SERVICIO DE FIRMA ELECTRÓNICA CERTIFICADA PARA DOCUMENTOS DE IFEMA

EXP. 20/171 - 2000017802

Pliego de Prescripciones Técnicas

Índice

1. Objeto

El objeto del presente contrato es el servicio de firma electrónica certificada para documentos de IFEMA. Un servicio que ahorre tiempo y costes en la obtención de documentos firmados conjuntamente tanto por personas de IFEMA como por terceros, con todas las garantías jurídicas de integridad y autenticidad, equivalentes a todos los efectos a las firmas manuscritas, pero sin papel.

Este servicio debe permitir tanto el uso manual como automático de todo el proceso: desde el envío de documentos a firma por internet, la obtención de las firmas válidas y la entrega de los documentos correctamente firmados a todos los interesados.

Debe ser un servicio que incorpore las medidas de seguridad solicitadas en el apartado 2.1, que ofrezca la máxima facilidad y conveniencia para que los partícipes puedan firmar desde cualquier lugar y con cualquier dispositivo, con la mira puesta en la eficiencia, la confidencialidad, la disponibilidad y la integridad. En particular, debe contar con medidas de seguridad que impidan el uso no autorizado de los certificados digitales de las personas de IFEMA. En definitiva, debe ser un servicio en el que IFEMA pueda depositar toda su confianza.

2. Alcance

2.1. Aplicación o portal web para el uso manual del servicio

Se solicita una aplicación, preferiblemente web, que permita a IFEMA la obtención de documentos firmados tanto por personas de IFEMA como por terceros. La solución ofrecida permitirá a los usuarios autorizados de IFEMA el acceso seguro a todas sus funcionalidades con cualquier navegador e impedirá los accesos no autorizados con medidas como las que se solicitan más adelante.

Todos los datos relacionados con IFEMA que contenga la solución tienen la consideración de datos sensibles y confidenciales de IFEMA. Por tanto, deben contar con el nivel de protección frente accesos no autorizados requeridos en este pliego. En particular, los certificados digitales de IFEMA que sea preciso configurar en la solución, deben estar protegidos de modo que no sea posible su uso no autorizado.

La solución incorporará como mínimo los procedimientos y las medidas de seguridad que se solicitan a lo largo de este documento, las que indica el apartado 2.1.1 y las que indica el Anexo para contratos de bienes y servicios con elementos relacionados con TI

La oferta indicará las medidas de seguridad y procedimientos con que cuenta la solución para impedir el acceso no autorizado a los datos y certificados digitales de IFEMA y a la propia aplicación. Por ejemplo, indicará dónde se encuentran los datos y certificados digitales, cómo se protegen, qué impide los accesos no autorizados, qué medidas de seguridad protegen los accesos, documentos, datos y certificados, qué medidas de autenticación tiene la aplicación, qué políticas de contraseñas tales como longitud y complejidad, bloqueos por números de accesos incorrectos, caducidad de contraseñas, etc. En todo caso, esas medidas y procedimientos deberán cumplir estrictamente, como mínimo, los requerimientos contenidos en el presente pliego, pudiendo incorporar la oferta medidas o requerimientos adicionales dirigidos a garantizar la seguridad y el buen funcionamiento de la aplicación.

El adjudicatario incorporará a la solución, con la conformidad de IFEMA, las medidas de seguridad necesarias para garantizar la seguridad frente a nuevas amenazas.

La solución contará al menos con los siguientes roles principales para sus usuarios:

- Rol para usuarios que desencadenan manualmente los procesos de firma, especificando los documentos y los firmantes. En adelante usuarios remitentes.
- Rol para los usuarios de IFEMA que firman los documentos con su propio certificado digital de persona física o jurídica. En adelante, usuarios firmantes internos.
- Rol para resto de usuarios, excluyendo firmantes internos, que deban firmar documentos. En adelante, terceros firmantes.

La aplicación propuesta debe contar con un procedimiento y unas medidas de seguridad adecuadas para impedir el acceso no autorizado a cualquiera de sus elementos tales como los documentos que contenga, los certificados digitales de los usuarios de IFEMA, sus funcionalidades, sus logs, etc.

En particular, sin que sea una enumeración cerrada, la oferta debe contener, al menos:

* Medidas de seguridad específicas para el acceso autenticado a la plataforma. Por ejemplo, políticas de longitud mínima de las contraseñas, complejidad y tiempo de validez de las mismas o la exigencia de doble factor de autenticación.

* Medidas de seguridad adecuadas para impedir el acceso ilícito, los intentos de adivinar contraseña y los ataques de diccionario. La aplicación permitirá configurar el número de reintentos no válidos de autenticación y el período entre los mismos, tras los cuales se debe bloquear la cuenta del usuario relacionada.

* Un procedimiento para desbloquear las cuentas bloqueadas, que permita que los usuarios legítimos puedan trabajar con pocas molestias pero que impida eficazmente los accesos no autorizados. En caso de incidencias con el acceso (bloqueo de cuenta, olvido de contraseña, etc.), un usuario legítimo debe poder acceder a la plataforma en menos de cuatro horas. En particular, la plataforma debe contar con procedimientos tales como desbloqueo automático tras un tiempo prudencial configurable de 15 minutos o más, email para la activación de la cuenta bloqueada a la dirección predefinida del usuario, teléfono de soporte, preguntas de seguridad con respuestas predefinidas, o cualquier procedimiento con una agilidad y eficiencia similar.

El adjudicatario deberá incorporar lo antes posible las mejoras en asuntos de seguridad que surjan en el futuro y que sean necesarias y adecuadas para impedir las amenazas y los ataques que puedan surgir de forma destacada y que ahora mismo no se pueden prever.

La aplicación funcionará en infraestructura que cuente con medidas que garanticen la confidencialidad de todos los elementos de la aplicación, datos, configuraciones, certificados, etc. respecto de otros clientes y usuarios de la misma infraestructura; medidas para recuperar la integridad de todos los elementos de la aplicación en caso de borrado, corrupción, o pérdida y Con medidas para garantizar una disponibilidad elevada y recuperarla lo antes posible en caso de incidente que impida su funcionamiento. El licitante incluirá en su oferta las explicaciones y evidencias que acrediten la conformidad y adecuación de su oferta en materia de seguridad a lo solicitado en este párrafo. Estas medidas y procedimientos deben poder recuperar en menos de 4 horas la disponibilidad y consistencia de la solución a una situación existente como máximo 24 horas antes del incidente.

La oferta deberá incluir la monitorización de los logs de accesos para identificar intentos ilícitos de acceso y la toma de medidas para mitigarlos. En particular y a modo de ejemplos, la oferta debe incluir la detección de los ataques de diccionario - tras lo que se averiguará la ubicación geográfica de las direcciones IPs y, si procede, se impedirá la comunicación desde dichas IPs- y

de los intentos de explotar vulnerabilidades en la aplicación web, así como la adopción de todas las medidas necesarias para mitigarlas.

Asimismo, el adjudicatario debe estar abierto a realizar modificaciones y mejoras en un tiempo aceptable en el funcionamiento de la aplicación, que sean razonables y de interés para IFEMA. Por ejemplo, cambios que faciliten la usabilidad o que mejoren la imagen de IFEMA y de sus documentos firmados ante terceros. Toda modificación que supere una jornada de esfuerzo se valorará aparte: el adjudicatario presentará presupuesto que deberá ser aprobado por IFEMA.

2.1.1. Seguridad

La oferta describirá las medidas de seguridad que permiten autenticar y acceder a los usuarios de cualquier tipo: remitentes, firmantes internos, administradores, etc. junto con las medidas que impiden el acceso ilícito a la plataforma, que deberán cumplir todos los requerimientos contenidos en el presente pliego. Las medidas deberán poder ser configuradas adecuadamente por el servicio de soporte del adjudicatario solo a petición de IFEMA. La aplicación propuesta debe permitir configurar, el número de reintentos tras los cuales se bloquea el acceso, la longitud y la complejidad de las contraseñas, el uso de un segundo factor de autenticación, y cualquier otro elemento necesario para lograr el equilibrio adecuado entre seguridad y usabilidad.

2.1.2. Usuarios remitentes

Los usuarios remitentes son los que tramitan los documentos que han de ~~a~~ firmar los usuarios firmantes, tanto internos como terceros. A continuación, se describen las funciones y el modo de funcionamiento que debe tener la aplicación que se solicita para los miembros del rol de usuarios remitentes.

Se solicita una aplicación, preferiblemente web, para los usuarios remitentes.

La aplicación contará con las funcionalidades necesarias para realizar envíos de documentos a firma, consultar el estado de los envíos realizados e incluso cancelar los envíos cuando su estado así lo permita.

La aplicación ofrecida debe permitir al usuario remitente configurar con facilidad el envío correcto del documento a la firma, tanto en lo que se refiere a los elementos principales, tales como la identificación de los documentos que forman parte del envío o quienes son los destinatarios con sus datos de contacto, como en lo que se refiere a los detalles de aspecto y usabilidad que se solicitan a continuación.

Por defecto, el envío a firma se producirá en cuanto esté completamente bien configurado.

El formato de los documentos a firmar será PDF en general. Se prevé que la mayoría de ellos tendrán concretamente formato PDF generados con MS Word de Office 365.

Aspecto, usabilidad:

La aplicación debe cumplir los siguientes requerimientos de aspecto y usabilidad:

Debe ser configurable el número de mensajes de recordatorio que recibirán los usuarios firmantes que no hayan firmado transcurrido un período, también configurable.

Debe ser configurable también la posición de las firmas en los documentos. Es decir, el usuario remitente debe poder especificar la ubicación en la que aparecerán en los documentos una vez firmados los detalles identificativos de los firmantes y de sus firmas.

Debe permitir que La cantidad de firmantes de un envío sea solo uno o más de uno, indiferentemente del tipo de usuarios firmantes internos o terceros. El caso previsto más frecuente son los envíos para dos firmantes: uno interno y otro externo, si bien la plataforma debe admitir la firma sea cual sea el número de firmantes.

El orden de firma debe ser configurable en los envíos con varios firmantes: los firmantes internos se podrán configurar como los últimos para que no reciban notificación ni documento pendiente de firma alguno hasta que todos los firmantes externos hayan firmado correctamente.

Debe ser sencillo para el usuario remitente encontrar los datos más relevantes que faciliten su trabajo habitual. En particular y a modo de ejemplo, Debe ser sencillo-consultar y encontrar los datos de los terceros firmantes de alta más reciente o conocer el estado de los envíos pendientes, cuántas notificaciones ha recibido cada firmante, si llegaron o no a su destinatario y el motivo -email o teléfono incorrecto-, etc.

Los mensajes de error de la aplicación para el usuario remitente deben ser claros y permitirle identificar y corregir por sí mismo la causa del error.

2.1.3. Usuarios firmantes internos

Los usuarios firmantes internos son los usuarios de IFEMA, normalmente altos cargos de la organización, que deben firmar los documentos que se les remita a firmar con su propio certificado digital de persona física o de persona jurídica.

Se solicita una aplicación, preferiblemente web, para los usuarios firmantes internos a la que accederán de forma segura para realizar su cometido.

Se requiere que la aplicación sea sumamente sencilla y que presente una usabilidad elevada para el usuario firmante interno. Para ello, debe cumplir, al menos, los requerimientos que se identifican a continuación:

La aplicación deberá mostrar al usuario firmante interno la lista de los documentos que tiene pendientes de firmar nada más acceder, sin pantallas intermedias ni requerimientos de claves adicionales.

En el caso de que en un envío a firma se haya configurado al usuario firmante interno como el último en firmar, lo cual será el caso más habitual, la aplicación no le mostrará los documentos pendientes de firmar por parte de otros usuarios. No obstante, la aplicación debe garantizar el acceso por los usuarios autorizados a esta documentación.

El usuario firmante interno podrá leer detenidamente uno por uno los documentos pendientes de firma cuantas veces sea necesario, accediendo en cuantas ocasiones lo necesite y con el dispositivo o navegador moderno que prefiera. Por ejemplo, PC, iPad, Chrome, Safari, etc.

El usuario firmante interno debe poder seleccionar con facilidad uno, varios o todos los documentos de su lista de documentos pendientes para rechazar o firmar todos los documentos seleccionados con una sola operación, tras la cual, desaparecerán de su lista de documentos pendientes. La operación más frecuente prevista es la de seleccionar varios o todos los documentos de la lista de pendientes y firmarlos de una sola vez, independientemente del número de documentos que contenga la selección. Es decir, firmar muchos documentos a la vez al final no debe ser una operación tediosa ni que requiera mucho más esfuerzo por parte del usuario firmante interno que firmar sólo un documento.

La plataforma permitirá con facilidad y de forma segura la incorporación o supresión de los certificados de firma electrónica obrantes.

Seguridad

Los certificados digitales de persona física o jurídica de los usuarios firmantes internos deben contar con la máxima protección frente a un uso no autorizado.

En el caso en que la solución propuesta requiera que el certificado digital de persona física o jurídica del usuario firmante interno se instale en la plataforma del adjudicatario, se indicarán en la oferta las medidas de seguridad que impiden el acceso, el uso y la obtención de copias de dicho certificado digital. IFEMA considerará aceptable la solución ofrecida en el caso que dichas medidas de seguridad sean adecuadas y no dejen lugar a dudas que se ha mitigado la amenaza del uso ilícito del certificado digital de persona física de un usuario firmante interno. Se consideran medidas adecuadas y suficientes, entre otras:

- Que no hubiese nunca copia del certificado digital en la plataforma del adjudicatario.
- En el caso de que haya copia del certificado en la plataforma del adjudicatario, que el uso de la clave privada esté protegido por su propio PIN o contraseña y sin almacenarlo junto con el certificado.

En el caso de que las medidas de seguridad propuestas sean diferentes de las dos anteriores sugeridas, el ofertante deberá, a requerimiento de IFEMA, completarlas o sustituirlas a su satisfacción.

2.1.4. Terceros firmantes

La plataforma ofrecida permitirá que los terceros puedan firmar con cualquiera de los siguientes tipos de firma electrónica, que deberán cumplir, en todo caso, los requisitos legalmente establecidos para su validez:

1. Con una firma electrónica avanzada basada en un certificado expedido por un prestador de servicios de certificación conforme a la Ley 59/2003, de firma electrónica (LFE).

En este caso, la aplicación ofrecida deberá ser capaz de realizar las comprobaciones necesarias para asegurar que la firma es correcta. En particular comprobará, al menos:

- Que el certificado procede de un prestador de servicios de certificación cuya información conste en la correspondiente dirección de internet de la Administración General del Estado a la que se refiere el artículo 30.2 LFE
- Que el propio certificado digital sea válido, que no esté revocado, que no haya expirado su período de validez.

El fallo de cualquiera de estas comprobaciones es un evento de seguridad del que IFEMA debe tener en seguida un dictamen del adjudicatario con todos los detalles para comprender si se trata de un fallo de operación o de un intento delictivo de fraude en el acto de la firma.

2. Con otro tipo de firma electrónica que pueda considerarse avanzada, de conformidad con la LFE que la define como la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su exclusivo control. En

particular, ha de ser una firma electrónica con autenticación de doble factor, email y mensaje en el móvil.

Cualquiera que sea el tipo de firma electrónica utilizado, la plataforma debe garantizar que el contenido de los documentos a firmar no puede ser modificados en forma alguna una vez incorporados a la plataforma y hasta el momento en que se firman.

La plataforma propuesta deberá permitir la tramitación de la firma por un tercero de acuerdo con el procedimiento que se expone a continuación:

El tercero firmante recibirá un email de notificación que le indicará con claridad que se encuentra ante un envío de documentos para firmar procedentes de IFEMA y le permitirá acceder con cualquier dispositivo a los documentos cuya firma se solicita. El caso habitual es que sea un solo documento.

El tercero firmante podrá leer y examinar el contenido de los documentos cuantas veces necesite y desde el navegador moderno y dispositivo de su preferencia.

El email de notificación contendrá las instrucciones sencillas necesarias para que el tercero firmante pueda por sí mismo acceder al documento y proceder a su firma. También contendrá un medio de contacto con el servicio de ayuda del adjudicatario en caso de duda o dificultad. Dicho servicio le ofrecerá los consejos e indicaciones oportunas para resolver su duda y para acceder y firmar correctamente los documentos del envío.

En caso de error al proceder a la firma de un documento, la aplicación de firma ofrecerá al tercero firmante mensajes claros de la causa del error para que pueda resolverlo por sí mismo, sin perjuicio de ofrecerle también el medio de contacto con el servicio de ayuda.

El tercero firmante podrá optar por utilizar cualquiera de las dos formas de firma electrónica indicadas, la firma electrónica avanzada basada en un certificado expedido por un prestador de servicios de certificación o la firma electrónica avanzada no basada en un certificado sino en una autenticación de doble factor: email y contraseña de un solo uso OTP enviada al teléfono móvil del firmante. En esta última, se recogerá el trazo, su velocidad y, si el dispositivo lo permite, su presión e inclinación. Se procederá finalmente a firmar los documentos con el certificado digital válido proporcionado por el adjudicatario.

Podrá existir varios firmantes dentro de la misma empresa (firma mancomunada) o en varias empresas (en caso de UTE).

2.1.5. Usuarios administradores

La aplicación ofertada deberá permitir a IFEMA realizar tareas de sistemas tales como, por ejemplo:

- ✓ Verificar la disponibilidad de las funcionalidades de la solución.
- ✓ El alta, la baja y la configuración de cuantos usuarios remitentes y usuarios firmantes internos sean necesarios.
- ✓ Bloqueo y desbloqueo de las cuentas de los tipos usuario remitente, firmante interno, usuarios administradores.
- ✓ Consulta de indicadores clave de la actividad de plataforma relevantes para el seguimiento del cumplimiento adecuado del presente contrato y consulta de los datos que necesita

habitualmente un administrador de sistemas para elevar internamente a otras instancias el estado del servicio de firma digital certificada de IFEMA. Por ejemplo, datos de consumos, de tiempos de disponibilidad. Datos de uso tales como cantidad de documentos enviados a firma por período, cantidad de documentos efectivamente firmados por firmantes internos, por terceros firmantes, firmados conjuntamente, etc. Cantidad de documentos enviados por remitente o por API por período, etc. Cantidad de documentos rechazados. Consumos de espacio, de ancho de banda, etc.

- ✓ Consulta de logs con información útil que contribuyan a la resolución de incidencias de cualquier tipo, en particular de incidencias relacionadas con en el uso del API.

- ✓ Reconfiguración de los parámetros de la interfaz API.

- ✓ Cualesquiera otras tareas de configuración de sistemas relacionadas con este servicio.

IFEMA deberá poder realizar estas tareas de sistemas en horario laboral mediante un procedimiento ágil y sencillo, basado en el acceso a soporte por medio de una dirección de email y número de teléfono. No se requiere una aplicación web de autoservicio para que los usuarios administradores puedan realizar por sí mismos alguna de las tareas de sistemas descritas. No obstante, en el caso que esté disponible tal aplicación en la oferta o lo estuviera durante la duración del contrato, IFEMA la utilizaría para realizar algunas de las tareas de sistemas en que recurrir a dicha aplicación de autoservicio resulte más sencillo, ágil y eficiente que el procedimiento basado en email y teléfono, a criterio de IFEMA. Sin perjuicio de la posibilidad de realizar siempre las tareas de sistemas por email y por teléfono.

A modo ilustrativo, en los últimos seis meses IFEMA sólo ha solicitado UNA actividad de administración de sistemas al proveedor actual.

2.2. API para el uso mecanizado del servicio

El adjudicatario deberá integrar la aplicación ofertada de forma transparente con el API del sistema SAP de IFEMA, sin más cambios en el sistema SAP que la dirección IP del adjudicatario y los datos de autenticación.

El sistema SAP de IFEMA puede desencadenar y gestionar automáticamente envíos a firma de documentos, tal y como lo haría de forma manual un usuario remitente, pero a través de un API fija que no se va a modificar.

IFEMA facilitará al adjudicatario la documentación completa del API que debe realizar para que el sistema SAP de IFEMA pueda integrarse correctamente y de forma transparente con su sistema de firma digital certificada. El esfuerzo de construir este API está estimado en menos de 15 jornadas para el adjudicatario.

El Sender es SAP ERP y el Receiver será el servicio con el API del adjudicatario. El Sender Channel es SOAP y el Receiver Channel HTTP.

La Plataforma de Firma Electrónica utilizará estos diez servicios REST proporcionados por el adjudicatario, que se relacionan a continuación:

1. **login**

2. **createReceiver**
3. **finishDocProcess**
4. **getReceivers**
5. **getReport**
6. **getReportByDocGuid**
7. **getSignedDocument**
8. **sendVidDelivery**
9. **trackingReceiver**
10. **updateReceiver**

2.3. Entorno De Pruebas

Las ofertas deberán incluir un entorno de pruebas de la plataforma de firma digital certificada para conectar el sistema SAP de desarrollo de IFEMA y realizar comprobaciones de su funcionamiento correcto ante cambios el sistema SAP de Ifema tales como nuevos desarrollos, aplicaciones de parches, etc.

El entorno de pruebas debe contar con la funcionalidad de usuario remitente suficiente para poder consultar el estado de los envíos a firma que realice el sistema SAP de desarrollo de IFEMA. Permitirá tanto configurar usuarios firmantes internos con certificados digitales emitidos por la prestador de servicios de certificación de pruebas de IFEMA, así como para firmantes externos. De tal forma que el entorno de pruebas pueda generar documentos técnicamente firmados pero inválidos jurídicamente.

3. Plan De Transición

IFEMA podrá utilizar de forma manual la plataforma de firma digital certificada del nuevo adjudicatario al momento de la formalización del contrato.

El API para emplear de forma automatizada la plataforma del adjudicatario, tanto la real como la del entorno de pruebas, estará disponible dentro de los treinta días siguientes a la formalización del contrato.