JUNTA DE ANDALUCIA

CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA

Herramienta centralizada de verificación de firmas

Acceso a documentos electrónicos

Versión: v02r05

Fecha: 30/12/2013

HOJA DE CONTROL

Título	Herramienta centralizada de verificación de firmas		
Entregable	Acceso a documentos electrónicos		
Nombre del Fichero	ASI_Herramienta Centralizada de Verificación de Firmas_v02r05.doc		
Autor	SCAE - DGPD		
Versión/Edición	v02r05	**Fecha Versión**	30/12/2013
		Nº Total Páginas	026

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
v01r00	Versión inicial	CHAP	CHAP	14/06/2013
v01r01	Actualización del documento	CHAP	CHAP	25/06/2013
v01r02	Actualización del documento	CHAP	CHAP	08/07/2013
v01r03	Actualización del documento	CHAP	CHAP	16/07/2013
v01r04	Actualización del documento	CHAP	CHAP	15/10/2013
v02r00	Actualización del documento	CHAP	CHAP	28/11/2013
v02r01	Actualización del documento	CHAP	CHAP	02/12/2013
v02r02	Actualización del documento	CHAP	CHAP	03/12/2013
v02r03	Actualización del documento	CHAP	CHAP	05/12/2013
v02r04	Actualización del documento	CHAP	CHAP	11/12/2013
v02r05	Actualización del documento	CHAP	CHAP	30/12/2013

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos	Cargo	Área	Nº Copias
Manuel Perera Domínguez	Jefe de Servicio	CHAP	1
José Ignacio Cortés Santos	Director de Proyecto	CHAP	1
Francisco González Guillén	Director de Proyecto	CHAP	1
Francisco Mesa Villalba	Director de Proyecto	CHAP	1

ÍNDICE

1 INTRODUCCIÓN

1.1 Objeto

El objetivo de la herramienta centralizada de verificación de firmas es posibilitar, tras el efectivo proceso de despliegue e integración, el cese en el despliegue de nuevas implantaciones de herramientas locales de verificación.

Las actuales herramientas de verificación quedarán pues disponibles para consulta durante el tiempo que se estime necesario. La ciudadanía dispondría, progresivamente, de un único punto para la verificación de documentos firmados electrónicamente en la Administración de la Junta de Andalucía, con garantía de su permanencia en el tiempo e independencia frente a cambios y reestructuraciones orgánicas.

La herramienta facilitará que las aplicaciones que actualmente utilizan la custodia de documentos en la plataforma @firma (ya sea la implantación corporativa u otras implantaciones locales) cesen en ello, sin que necesariamente la Consejería o entidad responsable del documento deba desarrollar e implantar una funcionalidad propia y específica de verificación.

Se trata de una actuación de impulso de adecuación al Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, por ejemplo en cuanto a la implantación de repositorios electrónicos de documentos, y en particular de la Norma Técnica de Interoperabilidad de Documento Electrónico, así como una contribución a la racionalización y homogeneización de los servicios de administración electrónica, tanto internos como aquellos puestos a disposición de la ciudadanía.

1.2 Alcance

Este documento se encuentra dirigido a:

- Dirección de proyecto para su revisión y validación.
- Conjunto de Organismos y entidades de la Junta de Andalucía para su conocimiento y realización de observaciones.

2 REQUISITOS GENERALES

Los requisitos generales para la construcción de la herramienta centralizada de verificación de firmas son los siguientes:

1. En la herramienta se implementará una funcionalidad básica (zona de administración) de alta/baja/modificación de "sistemas/repositorios" que custodian documentos firmados electrónicamente, con los cuales se integrará la herramienta, consiguiendo de esta forma, gestionar la relación de sistemas origen de ubicación de los documentos custodiados.

2. El nuevo código seguro de verificación aceptado por la herramienta centralizada de verificación de firmas se corresponderá con la especificación establecida para el metadato identificador normalizado de documento según la Norma Técnica de Interoperabilidad de Documento Electrónico. Este código se corresponde con la nomenclatura: ES_<Órgano>_<AAAA>_<ID_especifico>, donde concretamente el campo <ID_especifico> (código alfanumérico de 30 caracteres) estará construido en base a:

   a) Los 5 primeros caracteres se calcularán de forma aleatoria, formándose en base a un identificador base64 construidos en los rangos de a-z, A-Z y 0-9 (sin eñes), y que será asignado para cada sistema/repositorio.

   b) Los restantes 25 caracteres serán determinados por la Consejería o entidad responsable del sistema/repositorio siempre que cumplan con los principios deseables para la generación de un código seguro de verificación (impredecibilidad, uniformidad, resistencia a colisiones e irreversibilidad)

      En el Anexo II del presente documento, se presenta una propuesta, a modo de ejemplo, que contempla un código de 19 caracteres, quedando 6 caracteres de libre uso por la Consejería o entidad (para codificaciones propias, especificación de dominios funcionales, etc.)

   <Órgano> será el código correspondiente a la entidad responsable del sistema/repositorio en el Directorio Común DIR3.

   También se aceptarán códigos seguros de verificación que no se correspondan con identificadores normalizados de documentos, siempre considerándose que los 5 primeros caracteres corresponderán al identificador del sistema/repositorio.

3. La herramienta centralizada de verificación aceptará como entrada, aportada por el usuario final, con carácter general, un identificador normalizado de documento, con la estructura definida en la Norma Técnica de Interoperabilidad de Documento Electrónico o bien un código de verificación a modo actual:

   a) En caso de identificador normalizado de documento según la Norma Técnica de Interoperabilidad de Documento Electrónico o código seguro de verificación cuyos 5 primeros caracteres correspondan a un identificador de sistema/repositorio:

      i. Se determinará el "sistema/repositorio" que custodia el documento, a partir de su código identificativo que figurará en el identificador normalizado del documento, los 5 primeros caracteres.

      ii. Se invocará el correspondiente servicio definido para el "sistema/repositorio" para la obtención de la información.

      iii. Se procesarán los datos devueltos por el "sistema/repositorio" y se mostrarán los resultados al usuario final, atendiendo al apartado VIII (Acceso a documentos electrónicos) de la Norma Técnica de Interoperabilidad de Documento Electrónico.

   b) En otro caso, se supondrá que se trata de un código seguro de verificación correspondiente a un documento almacenado en la custodia de la implantación corporativa de la plataforma @firma, procediéndose a su recuperación.

4. La herramienta centralizada de verificación que se ponga a disposición pública en Internet no implementará una funcionalidad de incorporación de fichero firmado y de fichero de firma electrónica, para su validación (como actualmente existe en la herramienta de verificación asociada a la herramienta Portafirmas, funcionalidad que se prevé su eliminación en futuras versiones). Se pondrá una funcionalidad de este tipo a disposición d los servicios y unidades TIC de la Junta de Andalucía.

5. Las Consejerías y entidades para cada uno de los "sistemas/repositorios" que requieran integrarse con la herramienta centralizada de verificación de firmas deban adaptarse a las especificaciones de un servicio dado:

   a) En la especificación del servicio de integración se contemplará la estructura ENIDOC definida en la Norma Técnica de Interoperabilidad de Documento Electrónico para el intercambio de información con los "sistemas/repositorios".

   b) Adicionalmente a los metadatos definidos en la estructura ENIDOC, se contemplarán una serie de metadatos complementarios, no obligatorios, que podrán devolver los "sistemas/repositorios" que custodien documentos firmados electrónicamente.

   En el Anexo I del presente documento, se define las especificaciones del servicio de integración a implementar.

6. Cada Consejería o entidad responsable de un "sistema/repositorio" que se integre con la herramienta centralizada, deberá:

   a) Garantizar la disponibilidad de las herramientas de verificación que utilizara hasta el momento de la integración efectiva, por el tiempo que se considere necesario.

   b) Garantizar la disponibilidad del servicio que desarrolle y del propio "sistema/repositorio".

   c) Adaptar los "pies de firma" de los documentos firmados electrónicamente generados a partir de la fecha efectiva de integración con la herramienta, incorporándose el identificador normalizado / código seguro de verificación y la dirección de acceso a la herramienta o referencia a la misma.

3 DESCRIPCIÓN FUNCIONAL DEL SISTEMA

3.1 Arquitectura básica

La existencia de la herramienta centralizada de verificación de firmas para cualquier "sistema/repositorio" en general, hace necesario que la herramienta deba poder comunicarse con cualquiera de ellos de modo que interrogadas por un código de verificación, éstos puedan facilitar la siguiente información:

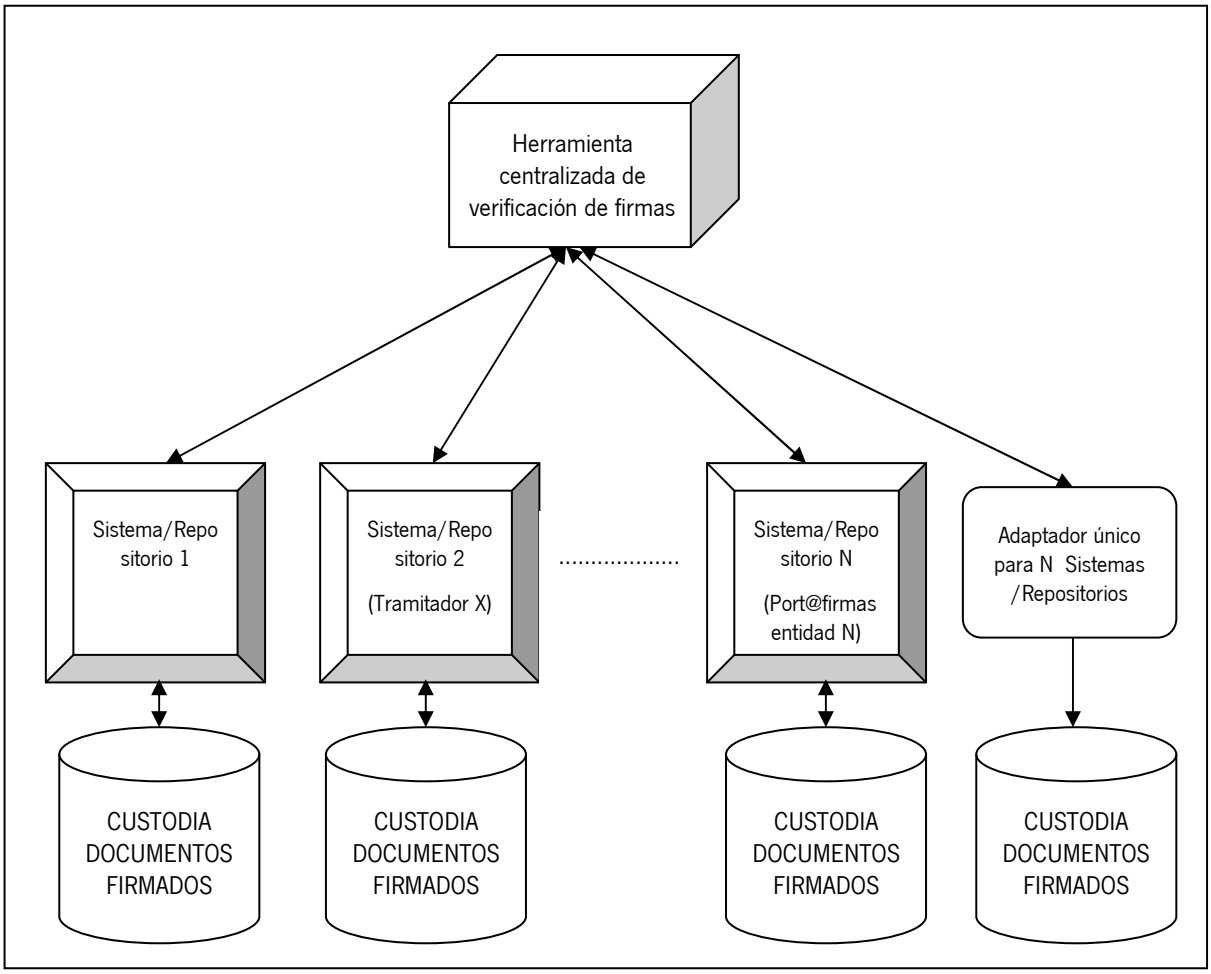
- Documento original firmado: necesario para poder facilitarlo al usuario que realiza la consulta y para poder verificar la integridad del documento.

- Firma electrónica: necesario para poder verificar la integridad de la transacción de firma.

- Metadatos ENI del documento electrónico: permitirá ofrecer información del documento firmado.

- Metadatos complementarios (opcional): permitirá ofrecer más información sobre el contexto del documento a verificar en los casos en los estén disponibles en el sistema/repositorio origen.

  Estos metadatos se encuentran descritos en el Anexo I, apartado 5.2 del presente documento.



Según el esquema propuesto los sistemas/repositorios origen adaptados mediante la implementación de la interface común genérica de "rescate" de documentos conviven con otros repositorios de documentos para los cuales se desarrolla un adaptador que implementa una interface similar al margen de la aplicación que "alimenta" de documentos el repositorio. De este modo, diversos sistemas/repositorios que se apoyaran en un repositorio documental común podrían obviar el desarrollo del sistema adaptador para cada sistema/repositorio y en lugar de ello sería suficiente con implementar un adaptador único para repositorio compartido entre esos sistemas/repositorios.

Un claro ejemplo de "adaptador" será aquel que implemente la interface de acceso a documentos en custodia de @firma para garantizar que el punto único de verificación de firmas pueda validar los códigos de verificación de firmas de los sistemas/repositorios que emplean la custodia de la plataforma @firma, sin perjuicio de la directriz general que no se debe continuar esta práctica.

Finalmente, es necesario destacar la necesidad de que en los códigos de verificación de firma se introduzca información que permita a la herramienta centralizada de verificación de firmas identificar el sistema/repositorio que custodia el documento de modo que se evite la indeseable situación en la que la herramienta de verificación de firmas deba interrogar a todos ellos.

3.2 Escenario habitual de uso

El funcionamiento básico de la herramienta centralizada de verificación de firmas sería el siguiente:

1. El usuario se autentica en el sistema, para ello se emplea alguno de los siguientes métodos:
    - Autenticación basada en certificado electrónico de persona física, en cuyo caso se cumplimentará una casilla denominada "Motivación de acceso" con uno de los siguientes valores posibles:
        - Ciudadanía.
        - Personal empleado público de la Junta de Andalucía en el ejercicio de sus funciones.
        - Otro personal empleado público en el ejercicio de sus funciones.
    - Autenticación basada en certificado electrónico de persona jurídica, en cuyo caso la aplicación mostrará un mensaje indicando tal circunstancia. Asimismo se mostrará un texto informativo de aviso (este texto puede mostrar un mensaje advirtiendo de que únicamente deberá recabar documentos en el ámbito y alcance del certificado electrónico para la persona jurídica en cuestión).
    - Autenticación basada en certificado electrónico de empleado público, en cuyo caso la aplicación mostrará un mensaje indicando tal circunstancia. Asimismo se mostrará un texto informativo de aviso (este texto puede mostrar un mensaje advirtiendo de que únicamente deberá recabar documentos en el ejercicio de sus funciones como empleado público de la Administración). Se cumplimentará una casilla denominada "Motivación de acceso" con uno de los siguientes valores posibles:
        - Personal empleado público de la Junta de Andalucía en el ejercicio de sus funciones.
        - Otro personal empleado público en el ejercicio de sus funciones.
2. El usuario facilita el código de verificación del documento.
3. La herramienta de verificación de firmas identifica el sistema/repositorio que custodia el documento.
4. Con la información anterior, la herramienta de verificación de firmas recupera el documento, firma e información complementaria empleando el protocolo común de comunicación definido.
5. La herramienta de verificación de firmas realizará la validación de la firma electrónica respecto de la fecha actual conforme a los criterios de la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración. Para esta validación se actualizarán los actuales servicios DSS de integración con las plataforma @firma.
6. La herramienta de verificación de firmas dispone la información recopilada al usuario.

3.3 Gestión de errores

Las posibles situaciones de error son las siguientes:

- La herramienta de verificación de firmas conoce el sistema/repositorio que custodia el documento, se comunica con él y ésta responde señalando que no conoce el código de verificación solicitado: se indicará al usuario que no se ha podido verificar la firma.
- La herramienta de verificación de firmas no conoce el sistema/repositorio que custodia el documento: se indicará al usuario que no se ha podido verificar la firma.
- Cuando la herramienta de verificación de firmas trata de comunicarse con el sistema/repositorio que custodia el documento y no es posible o éste devuelve un error:
    - Se indicará al usuario que en ese momento debido a problemas técnicos no es posible realizar la verificación requerida.

- Se crearán alertas (correo electrónico....) destinadas a los administradores de la herramienta de verificación de firmas y al del sistema/repositorio afectado para advertirles de la situación y tomen las medidas necesarias.

3.4 Migración hacia el punto único de verificación de firmas

Es importante destacar que la implantación de la herramienta centralizada de verificación de firmas no implica que de modo inmediato puedan desactivarse los diversos sistemas de verificación de firma actualmente implantados.

Los sistemas actuales no incorporan habitualmente ningún tipo de información en el código de verificación de firma sobre la aplicación desde la que realiza la firma, algo necesario según se ha justificado previamente.

A partir de que el Organismo o entidad solicite la integración con la herramienta centralizada de verificación de firmas deberá llevar a cabo las modificaciones correspondientes en los pies de firma de los informes de firma generados, actualizando:

- La actual URL de verificación por la nueva URL que enlaza con el punto único de verificación de firmas.
- El código seguro de verificación.

3.5 Trazabilidad

Será necesario que los usuarios de la herramienta centralizada de verificación de firmas se autentiquen con certificado electrónico reconocido como requisito previo para poder hacer uso de la herramienta, con el fin de garantizar la absoluta trazabilidad de todas las acciones que realicen. En concreto, la herramienta de verificación de firmas registrará al menos el histórico de accesos, intentos de acceso fallidos, registro de peticiones de verificación de documentos, incluyendo para ellas al menos la fecha, hora y el resultado obtenido.

La herramienta centralizada de verificación de firmas en ningún caso conservará documentos electrónicos de ninguna clase.

3.6 Verificaciones de disponibilidad de los sistemas de custodia

En el momento de registrar un nuevo sistema/repositorio de custodia en la herramienta centralizada de verificación de firmas, la herramienta de verificación de firmas deberá realizar de modo automatizado las comprobaciones necesarias que aseguren la visibilidad de red entre los sistemas y el correcto funcionamiento del sistema/repositorio añadido.

El alta o la modificación de la configuración de un sistema/repositorio origen en ningún caso requerirán de reinicios del sistema que impliquen cortes de servicio por breves que estos puedan ser.

Se deberá prever la posibilidad de verificaciones periódicas automatizadas para comprobar la disponibilidad de los sistemas/repositorios origen y la generación en su caso de alertas (correos,....) destinada a los responsables afectados.

3.7 Incorporación al centro de respaldo

Atendiendo al carácter crítico y a las exigencias de disponibilidad requeridas para la herramienta centralizada de verificación de firmas, ésta deberá incorporarse al centro de respaldo y continuidad de servicios de la Junta de Andalucía. Sin embargo es necesario señalar que en caso de contingencia, el servicio prestado desde el centro de respaldo podría ser incompleto dadas las dependencias en lo relacionado con la disponibilidad de los sistemas/repositorios integrados con la herramienta centralizada de verificación de firmas. Por tanto, los responsables de estos sistemas/repositorios también deberían promover su incorporación al centro de respaldo y continuidad servicios de la Junta de Andalucía.

4 TAREAS DE GESTIÓN DEL SISTEMA

4.1 Modelo de solicitud de alta/modificación/baja

Para la herramienta centralizada de verificación de firmas se requerirán labores de administración encaminadas a gestionar la relación de sistemas/repositorios origen de ubicación de los documentos custodiados. Se deberá confeccionar un modelo de solicitud de alta/modificación/baja de sistema/repositorio origen que contenga al menos la siguiente información:

- Organismo vinculado al sistema/repositorio
- Descripción y nombre del sistema/repositorio
- Identificador del sistema/repositorio (solo para modificaciones)
- Información sobre si es un sistema/repositorio de nueva creación o bien se trata de un sistema/repositorio que ya ha generado transacciones de firma y cuenta con su propio sistema de verificación.
- Parámetros de conexión al servicio (URLs desarrollo, URL producción, usuario de conexión, clave,....)
- Datos de contacto del responsable técnico y el responsable funcional.
- Correo electrónico al que se remitirán las alertas automáticas de aviso en caso de problemas de funcionamiento.

4.2 Protocolo de incorporación a la herramienta centralizada de verificación de firmas

Se describe a continuación el protocolo de incorporación de un sistema/repositorio que custodia documentos a la herramienta centralizada de verificación de firmas.

1 – RECEPCIÓN DE SOLICITUD

El procedimiento de recepción de solicitudes será el habitual en las plataformas y sistemas de administración electrónica: remisión de formulario cumplimentado y firmado.

Este formulario se publicará en la actual web de soporte y administración electrónica de la Junta de Andalucía (Plutón).

2 – ESTUDIO Y VALIDACIÓN DE LA SOLICITUD

Será necesario validar la corrección de los datos consignados en la solicitud y de ser necesario solicitar una subsanación solicitando la corrección de aquellos errores detectados.

3 – ASIGNACIÓN DE IDENTIFICADOR ÚNICO AL SISTEMA

En caso de alta, al nuevo sistema/repositorio que se incorpora se le asignará un identificador único (5 caracteres) permanente en el tiempo.

4 – GUÍAS DE ADAPTACIÓN PARA LOS SISTEMAS/REPOSITORIOS

Se facilitará a los Consejerías y entidades la información técnica necesaria para la integración con la herramienta centralizada y se prestará soporte técnico en la materia.

Será responsabilidad del responsable técnico del sistema/repositorio origen asegurar la correcta generación del código seguro de verificación y la adaptación de los "pies de firma".

5 – ALTA EN ENTORNO DE DESARROLLO

- Registro del sistema/repositorio origen en la zona de administración del punto único de verificación de firmas.
- Comprobación y resolución, en su caso, de visibilidad de red entre los dos sistemas.
- Ejecución de pruebas de integración (test id transacción de firma existente, no existente, sistema/repositorio origen no disponible, etc).

6 – ALTA EN ENTORNO DE PRODUCCIÓN

- Registro del sistema/repositorio origen en la zona de administración del punto único de verificación de firmas.
- Comprobación y resolución, en su caso, de visibilidad de red entre los dos sistemas.
- Ejecución de pruebas de integración (test id transacción de firma existente, no existente, sistema/repositorio origen no disponible, etc)

5 ANEXO I. ESPECIFICACIÓN DEL SERVICIO DE INTEGRACIÓN

En este anexo se describe cómo se realizará la interacción de los sistemas/repositorios que se quieran integrar con la herramienta centralizada de verificación de firmas a través de servicios web.

Todas las operaciones deben ser invocadas enviando (según el esquema definido para cada documento de entrada), un parámetro llamado cv (código de verificación), así como los datos de autenticación (usuario y contraseña).

El código de verificación se corresponde con el identificador normalizado del documento, que tomará la siguiente forma: ES_<Órgano>_<AAAA>_<ID_específico> donde:

1. <Órgano>: Código alfanumérico único para cada órgano/unidad/oficina extraído del Directorio Común gestionado por el Ministerio de Hacienda y Administraciones Públicas (Longitud: 9 caracteres).
2. <AAAA>: Año de la fecha de captura del documento. (Longitud: 4 caracteres).
3. <ID_específico>: Código alfanumérico que identifica de forma única al documento dentro de los generados por la administración responsable. Es indispensable que los 5 primeros caracteres sean el identificador único del sistema/repositorio proporcionado por el punto único de verificación de firmas. Para el resto de caracteres, se recomienda usar el código seguro de verificación propuesto en el Anexo II del presente documento. No obstante, cada administración puede diseñar el proceso de generación según sus necesidades, asegurando en cualquier caso los principios de impredecibilidad, uniformidad, resistencia a colisiones e irreversibilidad (Longitud: 30 caracteres).

También se admitirá un código de verificación que no corresponda a un identificador normalizado, siempre que los 5 primeros caracteres correspondan a un identificador de sistema/repositorio definido en la herramienta.

5.1 Estructura del mensaje a enviar

Se describen a continuación los campos cuyos datos deben ser proporcionados para realizar una petición con el objeto de obtener el documento custodiado.

NOMBRE	DESCRIPCIÓN	TIPO DATO	CARÁCTER
petición	Objeto que representa la petición realizada	XML [cadena de caracteres][1]	Obligatorio

[1] Identificar que este XML [cadena de caracteres], lo obtendrá la herramienta centralizada de verificación de firmas automáticamente mediante la representación en formato XML de los objetos java que componen la petición.

El tipo de **objeto petición se compone de los siguientes objetos Java**:

NOMBRE	DESCRIPCIÓN	TIPO DATO	CARÁCTER
idConsultado	Identificador de la petición	String	Obligatorio
ip	Identificador del host que realiza la petición	String	Obligatorio
perfil	Cadena con uno de los siguientes valores • Ciudadanía • Personal empleado público de la Junta de Andalucía en el ejercicio de sus funciones • Otro personal empleado público en el ejercicio de sus funciones	String	Obligatorio
certEP	Certificado de Empleado Público	CertificadoEP	Opcional
certPF	Certificado de Persona Física	CertificadoPF	Opcional
certPJ	Certificado de Persona Jurídica	CertificadoPJ	Opcional

Detalle del **objeto CertificadoEP**:

NOMBRE	DESCRIPCIÓN	TIPO DATO	CARÁCTER
cifEntidad	CIF de la entidad	String	Obligatorio
nif	NIF del empleado	String	Obligatorio
datosSirhus	Datos devueltos por el sistema SIRhUS	DatosSirhus	Obligatorio
nombreApellidosResponsable	Nombre y apellidos	String	Obligatorio
tipoCertificado	Tipo de certificado	String	Obligatorio
entidadEmisora	Nombre de la entidad emisora del certificado	String	Obligatorio

validoDesde	Fecha de inicio de validez del certificado	Date	Obligatorio
validoHasta	Fecha de fin de validez del certificado	Date	Obligatorio

Detalle del **objeto CertificadoPF**:

NOMBRE	DESCRIPCIÓN	TIPO DATO	CARÁCTER
nif	NIF de la persona	String	Obligatorio
nombreApellidosResponsable	Nombre y apellidos	String	Obligatorio
tipoCertificado	Tipo de certificado	String	Obligatorio
entidadEmisora	Nombre de la entidad emisora del certificado	String	Obligatorio
datosSirhus	Datos devueltos por el sistema SIRhUS	DatosSirhus	Obligatorio
validoDesde	Fecha de inicio de validez del certificado	Date	Obligatorio
validoHasta	Fecha de fin de validez del certificado	Date	Obligatorio

Detalle del **objeto CertificadoPJ**:

NOMBRE	DESCRIPCIÓN	TIPO DATO	CARÁCTER
nif	NIF de la persona	String	Obligatorio
cifEntidad	CIF de la entidad	String	Obligatorio
nombreEntidad	Nombre de la entidad emisora del certificado	String	Obligatorio
cifVinculada	CIF de la entidad vinculada	String	Obligatorio
nombreApellidosResponsable	Nombre y apellidos	String	Obligatorio
tipoCertificado	Tipo de certificado	String	Obligatorio
entidadEmisora	Nombre de la entidad emisora del certificado	String	Obligatorio

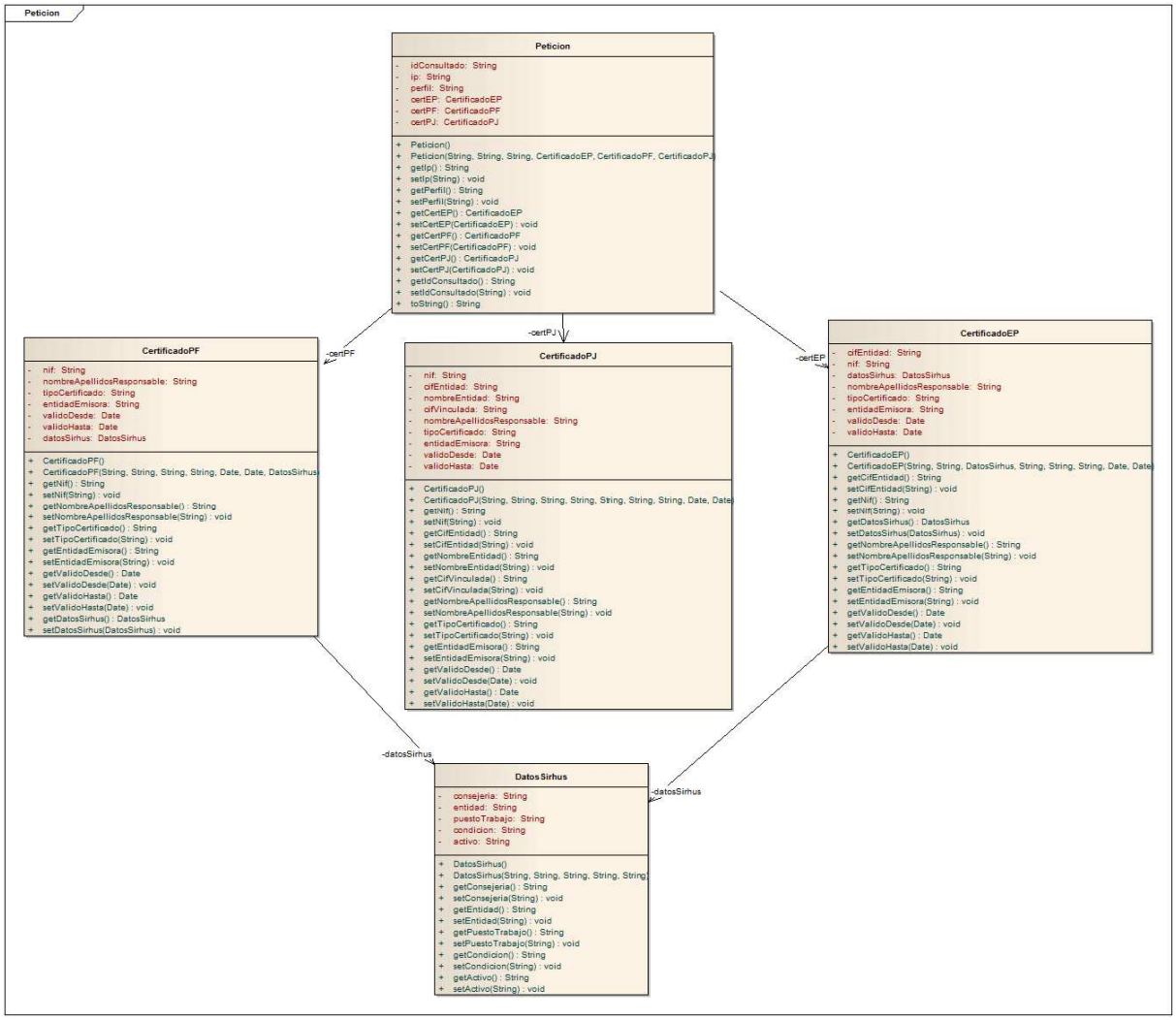
validoDesde	Fecha de inicio de validez del certificado	Date	Obligatorio
validoHasta	Fecha de fin de validez del certificado	Date	Obligatorio

Detalle del **objeto DatosSirhus**:

NOMBRE	DESCRIPCIÓN	TIPO DATO	CARÁCTER
consejeria	Nombre de la Consejería	String	Obligatorio
entidad	Entidad a la que pertenece	String	Obligatorio
puestoTrabajo	Puesto de trabajo	String	Obligatorio
condicion	Condición	String	Obligatorio
activo	Usuario activo en el sistema	String	Obligatorio

Será necesario incluir una cabecera con las credenciales de autorización (usuario y clave) en la petición del servicio de integración.

A continuación se muestra el diagrama UML con la relación entre las entidades descritas anteriormente:



5.2 Estructura del mensaje de salida

Se describen a continuación los campos que deben devolver los sistemas/repositorios tras la petición de consulta por parte de la herramienta centralizada de verificación de firma.

NOMBRE	DESCRIPCIÓN	TIPO DATO	CARÁCTER
codigoRespuesta	Código de respuesta, bien de respuesta correcta o de respuesta errónea	Tipificado. En el Anexo III del presente documento se especifican los posibles códigos de respuesta.	Obligatorio
mensajeRespuesta	Mensaje de respuesta	Cadena de caracteres	Obligatorio
idEni	Identificador normalizado del documento ENI	Cadena de caracteres	Obligatorio
documentoENI	Documento ENI	XML [cadena de caracteres cuyo contenido se corresponde con lo definido en la Norma Técnica de Interoperabilidad del Documento Electrónico[2]]	Obligatorio
informeFirma	Documento PDF de justificante de firma, en el que se incluye el pie de firma. En el caso de que se devuelva este fichero, se mostrará al usuario final la posibilidad de acceder al mismo.	Fichero [cadena de bytes]	Opcional

[2] Identificar que es necesario incluir nuevos valores para el campo "*TipoFirmasElectronicas*" de forma que se puedan contemplar formatos de firma no incluidos en la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración, sin perjuicio de que no se deba continuar con la utilización de los mismos. Se han incluido los tipos de firmas:

- **TF98**: para formatos de firma CMS.
- **TF99**: para otros formatos de firma (por ejemplo PKCS#7).

textoLibre	Texto libre de respuesta para ser mostrado al usuario final. Si este campo se complementa por el sistema/repositorio se mostrará al usuario única y exclusivamente dicho texto, ignorando el resto de la información.	Cadena de caracteres	Opcional
textoAdicional	Texto libre adicional de respuesta para ser mostrado al usuario final, junto con los demás resultados del proceso	Cadena de caracteres	Opcional
generadorFirma	En caso de firma electrónica basada en certificado, componente o herramienta utilizada para su generación.	Cadena de caracteres	Opcional
marcaTiempo	Información de utilidad para las firmas electrónicas que no incorporen sello de tiempo. Marca de tiempo de generación / incorporación del documento al sistema/repositorio y conforme al artículo 15 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.	Fecha	Opcional
validacionCertificadosFirma	Validación de certificados en el momento de realizar la firma basada en certificado electrónico.	Booleano	Opcional
selloTiempoRequerido	Indica si el sello de tiempo es o no requerido	Booleano	Opcional
identificadorDocumentoSustituto	Identificador normalizado que, en su caso, hubiera sustituido al documento al cual se intenta acceder	Cadena de caracteres	Opcional
campoAdicional	Campo adicional que se utilizará para posibles necesidades futuras.	Cadena de caracteres	Opcional

A continuación se muestra el diagrama UML con la relación entre las entidades descritas anteriormente:

6 ANEXO II. GENERACIÓN DE CÓDIGO SEGURO DE VERIFICACIÓN

Este anexo presenta, a modo de ejemplo, una propuesta para calcular los 25 caracteres últimos para formar un código seguro de verificación.

a. En primer lugar, se generará una cadena de caracteres concatenando la dirección MAC del servidor, la fecha actual en milisegundos y un número aleatorio.
b. Sobre esta cadena de caracteres resultante, se aplica un algoritmo SHA1 para generar un hash, el cual será truncado a 96 bits.
c. Una vez obtenido este código, se codificará en base64 con el fin de obtener 19 caracteres alfanuméricos en los rangos de a-z, A-Z, 0-9, $ y &.
d. A estos 19 caracteres se le concatenarán 6 caracteres, siendo éstos de libre uso por la Consejería o entidad (para codificaciones propias, especificación de dominios funcionales, etc.)

Cada Consejería, entidad, sistema/repositorio, puede utilizar otros medios para la generación de los códigos, atendiendo a sus prácticas, políticas y necesidades en materia de gestión documental.

7 ANEXO III. TIPIFICACIÓN DEL CÓDIGO DE RESPUESTA

El servicio de integración proporcionado por los sistemas/repositorios debe devolver un código de respuesta (campo codigoRespuesta) que estará tipificado en base a los siguientes valores:

CÓDIGO RESPUESTA	DESCRIPCIÓN
0	Respuesta correcta.
1	Credenciales de autorización (usuario y clave) en la petición del servicio de integración errónea. Solución: Enviar las credenciales de autorización de forma correcta. Consultar con el administrador de la Herramienta de verificación de firmas.
2	Documento no encontrado en base al campo CV remitido y no existe un identificador normalizado de documento que sustituya al CV remitido. Solución: Consultar con el administrador del sistema/repositorio.
3	Firma del documento no encontrada en base al campo CV remitido. Solución: Consultar con el administrador del sistema/repositorio.
4	Documento no encontrado en base al campo CV remitido, pero existe un identificador normalizado de documento que sustituye al CV remitido. Solución: Devolver el mensaje "El documento solicitado no se encuentra disponible" y el identificador del documento Electrónico que lo sustituye.
90	Error técnico de acceso a los datos por parte del sistema/repositorio. Solución: Ponerse en contacto con el administrador del sistema/repositorio para que se solucione la incidencia.

Estos códigos de respuestas serán ampliados en base a las necesidades que vayan surgiendo durante la implantación de la solución.

8 ANEXO IV. AYUDA AL INTEGRADOR DE APLICACIONES

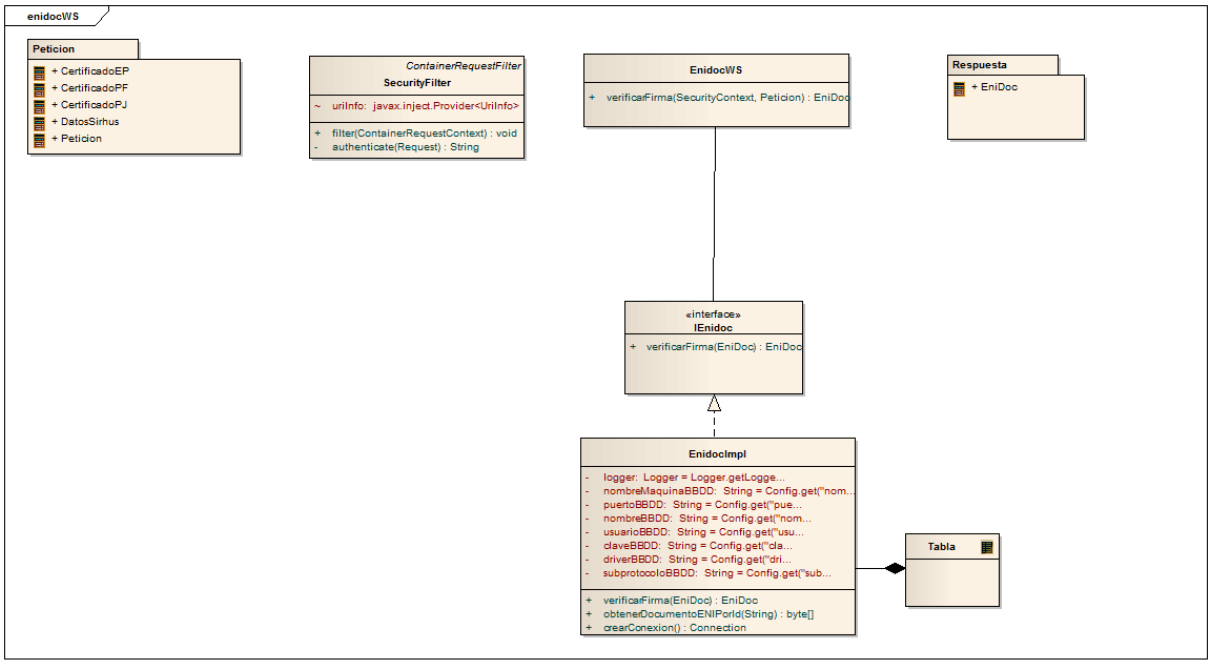
La implementación que deberán realizar los sistemas/repositorios con las que se integra la herramienta centralizada de verificación de firmas, a través del contenedor web de servicios REST consistirá en la **reimplementación del método verificarFirma**.

A continuación se muestra un ejemplo de implementación de este método con el objetivo de guiar a los desarrolladores en la secuencia de pasos a seguir para obtener el documento en formato ENIDOC.

```
public EniDoc verificarFirma(EniDoc eniDoc) {

        // Recuperar el identificador normalizado del documento electrónico ENI
        // (ES_A01002823_2013_APPLI001202336138600203236646 8)
        String idEni = eniDoc.getIdEni();

        // TODO Tratamiento opcional del identificador normalizado para acceder
        // al modelo de datos en caso de ser necesario para obtener el documento

        // TODO Obtener documento de BBDD mediante el identificador facilitado
        byte[] documento = obtenerDocumentoENIPorId(idEni);
        String documentoStr = new String(documento);

        // TODO Rellenar el objeto EniDoc
        // 1.- String que contiene el documento electrónico ENI. Obligatorio.
        eniDoc.setDocumentoENI(documentoStr);

        // 2.- Array de bytes que contiene el documento original con el cajetín
        // de firma incorporado. Opcional.
        byte[] informeFirma = new byte[1024];
        eniDoc.setInformeFirma(informeFirma);

        // 3.- Texto libre de respuesta para ser mostrado al usuario final. Si
        // este campo se complementa se dispondrá al usuario única y
        // exclusivamente dicho texto, ignorando el resto de la información.
        // Opcional.
        String textoLibre = "";
        eniDoc.setTextoLibre(textoLibre);

        // 4.- Texto libre adicional de respuesta para ser mostrado al usuario
```

```
        // final, junto con los demás resultados del proceso. Opcional.
        String textoAdicional = "";
        eniDoc.setTextoAdicional(textoAdicional);

        // 5.- En caso de firma electrónica basada en certificado, componente o
        // herramienta utilizada para su generación. Opcional.
        String generadorFirma = "";
        eniDoc.setGeneradorFirma(generadorFirma);

        // 6.- Información de utilidad para las firmas electrónicas que no
        // incorporen sello de tiempo. Opcional.
        Date marcaTiempo = new Date();
        eniDoc.setMarcaTiempo(marcaTiempo);

        // 7.- Campo adicional que se utilizará para posibles necesidades
        // futuras, en el caso que se requiera alguna información adicional.
        String campoAdicional = "";
        eniDoc.setCampoAdicional(campoAdicional);

        // Devolver el objeto EniDoc relleno.
        return eniDoc;
}
```

Se muestra el diagrama UML de relación entre componentes:



9 REFERENCIAS

Objeto	Referencia
Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.	http://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-1331
Norma Técnica de Interoperabilidad de Documento electrónico	http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-13169
Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración	http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-13171
REST	http://es.wikipedia.org/wiki/Representational_State_Transfer