



JUNTA DE ANDALUCÍA

CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA

Presentación

Herramienta Centralizada de Verificación

Herramienta Centralizada de Verificación

Índice

1. Introducción

1.1 ¿Qué es? ¿Cuál es su objetivo?

1.2 Evolución de VerificarFirma a la HCV

2. Validación a partir de código de verificación

2.1 Estructura de intercambio de información

2.2 Código de verificación

2.3 Metadato Identificador del documento electrónico

2.4 Escenario habitual de uso

3. Validación a partir de fichero de firma

3.1 Escenario habitual de uso

4. Servicio de Integración - EnidocWS

4.1 Componente EnidocWS

4.2 Descripción del servicio de integración

5. Integración con EnidocWS

5.1 Modos de integración

5.1 Ejemplo de implementación

Herramienta Centralizada de Verificación

Índice

1. Introducción

1.1 ¿Qué es? ¿Cuál es su objetivo?

1.2 Evolución de VerificarFirma a la HCV

2. Validación a partir de código de verificación

2.1 Estructura de intercambio de información

2.2 Código de verificación

2.3 Metadato Identificador del documento electrónico

2.4 Escenario habitual de uso

3. Validación a partir de fichero de firma

3.1 Escenario habitual de uso

4. Servicio de Integración - EnidocWS

4.1 Componente EnidocWS

4.2 Descripción del servicio de integración

5. Integración con EnidocWS

5.1 Modos de integración

5.1 Ejemplo de implementación

Introducción

¿Qué es la Herramienta Centralizada de Verificación?

La Herramienta Centralizada de Verificación (HCV) implementa un **servicio para la práctica de la verificación**, mediante un código generado electrónicamente, de documentos firmados electrónicamente en la Administración de la Junta de Andalucía, para el contraste de su autenticidad y la comprobación de su integridad.

¿Cuál es su objetivo?

El propósito de la herramienta centralizada de verificación es:

- Disponer de cara a la ciudadanía de un **único punto** que permita homogeneizar y unificar la práctica de la verificación de documentos en la Administración de la Junta de Andalucía.
- Posibilitar el **cese en el despliegue de nuevas implantaciones** de herramientas locales de verificación.

Se trata de una actuación de impulso de **adecuación** al Esquema Nacional de Interoperabilidad (ENI) en el ámbito de la Administración Electrónica, y en particular de la **Norma Técnica de Interoperabilidad de Documento Electrónico**.

Introducción

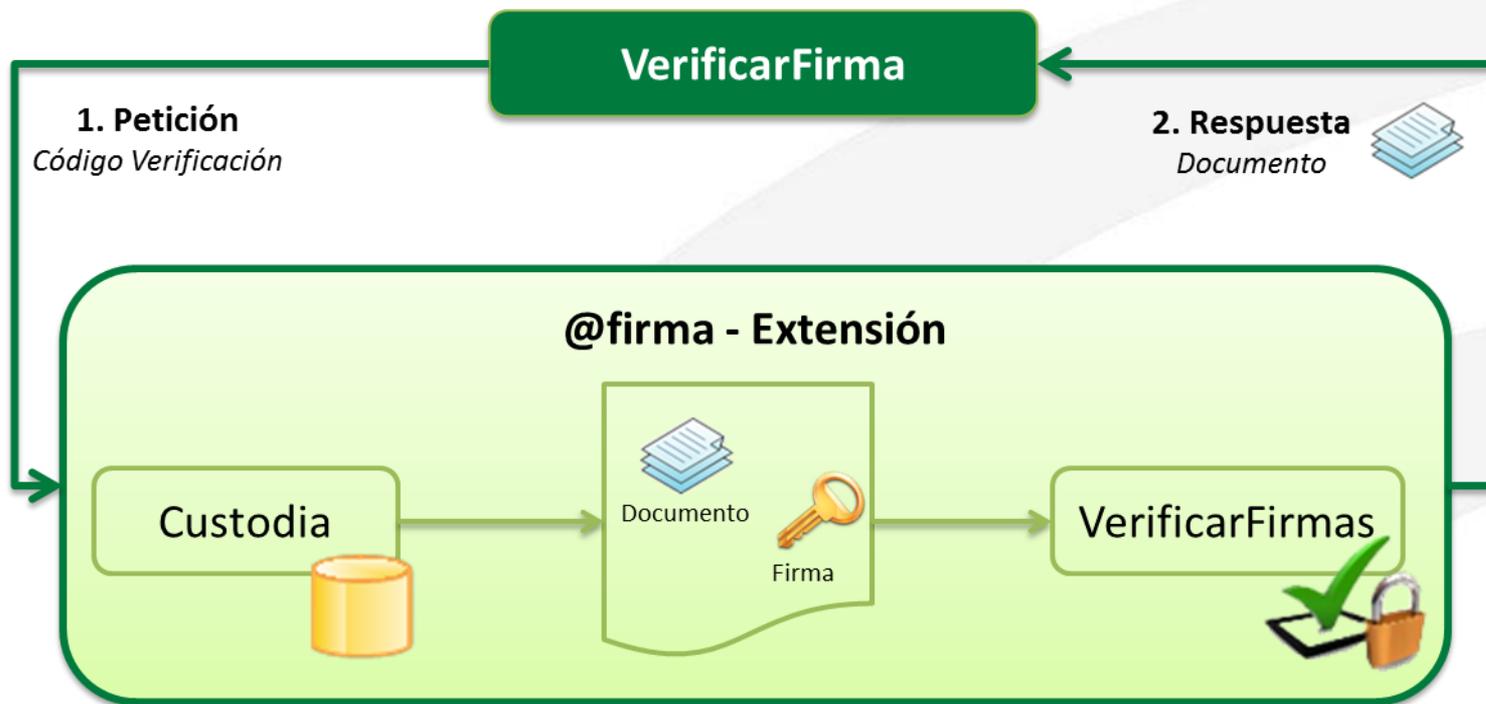
HCV: Sistema único de verificación de firmas

- La HCV es la única herramienta que debe utilizarse para la práctica de la verificación, mediante un código generado electrónicamente, de documentos firmados electrónicamente en la Administración de la Junta de Andalucía, para el contraste de su autenticidad y la comprobación de su integridad.
- A partir del 31/03/2016 no se prestará soporte técnico para otras herramientas con propósito similar que puedan estar implantadas.
- La próxima versión de la herramienta Portafirmas, que se liberará en breve, dejará de utilizar una implantación específica de una herramienta de este tipo, y se integrará con la HCV.

Introducción

Evolución de VerificarFirma a la Herramienta Centralizada de Verificación

La situación anterior del sistema VerificarFirma se representa de la siguiente manera:



Herramienta Centralizada de Verificación

Índice

1. Introducción

1.1 ¿Qué es? ¿Cuál es su objetivo?

1.2 Evolución de VerificarFirma a la HCV

2. Validación a partir de código de verificación

2.1 Estructura de intercambio de información

2.2 Código de verificación

2.3 Metadato Identificador del documento electrónico

2.4 Escenario habitual de uso

3. Validación a partir de fichero de firma

3.1 Escenario habitual de uso

4. Servicio de Integración - EnidocWS

4.1 Componente EnidocWS

4.2 Descripción del servicio de integración

5. Integración con EnidocWS

5.1 Modos de integración

5.1 Ejemplo de implementación

Validación a partir de código de verificación

Estructura de intercambio de información

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

Contenido: documento original necesario para poder facilitarlo al usuario que realiza la consulta y para poder verificar la integridad del documento

Firma/s: necesario para poder verificar la integridad de la transacción de las firmas.

Metadatos: permitirá ofrecer información del documento firmado.

Campos 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.

Validación a partir de código de verificación

Código de verificación

El nuevo **código de verificación** aceptado por la herramienta centralizada de verificación será una cadena de 30 caracteres de los cuales los 5 primeros serán los del identificador único del sistema/repositorio. Los 25 caracteres restantes deberán cumplir con los requisitos que ha de tener un código seguro de verificación en cuanto a impredecibilidad, resistencia a colisiones, unicidad e irreversibilidad. La **documentación técnica** de la HCV propone un algoritmo de generación de códigos seguros de verificación.

Validación a partir de código de verificación

Metadato Identificador del documento electrónico

En aquellos casos en los que el repositorio/sistema que custodia el documento no esté en disposición de asignar identificadores normalizados de documentos según lo dispuesto en la Norma Técnica de Interoperabilidad de Documento Electrónico, como por ejemplo en el ámbito de las entidades no incorporadas al Directorio Común de Unidades Orgánicas, el metadato “Órgano” deberá adoptar el valor “XXXXXXXXXX”. Ante esta circunstancia, la HCV ocultará en la pantalla resultante de una validación el área de metadatos.

Si se asigna un valor al metadato mínimo obligatorio **Identificador** del Documento Electrónico deberá cumplir con los requisitos definidos por la la Norma Técnica de Interoperabilidad del Documento Electrónico y, adicionalmente, los requisitos exigidos por la HCV.

<IDIOMA>_<ÓRGANO>_<AAAA>_<ID_ESPECIFICO>	
<IDIOMA>	Código del idioma o lengua cooficial del documento: - <i>ES: español</i>
<ÓRGANO>	Siguiendo lo establecido en el Directorio Común (DIR3)
<AAAA>	Año de la fecha de captura del documento
<ID_ESPECIFICO>	Código alfanumérico que identifica de forma única al documento dentro de los generados por la administración responsable. (Longitud: 30 caracteres) ▪Es indispensable que los 5 primeros caracteres sean el identificador único del sistema/repositorio proporcionado por la HCV. ▪Para el resto de caracteres, cada administración puede diseñar el proceso de generación según sus necesidades, asegurando en cualquier caso su unicidad y que no coincidan con el valor del código de verificación.

Validación a partir de código de verificación

Escenario habitual de uso

1. Autenticación en la herramienta

El usuario puede autenticarse en la herramienta mediante **certificado electrónico**, pudiéndose el mismo de persona física, persona jurídica o empleado público, o bien, mediante **usuario y contraseña de correo (LDAP)** siempre que el acceso sea desde Red Corporativa de la Junta de Andalucía.

Se determinan tres perfiles de acceso a la herramienta:

1. Personal empleado público de la Junta de Andalucía en el ejercicio de sus funciones.
2. Otro personal empleado público en el ejercicio de sus funciones.
3. Ciudadanía.

La herramienta centralizada de verificación determinará el perfil según el tipo de acceso:

Certificado:

- **Persona Física:** el usuario podrá seleccionar entre todos los perfiles disponibles “Ciudadanía” “Personal empleado público de la Junta de Andalucía en el ejercicio de sus funciones” u “Otro personal empleado público en el ejercicio de sus funciones”.
- **Persona Jurídica:** se determinará por defecto el perfil de “Ciudadanía”.
- **Empleado Público:** se determinará por defecto el perfil de “Otro personal empleado público en el ejercicio de sus funciones”, en caso de que pertenezca a la Junta de Andalucía será entonces “Personal empleado público de la Junta de Andalucía en el ejercicio de sus funciones”.

LDAP:

El acceso mediante usuario y contraseña equivale al acceso como “Personal empleado público de la Junta de Andalucía en el ejercicio de sus funciones”

Validación a partir de código de verificación

Escenario habitual de uso

2. Petición de acceso a documento

En este punto se sigue el siguiente flujo de acciones:

- I. El usuario facilita el código de verificación del documento.
 - i. Se requerirá al usuario que indique un motivo de acceso al documento según se haya configurado para cada perfil de acceso.
- II. Con la información anterior, la herramienta de verificación invoca el correspondiente servicio web definido para el sistema/repositorio y recupera el documento, firma e información complementaria empleando el protocolo común de comunicación definido.
- III. La herramienta de verificación 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 utilizan los actuales servicios DSS de integración con la plataforma @firma.

Validación a partir de código de verificación

Escenario habitual de uso

Datos de la persona que realiza la consulta

Nombre y apellidos:	NIF:
NOMBRE APELLIDO1 APELLIDO2	12345678Z
Tipo de certificado:	
FNMT PF	
Motivación del acceso:	
<input checked="" type="radio"/> Ciudadanía	
<input type="radio"/> Personal empleado público de la Junta de Andalucía en el ejercicio de sus funciones	
<input type="radio"/> Otro personal empleado público en el ejercicio de sus funciones	

Datos de la consulta

Código de verificación:
<input type="text" value="ES_A01002823_2014_7yElx367415352w6nIU8F1+imT5dQi"/>
Motivo de acceso al documento:
<input type="text"/>
<input type="button" value="LIMPIAR"/> <input type="button" value="CONSULTAR"/>

Ejemplo de autenticación y consulta mediante certificado electrónico de **persona física**.

Validación a partir de código de verificación

Escenario habitual de uso

3. Disposición de la información

La herramienta de verificación muestra la información recopilada al usuario, y pone a su disposición el fichero original firmado, ofreciendo también la posibilidad de descargar el documento ENI, sus firmas electrónicas y su informe de firma, en caso de que este haya sido facilitado por el sistema/repositorio consultado.

Información detallada de firmas

Firma: **CAdES detached/explicit signature** 
Resultado de la validación: **La firma es válida**
Información de firmantes:
Nombre completo: **XXXXXXXXXXXXXXXXXXXXXXXXXXXX**
Sello de tiempo: **24/04/2014 17:58:04**

Metadatos mínimos obligatorios del documento electrónico

Versión NTI: **http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e**
Identificador: **ES_A01002823_2014_7yElx367415352w6nlU8F1+imT5dQi**
Órgano: **A01002823**
Fecha de captura: **24/04/2014 17:58:04**
Origen: **Administración**
Estado de elaboración: **Copia electrónica auténtica de documento papel**
Nombre de formato: **PDF**
Tipo documental: **Contrato**

Datos complementarios del documento electrónico

Comentarios: **Texto adicional de prueba mostrado al usuario**
Generador de firma: **Cliente @firma 3.3.1_12**

Ficheros descargables

 **Descargar fichero original**
 **Descargar documento ENI**

Herramienta Centralizada de Verificación

Índice

1. Introducción

1.1 ¿Qué es? ¿Cuál es su objetivo?

1.2 Evolución de VerificarFirma a la HCV

2. Validación a partir de código de verificación

2.1 Estructura de intercambio de información

2.2 Código de verificación

2.3 Metadato Identificador del documento electrónico

2.4 Escenario habitual de uso

3. Validación a partir de fichero de firma

3.1 Escenario habitual de uso

4. Servicio de Integración - EnidocWS

4.1 Componente EnidocWS

4.2 Descripción del servicio de integración

5. Integración con EnidocWS

5.1 Modos de integración

5.1 Ejemplo de implementación

Validación a partir de fichero de firma

Escenario habitual de uso

Si se accede a la herramienta de verificación desde la Red Corporativa de la Junta de Andalucía se muestra la posibilidad de realizar validaciones de firma.



Se accede, por tanto, a la funcionalidad de validar firmas, mediante la cual se podrá validar un fichero de firma adjuntándolo en el formulario, en ocasiones es posible que se precise el documento original, que también podrá ser adjuntado de forma análoga.

Validación de firmas

Puede comprobar la validez de una firma electrónica mediante la plataforma @firma. Para ello siga los siguientes pasos:

Seleccione la firma a validar

No se ha seleccionado ningún archivo.

Validación a partir de fichero de firma

Escenario habitual de uso

Una vez incorporada la firma a validar, se comunica con @firma para comprobar su validez y se obtiene una pantalla de resultado que muestra información relevante de la propia firma, así como la posibilidad de descargar ficheros asociados a la misma.

Resultado de Validar Firma

Detalle de la validación

Resultado de la validación: **La firma es válida** ✓
 Tipo de firma: **XADES-EPES**
 Modo de firma: **ENVELOPED**
 Fecha y hora de la validación: **30/09/2015 13:53:31**

Informes de firma individuales

Firma 1
 Resultado de la validación: **La firma es valida**
 Fecha y hora del sello de tiempo: **La firma no tiene sello de tiempo**
 Identificador de la política: http://www.facturae.es/politica_de_firma_formato_facturae/politica_de_firma_formato_facturae_v3_1.pdf
 Información del certificado:

Asunto	CN=NOMBRE <small>NOMBRE Y APELLIDOS Y NOMBRE APELLIDOS Y APELLIDOS Y APELLIDOS - NIF</small> ,OU= <small>NOMBRE Y APELLIDOS</small> ,OU=FNMT Clase 2 CA,O=FNMT,C=ES
Nombre y apellidos	<small>NOMBRE Y APELLIDOS Y NOMBRE APELLIDOS Y APELLIDOS Y APELLIDOS</small>
Entidad Emisora	FNMT
Tipo de certificado	FNMT PF
Fecha de creación	20/10/2014 08:54:03
Fecha de caducidad	20/10/2017 08:54:03

 **Descargar certificado**

Ficheros descargables

 **Descargar documento original**

Validación a partir de fichero de firma

Ejemplo de validación: Certificado FNMT AC Usuarios

1. Validación de firma realizada con certificado de persona física FNMT AC Usuarios revocado.

Resultado de Validar Firma

Detalle de la validación

Resultado de la validación: Error en el proceso de validación. **El certificado firmante esta revocado** ❌
 Tipo de firma: CADES-BES
 Fecha y hora de la validación: 01/10/2015 14:30:22

Informes de firma individuales

Firma 1

Resultado de la validación: **El certificado firmante esta revocado**
 Fecha y hora del sello de tiempo: **La firma no tiene sello de tiempo**
 Información del certificado:

Asunto	CN=APELLIDO1PF APELLIDO2PF PRUEBASPF - 00000000T,2.5.4.4=#0C174150454C4C49444F315046204150454C4C49444F325046,2.5.4.42=#0C095052554542
Nombre y apellidos	PRUEBASPF APELLIDO1PF APELLIDO2PF
Entidad Emisora	FNMT-RCM
Tipo de certificado	FNMT PERSONA FISICA
Fecha de creación	04/11/2014 17:53:29
Fecha de caducidad	04/11/2018 17:53:29

 [Descargar certificado](#)

VOLVER

IMPRIMIR

Validación a partir de fichero de firma

Ejemplo de validación: Certificado FNMT Sello electrónico

2. Validación de firma realizada con certificado de sello electrónico emitido por FNMT

Resultado de Validar Firma

Detalle de la validación

Resultado de la validación: **La firma es válida** ✓
 Tipo de firma: **CADES-T**
 Fecha del sello de tiempo más reciente: **29/07/2015 13:53:55**
 Fecha y hora de la validación: **01/10/2015 14:34:58**

Informes de firma individuales

Firma 1
 Resultado de la validación: **La firma es válida**
 Fecha y hora del sello de tiempo: **29/07/2015 13:53:55**
 Información del certificado:

Asunto	CN=DIRECCION GENERAL DE POLITICA DIGITAL,SERIALNUMBER=S4111001F,OU=sello electrónico,O=JUNTA DE ANDALUCIA,C=ES
Entidad Emisora	FNMT-RCM
Tipo de certificado	FNMT AC - SELLO ELECTRONICO
Fecha de creación	19/05/2015 18:52:35
Fecha de caducidad	19/05/2018 18:52:35

 [Descargar certificado](#)

Ficheros descargables

 [Descargar documento original](#)

VOLVER

IMPRIMIR

Validación a partir de fichero de firma

Ejemplo de validación: Certificado FNMT AC Componentes Informáticos

3. Validación de firma realizada con certificado de componente emitido por FNMT AC Componentes Informáticos

Resultado de Validar Firma

Detalle de la validación

Resultado de la validación: **La firma es válida** ✓
 Tipo de firma: **CADES-BES**
 Fecha y hora de la validación: **01/10/2015 14:40:21**

Informes de firma individuales

Firma 1
 Resultado de la validación: **La firma es valida**
 Fecha y hora del sello de tiempo: **La firma no tiene sello de tiempo**
 Información del certificado:

Asunto	CN=ws024.juntadeandalucia.es,SERIALNUMBER=S4111001F,OU=CONSEJERIA DE HACIENDA Y ADMINISTRACION PUBLICA,O=JUNTA DE ANDALUCIA,L=SEVILLA,C=ES
Entidad Emisora	FNMT-RCM
Tipo de certificado	FNMT SSL estandar PJ
Fecha de creación	10/09/2014 15:29:20
Fecha de caducidad	10/09/2017 15:29:19

 [Descargar certificado](#)

Ficheros descargables

 [Descargar documento original](#)

VOLVER

IMPRIMIR

Herramienta Centralizada de Verificación

Índice

1. Introducción

1.1 ¿Qué es? ¿Cuál es su objetivo?

1.2 Evolución de VerificarFirma a la HCV

2. Validación a partir de código de verificación

2.1 Estructura de intercambio de información

2.2 Código de verificación

2.3 Metadato Identificador del documento electrónico

2.4 Escenario habitual de uso

3. Validación a partir de fichero de firma

3.1 Escenario habitual de uso

4. Servicio de Integración - EnidocWS

4.1 Componente EnidocWS

4.2 Descripción del servicio de integración

5. Integración con EnidocWS

5.1 Modos de integración

5.1 Ejemplo de implementación

Servicio de Integración - EnidocWS

Componente EnidocWS

Para los sistemas/repositorios que requieran integrarse y hacer uso de las funcionalidades disponibles en la herramienta centralizada de verificación, se presenta el **componente EnidocWS**.

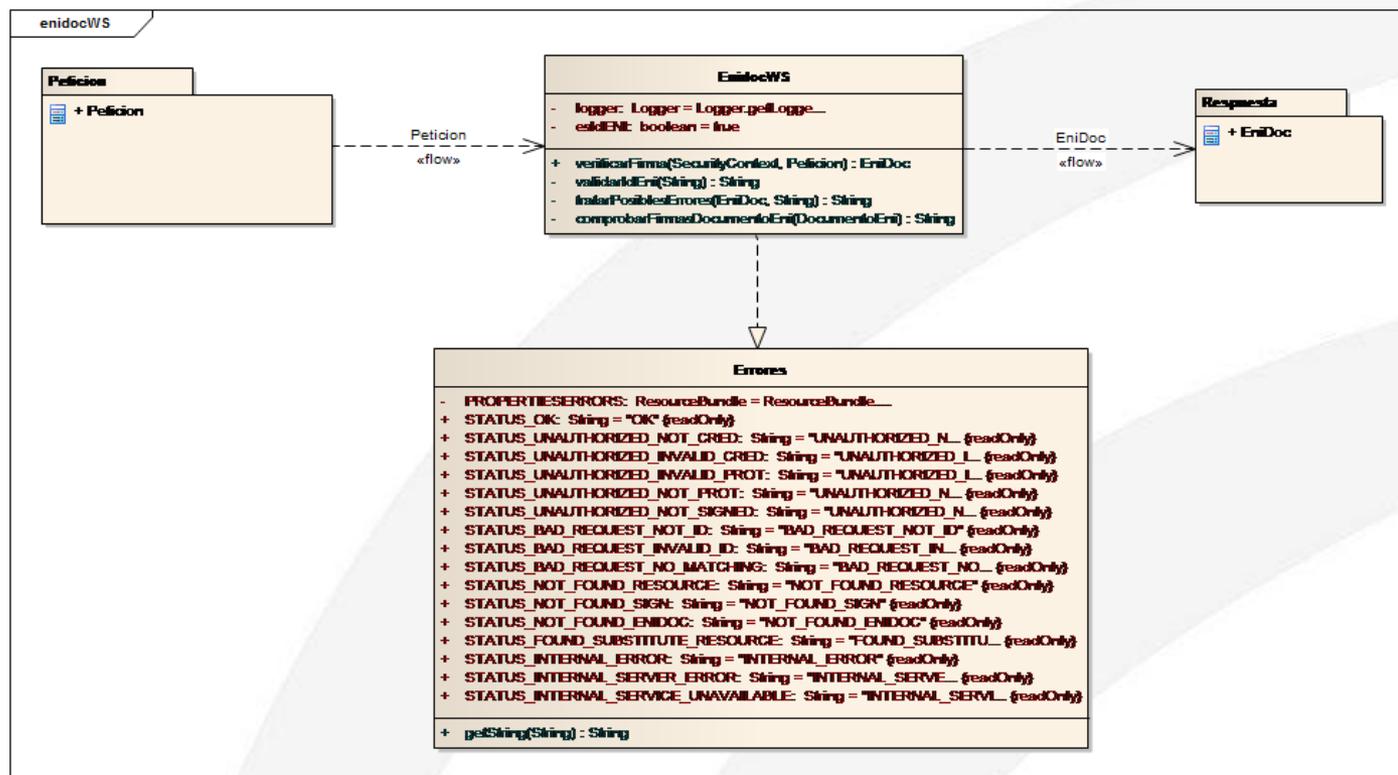
Este componente ofrece un **Servicio Web**, cuya operativa se centra en recuperar un Documento Electrónico con el formato definido en la NTI de Documento Electrónico, y proporcionar la información requerida por la herramienta centralizada de verificación. Esto permite abstraer al integrador del desarrollo de un servicio web para tal fin y de la especificación del mismo, facilitando de esta manera una rápida interacción con la herramienta.

Este servicio web ha sido desarrollado bajo REST (*Representational State Transfer*, técnica de arquitectura software para sistemas hipermedia distribuidos), haciendo uso del framework *Jersey* para implementación de Servicios Web RESTful en Java.

Servicio de Integración - EnidocWS

Descripción del servicio de integración

Se muestra el diagrama que representa el **flujo de integración** y la relación entre las distintas clases que conforman el componente:



La implementación que deberán realizar los sistemas/repositorios que se integren con la herramienta centralizada de verificación, consistirá, principalmente, en la implementación de un método estático que recibe como parámetro de entrada un objeto de tipo **Petición** y devuelve como respuesta un objeto de tipo **Enidoc**, cuyo contenido será un documento ENI acompañado de un conjunto de campos adicionales.

Servicio de Integración - EnidocWS

Estructura de la Petición

El objeto cuyos datos serán proporcionados por la herramienta centralizada de verificación, denominado **Peticion** es el siguiente:

NOMBRE	DESCRIPCIÓN	TIPO DATO	CARÁCTER
peticion	Objeto que representa la petición realizada por la herramienta centralizada de verificación.	Peticion	Obligatorio

El tipo de objeto Peticion se compone de los siguientes parámetros:

NOMBRE	DESCRIPCIÓN	TIPO DATO	CARÁCTER
idConsultado	Identificador de la petición. Será el código seguro de verificación facilitado por el usuario a la HCV.	String	Obligatorio
ip	Identificador del host que realiza la petición.	String	Obligatorio
perfil	Cadena con uno de los siguientes valores <ul style="list-style-type: none"> • 0: Ciudadanía • 1: Personal empleado público de la Junta de Andalucía en el ejercicio de sus funciones • 2: Otro personal empleado público en el ejercicio de sus funciones 	String	Obligatorio
motivo	Motivo por el cual el usuario desea acceder al documento.	String	Opcional
certEP	Certificado de Empleado Público	CertificadoEP	Opcional
certPF	Certificado de Persona Física	CertificadoPF	Opcional
certPJ	Certificado de Persona Jurídica	CertificadoPJ	Opcional

Servicio de Integración - EnidocWS

Estructura de la Petición

Detalle del objeto **CertificadoEP**:

NOMBRE	DESCRIPCIÓN	TIPO DATO	CARÁCTER
cifEntidad	CIF de la entidad	String	Obligatorio
nif	NIF del empleado	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	Opcional

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	Opcional

Servicio de Integración - EnidocWS

Estructura de la Petición

Detalle del objeto **CertificadoPJ**:

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

Detalle del objeto **DatosSirhus**:

NOMBRE	DESCRIPCIÓN	TIPO DATO	CARÁCTER
consejeria	Nombre de la Consejería	String	Obligatorio
organismoAutonomo	Entidad a la que pertenece	String	Obligatorio
centroDirectivo	Centro directivo	String	Obligatorio
puestoTrabajo	Puesto de trabajo	String	Obligatorio
provincia	Provincia	String	Obligatorio
situacion	Situación	String	Obligatorio

La obtención de datos del sistema SIRhUS a partir del NIF es "tolerante a fallos" en el sentido de que si no se obtiene respuesta en un tiempo prudencial, o bien se obtiene una respuesta errónea, se completará el objeto con los correspondientes campos vacíos.

Servicio de Integración - EnidocWS

Estructura de la Respuesta

El objeto de respuesta, denominado EniDoc, que deben devolver los sistemas/repositorios tras la petición de consulta por parte de la herramienta, es el siguiente:

NOMBRE	DESCRIPCIÓN	TIPO DATO	CARÁCTER
eniDoc	Objeto que representa la respuesta a devolver por los sistemas/repositorios	EniDoc	Obligatorio

El tipo de objeto **EniDoc** se compone de los siguientes parámetros:

NOMBRE	DESCRIPCIÓN	TIPO DATO	CARÁCTER
documentoENI	<p>Documento ENI, cuyo contenido se corresponde con lo definido en la NTI de Documento Electrónico.</p> <p>En aquellos casos en los que el repositorio/sistema que custodia el documento no esté en disposición de asignar identificadores normalizados de documentos según lo dispuesto en la Norma Técnica de Interoperabilidad de Documento Electrónico, como por ejemplo en el ámbito de las entidades no incorporadas al Directorio Común de Unidades Orgánicas, el metadato "Órgano" deberá adoptar el valor "XXXXXXXXXX". Ante esta circunstancia, la HCV ocultará en la pantalla resultante de una validación el área de metadatos.</p>	Fichero [array de bytes]	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 [array de bytes]	Opcional

Servicio de Integración - EnidocWS

Estructura de la Respuesta

NOMBRE	DESCRIPCIÓN	TIPO DATO	CARÁCTER
textoLibre	Texto libre de respuesta para ser mostrado al usuario final. Si este campo se completa por el sistema/repositorio se mostrará al usuario única y exclusivamente dicho texto, ignorando el resto de la información.	String	Opcional
textoAdicional	Texto libre adicional de respuesta para ser mostrado al usuario final, junto con los demás resultados del proceso.	String	Opcional
generadorFirma	En caso de firma electrónica basada en certificado, componente o herramienta utilizada para su generación.	String	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.	Date	Opcional
validacionCertificadosFirma	Validación de certificados en el momento de realizar la firma basada en certificado electrónico.	boolean	Opcional
selloTiempoRequerido	Indica si el sello de tiempo es o no requerido.	boolean	Opcional

Servicio de Integración - EnidocWS

Estructura de la Respuesta

NOMBRE	DESCRIPCIÓN	TIPO DATO	CARÁCTER
identificadorDocumentoSustituto	Identificador normalizado que, en su caso, hubiera sustituido al documento al cual se intenta acceder.	String	Opcional
depositoSeguro	Indica si la firma electrónica está almacenada en un depósito seguro.	boolean	Opcional
descargarFirmaydocumentoENI	Indica si se desea habilitar que la persona usuaria de la herramienta pueda descargar el correspondiente fichero de firma electrónica y el documento ENI.	boolean	Opcional
tipoFirmaNoNormalizada	Se considera este campo, en el caso de que el tipo de firma no esté contemplado en la adaptación al NTI.	TipoFirmaNoNormalizada [Tipificado ¹]	Opcional
campoAdicional	Campo adicional que se utilizará para posibles necesidades futuras.	String	Opcional

¹ Se han incluido los tipos de firmas:

- TF97: para formatos de firma CMS
- TF98: para formatos de firma XMLDSig
- TF99: para otros formatos de firma (por ejemplo PKCS#7).

En el caso de que este campo venga informado, la herramienta de verificación informará a los usuarios el tipo de firma indicada por el valor de este campo. Es decir, el valor de este campo prevalece sobre el valor del campo documentoENI en el que se indica el tipo de firma, el cuál es obligatorio.

Herramienta Centralizada de Verificación

Índice

1. Introducción

1.1 ¿Qué es? ¿Cuál es su objetivo?

1.2 Evolución de VerificarFirma a la HCV

2. Validación a partir de código de verificación

2.1 Estructura de intercambio de información

2.2 Código de verificación

2.3 Metadato Identificador del documento electrónico

2.4 Escenario habitual de uso

3. Validación a partir de fichero de firma

3.1 Escenario habitual de uso

4. Servicio de Integración - EnidocWS

4.1 Componente EnidocWS

4.2 Descripción del servicio de integración

5. Integración con EnidocWS

5.1 Modos de integración

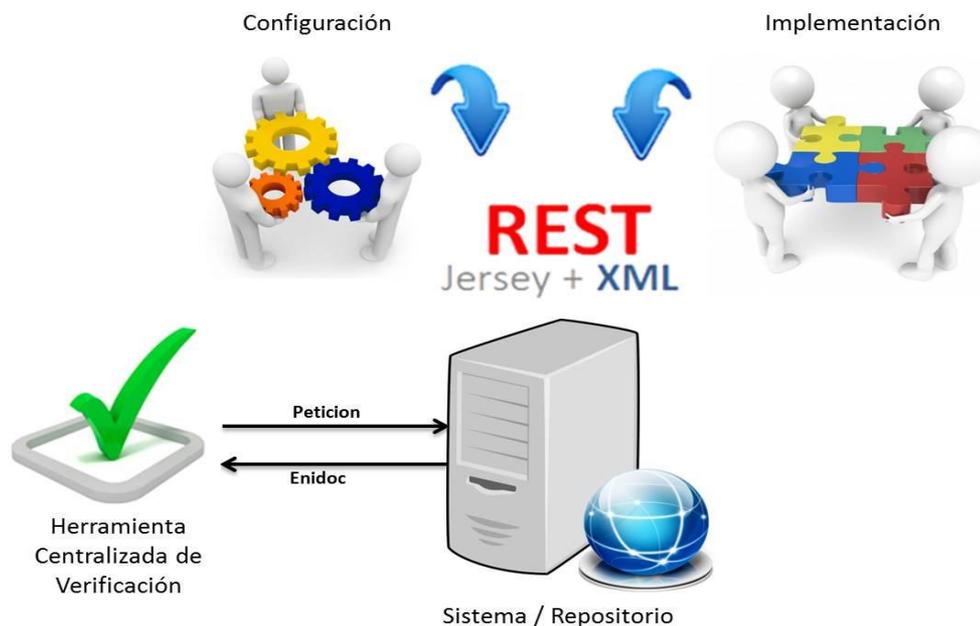
5.1 Ejemplo de implementación

Integración con EnidocWS

Modos de integración

Para integrar el sistema/repositorio deseado con el componente “EnidocWS”, se ofrecen dos alternativas en función de las necesidades y/o limitaciones del propio sistema/repositorio:

- A. Librería** (archivo jar) para que sea integrada en el propio sistema/repositorio que custodia la información. Para utilizar este método de integración se debe tener en cuenta, como requisito técnico, que el sistema/repositorio debe ejecutarse sobre una **JDK 6 o superior**.
- B. Aplicación web** (archivo war) que contiene la librería del punto anterior, para que sea desplegada en un contendor web **Tomcat** con **JDK 1.6**.



Integración con EnidocWS

Modos de integración: A - Incorporación de la librería “enidocWS”

Si se desea utilizar este método de integración hay que tener en cuenta, como requisito técnico, que **el sistema/repositorio debe ejecutarse sobre una JDK 6 o superior.**

Pasos a seguir:

Para la integración del componente será necesario seguir los siguientes pasos:

1. Incluir las **dependencias** java en el classpath del sistema.
2. Definir el **servlet** del servicio en el fichero web.xml.
3. Establecer la configuración adecuada en el **fichero de propiedades** enidocWS.properties e incluirlo en el classpath del sistema.
4. Implementar la **clase de recuperación** de la información requerida por la herramienta centralizada.

Integración con EnidocWS

Modos de integración: A - Incorporación de la librería "enidocWS"

Dependencias software:

- **Aplicaciones desarrolladas con Maven**

El componente "enidocWS" puede ser incluido en aplicaciones desarrolladas en maven añadiendo la siguiente dependencia al fichero pom.xml de la aplicación:

```
<dependency>
  <groupId>es.juntadeandalucia.nti</groupId>
  <artifactId>enidocWS</artifactId>
  <version>X.X</version>
</dependency>
```

Del mismo modo es necesario incluir la referencia al repositorio de software donde se encuentra el componente. Este componente puede encontrarse en el Repositorio Maven del Servicio de Coordinación de Administración Electrónica:

```
<repository>
  <id>RepositorioMavenSCAE</id>
  <name>Repositorio de la Junta de Andalucía</name>
  <url>https://ws024.juntadeandalucia.es/maven/browse</url>
</repository>
```

Integración con EnidocWS

Modos de integración: A - Incorporación de la librería "enidocWS"

Dependencias software:

- **Aplicaciones sin Maven**

Son necesarias una serie de dependencias (archivos jar) que deben estar en el classpath de ejecución de la librería principal para su correcto funcionamiento. La librería que implementa el servicio se denomina **enidocWS-x.x.jar** y las dependencias mencionadas son:

- com.google.guava:guava:jar:14.0.1
- com.sun.xml.wsit:xmlsec:jar:1.1
- commons-lang:commons-lang:jar:2.3
- commons-logging:commons-logging:jar:1.1.1
- es.juntadeandalucia.nti:conversor-eni:jar:1.2.0
- javax.annotation:javax.annotation-api:jar:1.2
- javax.servlet:javax.servlet-api:jar:3.1.0
- javax.validation:validation-api:jar:1.1.0.Final
- javax.ws.rs:javax.ws.rs-api:jar:2.0
- javax.xml.stream:stax-api:jar:1.0-2
- log4j:log4j:jar:1.2.17
- org.codehaus.castor:castor-core:jar:1.3.2
- org.codehaus.castor:castor-xml:jar:1.3.2
- org.glassfish.hk2.external:asm-all-repackaged:jar:2.2.0-b21
- org.glassfish.hk2.external:cglib:jar:2.2.0-b21
- org.glassfish.hk2.external:javax.inject:jar:2.2.0-b21
- org.glassfish.hk2:hk2-api:jar:2.2.0-b21
- org.glassfish.hk2:hk2-locator:jar:2.2.0-b21
- org.glassfish.hk2:hk2-utils:jar:2.2.0-b21
- org.glassfish.hk2:osgi-resource-locator:jar:1.0.1
- org.glassfish.jersey.containers:jersey-container-servlet-core:jar:2.4.1
- org.glassfish.jersey.core:jersey-client:jar:2.4.1
- org.glassfish.jersey.core:jersey-common:jar:2.4.1
- org.glassfish.jersey.core:jersey-server:jar:2.4.1
- stax:stax:jar:1.2.0
- stax:stax-api:jar:1.0.1

Integración con EnidocWS

Modos de integración: A - Incorporación de la librería "enidocWS"

Fichero "web.xml":

Es requisito indispensable para llevar a cabo la integración que se defina el siguiente servlet, como cualquier otro integrante de la aplicación web cliente, en el fichero "web.xml".

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app version="2.4" xmlns=http://java.sun.com/xml/ns/j2ee
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd">
<display-name>Web Service Enidoc</display-name>
<servlet>
    <servlet-name>EnidocService</servlet-name>
    <servlet-class>org.glassfish.jersey.servlet.ServletContainer</servlet-class>
    <init-param>
        <param-name>jersey.config.server.provider.classnames</param-name>
        <param-value>es.juntadeandalucia.nti.ws.eni.services.EnidocWS</param-value>
    </init-param>
    <load-on-startup>1</load-on-startup>
</servlet>
<servlet-mapping>
    <servlet-name>EnidocService</servlet-name>
    <url-pattern>/rest/eni/*</url-pattern>
</servlet-mapping>
</web-app>
```

Integración con EnidocWS

Modos de integración: A - Incorporación de la librería “enidocWS”

Fichero de propiedades “enidocWS.properties”

Para configurar el componente, tan sólo hay que establecer las propiedades del fichero “enidocWS.properties” e incluirlo en el *classpath* del sistema que lo integra.

```
# Información de correspondencia entre la HCV y el repositorio/sistema integrado
# usuario dado de alta en la HCV
usuarioWS = usuario
# password del usuario dado de alta en la HCV
passwordWS = pass
# clase (indicando ruta del paquete separado por puntos ‘.’) donde se implementara el método
claseWS = paquete.clase.MiClase
# nombre del método que recibe como parámetro el objeto Peticion y devuelve Enidoc
metodoWS = nombreMetodo
```

Como **alternativa** de configuración basada en fichero de propiedades, el componente permite invocar interfaces definidas encargadas de obtener la configuración de la herramienta. Las implementaciones que puedan hacerse de estas interfaces podrán rescatar la configuración de bases de datos u otros orígenes.

Integración con EnidocWS

Modos de integración: A - Incorporación de la librería "enidocWS"

Clase a invocar por el Servicio Web

Es necesario realizar la implementación de una clase que contenga un método, necesariamente **estático**, con la siguiente especificación:

```
public static EniDoc nombreMetodo (Peticion peticion)
```

Sobre este método recae la responsabilidad de obtener el documento ENI del sistema/repositorio integrado, así como el resto de información complementaria, para devolver el objeto esperado a la herramienta centralizada de verificación. Siendo responsabilidad de los sistemas/repositorios el **definir e implantar criterios y políticas para la gestión de las peticiones de acceso**, de manera que cada petición de acceso sea validada, teniendo en cuenta para ello la información que para cada petición se remite desde la herramienta. En caso de que se concluya que no procede aportar el documento a la persona usuaria de la herramienta, en la respuesta a generar por el sistema o repositorio se deberá expresar un texto informativo que se le mostrará a la misma.

Integración con EnidocWS

Modos de integración: B. Despliegue de la aplicación “enidocWS”

En caso de que no sea posible realizar la integración a través de la librería debido a incompatibilidades con las dependencias o al requisito de ejecutarse sobre una JDK 6 o superior, se pone a disposición una **aplicación intermedia** entre la herramienta centralizada de verificación y el sistema/repositorio, que ofrecerá el servicio web de comunicación.

Para la correcta implantación de la aplicación, los **pasos a seguir** de **forma análoga al caso de integración A** son:

1. Establecer la configuración adecuada en el fichero de propiedades enidocWS.properties.
2. Implementar **la clase de recuperación** de la información requerida por la herramienta centralizada.

Para acceder al modelo de datos del sistema/repositorio, es posible que sea necesario hacer uso de JDBC. Para ello habría que definir el DataSource correspondiente en el fichero context.xml.

Una vez configurada la aplicación e implementado el código necesario, se debe generar el war de la aplicación y desplegarlo en un servidor de aplicaciones **Tomcat** con **JDK 1.6**.

Integración con EnidocWS

Ejemplo de implementación del método a invocar

A continuación se muestra un ejemplo básico de implementación del método de recuperación de la información requerida por la herramienta centralizada de verificación:

```
public static EniDoc nombreMetodo (Peticion peticion) {  
  
    // 1.- Crear el objeto EniDoc que debemos rellenar  
    EniDoc eniDoc = new EniDoc();  
  
    // 2.- TODO Tratamiento opcional de los datos de la Peticion para definir e implantar  
    criterios y políticas para la gestión de las peticiones de acceso al documento  
    String idConsultado = peticion.getIdConsultado();  
  
    // 3.- TODO Obtener documento de BBDD mediante el CSV consultado  
    byte[] documentoBytes = obtenerDocumentoENIPorId(csvConsultado);  
  
    // Si el documento vinculado al CSV no existe en el repositorio  
    if (documentoBytes == null) {  
        eniDoc = new EniDoc();  
        eniDoc.setCodigoRespuesta(ErroresEni.STATUS_NOT_FOUND_RESOURCE);  
    }  
}
```

Integración con EnidocWS

Ejemplo de implementación del método a invocar

```
// Si el documento vinculado al CSV existe en el repositorio
else {

    // 4.- TODO Rellenar el objeto EniDoc
    // 4.1 - Complimentar el parámetro obligatorio.
    Array de bytes que contiene el documento electrónico ENI.
    eniDoc.setDocumentoENI(documentoBytes);

    // 4.2 - Complimentar los parámetros opcionales.
    // Campo que recoge expresamente, en el caso de firma electrónica basada en certificado,
    // si en su momento se validaron los certificados electrónicos utilizados para la firma.
    boolean validacionCertificadosFirma = true;
    eniDoc.setValidacionCertificadosFirma(validacionCertificadosFirma);

    // Campo que indica si se desea habilitar que la persona usuaria de la herramienta pueda
    // descargar el correspondiente fichero de firma electrónica y el fichero en formato ENI.
    boolean descargarFirmaydocumentoENI = true;
    eniDoc.setDescargarFirmaydocumentoENI(descargarFirmaydocumentoENI);

    // 5.- Devolver el objeto EniDoc relleno.
    return eniDoc;
}
}
```