JUNTA DE ANDALUCIA

CONSEJERÍA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA

Firma XAdES del íncide del expediente electrónico

Guía de integración

Versión: v01r01

Fecha: 12/06/2017

HOJA DE CONTROL

Título	Guía de integración		
Entregable	Guía de integración		
Nombre del Fichero	20170612 ENI_FirmaExpedienteXAdES_v01r01.odt		
Autor	CHAP		
Versión/Edición	v01r01	**Fecha Versión**	12/06/2017
Aprobado por	-	**Fecha Aprobación**	12/06/2017
		Nº Total Páginas	10

REGISTRO DE CAMBIOS

Versión	Causa del Cambio	Responsable del Cambio	Área	Fecha del Cambio
v01r01	Versión inicial	CHAP	-	12/06/2017

Nombre y Apellidos	Cargo	Área	Nº Copias
Manuel Perera Domínguez	Jefe de Servicio	Servicio de Coordinación de Administración Electrónica	1
Francisco Mesa Villalba	Gabinete de Administración Electrónica	Servicio de Coordinación de Administración Electrónica	1
José Ignacio Cortés Santos	Gabinete de Administración Electrónica	Servicio de Coordinación de Administración Electrónica	1

ÍNDICE

Sumario

1 INTRODUCCIÓN

1.1 Objeto

El Esquema Nacional de Interoperabilidad, regulado por el Real Decreto 4/2010, de 8 de enero, establece el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.

En su disposición adicional primera se establecen las Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones Públicas. Entre ellas, se encuentra la Norma Técnica de Interoperabilidad de Expediente electrónico, en la cual se trata su estructura y formato, así como las especificaciones de los servicios de remisión y puesta a disposición.

La NTI de Expediente electrónico establece que los componentes del expediente electrónico son sus metadatos mínimos obligatorios, el índice, y la firma electrónica de este. Esta NTI prevé distintos formatos de firma electrónica para el índice, si bien en la práctica se impone de facto el uso del formato "*XAdES Enveloped*" dado que que es el único formato de firma para el índice electrónico admitido por el proyecto INSIDE liderado por el Ministerio de Hacienda y Función Pública.

En el presente documento se ofrecerán las directrices técnicas a seguir para firmar electrónicamente en formato "*XAdES Enveloped*" el índice de la estructura de intercambio del expediente electrónico.

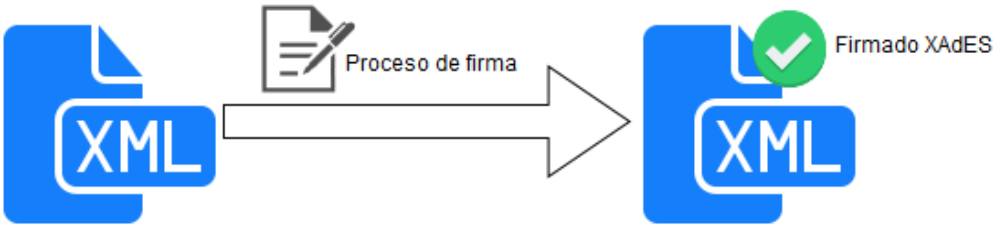
1.2 Alcance

Este documento se encuentra dirigido a:

- Integradores y desarrolladores de sistemas de tramitación en los que se deba generar expedientes electrónicos conformes al formato de intercambio definido en el Anexo 2 de la NTI de Expediente electrónico.

2 FIRMA ELECTRÓNICA XADES-ENVELOPED

El formato de firma electrónica "*XAdES Enveloped*" es un formato de firma electrónica implícita en el que los datos firmados y la firma electrónica se almacenan en una única estructura en formato XML. En esta estructura XML, una subestructura XML contiene la firma electrónica de otra subestructura XML.



En el caso de la firma electrónica de la estructura de intercambio del expediente electrónico definida en la NTI, el XML resultante del proceso de firma tiene la particularidad de a la vez ser:

1. Una estructura de intercambio de expediente electrónico, que puede por tanto ser verificada por sistemas de verificación de expedientes como HCV o INSIDE.
2. Una firma electrónica en formato XAdES Enveloped, que puede por tanto ser verificada en sistemas de verificación de firma electrónica como VALIDA o VALIDe de MINHFP.

Se describen a continuación los pasos a realizar para incorporar una firma electrónica "*XAdES Enveloped*" a una estructura de intercambio XML de expediente electrónico cuyo índice aún no ha sido firmado.

2.1 Identificador del nodo XML a firmar

Es necesario en primer lugar establecer el alcance de los datos que van a ser firmados. En el caso de un expediente electrónico, se firmará la etiqueta "*IndiceContenido*", la cual deberá tener un atributo "*id*" con un valor único que la identifique. Considérese el siguiente ejemplo de índice de un expediente electrónico, contenedor de dos documentos:

```
<eniexpind:IndiceContenido Id="datosafirmar">
    <eniconexpind:FechaIndiceElectronico>2017-06-01T14:01:38.709+02:00</eniconexpind:FechaIndiceElectronico>
    <eniconexpind:DocumentoIndizado Id="_76000306">
            <eniconexpind:IdentificadorDocumento>ES_A01018360_2017_EdEnI00000000000000000000000007</eniconexpind:IdentificadorDocumento>
            <eniconexpind:ValorHuella>qk5E+QL7fwIY1T/oU1+PGlIxeWbN+/9s8J0qHDuknr0=</eniconexpind:ValorHuella>
            <eniconexpind:FuncionResumen>SHA256</eniconexpind:FuncionResumen>
            <eniconexpind:FechaIncorporacionExpediente>2017-06-01T14:01:21.076+02:00</eniconexpind:FechaIncorporacionExpediente>
    </eniconexpind:DocumentoIndizado>
    <eniconexpind:DocumentoIndizado Id="_76000306">
            <eniconexpind:IdentificadorDocumento>ES_A01018360_2017_EdEnI00000000000000000000000008</eniconexpind:IdentificadorDocumento>
            <eniconexpind:ValorHuella>qk5A+tL7fwIY1T/oU1+PGlIxeWbN+/9s8J0qHDuknr2=</eniconexpind:ValorHuella>
            <eniconexpind:FuncionResumen>SHA256</eniconexpind:FuncionResumen>
            <eniconexpind:FechaIncorporacionExpediente>2017-06-01T14:01:23.076+02:00</eniconexpind:FechaIncorporacionExpediente>
    </eniconexpind:DocumentoIndizado>
</eniexpind:IndiceContenido>
```

En el ejemplo, el nodo de los datos a firmar se identificaría como aquel cuyo atributo "*Id*" toma el valor "*datosafirmar*".

2.2 Identificar la ubicación donde se custodiará la firma electrónica

El expediente electrónico de partida cuyo índice va a ser firmado debe contar con la subestructura XML donde se alojará la firma electrónica XAdES Enveloped. Esta estructura será como la que se muestra a continuación:

```
<enids:firmas>
        <enids:firma>
                <enids:TipoFirma>TF03</enids:TipoFirma>
                <enids:ContenidoFirma></enids:ContenidoFirma>
        </enids:firma>
</enids:firmas>
```

Como puede verse, el valor "*TipoFirma*" será en todo caso TF03, correspondiente con la codificación que para la firma "XAdES *enveloped* signature" se realiza en la NTI de Expediente electrónico. El contenido de la etiqueta "*FirmaConCerticado*" estará inicialmente vacío, ya que será ahí donde se inserte la firma electrónica una vez que esta se realice.

2.3 Parámetros requeridos por el cliente de firma electrónica

Los parámetros para realizar la firma electrónica será similares tanto para la firma electrónica con los componentes Miniapplet/Autofirma como para la firma electrónica con el componente "afirma-signer-delegate" en los casos en los que la firma electrónica se realice con un certificado de sello de tiempo de actuación administrativa automatizada. En ambos casos serán los siguientes:

Parámetro	**Valor**
Formato	AUTO
Algoritmo	SHA1 con RSA
ExtraParams	format=XAdES Enveloped noteToSign=datosafirmar[1] nsertEnvelopedSignatureOnNodeByXPath=//*[local-name()='FirmaConCertificado'][2]

2.4 Código de ejemplo de firma electrónica

En este apartado vamos a explicar como realizar la firma electrónica XAdES Enveloped mediante el uso del Miniapplet/Autofirma como con el componente afirma-signer-delegate.

De inicio disponiemos del XML de un expediente ENI sin firmar, codificado en Base64. (expENI)

```
ByteArrayOutputStream out = new ByteArrayOutputStream();
expENI.storeToXMLSinValidar(out);
String contenidoXML=Base64.encode(out.toByteArray());
```

[1]El valor concreto será el asignado al atributo "Id" de la etiqueta "IndiceContenido".
[2]El valor será siempre el mismo. Marca la ruta Xpath del nodo donde se custodiará la firma electrónica.

El contenido del XML sin firmar codificado en base64 será la información a firmar con el cliente de firma.

Ejemplo Miniapplet/Autofirma

1. Para realizar la firma del expediente utilizando el miniapplet se debe realizar una configuración como la siguiente.

```
function firmarConApplet() {

    document.getElementById('firmaB64').value = "";
    try{
        //DEFINICION DE PARAMETROS
        var algoritmoFirma = 'SHA256withRSA';
        var tipoFirma = 'Auto';
        var signatureformat = 'BES';
        //ID de IndiceContenido
        var nodeToSign='datosafirmar';
        var numSerieCert='(número de serie del certificado del usuario)';
        var params = '';
        var format='XAdES Enveloped';
        var insertEnvelopedSignatureOnNodeByXPath="//*[local-name()='FirmaConCertificado']";
        params = 'format='+format+'\nfilters=nonexpired:;signingCert:;qualified:'+numSerieCert+
                 '\nnodeToSign='+nodeToSign+'\ninsertEnvelopedSignatureOnNodeByXPath='+
                 insertEnvelopedSignatureOnNodeByXPath+'';
        //FIRMA EL DOCUMENTO
        MiniApplet.sign(cadenaFirma, algoritmoFirma, tipoFirma, params, firmaExito, firmaError);
        } catch(e) {
            showErrorCallback(MiniApplet.getErrorType(), MiniApplet.getErrorMessage());
    }
}
```

Los valores que se encuentran entre paréntesis y el Id de IndiceContenido, son valores que variarán con el expediente ENI que queremos formar y con el número del certificado del usuario. Así como el algoritmoFirma también es editable.

2. Una vez firmado el expediente pasamos a incorporar el sellado de tiempo.
    1. Definimos las propiedades de afirma:

```
            /*
            * Definición del fichero de propiedades
            */
            if (afirmaProperties == null) {
                    afirmaProperties = new Properties();
                    afirmaProperties.put("afirma.idapp", "idAplicacionAfirma");
                    afirmaProperties.put("afirma.user", "userAppAfirma");
                    afirmaProperties.put("afirma.password", "passUserAfirma");
                    afirmaProperties.put("afirma.host", "datosServidorAfirma");
                    afirmaProperties.put("afirma.hashalgorithm", "SHA-256");
                    afirmaProperties.put("afirma.version6", true);
                    afirmaProperties.put("afirma.xmlsignaturemode", "ENVELOPED");
                    afirmaProperties.put("afirma.signatureform", "BES");
                    afirmaProperties.put("afirma.signaturetype", "XAdESv1.3.2");
            }
```

    2. Se instancia el componente con las propiedades establecidas:

```
            AfirmaClient afirmaClient = new AfirmaClientImpl(
                    new AfirmaConfiguration().configure(afirmaProperties));
```

    3. Realizamos el sellado de tiempo, por lo que se actualizará la firma.

```
VerifySignatureResponse verifySignatureResponse = afirmaClient.dssAfirmaUpgrade(signBase64,
            AfirmaClient.SignatureType.XadES_v132, AfirmaClient.XmlSignatureMode.ENVELOPED,
            AfirmaClient.SignatureForm.T);

VerifyClient verifyClient = new VerifyClientImpl(afirmaClient);

firmaUpgradeB64 = verifySignatureResponse.getUpgradedSignature();
```

En la variable firmaUpgradeB64 tendremos el contenido de la firma actualizada y con sello de tiempo que a su vez es el contenido del XML.

Ejemplo componente afirma-signer-delegate

Para realizar la firma del índice del expediente utilizando el componente afirma-signer-delegate se debe seguir los siguientes pasos:

1. Configuración de las propiedades para crear posteriormente una instancia del objeto SignerDelegate:

```
Properties afirmaPropertiesSignerDelegate = new Properties();
afirmaPropertiesSignerDelegate.put("signer.ks.path", ksPath);
afirmaPropertiesSignerDelegate.put("signer.ks.type", ksType);
afirmaPropertiesSignerDelegate.put("signer.ks.password", ksPass);
afirmaPropertiesSignerDelegate.put("signer.ks.cert.alias", certAlias);
afirmaPropertiesSignerDelegate.put("signer.hashalgorithm", hashAlgorithm);
```

2. Se instancia el componente con la configuración establecida:

```
SignerDelegateServerConfiguration configuracion = new SignerDelegateServerConfiguration()
    .configure(afirmaPropertiesSignerDelegate);
SignerDelegate signerDelegate = new SignerDelegateImpl(configuracion);
```

3. Siendo 'datosafirmar' el valor concreto asignado al atributo “Id” de la etiqueta “IndiceContenido'' se debe establecer un mapa de objetos String con los siguientes parámetros extras:

```
String [] params = { "nodeToSign="+ datosafirmar,
    "insertEnvelopedSignatureOnNodeByXPath=//*[local-name()='FirmaConCertificado']",
    "format=XAdES Enveloped"};
```

4. Llamada al método de firma que proporciona el componente de firma delegada. Se debe establecer la llamada al método de nombre 'signWithParams' para poder asignar los parámetros extras y así realizar la firma de forma correcta.

```
byte[] sign = signerDelegate.signWithParams(xmlExp,
            SignatureType.XAdES_ENVELOPED , SignatureMode.IMPLICIT , false , params);
```

5. Las firmas generadas con el componente se generan con los perfiles básicos BES (Basic Electronic Signature) y EPES (Explicit Policy Electronic Signature), con lo cual una vez obtenido el array de bytes pertenecientes al xml del expediente firmado se deberá realizar el sellado de tiempo de igual forma que se realiza en el ejemplo del Miniapplet/Autofirma.

El XML resultante del proceso de firma deberá poder verificarse como expediente electrónico en el apartado ENI de la HCV o bien como firma electrónica en el apartado VALIDA de la HCV.

2.5 Modificaciones del expediente electrónico posteriores a su firma.

Dado que en la firma XadES Enveloped de un expediente electrónico solo se firma la etiqueta "*IndiceContenido*", es posible realizar modificaciones sobre el XML de intercambio a excepción de lo contenido por la citada etiqueta y lo contenido por la etiqueta "FirmaConCertificado" sin que con ello se invalide la firma electrónica. Así, por ejemplo, podría modificarse el valor de cualquiera de los metadatos mínimos obligatorios del expediente, o bien podría incorporarse o modificarse el fichero de visualización del expediente posteriormente a la firma electrónica de este, sin que con ello la firma se viera invalidada.

Supóngase como ejemplo que en el fichero de visualización del expediente se desea incorporar información sobre la firma electróncia del índice. No se puede disponer de la información de la firma hasta que esta se completa, por lo que necesariamente se deberá insertar el fichero de visualización del índice después de que la firma se haya realizado. Para realizar esta modifcación del fichero de visualización se podría contar, antes de realizar la firma del expediente, con una variable a sustituir en el fichero XML del expediente que marque la ubicación donde se alojará la estructura Base64 del fichero de visualización del índice.

```
<eniexp:VisualizacionIndice>
        <enifile:ValorBinario>${visualizacionindice}</enifile:ValorBinario>
        <enifile:NombreFormato>PDF</enifile:NombreFormato>
</eniexp:VisualizacionIndice>
```

Una vez que se ha realizado la firma electrónica del expediente, se podrá generar un fichero de visualización donde se incorpore los datos de la firma, y este fichero de visualización se podrá codificar en Base64 y ser insertado en el expediente ya firmado sin que con ello se invalide su firma electrónica.

A continuación veremos un ejemplo de como insertar el fichero de visualización codificado en Base64 en el expediente ya firmado.

```
String visuExp = Base64.encode(valorBinario);

byte[] cadenaAux = Base64.decode(firmaUpgradeB64);
String resultadoExp = new String(cadenaAux);
resultadoExp = resultadoExp.replace("${visualizacionindice}", visuExp);
```

La variable valorBinario contiene el array de bytes del fichero de visualización, una vez codificado se mete en la variable visuExp que es el contenido que vamos a insertar en el XML.

La variable firmaUpgradeB64 como vimos en el ejemplo del Miniapplet contiene la firma que es a su vez el contenido del XML codificado en Base64.

Insertaremos el contenido de visuExp con la ayuda del método String.replace como podemos ver en el ejemplo.

La variable resultadoExp ya contendría el contenido del XML actualizado con el fichero de visualización.

3 REFERENCIAS

Objeto	Referencia
Esquema Nacional de Interoperabilidad	http://www.boe.es/buscar/act.php?id=BOE-A-2010-1331
NTI de Expediente Electrónico	http://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-13170
VALIDe	https://valide.redsara.es/valide/
INSIDE	http://administracionelectronica.gob.es/ctt/inside#.V5B7zFIppXE