certicámara.

Validez y seguridad jurídica electrónica

Componente Firma Digital en JAVA

Documento de especificación y contexto:

Versión 1.0

IDENTIFICADOR	Sign4J.pdf
NOMBRE DEL DOCUMENTO	Documento inicial de documentación.
ESTADO DEL DOCUMENTO	Aprobado
ÁREA	Consultoría
RESPONSABLES	**Andrés Felipe Escobar Fernández** (andres.escobar@certicamara.com) **Jhon Edgar Gonzalez Amortegui** (jhon.gonzalez@certicamara.com)
REVISORES	**Carlos Orlando Peña** (carlos.pena@certicamara.com)

CONTROL DE VERSIONES DEL DOCUMENTO

Versión	Fecha creación	Fecha liberación	Descripción cambio

CONTROL DE REVISIONES Y APROBACIONES

Revisado por	Firma	Fecha

Tabla de Contenidos

Documento de Especificación y contexto del Componente de Firma Digital en Java

1. INTRODUCCIÓN

Certicámara S.A. ha desarrollado un Componente API que permite firmar y/o cofirmar varios documentos en formato PKCS#7 Attached y Detached, así como en formatos XML Enveloped, Enveloping, Detached y archivos en formato PDF.

2. OBJETIVOS

- Documentar el uso de las funcionalidades y el uso del Componente de Firma Digital en Java.

3. VERSIÓN DEL SERVICIO

- 1.0

4. DUEÑOS DEL SERVICIO

Responsable	Certicámara – Ing. Carlos Peña.
Responsable	Área: Consultoría
Informado	

5. FUNCIONALIDADES DEL API.

Este componente API permite firmar digitalmente un documento con un certificado digital en formato p12. Los tipos de documentos que puede firmar este componente API son:

- PKCS#7 Attached
- PKCS#7 Detached
- PKCS#7 Attached Distribuido
- XML Enveloped
- XML Enveloping
- XML Detached
- PDF (PaDES)
- PDF (PaDES) Distribuido

Para firmar un documento se debe especificar en una clase de parámetros toda la configuración relacionada para firma, el certificado con el que se va firmar, bytes del documento a firmar, configuración para validar la revocación de la firma, y demás configuraciones propias para cada firma que se irán describiendo en el presente documento.

Para realizar una firma se debe crear un objeto ***Sign*** que en su contructor recibe una lista de la clase de propiedades, lo que quiere decir que con este componente es posible agrupar en una lista todos los documentos que se van a firmar y firmarlos todos en una iteración. Esta clase tiene un método *signData()* que permite firmar los documentos que están en la lista de parámetros y devuelve una respuesta por cada objeto de parámetros ingresado.

5.1. Creación de un objeto de firma

Para la creación de un objeto firma, se encapsuló la funcionalidad de creación de objetos firma en una clase llamada ***SignFactory*** que tiene un método estático *getSigner* que recibe un String que indica cual tipo de firmante se requiere (PKCS#7 Attached, XML Enveloped, etc.) y recibe un ArrayList de tipo de ***SignatureParameters*** que es en donde se encapsula toda la configuración para firmar un documento. El siguiente es un ejemplo para firmar una lista de signParameters de tipo PKCS#7.

```
Sign s = SignFactory.getSigner(SignFactory.PKCS7, signatureParameters);
s.signData();
```

5.1.1. Método *getSigner* de la clase *SignFactory*.

El método *getSigner* de la clase ***SignFactory*** recibe dos parámetros, es un String que indica el tipo de firma, podemos elegir entre diferentes atributos estáticos de la clase ***SignFactory***, estos atributos son:

Atributo	Valor	Tipo
PKCS7	pkcs7.PKCS7Sign	String
PKCS7Hash	pkcs7.PKCS7SignHash	String
XMLEnveloped	xml.XmlEnveloped	String
XMLEnveloping	xml.XmlEnveloping	String
XMLDetached	xml.XmlDetached	String
PDF	pdf.PdfSign	String

Para la lista de SignatureParameters se debe definir de la siguiente manera:

```
ArrayList<SignatureParameters> lista = new ArrayList<SignatureParameters>();
lista.add(signParameters);
```

En donde la variable *signParameters* es una implementación de la clase ***SignatureParameters***. Existen los siguientes tipos de implementaciones de ***SignatureParameters***:

Tipos de Firma	Implementación SignatureParameters
• **PKCS#7 Attached** • **PKCS#7 Detached** • **PKCS#7 Attached Hash**	PKCS7Parameters
• **XML Enveloped** • **XML Enveloping**	XMLParameters

• **XML Detached**	XMLDetachedParameters
• **PDF**	PDFParameters

Existen 3 atributos comunes para todos los ***SignatureParameters***, que son:

- **Byte[]** *bytesToSign*: Son los bytes del documento que se van a firmar.
- **RevocationVerify** *revocationVerify*: es la configuración para validar el certificado de firma y los certificados con los que ya se firmó el documento (si ya está firmado).
- **CertificateConfiguration** *certificateConf*: es la configuración para identificar el método con el que se va acceder al certificado en formato p12 con el que se va a firmar.

5.1.2. RevocationVerify.

El componente API de firma no solo firma digitalmente un documento sino también verifica el documento al finalizar la operación para validar que las firmas que hay en el documento estén válidas. Para generar un objeto ***RevocationVerify*** se debe ejecutar el siguiente código:

```
RevocationVerify p = new RevocationVerify("CRL_ONLY",new
GregorianCalendar(),"c:/temp/crl","http://oscp.certicamara.com");

p.setKeyStorePath("c:/temp/keystore/Keystore");
```

El constructor recibe 4 parámetros que son los siguientes en orden:

Atributo	Valor	Tipo
Tipo de verificación de Revocación	Tiene 4 posible valores: “CRL_ONLY” “OSCP_ONLY” “OSCP_CRL” “CRL_OSCP”	String
Calendar	Fecha para la cual se quiere validar la validez de la firma, si es null coje la fecha actual del sistema.	Calendar
Dirección CRL	Se indica la ruta absoluta de la carpeta en la cual se encuentran las crl.	String
Dirección OCSP	Se indica la dirección URL en donde se válida la revocación por OCSP.	String

Además de crear el objeto se le debe indicar la ruta absoluta en donde se encuentra el keystore en donde están almacenados los certificados públicos de las entidades de confianza, como el de Certicamara. Con esta configuración ya es posible validar los certificados con los que se realizaron la firma.

5.1.3. CertificateConfiguration

Esta también es una clase abstracta que tiene 3 tipos de implementaciones: cuando se accede al certificado con los bytes de este, cuando el certificado está adentro de un keystore o cuando se

tiene el certificado ya en formato X509. Cada implementación en su constructor recibe todos los parámetros como se presenta a continuación:

Tipos de configuración de certificado	Constructores
CertificateFromBytes	1. Byte[] *bytesCertificado*, String *passwordDelCertificado* 2. Byte[] *bytesCertificado*, String *passwordDelCertificado*, String *aliasDelCertificado*
CertificateFromKeystore	1. KeyStore *keystoreCertificado*, String *passwordDelCertificado* 2. KeyStore *keystoreCertificado*, String *passwordDelCertificado*, String *aliasDelCertificado*
CertificateFromX509	1. X509Certificate *certificadoX509*, PrivateKey *llavePrivada* 2. X509Certificate *certificadoX509*, PrivateKey *llavePrivada*, Certificate[] *cadenaDeCertificacion*

Un ejemplo de implementación:

```
CertificateConfiguration cert = new
CertificateFromBytes(UtilsSign.getBytesFromFile(p12Certificate),certificatePassw
ord);
```

En donde la variable *p12Certificate* es la ruta absoluta en donde se encuentra el archivo del certificado en formato p12, y la variable *certificatePassword* es el password del certificado con el que se va a firmar.

5.1.4. Respuesta del Sign: List<ProcessResponseSign>.

Como al firmar le pasamos una lista de parámetros de configuración de firma, para cada elemento de esa lista debe existir una respuesta. Para cada configuración existe una clase respuesta llamada ProcessResponseSign en donde tiene los siguientes elementos:

Atributo	Valor	Tipo
Exito	Es el booleano que indica si la operación de firma fue exitosa o no.	boolean
MessageResponse	Lista de mensajes que indica cuales fueron los problemas que se presentaron si ocurrió algún error a la hora de firmar. Cada mensaje tiene un código y un mensaje.	List<MessageResponse>
Resultado	Son los bytes del documento firmado si la operación fue exitosa, sino son null.	Byte[]

Un ejemplo sobre como iterar sobre este objeto:

```
Sign s = SignFactory.getSigner(SignFactory.PKCS7, list);

List<ProcessResponseSign> prs = s.signData();
for(ProcessResponseSign pp :prs){
	if(pp.isExito()){
	UtilsSign.saveSignedFile("c:/temp/pkcs.p7z", pp.getResultado());
	}else{
		for(MessageResponse mm : pp.getMessageResponse()){
		System.out.println(mm.getCodigo()+" "+mm.getMensaje());
		}
	}
}
```

El anterior fue un ejemplo en donde recorremos la lista de respuesta y si la repuesta fue satisfactoria, guardamos el archivo firmado generado en una ruta. Si la respuesta es inválida se imprime en consola el código del error y el mensaje con la descripción. Adicionalmente la clase ***MessageResponse*** tiene otro atributo que se llama *Trace*, en donde se indica la traza del error.

A continuación se presentara la forma en cómo se debe invocar el componente para realizar una firma de los tipos actualmente soportados por este componente API.

5.2. FIRMA EN FORMATO PKCS#7

A continuación se explica como se debe realizar implementación de un programa que realice firmas en este formato. En resumidas cuentas para desarrollar un fragmento de código que realice la firma en este formato debemos primero, crear un objeto PKCS7Parameters, en donde se guardan todos los parámetros que necesita la firma, y luego se construye un objeto Sign cuyo constructor recibe como parámetros la lista de objetos PKCS7Parameters y el tipo de firma que se quiere realizar, luego se llama al método ***signData***.

5.2.1. PKCS7Parameters

Esta es la clase de configuración para realizar una firma tanto en PKCS#7 Attached y Detached. El constructor de esta clase, como ya ha sido indicado, recibe:

- **Byte[]** *bytesToSign*: Son los bytes del documento que se van a firmar.
- **RevocationVerify** *revocationVerify*: es la configuración para validar el certificado de firma y los certificados con los que ya se firmó el documento (si ya está firmado para formato Attached).
- **CertificateConfiguration** *certificateConf*: es la configuración para identificar el método con el que se va acceder al certificado en formato p12 con el que se va a firmar.
- **Boolean** *attached*: es el booleano que indica si la firma es attached o detached.

Además tiene un atributo adicionar que se puede configurar; en las firmas Attached se le puede indicar cuál es el nombre del archivo y la extensión del archivo que se va a firmar, esto se indica puesto que a la hora de extraer el contenido de la firma no se sabe en qué formato pueda estar esos bytes que se firmaron. A continuación se presenta un ejemplo de configuración del

PKCS7Parameters:

```
PKCS7Parameters signParameters = new
PKCS7Parameters(UtilsSign.getBytesFromFile(fileToSignPath),
      revocationVerify,certificateConfiguration,true);
signParameters.setFileNameAndExtension(fileToSignName);
```

5.2.2. Firma en formato PKCS#7 Attached

Para realizar el firmado en formato PKCS#7 Attached se colocar le booleano del constructor de PKCS7Parameters en true. Un ejemplo de firma es el siguiente:

```
CertificateConfiguration certificateConfiguration = new
CertificateFromBytes(UtilsSign.getBytesFromFile(pkcs12Path),pkcs12Password);

RevocationVerify revocationVerify = new
RevocationVerify("OCSP_ONLY",null,null,null);
revocationVerify.setKeyStorePath(resourcesPath+"/keystore/Keystore");

PKCS7Parameters signParameters = new
PKCS7Parameters(UtilsSign.getBytesFromFile(fileToSignPath),
            revocationVerify,certificateConfiguration,true);
signParameters.setFileNameAndExtension(fileToSignName);

ArrayList<SignatureParameters> list = new ArrayList<SignatureParameters>();
list.add(signParameters);

Sign s = SignFactory.getSigner(SignFactory.PKCS7, list);

List<ProcessResponseSign> prs = s.signData();

for(ProcessResponseSign pp :prs){
      if(pp.isExito()){
      UtilsSign.saveSignedFile("c:/temp/pkcs7.p7z",pp.getResultado());
      }else{
      for(MessageResponse mm : pp.getMessageResponse()){
            System.out.println(mm.getCodigo()+" "+mm.getMensaje());
      }
      }
}
```

5.2.3. Firma en formato PKCS#7 Detached

Para realizar el firmado en formato PKCS#7 Attached se debe colocar el booleano del constructor de PKCS7Parameters en false. Un ejemplo de firma es el siguiente:

```
CertificateConfiguration certificateConfiguration = new
CertificateFromBytes(UtilsSign.getBytesFromFile(pkcs12Path),pkcs12Password);
```

```
RevocationVerify revocationVerify = new
RevocationVerify("OCSP_ONLY",null,null,null);
revocationVerify.setKeyStorePath(resourcesPath+"/keystore/Keystore");

PKCS7Parameters signParameters = new
PKCS7Parameters(UtilsSign.getBytesFromFile(fileToSignPath),
            revocationVerify,certificateConfiguration,false);
signParameters.setFileNameAndExtension(fileToSignName);

ArrayList<SignatureParameters> list = new ArrayList<SignatureParameters>();
list.add(signParameters);

Sign s = SignFactory.getSigner(SignFactory.PKCS7, list);

List<ProcessResponseSign> prs = s.signData();

for(ProcessResponseSign pp :prs){
      if(pp.isExito()){
      UtilsSign.saveSignedFile("c:/temp/pkcs7D.p7s", pp.getResultado());
      }else{
      for(MessageResponse mm : pp.getMessageResponse()){
            System.out.println(mm.getCodigo()+" "+mm.getMensaje());
      }
      }
}
```

5.2.4. Firma en formato PKCS#7 Attached Distribuido

Para realizar el firmado en formato PKCS#7 Attached Distribuido se debe indicar en el SignFactory que el tipo de firma es PKCS7Hash y hacer uso del Applet de firma. Un ejemplo de firma es el siguiente:

```
String hashesPkcs7 = null;
PKCS7SignHash s2 = null;
try{
      archivoSignPath1 = pathResources + "/dataIn/Archivo_Importante.txt";
      fileToSignName = "ArchivoImportáanñññtesfsdfdfsdf.txt";
      RevocationVerify revocationVerify = new RevocationVerify("CRL_ONLY", null,
      "C:/CRL/crl", null);
      revocationVerify.setKeyStorePath(pathResources+"/keystore/Keystore");
      CertificateConfiguration cert = new CertificateConfiguration() {
      @Override
            public void validate() throws CertificateInitException {
            }
      };
      ArrayList<SignatureParameters> listaPkcs7 = new
```

```
	ArrayList<SignatureParameters>();
	for(int i=0; i<1; i++){
		PKCS7Parameters signParameterspkcs7 = new
	PKCS7Parameters(UtilsSign.getBytesFromFile(archivoSignPath1),
	revocationVerify, cert, true);
		if(isFilenameValid(fileToSignName)){
			signParameterspkcs7.setFileNameAndExtension(fileToSignName);
		}
		else{
			signParameterspkcs7.setFileNameAndExtension("defaultName.dat");
		}
		listaPkcs7.add(signParameterspkcs7);
	}
	s2 = (PKCS7SignHash) SignFactory.getSigner(SignFactory.PKCS7Hash, listaPkcs7);
	hashesPkcs7 = s2.getHashs();
}
catch(Exception e){
	e.printStackTrace();
	request.setAttribute("hash",e.toString());
}
ArrayList<Sign> lista = new ArrayList<Sign>();
lista.add(s2);
session.setAttribute("hash", hashesPkcs7);
session.setAttribute("ListaHashSigned", lista);
```

En donde lo primero que debemos hacer es obtener el hash de los documentos que se van a firmar.

```
function setAppletText() {
	var applet = document.getElementById('appletfirma');
	var timediv = document.getElementById('txtHash');
	applet.Sign(timediv.value, "archivoDist", false);
}

function setSign(value){
	var field = document.getElementById('Firma');
	field.value = value;
}
```

Luego obtenemos la firma de los documentos por medio del Applet de Firma.

```
ArrayList<Sign> lista = (ArrayList<Sign>) session.getAttribute("ListaHashSigned");
PKCS7SignHash s2 = (PKCS7SignHash)lista.get(1);
String[] hashesFirmados = request.getParameter("Firma").split("%");
String hashesFirmadosPkcs7 = "";
for(int i=0;i<s2.signatureParameters.size(); i++){
	hashesFirmadosPkcs7 += hashesFirmados[i]+"%";
}
List<ProcessResponseSign> listaRPkcs7 = new ArrayList<ProcessResponseSign>();
try {
```

```
		listaRPkcs7.addAll(s2.joinPKCS7Signatures(hashesFirmadosPkcs7));
	}
	catch (SignException e) {
		e.printStackTrace();
	}
	k = 0;
	for(ProcessResponseSign processResponseSign: listaRPkcs7){
		if(processResponseSign.isExito()){
		//Ejemplo para descargar el archivo firmado.
			session.removeAttribute("isHash");
			verificarPkcs7(listaRPkcs7.get(k).getResultado());
		//response.setContentType("application/pkcs7-mime");
		//response.setHeader("Content-Disposition","attachment; filename =
		"+"ArchivoFirmado.p7z");
		//ServletOutputStream op = response.getOutputStream();
		//.write(listaRPkcs7.get(k).getResultado());
		//op.flush();
		//op.close();
			UtilsSign.saveSignedFile("C:/Users/jhon.triana/Desktop/prueba/prueba"+k+
		".p7z",listaRPkcs7.get(k).getResultado() );
			k++;
		}
		else{
			k++;
			String error="";
			for(MessageResponse messageResponse:
	processResponseSign.getMessageResponse()){
				error += ("Error al firmar documentos: Código:
	"+messageResponse.getCodigo()+" Mensaje: "+messageResponse.getMensaje());
			}
			session.setAttribute("error", error);
			response.sendRedirect("index.jsp");
		}
	}
```

Como último paso unimos la firma con el documento original

5.3. FIRMA EN FORMATO XML

A continuación se explica cómo se debe realizar implementación de un programa que realice firmas en este formato. En resumidas cuentas para desarrollar un fragmento de código que realice la firma en este formato debemos primero, crear un objeto ***XmlParameters***, en donde se guardan todos los parámetros que necesita la firma, y luego se construye un objeto Sign cuyo constructor recibe como parámetros la lista de objetos ***XmlParameters*** y el tipo de firma que se quiere realizar, luego se llama al método ***signData***.

5.3.1. XMLParameters

Esta es la clase de configuración para realizar una firma tanto en XML enveloped y enveloping. El constructor de esta clase, como ya ha sido indicado, recibe:

- **Byte[]** *bytesToSign*: Son los bytes del documento que se van a firmar.
- **RevocationVerify** *revocationVerify*: es la configuración para validar el certificado de firma y los certificados con los que ya se firmó el documento
- **CertificateConfiguration** *certificateConf*: es la configuración para identificar el método con el que se va acceder al certificado en formato p12 con el que se va a firmar.
- **String** *tagToSign*: es el string que indica cual es el tag con el id a firmar, si el string es vacío se firma todo el documento.
  Si se requiere firmar un tag debe tener la siguiente forma el XML:
  <firma id="tagFirma">Firma XML</firma>
  El String de *tagToSign* debe decir tagFirma puesto que pueden existir varios tag firma y se debe indicar cual tag específicamente se debe firmar.

A continuación se presenta un ejemplo de configuración del XmlParameters:

```
XmlParameters xmlParameters = new XmlParameters
(UtilsSign.getBytesFromFile(fileToSignPath),
      revocationVerify,certificateConfiguration, tagToSign);
```

5.3.2. Firma en formato XML Enveloped

Para realizar el firmado en formato XML Enveloper se debe indicar en el SignFactory que el tipo de firma es XML Enveloped. Un ejemplo de firma es el siguiente:

```
CertificateConfiguration certificateConfiguration = new
CertificateFromBytes(UtilsSign.getBytesFromFile(pkcs12Path),pkcs12Password);

RevocationVerify revocationVerify = new
RevocationVerify("OCSP_ONLY",null,null,null);
revocationVerify.setKeyStorePath(resourcesPath+"/keystore/Keystore");

XmlParameters xmlParameters = new XmlParameters
(UtilsSign.getBytesFromFile(fileToSignPath),
      revocationVerify,certificateConfiguration, tagToSign);

ArrayList<SignatureParameters> list = new ArrayList<SignatureParameters>();
list.add(xmlParameters);

Sign s = SignFactory.getSigner(SignFactory.XMLEnveloped, list);

List<ProcessResponseSign> prs = s.signData();

for(ProcessResponseSign pp :prs){
      if(pp.isExito()){
      UtilsSign.saveSignedFile("c:/temp/enveloped.xml",pp.getResultado());
      }else{
```

```
	for(MessageResponse mm : pp.getMessageResponse()){
		System.out.println(mm.getCodigo()+" "+mm.getMensaje());
	}
	}
}
```

5.3.3. Firma en formato XML Enveloping

Para realizar el firmado en formato XML Enveloping se debe indicar en el SignFactory que el tipo de firma es XML Enveloping. Un ejemplo de firma es el siguiente:

```
CertificateConfiguration certificateConfiguration = new
CertificateFromBytes(UtilsSign.getBytesFromFile(pkcs12Path),pkcs12Password);

RevocationVerify revocationVerify = new
RevocationVerify("OCSP_ONLY",null,null,null);
revocationVerify.setKeyStorePath(resourcesPath+"/keystore/Keystore");

XmlParameters xmlParameters = new XmlParameters
(UtilsSign.getBytesFromFile(fileToSignPath),
	revocationVerify,certificateConfiguration, tagToSign);

ArrayList<SignatureParameters> list = new ArrayList<SignatureParameters>();
list.add(xmlParameters);

Sign s = SignFactory.getSigner(SignFactory.XMLEnveloping, list);

List<ProcessResponseSign> prs = s.signData();

for(ProcessResponseSign pp :prs){
	if(pp.isExito()){
	UtilsSign.saveSignedFile("c:/temp/enveloping.xml",pp.getResultado());
	}else{
	for(MessageResponse mm : pp.getMessageResponse()){
		System.out.println(mm.getCodigo()+" "+mm.getMensaje());
	}
	}
}
```

5.4. FIRMA EN FORMATO XML Detached

A continuación se explica cómo se debe realizar implementación de un programa que realice firmas en este formato. En resumidas cuentas para desarrollar un fragmento de código que realice la firma en este formato debemos primero, crear un objeto ***XmlDetachedParameters***, en donde se guardan todos los parámetros que necesita la firma, y luego se construye un objeto Sign cuyo constructor recibe como parámetros la lista de objetos ***XmlDetachedParameters*** y el tipo de firma que se quiere realizar, luego se llama al método ***signData***.

5.4.1. XMLDetachedParameters

Esta es la clase de configuración para realizar una firma XML Detached. El constructor de esta clase, como ya ha sido indicado, recibe:

- **Byte[]** *bytesToSign*: Son los bytes del documento que se van a firmar.
- **RevocationVerify** *revocationVerify*: es la configuración para validar el certificado de firma y los certificados con los que ya se firmó el documento
- **CertificateConfiguration** *certificateConf*: es la configuración para identificar el método con el que se va acceder al certificado en formato p12 con el que se va a firmar.
- **String** *uriXML*: es el string que indica la ruta absoluta del documento a firmar (de tipo file:///) un ejemplo de una uriXML es:
  "file:///C:/Temp/docs/ArchivoXML.xml"

A continuación se presenta un ejemplo de configuración del XmlDetachedParameters:

```
XmlDetachedParameters xmlParameters = new XmlDetachedParameters
(UtilsSign.getBytesFromFile(fileToSignPath),
      revocationVerify,certificateConfiguration, uriXML);
```

5.4.2. Firma en formato XML Detached

Para realizar el firmado en formato XML Detached se debe indicar en el SignFactory que el tipo de firma es XML Detached. Un ejemplo de firma es el siguiente:

```
CertificateConfiguration certificateConfiguration = new
CertificateFromBytes(UtilsSign.getBytesFromFile(pkcs12Path),pkcs12Password);

RevocationVerify revocationVerify = new
RevocationVerify("OCSP_ONLY",null,null,null);
revocationVerify.setKeyStorePath(resourcesPath+"/keystore/Keystore");

XmlDetachedParameters xmlParameters = new XmlDetachedParameters
(UtilsSign.getBytesFromFile(fileToSignPath),
      revocationVerify,certificateConfiguration, uriXML);

ArrayList<SignatureParameters> list = new ArrayList<SignatureParameters>();
list.add(xmlParameters);

Sign s = SignFactory.getSigner(SignFactory.XMLDetached, list);

List<ProcessResponseSign> prs = s.signData();

for(ProcessResponseSign pp :prs){
      if(pp.isExito()){
      UtilsSign.saveSignedFile("c:/temp/detached.xml",pp.getResultado());
      }else{
      for(MessageResponse mm : pp.getMessageResponse()){
```

```
                System.out.println(mm.getCodigo()+" "+mm.getMensaje());
        }
        }
}
```

5.5. FIRMA EN FORMATO PDF

A continuación se explica cómo se debe realizar implementación de un programa que realice firmas en este formato. En resumidas cuentas para desarrollar un fragmento de código que realice la firma en este formato debemos primero, crear un objeto ***PDFParameters***, en donde se guardan todos los parámetros que necesita la firma, y luego se construye un objeto Sign cuyo constructor recibe como parámetros la lista de objetos ***PDFParameters*** y el tipo de firma que se quiere realizar, luego se llama al método ***signData***.

5.5.1. PDFParameters

Esta es la clase de configuración para realizar una pdf. El constructor de esta clase, como ya ha sido indicado, recibe:

- **Byte[]** *bytesToSign*: Son los bytes del documento que se van a firmar.
- **RevocationVerify** *revocationVerify*: es la configuración para validar el certificado de firma y los certificados con los que ya se firmó el documento
- **CertificateConfiguration** *certificateConf*: es la configuración para identificar el método con el que se va acceder al certificado en formato p12 con el que se va a firmar.

Adicionalmente, en el PDF se puede configurar otros atributos adicionales como para cifrarlo, estamparlo, etc. Que se describirán a continuación.

- Para añadir información de la firma, como lo es la razón de la firma y la localización de la firma, se debe llamar al método *setInformation* e ingresar 2 strings que indican la razón y la localización de firma:

```
signParameters.setInformation(signReason, signLocation);
```

- Para añadir imagen a la firma o un indicativo visual de la firma se debe llamar al método *setImageSettings* de la siguiente manera:

```
signParameters.setImageSettings(signFieldName,
UtilsSign.getBytesFromFile(pdf2SignImagePath),
new Rectangle(lowerLeftX,lowerLeftY, upperRightX,upperRightY),
signPage,
imageValidation,
contentSignature,
RenderingMode.DESCRIPTION);
```

En donde el orden de los parámetros son:

- ✓ signFielName: es un String con el nombre de la firma. Este campo debe ser único para cada firma.
- ✓ Los bytes de la imagen que puede tener la firma. Si no se quiere ingresar imagen se puede enviar en null este campo.
- ✓ Se debe crear un Rectangle que indica en qué posición del pdf va ir la imagen de la firma. Los datos que recibe esta clase son enteros positivos. Entonces los 2 primeros enteros son

la coordenada de la esquina inferior derecha y los siguientes 2 enteros es la coordeanda de la derecha superior izquierda.

- ✓ Se debe también indicar la página en donde va ir la firma. Debe ser un entero positivo y menor al número máximo de páginas del Pdf.
- ✓ imageValidation: es un booleano que indica si en la imagen debe salir la validación de la firma que muestra el Adobe Reader.
- ✓ contentSignature: es un texto, si se requiere si no se deja un String vacio, que sale en la posición de la firma. Este texto se adapta a la dimensión del rectángulo que se indicó.
- ✓ RenderingMode: es el tipo de impresión de la firma. Actualmente exite:
  - DESCRIPTION : pone solo la información en la variable contentSignature.
  - NAME_DESCRIPTION : pone información relevante sobre la firma.

➢ Para añadir cifrar el documento con una clave se debe realizar de la siguiente forma:

```
signParameters.setEncryption(permissions, password, strench);
```

En donde el orden de parámetros es:

- ✓ Permissions: los permisos del PDF.
- ✓ Password: es el password con el que se va a cifrar el PDF.
- ✓ Strench: es un boolean que indica si el algoritmo para cifrar es de 128bits o no (de 64 bits).

Es de aclarar que no se puede cofirmar un PDF.

➢ Para añadir una estampa al documento se debe realizar de la siguiente forma:

```
TSAAuthentication autenticacion = new
TSACertAuthentication(UtilsSign.getBytesFromFile(certificatePathStamp),
certificateStampPass);

TSAProperties tsaProperties = new TSAProperties(tsaURL, tsaPolicyOID,
hashAlgorithm, autenticacion);

signParameters.setTimeStampSettings(tsaProperties);
```

En donde el objeto ***TSAAuthentication*** es la clase que indica cómo se va autenticar frente a la TSA, existen 3 implementaciones: por Certificado, por Usuario y Password y sin ningún tipo de autenticación. Lo siguiente es crear un ***TSAProperties*** en donde se le indica:

- ✓ La dirección URL en donde esta publicada la TSA.
- ✓ La política OID de la TSA. Puede ser vacía.
- ✓ El tipo de algoritmo con el que se le va sacar el hash (SHA-1, SHA-256, SHA-512, etc.).
- ✓ Y el TSAAuthentication.

Finalmente se agrega al ***PDFParameters*** la configuración de la TSA.

➢ Para añadir verificación LTV se debe realizar de la siguiente forma:

```
TSAAuthentication autenticacion = new
TSACertAuthentication(UtilsSign.getBytesFromFile(certificatePathStamp),
certificateStampPass);

TSAProperties tsaProperties = new TSAProperties(tsaURL, tsaPolicyOID,
```

```
hashAlgorithm, autenticacion);

RevocationVerify revocationVerify = new
RevocationVerify("CRL_ONLY",null,"C:/Temp/CRLS/",null);

signParameters.setLtv(tsaProperties, revocationVerify);
```

En donde el objeto ***TSAAuthentication*** es la clase que indica cómo se va autenticar frente a la TSA, existen 3 implementaciones: por Certificado, por Usuario y Password y sin ningún tipo de autenticación. Lo siguiente es crear un ***TSAProperties*** en donde se le indica:

- ✓ La dirección URL en donde esta publicada la TSA.
- ✓ La política OID de la TSA. Puede ser vacía.
- ✓ El tipo de algoritmo con el que se le va sacar el hash (SHA-1, SHA-256, SHA-512, etc.).
- ✓ Y el TSAAuthentication.

Este objeto se utiliza para realizar la estampa de tiempo de la CRL. El objeto ***TSAProperties*** puede ser el mismo objeto que se definió en la estampa del documento.
Además se debe indicar la ruta del acceso de la CRL con el objeto ***RevocationVerify*** que también puede ser el mismo definido en el constructor del ***PDFParameters***.
Finalmente se agrega al ***PDFParameters*** la configuración de la TSA y el tipo de revocación.

A continuación se presenta un ejemplo de configuración del PdfParameters:

```
PdfParameters signParameters = new
PdfParameters(UtilsSign.getBytesFromFile(pdf2SignPath),revocationVerify,cert);

signParameters.setInformation(signReason, signLocation);

signParameters.setImageSettings(signFieldName,
UtilsSign.getBytesFromFile(pdf2SignImagePath),
new Rectangle(lowerLeftX,lowerLeftY,upperRightX,upperRightY),signPage,
false, contentSignature, RenderingMode.DESCRIPTION);

signParameters.setTimeStampSettings(tsaProperties);

signParameters.setEncryption(permissions, password, strench);

signParameters.setLtv(tsaProperties, revocationVerify);
```

5.5.2. Firma en formato PDF

Para realizar el firmado en formato PDF se debe indicar en el SignFactory que el tipo de firma es PDF. Un ejemplo de firma es el siguiente:

```
CertificateConfiguration cert = new
CertificateFromBytes(UtilsSign.getBytesFromFile(p12Certificate),certificatePassw
ord);

RevocationVerify revocationVerify = new
```

```
RevocationVerify("CRL_ONLY",null,"C:/Temp/CRLS/",null);
revocationVerify.setKeyStorePath(pathResources+"c:/Temp/keystore/Keystore");

TSAAuthentication autenticacion = new
TSACertAuthentication(UtilsSign.getBytesFromFile(certificatePathStamp),certifica
teStampPass);

TSAProperties tsaProperties = new TSAProperties(tsaURL, tsaPolicyOID,
hashAlgorithm, autenticacion);

PdfParameters signParameters = new
PdfParameters(UtilsSign.getBytesFromFile(pdf2SignPath),revocationVerify,cert);

signParameters.setInformation(signReason, signLocation);

signParameters.setImageSettings(signFieldName,
UtilsSign.getBytesFromFile(pdf2SignImagePath),
new Rectangle(lowerLeftX,lowerLeftY,upperRightX,upperRightY),signPage,
false, contentSignature, RenderingMode.DESCRIPTION);

signParameters.setTimeStampSettings(tsaProperties);

signParameters.setEncryption(permissions, password, strench);

signParameters.setLtv(tsaProperties, revocationVerify);

ArrayList<SignatureParameters> lista = new ArrayList<SignatureParameters>();

lista.add(signParameters);

Sign s = SignFactory.getSigner(SignFactory.PDF, lista);

List<ProcessResponseSign> listaR = s.signData();

for(ProcessResponseSign pp :listaR){
      if(pp.isExito()){

      UtilsSign.saveSignedFile("C:/temp/pdf.pdf", pp.getResultado());

      }else{
            for(MessageResponse mm : pp.getMessageResponse()){
                  System.out.println(mm.getCodigo()+" "+mm.getMensaje());
            }
      }

}
```

5.5.3. Firma en formato PDF Distribuido

Para realizar el firmado en formato PDF Distribuido se debe indicar en el SignFactory que el tipo de firma es PDF y hacer uso del Applet de firma. Un ejemplo de firma es el siguiente:

```
String hashesPdf = null;
PdfSign s1 = null;
try{
	archivoSignPath2 = pathResources + "/dataIn/Documento_SinFirmar.pdf";
	RevocationVerify revocationVerify = new RevocationVerify("CRL_ONLY", null,
	"C:/CRL/crl", null);
	revocationVerify.setKeyStorePath(pathResources+"/keystore/Keystore");
	CertificateConfiguration cert = new CertificateConfiguration() {
	@Override
		public void validate() throws CertificateInitException {
		}
	};
	TSAAuthentication autenticacion = new
	TSACertAuthentication(UtilsSign.getBytesFromFile(certificatePathStamp),
	certificateStampPass);
	TSAProperties tsaProperties = new TSAProperties(tsaURL, tsaPolicyOID,
	hashAlgorithm, autenticacion);
	ArrayList<SignatureParameters> listaPdf = new
	ArrayList<SignatureParameters>();
	for(int i=0; i<1; i++){
		PdfParameters signParameterspdf = new
	PdfParameters(UtilsSign.getBytesFromFile(archivoSignPath2), revocationVerify,
	cert);
		signParameterspdf.setInformation(signReason, signLocation);
			signParameterspdf.setImageSettings(signFieldName,
		UtilsSign.getBytesFromFile(pdf2SignImagePath), new Rectangle(lowerLeftX,
	lowerLeftY, upperRightX, upperRightY), signPage, false, contentSignature,
	RenderingMode.DESCRIPTION);
		signParameterspdf.setTimeStampSettings(tsaProperties);
		listaPdf.add(signParameterspdf);
	}
	s1 = (PdfSign) SignFactory.getSigner(SignFactory.PDF, listaPdf);
	hashesPdf = s1.getHashs();
}
catch(Exception e){
	e.printStackTrace();
	request.setAttribute("hash",e.toString());
}
ArrayList<Sign> lista = new ArrayList<Sign>();
lista.add(s1);
session.setAttribute("hash", hashesPdf);
session.setAttribute("ListaHashSigned", lista);
```

En donde lo primero que debemos hacer es obtener el hash de los documentos que se van a firmar.

```
function setAppletText() {
	var applet = document.getElementById('appletfirma');
	var timediv = document.getElementById('txtHash');
	applet.Sign(timediv.value, "archivoDist", false);
}

function setSign(value){
	var field = document.getElementById('Firma');
	field.value = value;
}
```

Luego obtenemos la firma de los documentos por medio del Applet de Firma.

```
ArrayList<Sign> lista = (ArrayList<Sign>) session.getAttribute("ListaHashSigned");
PdfSign s1 = (PdfSign)lista.get(0);
String[] hashesFirmados = request.getParameter("Firma").split("%");
String hashesFirmadosPdf = "";
for(int i=0;i<s1.signatureParameters.size(); i++){
	hashesFirmadosPdf += hashesFirmados[i]+"%";
}
List<ProcessResponseSign> listaRPdf = new ArrayList<ProcessResponseSign>();
try {
	listaRPdf.addAll(s1.joinPDFSignatures(hashesFirmadosPdf));
}
catch (SignException e) {
	e.printStackTrace();
}
int k=0;
//Se recupera la lista en donde esta la configuracion de los hashes
for(ProcessResponseSign processResponseSign: listaRPdf){
	if(processResponseSign.isExito()){
		verificarPdf(listaRPdf.get(k).getResultado());
	//Ejemplo para descargar el archivo firmado.
		session.removeAttribute("isHash");
	//response.setContentType(" application/pdf ");
	//response.setHeader("Content-Disposition","attachment; filename =
	"+"ArchivoFirmado.pdf");
	//ServletOutputStream op = response.getOutputStream();
	//op.write(listaRPdf.get(k).getResultado());
	//op.flush();
	//op.close();

		UtilsSign.saveSignedFile("C:/Users/jhon.triana/Desktop/prueba/prueba" +
k + ".pdf",listaRPdf.get(k).getResultado() );
		k++;
	}
```

```
	else{
		k++;
		String error="";
		for(MessageResponse messageResponse:
processResponseSign.getMessageResponse()){
			error += ("Error al firmar documentos: Código:
"+messageResponse.getCodigo()+" Mensaje: "+messageResponse.getMensaje());
		}
		session.setAttribute("error", error);
		response.sendRedirect("index.jsp");
	}
}
```

Como último paso unimos la firma con el documento original

6. Precondiciones

- Se debe ejecutar en una plataforma java 1.6 en adelante.
- Se deben tener permisos de lectura sobre los archivos que se quieren firmar.
- Para realizar la co-firma de un archivo en cualquier formato, todas las firmas anteriores deben ser validas, de lo contrario el componente no dejará realizar la cofirma.
- Se deben contar con certificados validos para realizar el proceso de firma.

sig:uid=CC1032388038