

PLATAFORMA AVANZADA DE FIRMA ELECTRÓNICA: APPLET DE FIRMA y 4SIGN

Índice del documento

1. Firma en el cliente: Applet de firma	3
2. Plataforma de servicios de firma digital de 4Sign	6
4Sign Sign Service: Firma digital multi-formato	6
4Sign Sign Service: Verificación de la validez de los certificados digitales.....	6
4Sign Sign Service: Custodia de certificados y claves. HSM	7
4Sign Sign Service: Sellado de tiempos.....	7
4Sign Sign Service: Servicio de firma batch desasistida en el servidor	7
4Sign eInvoice: Factura electrónica.....	7
4Sign Repository: Archivo digital de documentos firmados.....	8
3. Servicio de portafirmas: Administración, gestión, acceso y firma de documentación electrónica	9
Resumen de características.....	9
Integración con aplicaciones existentes	10
Generación de la información necesaria en formato XML para su posterior firma y preservación.	10
Generación de la lista de personas que deben firmar el documento generado.	10
Gestión de los eventos de finalización del proceso de firma.	11
Publicación de metadatos	11
Integración de la plataforma de firma con los sistemas existentes	12
Visualización e impresión de la documentación electrónica	12
4. Descripción técnica de la solución.....	13
Introducción	13
Administración	13
Aplicaciones	13
Servicios	15
5. Soporte de soluciones HSM	18

1. Firma en el cliente: Applet de firma

El componente de firma es un componente rico (*applet Java*) para la realización de firma electrónica avanzada. Su funcionamiento es muy simple, ya que dada una entrada de datos y una configuración base, es capaz de realizar una firma digital sobre los datos de entrada y devolver como resultado una representación de la firma en el formato definido en la configuración.

Este componente de firma corresponde al proyecto *CryptoApplet* desarrollado por la Universitat Jaume I de Castellón y del cual 4TIC tiene una licencia de comercialización adquirida mediante convenio.

Características generales

- *Applet Java* compatible con versiones de la máquina virtual de *SUN 1.5* o superiores.
- Soporte multi-plataforma, compatible con *Windows XP/Vista/7* (tanto para *Internet Explorer* como para *Firefox*, con el UAC activado), *Linux* y *MacOSX* (sólo *Firefox*).
 - Soporte multi-idioma.
 - Soporte para múltiples formatos de firma (PKCS#1, CMS, XML Signature, XAdES, PDF y ODF).
- Gestión transparente de los certificados con los que se va a firmar, mediante el acceso directo al *CryptoAPI* si se utiliza *Microsoft Internet Explorer* o *PKCS#11* si se usa *Firefox*.
- Acceso a la lista de los certificados instalados en los navegadores de la familia *Mozilla* sin necesidad de solicitar la clave de acceso.
- Soporte para el DNI electrónico (DNIe) tanto en *Internet Explorer* como en *Firefox*.
- Menú de carga del controlador de dispositivo *PKCS#11* que permite añadir nuevos dispositivos de firma instalados en el cliente.
- Archivo de configuración de firma en PDF que permite seleccionar los campos "*Reason*", "*Location*" y "*Contact*", así como los certificados raíz de las autoridades con las que se permitirá realizar la firma del documento.

- *API JavaScript* para la completa parametrización de la aplicación.

Funciones de entrada/salida

El *applet* recibe la información a firmar desde una fuente de entrada totalmente configurable. En el contexto del *applet*, existen dos formas de obtener la entrada de datos y de generar la información de salida:

- Accediendo directamente a los elementos de la página *HTML* que lo contiene (mediante *JavaScript*, accediendo a un elemento del *DOM*. P.ej. campo *hidden*).
- A través de una *URL*. Realizando la lectura de los datos a firmar por *HTTP* y haciendo un *POST* a una *URL* destino cuando se complete el proceso de firma.

Adicionalmente, existe un *API* que permite la implementación de nuevos tipos de conectores para lectura/escritura de datos.

Este sistema de entrada/salida permite la conexión directa del componente de firma a sistemas *REST* como *4Sign* (capa de servicios de la oferta), el cual se encarga de proporcionar los datos a firmar desde el portafirmas y guardar el resultado de la firma en el repositorio digital.

Formatos de salida

Una vez completado el proceso de firma, el *applet* es capaz de generar, en función de lo que hayamos especificado en la configuración, una serie de formatos criptográficos o estándares de representación.

Los formatos de representación de firma soportados, son los siguientes:

- Firma "en bruto", *PKCS#1* o *RAW*. Para el formato *RAW* el *applet* obtendrá los datos de entrada, los resumirá utilizando el algoritmo de firma *SHA1* y devolverá un *PKCS#1* con *padding* que contendrá el *hash* de los datos de entrada firmados.
- *CMS/PKCS#7*. A partir de los datos de entrada se calculará el resumen *SHA1* de los mismos y se generará una estructura *PKCS#7* que se ofrecerá como resultado.
- Firma *PDF*. Dada la entrada de datos, el *applet* sitúa una firma invisible en el documento *PDF* que puede ser verificada por *Adobe Reader*. Los campos *Reason*, *Location* y *Contact* de la firma son configurables. En la firma generada se incluye el certificado del firmante y el de la *CA* raíz o intermedia que lo expidió. Adicionalmente y para completar la firma generada, es posible la inclusión de un sellado de tiempo.

- Firma *ODF*. Generación de un formato de firma XML Signature en documentos ODF reconocible por OpenOffice.
- *XML Signature*. Posibilidad de firma documentos XML de entrada, generando un formato de salida que cumple el estándar *XML Signature* y que se representará “*enveloped*” en el documento original.
- *XAdES-X-L* en formato *DigiDoc*. El *applet* permite la generación de firma digital avanzada compatible con la especificación *TS 101 903 - V1.2.2* del *ETSI*, siendo capaz de generar los formatos *XAdES*, *XAdES-T* y *XAdES-X-L*. El *applet* generará uno u otro formato dependiendo de la configuración.

La salida XML como resultado del proceso de firma, se obtendrá en formato *DigiDoc 1.4*. *DigiDoc* es un formato simple de representación de documentos firmados que permite consignar en un mismo documento los datos originales en formato base64 y la información criptográfica asociada “*enveloped*” en formato *XAdES*. Esta forma de representar la información nos permite firmar con *XAdES* tanto documentos XML, como otros formatos binarios.

Las particularidades, de un modo general, de estos formatos son:

- *XAdES-BES* o *XAdES-EPES*. Es el formato más básico, equiparable al generado por el formato de firma *XMLDsig* más ciertos datos adicionales relativos al certificado del firmante y a la hora que ofreció su máquina (es el mínimo exigido por el Ministerio de Economía para firmar facturas electrónicas en formato *Facturae*).
- *XAdES-T*. Amplía la información consignada en el formato anterior con un sello de tiempo, obtenido de la autoridad de sellado de tiempo indicada en el fichero de configuración.
- *XAdES-X-L*. Contiene datos relativos a la validación con el objetivo de permitir que esta perdure en el tiempo, estos datos son básicamente aquellos en relación a la respuesta *OCSP* recibida con respecto a la validación del certificado, además del ya indicado sello de tiempo.

Como complemento, el *applet* también soporta la realización de firmas en paralelo para el formato *XAdES*. De esta forma, podemos almacenar el documento XML original junto con todas las firmas consignadas por los distintos involucrados en el proceso.

- *XAdES-X-L enveloped*. Permite añadir a cualquier formato XML definido (por ejemplo, una factura electrónica en formato *Facturae 3.1*), una firma “*enveloped*” en formato *XAdES*. La única diferencia con la especificación anterior, es la que este tipo de formato de salida no es dependiente de ninguna definición concreta de formato como *DigiDoc*. Es el desarrollador el encargado de gestionar el formato a utilizar y de indicar qué información debe ser firmada dentro del mismo. Esta implementación está basada en las librerías del MITyC.

2. Plataforma de servicios de firma digital de 4Sign

4Sign es una plataforma de servicios que da soporte a las tareas de administración electrónica, permitiendo su uso e integración con otras aplicaciones internas, independientemente del lenguaje en el que estén desarrolladas. Este servicio permite, vía interfaz *REST* o *SOAP*, satisfacer todas las necesidades del cliente en materia de firma digital multi-formato.

4Sign Sign Service: Firma digital multi-formato

Con soporte para firma en bruto, *CMS/PKCS#7*, *XML Signature* o *XAdES-X-L*, permite firmar o verificar documentos *PDF* (firma reconocida por *Adobe Acrobat*), documentos de *OpenDocument* (firma reconocida por *OpenOffice*) o cualquier otro tipo de documento.

Para la firma de documentos, la aplicación permite la carga de una serie de certificados de aplicación. De igual forma, si los servicios de validación *OCSP* o de sellado de tiempo requieren algún certificado específico para su acceso, estos también pueden ser configurados. De esta manera, se consigue la independencia de la herramienta respecto a los certificados o autoridades de certificación empleadas.

Al margen de los formatos de firma generales como pueden ser *CMS/PKCS#7*, *XML Signature* o *XAdES-X-L*, se ofrece la posibilidad de firmar documentos *PDF*, de forma que *Acrobat Reader* y otras aplicaciones que lo soporte, pueden verificar el documento y validar la firma que en él se incluye. En el caso de firma de documentos *PDF*, también existe la posibilidad de acompañar la firma de un sello de tiempos a la hora de su generación.

Finalmente, también se soporta la firma y verificación de documentos en formato *OpenDocument*, los cuales son capaces de albergar el resultado de la firma digital en formato *XML Signature*.

4Sign Sign Service: Verificación de la validez de los certificados digitales

El módulo de verificación de certificados permite verificar el estado de los certificados que utilizan los usuarios, soportando incluso la validación del *DNi*e.

Cada autoridad certificadora ofrece un sistema de verificación de los certificados que emite. Esta verificación, dependiendo de cada caso, puede ser desde la publicación de una *CRL*, la puesta en marcha de un servicio *OCSP* o un *Web Service* propio de consulta.

De esta forma, este módulo de verificación le ofrecerá un interfaz homogéneo para la consulta del estado de sus certificados, independientemente de la entidad que los haya emitido.

4Sign Sign Service: Custodia de certificados y claves. HSM

Almacenamiento de los certificados y claves de la organización de forma segura mediante la integración de 4Sign con soluciones hardware de custodia de claves (HSM) como las proporcionadas por *SafeNet*.

4Sign Sign Service: Sellado de tiempos

El servicio de sellado certificado de tiempos permite establecer de forma segura e irrefutable el momento de publicación de un documento electrónico o de envío de una notificación telemática.

Aunque los formatos de firma *XML* avanzados, como es el caso de *XAdES-X-L*, ya incluyen un sellado de tiempo en su estructura criptográfica, es posible generar una marca de tiempo que de testimonio del instante exacto de la consecución de una acción para cualquier tipo de documento, sea XML o no.

4Sign Sign Service: Servicio de firma batch desasistida en el servidor

Este servicio permite la firma de forma automatizada de lotes extensos de documentos que no requieren la firma con un certificado personal y que pueden ser procesados de forma batch.

4Sign Invoice: Factura electrónica

Con este servicio se permite firmar o verificar facturas electrónicas emitidas en el formato *Facturae* definido por el Ministerio de Economía y Hacienda o en el estándar internacional *UBL*.

Si a la implantación de la factura electrónica en una organización le eliminamos la complejidad de tener que gestionar el componente criptográfico, todo se simplifica sobremanera.

Gracias a este módulo se pueden firmar las facturas emitidas con un certificado de aplicación o validar la firma de las que se reciban, de una forma sencilla e integrada.

Posteriormente, utilizando el módulo de archivo que presentaremos a continuación, sólo se tendrá que preservarlas, eliminando la necesidad de su impresión y archivo.

4Sign Repository: Archivo digital de documentos firmados

Archivo y preservación de todos los documentos digitales que se firman en su organización. El almacenamiento de forma segura mediante este servicio de archivo permitirá que los documentos de la organización permanezcan accesibles durante largos periodos de tiempo.

Los documentos podrán consultarse a través de un servicio especializado de búsqueda que permitirá su recuperación y serán preservados junto con los metadatos que los definen para su mejor clasificación y búsqueda.

3. Servicio de portafirmas: Administración, gestión, acceso y firma de documentación electrónica

El servicio de portafirmas es uno de los elementos clave para conseguir integrar un sistema de firma y preservación de documentación electrónica, con un conjunto de aplicaciones ya existentes.

Este servicio utiliza la mayor parte de los servicios expuestos por 4Sign en los distintos módulos ofrecidos (Sign Service, Repository, Reports y Events).

Resumen de características

- Gestión de la documentación electrónica, ya sea firmada o pendiente de firma. Permite el acceso para la inserción, consulta y verificación de cualquiera de los documentos almacenados.
- Posibilidad de firma de un documento pendiente de distintos modos (ver 4Sign Sign Service):
 - Modo cliente. Con el uso del *applet* de firma por el usuario implicado, interactuando a través de su portafirmas.
 - Modo servidor. Mediante un proceso que se ejecuta en el servidor y que hace uso de un certificado de aplicación previamente establecido.
- Gestión del flujos de trabajo entre los distintos usuarios implicados en el proceso de firma de un documento electrónico, permitiendo la firma individual de un documento, su firma en serie o su firma en paralelo.
- Sistema de gestión de eventos. Reactividad a cualquiera de los eventos que se producen durante el proceso de firma y que pueden suponer actualizaciones el sistema cliente con el que se integra el portafirmas (ver 4Sign Events).
- Sistema de metadatos para una consulta rápida de los distintos atributos de un documento electrónico firmado y preservado en el portafirmas (ver 4Sign Repository).
- Opciones avanzadas de visualización de documentación mediante un sistema de plantillas XSL que permite la representación de la información firmada en distintos formatos (ver 4Sign Reports).

Integración con aplicaciones existentes

Este es una de las características más importantes del sistema y que garantiza que pueda ser finalmente una herramienta útil y poco intrusiva.

Para dotar a una aplicación ya desarrollada de capacidades de firma digital, esta debe poder cumplir tres puntos fundamentales:

Generación de la información necesaria en formato *XML* para su posterior firma y preservación.

Estos documentos *XML* pendientes de firma, pueden ser almacenados de forma temporal hasta que se complete la firma por parte del usuario en el portafirmas o en un archivo digital auxiliar (*Fedora Commons* o *DSpace*), en función de las necesidades de cada sistema. Hay que tener en cuenta, que el resultado final del proceso de firma sería aconsejable que fuera almacenado siempre en un archivo digital para su posterior preservación, pudiendo complementarlo con los metadatos que fueran necesarios.

Posteriormente, para su presentación en formato *PDF*, existe la posibilidad de crear una hoja de estilos *XSL* que lleve a cabo la transformación, consignando siempre al pie del documento generado, la información de:

- Quién o quienes firmaron el documento.
- Cuando realizaron la firma cada uno de ellos.
- La referencia que se debe introducir en el servicio de verificación electrónica para constatar la autenticidad del documento impreso (código seguro de verificación al pie de la firma).

Generación de la lista de personas que deben firmar el documento generado.

La definición de una lista de usuarios involucrados en el proceso de firma permitirá al portafirmas la gestión del flujo de procesamiento del documento. De esta forma, se podrá ir mostrando en el portafirmas personal de cada uno de ellos, en un orden establecido o no, cada uno de estos documentos.

Gestión de los eventos de finalización del proceso de firma.

Durante el proceso de firma, cada vez que un usuario firma un documento, existe la posibilidad de añadir una acción que permita "marcar" en el sistema de información del cliente cualquier estado que sea de su interés (por ejemplo, enviar un SMS al siguiente usuario que ha de firmar el documento cuando el anterior ya ha completado el proceso, o marcar un documento de gestión económica como emitido cuando el usuario lo firma).

Para conseguir esto, la aplicación de portafirmas permite la definición de una serie de *triggers* o gestores de eventos que son capaces de realizar acciones en base a una sencilla API. Ejemplos de eventos soportados:

- Documento insertado en el portafirmas.
- Firma completada por un usuario.
- Proceso de firma que involucra a más de un usuario finalizado.
- Proceso de firma cancelado.

Publicación de metadatos

Para conseguir una mejor integración de la información gestionada por el portafirmas, con el sistema de información en el que está implantado, el portafirmas expondrá una serie de metadatos de simple consulta:

- Usuario que realizó la solicitud.
- Usuario o usuarios que posteriormente la firmaron.
- Fecha de inserción de la solicitud.
- Fecha de firma de cada uno de los usuarios involucrados en el proceso.
- Tipo del documento (acta, certificado de notas, factura, etc). En función del tipo de documento generado, tendremos disponible una o varias plantillas XSL para su visualización en distintos formatos si fuera necesario (*HTML*, *PDF* u otros).
- Información opcional acerca de la clave primaria o información de referencia del registro de base de datos asociado en el sistema de información del cliente. Esta información interna puede resultar muy útil a la hora de enlazar la información del portafirmas con otras partes del sistema de información.
- Tipo de procesamiento del documento:

- A procesar por el usuario en cliente. Supone la visualización del documento en el portafirmas de un usuario concreto y su firma digital mediante el *applet* criptográfico.
- A procesar por el servidor. Supone la firma digital del documento por los servicios de servidor ofrecidos por 4Sign y que harán uso de un certificado de aplicación previamente definido.

Integración de la plataforma de firma con los sistemas existentes

4Sign es capaz de generar mensajes JMS en respuesta a los eventos que se producen dentro de la plataforma. Mediante este mecanismo permiten que cualquier aplicación de terceros pueda consumir estos eventos de forma asíncrona y disponer de la información mínima necesaria para su procesamiento.

4Sign Events permite la puesta en funcionamiento de una cola de mensajes JMS basada en Apache ActiveMQ. Si la organización no dispone de un servidor JMS, este módulo puede ser empleado para este fin.

Al margen del propio servidor JMS, se añaden una serie de servicios REST que enriquecen la administración ofrecida, exportando estadísticas de la cola de mensajes y dando acceso a ciertas funciones de administración como el purgado de colas.

Visualización e impresión de la documentación electrónica

La mayor parte de la documentación electrónica que gestiona el portafirmas suele estar en formato XML. Es por ello que la plataforma debe contar con una serie de servicios de publicación para la visualización, transformación y publicación de documentación electrónica en formato PDF.

4Sign Reports permite asignar una plantilla XSL a cualquier tipo de documento XML gestionado por el portafirmas. Esta plantilla XSL será la responsable de transformar el XML original en PDF y de añadirle en el pie (si es pertinente) toda la información relativa a los firmantes, código seguro de verificación, etc.

Adicionalmente, 4Sign Reports cuenta con un servicio batch para el procesamiento de remesas de documentos de gran tamaño. Por ejemplo: Remesas de recibos, actas académicas, expedientes de estudiantes, etc.

4. Descripción técnica de la solución

Introducción

La plataforma de firma 4Sign:

- Es una plataforma de servicios con interfaz REST y SOAP, por lo que cumple con los requisitos de interoperabilidad.
- Ofrece un componente de cliente rico para las funciones de firma avanzada (applet criptográfico).
- Los interfaces de usuarios son web y están desarrollados con un framework de cliente cliente (ExtJS), los cuales interactúan con los servicios mediante interfaz REST.
- Permite trabajar con distintas autoridades de certificación.
- Permite integrar el soporte para distintas políticas de firma en los procesos de firma y posterior verificación (actualmente se incorpora la política de Facturae 3.0 y 3.1 en el módulo 4Sign eInvoice).

Administración

La plataforma de firma 4Sign:

- Permite la parametrización de todos los módulos existentes desde un único punto.
- Ofrece una documentación completa tanto de las APIs REST de los servicios expuestos, como del proceso de instalación de la plataforma, configuración de los módulos y uso (incluyendo código de ejemplo y tests unitarios JUnit para la verificación de todos los servicios expuestos).
- Gestión de transformaciones de documentos XML a PDF.
- Permite agregar nuevas CAs tanto a los servicios de firma como al componente de firma de cliente.

Aplicaciones

Requisitos generales

La plataforma de firma 4Sign:

- Soporta la definición de múltiples idiomas a la hora de presentar cualquier tipo de mensaje.

- Ofrece aplicaciones web que disponen de filtros de autenticación para proteger los recursos en base al sistema de autenticación del cliente.
- Ofrece interfaces web basados en estándares y que permiten el acceso del usuario con cualquier tipo de navegador (IE 6/7/8, Firefox y basados en WebKit como Chrome/Safari).

Firma de documentos custodiados por el usuario

La plataforma de firma 4Sign:

- En su componente de firma en cliente, se ofrece soporte para cualquier tipo de tarjeta criptográfica que disponga de un CSP en Windows/IE o de un interfaz PKCS#11.
- Todos los formatos de firma propuestos son ampliamente soportados.
- Al margen del applet de firma, la plataforma dispone de un plugin que se integra con OpenOffice y que permite firmar desde el interfaz de usuario tanto documentos ODF como PDF. Adicionalmente, 4TIC está trabajando en la incorporación de clientes de firma para dispositivos móviles basados en Android y Iphone.

Validación de documentos

La plataforma de firma 4Sign:

- Expone servicios de validación de cualquier formato de firma soportado.
- Ofrece la posibilidad de acceder a los servicios de validación desde la aplicación de portafirmas.
- Permite extraer la información básica de cualquier documento almacenado y firmado (firmante, fecha de firma, etc).

Portafirmas corporativo

La plataforma de firma 4Sign:

- Incorpora una aplicación web de portafirmas en la que el usuario puede:
 - Acceder a los documentos pendientes de firma y a los documentos que ha firmado en algún momento.
 - Visualizar los documentos del portafirmas apoyándose en el servicio de visualización de documentos 4Sign Reports.
 - Firmar los documentos pendientes.
 - Validar los documentos firmados.

- Soporta en esta aplicación web los flujos de firma, las firmas múltiples y las firmas en bloque.
- Trata todos los eventos que se producen en el sistema y los publica como mensajes JMS, permitiendo la integración de aplicaciones de terceros que puedan ser reactivas a operaciones gestionadas por la plataforma.
- El módulo de portafirmas se compone de un interfaz web que interactúa vía la API cliente de 4Sign con el servicio REST de portafirmas.

Comprobación de códigos seguros de verificación

La plataforma de firma 4Sign:

- Permite establecer los niveles de acceso a los documentos gestionados por el sistema (públicos, públicos mediante autenticación previa y privados).

Administración del repositorio de documentos

La plataforma de firma 4Sign:

- Se integra totalmente con herramientas de gestión archivística y de preservación de documentación como Fedora Commons o DSpace. En este sentido ofrece un módulo específico para la interacción con el repositorio llamado 4Sign Repository, el cual permite realizar las operaciones básicas de consulta, inyección, borrado o recuperación de objetos digitales mediante un interfaz REST unificado.

Servicios

Condiciones comunes

La plataforma de firma 4Sign:

- Soporte completo para REST y SOAP en el acceso a los servicios.
- Solución Java totalmente compatible con cualquier servidor de aplicaciones y que no requiere de un servidor J2EE para su ejecución (aunque también los soporta). Esta solución basada en Spring Framework, se ha desplegado tanto en servidores J2EE (JOnAS, JBoss o Glassfish), como en servidores ligeros (Tomcat y Jetty).
- Tanto los interfaces de usuario, como el catálogo de mensajes están totalmente internacionalizados.

- Catálogo de mensajes basado en un registro de mensajes totalmente tipificado y codificado. En la documentación del API REST es posible consultar todos los errores tratados en cada método del API.

Planificación

La plataforma de firma 4Sign:

- Cuenta con una librería cliente (4Sign Client API) que simplifica la conexión de aplicaciones con los servicios REST expuestos en el servidor. Esta API cliente representa un conjunto de Stubs que ofrecen una interfaz completa a los servicios existentes. La API cliente estaría disponible desde el inicio del proyecto y ya cuenta con una documentación detallada.
- Para simplificar la distribución del API cliente, 4Sign Client se ofrece como un JAR a incorporar a las aplicaciones que necesiten conexión con los servicios de la plataforma de firma.
- Este cliente permite la conexión a los servicios existentes en claro (si la aplicación está en una red privada protegida) o mediante SSL con autenticación en cliente mediante certificados (si queremos ofrecer un nivel extra de seguridad en las comunicaciones).

Validación de certificados

La plataforma de firma 4Sign:

- Permite la validación de cualquier certificado mediante servicios OCSP o consulta de CRLs. Estos servicios pueden recibir la URL de acceso a los servidores OCSP o de descarga de las CRLs o pueden, de forma automática, intentar extraer esta información del propio certificado a validar.

Sellado electrónico

La plataforma de firma 4Sign:

- Permite realizar sellos electrónicos sobre documentos.
- Permite la custodia de certificados y claves en dispositivos hardware de almacenamiento o HSM. Este tipo de operaciones pueden asegurarse al máximo utilizando el modo de conexión SSL del 4Sign Client.

Repositorio de documentos

La plataforma de firma 4Sign:

- Incorpora o es capaz de integrarse con archivos digitales de preservación documental como Fedora Commons o DSpace.
- Almacena cada objeto digital en el repositorio utilizando como identificador el código de verificación segura que identifica al documento electrónico en el portafirmas.
- Cada objeto digital acompañado se almacena con un conjunto definido de metadatos que puede personalizarse. Los metadatos disponibles para etiquetar los objetos digitales, son los recogidos en el estándar Dublin Core.
- Ofrece como parte del API cliente una serie de métodos para poder guardar, recuperar, borrar y buscar documentos en el archivo digital.
- En caso de utilizar Fedora Commons, 4TIC es especialista en el diseño de modelos de objetos que permitan personalizar al detalle cómo se van a almacenar los objetos digitales en el repositorio y qué relaciones se van a modelar.

Portafirmas corporativo

La plataforma de firma 4Sign:

- Dispone de un servicio que expone con interfaz REST todos los métodos de gestión del portafirmas.
- Permite la definición de flujos de firma para cada documento insertado en el sistema.

Validación de documentos firmados

La plataforma de firma 4Sign:

- Ofrece un completo servicio de validación de documentos firmados.

Comprobación de códigos seguros de verificación

5. Soporte de soluciones HSM

4TIC es partner oficial de SafeNet y ha certificado su productos de firma digital 4Sign y su producto de administración electrónica OpenSAT para el uso del hardware de custodia de claves que ofrece esta empresa.

4TIC está en proceso de obtención de la certificación del otro gran fabricante de HSMs, como es nCipher.