCM. No se aceptarán certificados emitidos por otros prestadores ni certificados wildcard.
(4) La integración con la fachada de tickets deberá realizarse mediante la librería "afirma-authentication-client" del Kit de Integración.
(5) La autenticación mediante el cliente de firma electrónica debe respetar las indicaciones recomendadas en el documento "Buenas prácticas de seguridad en los procesos de autenticación y firma" disponible en la Web de Soporte a la Administración Electrónica.
(6) Las funcionalidades de acceso al módulo de validación de @firma se realizarán mediante la librería "afirma-dss-client" del Kit de Integración.
(7) La funcionalidad de firma delegada o firma de servidor se realizará mediante la librería "afirma-signer-delegate" del Kit de Integración.