Tabla de contenido

[Documento técnico 2](#_Toc374695658)

[Propuesta Intercambio de información 2](#_Toc374695659)

para el material de Uso Aeronáutico [2](#_Toc374695660)

[INTRODUCCIÓN 2](#_Toc374695661)

[Objetivo: 2](#_Toc374695662)

[Alcance: 2](#_Toc374695663)

[Seguridad: 2](#_Toc374695664)

[Proceso 3](#_Toc374695665)

[Generación de Llave privada y pública “openssl” PKCS8 3](#_Toc374695666)

[Ejemplo código Java 3](#_Toc374695667)

[Lectura de la llave privada. 3](#_Toc374695668)

[Lectura de la llave pública. 4](#_Toc374695669)

[Cifrar 4](#_Toc374695670)

[Descifrar 4](#_Toc374695671)

[Métodos: 6](#_Toc374695672)

[Método “consultaFormM03” 6](#_Toc374695673)

[Método “registroCertificado” 7](#_Toc374695674)

# **Documento técnico**

# **Propuesta Intercambio de información**

# **para el material de Uso Aeronáutico**

# INTRODUCCIÓN

## Objetivo:

Optimizar el proceso de intercambio de información relacionadas con el ingreso de material destinado a la reparación y mantenimiento de aeronaves, equipos para la recepción de pasajeros, recepción, manipuleo y despacho de carga, y demás bienes necesarios para la operación de aeronaves nacionales o internacionales, así como aquel destinado al uso de los servicios técnicos en tierra, utilizando *Web Services* y la arquitectura correspondiente a los mismos (Web Services, SOAP, XML, WSDL).

* SOAP (Simple Object Access Protocol): Protocolo sobre los que se establece el intercambio.
* XML (Extensible Markup Language): Formato estándar sobre el cual se intercambiarán los datos.
* WSDL (Web Services Description Languages): Es el lenguaje de la interfaz pública para los servicios Web. Es una descripción basada en XML de los requisitos funcionales necesarios para establecer una comunicación con los servicios Web.

## Alcance:

La Aduana Nacional de Bolivia desarrollará el *web services* “wsMaterialUsoAeronautico”, el mismo implementa el siguiente método:

* **memorizaMUA,** este método debe grabar en la base de datos de la ANB los datos enviados desde el cliente Web Services en una estructura XML que contiene datos de cabecera y detalle del formulario MUA, con estado de Memorizado, como respuesta devuelve el número de trámite y el resultado de la operación, caso contrario las excepciones producidas.
* **devuelveMemorizadoMUA,** este método recibe el número de tramite MUA Memorizado y devuelve información del formulario MUA en una estructura XML.
* **modificaMemorizadoMUA,** este método debe actualizar en la base de datos de la ANB los datos enviados desde el cliente Web Services en una estructura XML que contiene datos de cabecera (adjuntando el número de trámite para modificar) y detalle del formulario MUA, con estado de Memorizado, como respuesta devuelve el número de trámite y el resultado de la operación, caso contrario las excepciones producidas.
* **registraMemorizadoMUA,** este método debe modificar el estado del trámite de Memorizado ha Registrado, en la base de datos de la ANB, el cliente Web Services, debe enviar el número de tramite con estado Memorizado.

## **Seguridad:**

En la implementación del servicio Web de información de Material de Uso Aeronáutico, el acceso a la información y los servicios necesitan un grado de fiabilidad y confianza en el medio de comunicación. Para ello cualquier operación que se realice a través de medios electrónicos requiere “asegurar la integridad del contenido y autenticar al remitente y receptor”

La solución adoptada para garantizar la seguridad en el uso de medios electrónicos está basada en la criptografía, es decir cifrar y descifrar información que hagan posible el intercambio de mensajes de manera que solo puedan ser leídos por las personas a quienes van dirigidos.

Para lo indicado utilizaremos técnicas de criptografía asimétrica (PKCS8) este concepto se basa en un par de llaves. Cada mitad del par (una llave) puede cifrar información que solo la otra parte (la otra llave) podrá descifrar. Una parte del par de llaves, la llave privada, es solo conocida por el propietario la otra parte, la llave pública será puesta en conocimiento de la institución con la cual se realizará la comunicación.

A través del cifrado asimétrico garantizaremos la confidencialidad, integridad, autenticidad y el no repudio.

## **Proceso**

* El proceso iniciará con la obtención del par de llaves en cada entidad.
* Posteriormente se deberá realizar el intercambio de las llaves públicas, entre ambas entidades.
* En la solicitud de un servicio (solicitante) y su respuesta (proveedor) deberá proceder a firmarse de manera digital todo el contenido del mensaje (XML string).

## **Generación de Llave privada y pública “openssl” PKCS8**

1. Para la generación de llave privada.

openssl genrsa -out rsaprivkey.pem 1024

1. Generación de llave publica.

openssl rsa -in rsaprivkey.pem -pubout -outform DER -out rsapubkey.der

1. Cambio de formato de la privada “DER” de la llave privada.

openssl pkcs8 -topk8 -inform PEM -outform DER -in rsaprivkey.pem -out rsaprivkey.der –nocrypt

## Ejemplo código Java

### Lectura de la llave privada.

File f = new File("/home/oracle/llave/ rsaprivkey.der");

FileInputStream fis = new FileInputStream(f);

DataInputStream dis = new DataInputStream(fis);

byte[] keyBytes = new byte[(int)f.length()];

dis.readFully(keyBytes);

dis.close();

PKCS8EncodedKeySpec spec = new PKCS8EncodedKeySpec(keyBytes);

KeyFactory kf = KeyFactory.getInstance("RSA");

PrivateKey privateKey = kf.generatePrivate(spec);

La llave privada esta almacena en privateKey.

### Lectura de la llave pública.

File f = new File("/home/oracle/llave/public.der");

FileInputStream fis = new FileInputStream(f);

DataInputStream dis = new DataInputStream(fis);

keyBytes = new byte[(int)f.length()];

dis.readFully(keyBytes);

dis.close();

X509EncodedKeySpec spec1 = new X509EncodedKeySpec(keyBytes);

KeyFactory kf1 = KeyFactory.getInstance("RSA");

publicKeyAN publicKey = kf1.generatePublic(spec1);

La llave pública esta almacena en publicKey.

### Cifrar

//mensaje a cifrar

msg=”<?xml version="1.0" encoding="UTF-8" standalone="no"?><consultaMicDta><registroManifiesto>201 2012 7318</ registroManifiesto ></ consultaMicDta>”

//instancia CIPHER

Cipher rsa;

//definición del algoritmo.

rsa = Cipher.getInstance("RSA");

//asignación de la llave privada

rsa.init(Cipher.ENCRYPT\_MODE, privateKey);

//cifrado del mensaje

byte[] doFinal = rsa.doFinal(msg.getBytes("UTF8"));

//conversión a 64 bits

msg = new String(org.bouncycastle.util.encoders.Base64.encode(doFinal), "UTF-8");

//en “msg” se tiene el mensaje Cifrado.

### Descifrar

//mensaje a descifrar en 64 bits

Msg=” f3euHnyf1Mztwj+jdpwYC3hbCJcBcHk8RiuHXxnTs/bsGuKhLp9PzcIVhLxp75TlWFSMWV0h6ppYreg5YD5bTTts/wTwzEKCuDYceLinXMT3JueLTMvgc5GKsj60TMzlUYqJ2eDdiZbQmTUj+McLgBhMpZUh8y+ZRXubLLZFm+zb3e37GeIDFR4FARB4/WmdRCvhDzIHHfspD7sZDSgWLnKM+2YUu72KpH6c+1sOUyo19S18gDZ26rKO+/wJ28cwsCh6ygdIVREPYQw7/w95+dGvD+k4XENDC7Eta2A73dd/bktxLgEqPP6yaF0eTrfad7CO7i/A7ux0O16EwbcI5g==”

//instacia CIPHER y definición del algoritmo

Cipher cipher = Cipher.getInstance("RSA");

//asignación de la llave pública

cipher.init(Cipher.DECRYPT\_MODE, publicKey);

//revertir de 64 bits.

BASE64Decoder decoder = new BASE64Decoder();

//descifrar el mensaje

byte[] raw = decoder.decodeBuffer(msg);

byte[] stringBytes = cipher.doFinal(raw);

//obtención del mensaje original

msg = new String(stringBytes, "UTF8"));

//en “msg” se tiene el mensaje original (descifrado)

Métodos:

Método “memorizaMUA”

Este método debe grabar en la base de datos de la ANB los datos enviados desde el cliente Web Services en una estructura XML que contiene datos de cabecera y detalle del formulario MUA, con estado de Memorizado, como respuesta devuelve el número de trámite y el estado de la solicitud.

En caso de presencia de error el método ***devuelve una excepción.***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nombre | **wsMaterialUsoAeronautico** | | | | | |
| NameSpace |  | | | | | |
| Ubicación | Testing |  | | | | |
| Producción |  | | | | |
| WebMethod | **memorizaMUA** | Descripción | memorizaMUA | | | |
| Parámetros de Entrada | Parámetro | | Descripción | Tipo |
| datoCabecera | codigoAduana | Código que indica la aduana en la que se está realizando la operación.  Ejemplo: 211 (Aeropuerto El Alto). | String |
| numeroNIT | Número de Identificación Tributaria.  Ejemplo: 1025454752 | String |
| tipoOperacion | Tipo de operación que se realizara.  Los valores permitidos son:   * 91 (Ingreso de MUA) * 92 (Ingreso de material AOG) * 93 (Traspaso de MUA) | String |
| observacion | Observación respectó a la información introducida.  *Longitud máxima de 500 caracteres.* | String |
| datoItem | numeroItem | Secuencial de ítem | int |
| deposito | Código del Depósito Aeronáutico utilizado.  Ejemplo: 211000635ZFC | String |
| ubicacion | Ubicación en Depósito Aeronáutico  *Longitud máxima de 200 caracteres.* | String |
| codigoMercancia | Consignar el código de la mercancía asignado por el listado del anexo 1. Un mismo producto deberá estar identificado por un único código de mercancía. | String |
| numeroMatriculaNave | Nro. de Matrícula - Nave | String |
| numeroSerie | Número de serie de la mercancía. | String |
| estadoMercancia | Estado de la mercancía.  Los valores permitidos son:   * 0 (Nueva) * 1 (Usada) | String |
| cantidad | Cantidad de la mercancía expresada en su menor unidad de medida. | Double |
| peso | Peso neto de la mercancía expresada en kilogramos. | Double |
| paisOrigen | País de origen o fabricación de la mercancía.  Los valores permitidos son:   * AU (Australia) * BO (Bolivia) * US (Estados Unidos) * JP (Japón) * Etc….   *Longitud máxima de 2 caracteres.* | string |
| valorFOB | Monto que se debe retener en Bolivianos o su equivalente | Double |
| datoDocumentoAdicional | numeroDocumento | Secuencial de Documento | int |
| documentoSoporte | Consignar el número del tipo de documento soporte.  Los valores permitidos son:   * 141 (Lista de Empaque) * 380 (Factura Comercial) * 740 (Guia Aerea – Airway Bill) * 785 (Manifiesto de Carga) * 901 (Parte de Recepcion/Planilla de Recepcion) * 944 (Autorizacion Previa Min. Defensa) * B02 (Certificado Toxicologico) * C14 (Form 250 Declaracion Jurada de Equipaje Acompañado RD01-002-08 Cir25/08) * C53 (Auto. Previa aparatos de telecomunicación – ATT L1632-DS71-572)   *Longitud máxima de 3 caracteres.* | string |
| nombreRazonSocialEmisor | Consignar el nombre o razón social del emisor del documento.  *Longitud máxima de 50 caracteres.* | string |
| numeroDocumento | Consignar el número de documento  *Longitud máxima de 20 caracteres.* | string |
| fechaEmision | Consignar la fecha de emisión del documento | date |
| importe | Consignar el importe | Double |
| tipoMoneda | Consignar la Moneda de la factura.  Los valores permitidos son:   * AUD (Dólar Australiano) * BOB (Boliviano) * USD (Dólar Estados Unidos) * JPY (Yen Japones) * Etc….   *Longitud máxima de 3 caracteres.* | string |
| tipoDeCambio | Consignar el tipo de cambio de la moneda de la factura | Double |
| Parámetros de Salida | numeroTramite | | Código de Tramite, que identifica un correlativo por gestión y aduana.  *Formato:* yyyyaaaTnnnn  *Ejemplo: gestión 2014 aduana 211*  2014211T1, 2014211T654  *gestión 2014 aduana 311* 2014311T23 | String |
| estadoSolicitud | | Igual a “OK” en caso de ser exitosa la recepción. | String |
| |  | | --- | | EJEMPLO:  **Solicitud**  <?xml version="1.0" encoding="UTF-8" standalone="no"?>  <datosFormularioMUA>  <datoCabecera>  <codigoAduana>211</codigoAduana>  <numeroNIT>1020255020</numeroNIT>  <tipoOperacion>91</tipoOperacion>  <observacion>Operacion AOG</observacion>  </datoCabecera>  <items>  <datoItem>  <numeroItem>1</numeroItem>  <deposito>211000635ZFC</deposito>  <ubicacion>sector 4 bloque 14</ubicacion>  <codigoMercancia>02.01.02</codigoMercancia>  <numeroMatriculaNave>AFRDV3434</numeroMatriculaNave>  <numeroSerie>4545478KUJH</numeroSerie>  <estadoMercancia>0</estadoMercancia>  <cantidad>400.00</cantidad>  <peso>2000.00</peso>  <paisOrigen>JP</paisOrigen>  <valorFOB>4500.50</valorFOB>  </datoItem>  <datoItem>  <numeroItem>2</numeroItem>  <deposito>211000635ZFC</deposito>  <ubicacion>sector 4 bloque 54</ubicacion>  <codigoMercancia>03.01.02</codigoMercancia>  <numeroMatriculaNave>AFRDV3434</numeroMatriculaNave>  <numeroSerie>45454DREDS345</numeroSerie>  <estadoMercancia>1</estadoMercancia>  <cantidad>200</cantidad>  <peso>1000.00</peso>  <paisOrigen>CH</paisOrigen>  <valorFOB>2000.50</valorFOB>  </datoItem>  </items>  <documentosAdicionales>  <datoDocumentoAdicional>  <numeroDocumento>1</numeroDocumento>  <documentoSoporte>380</documentoSoporte>  <nombreRazonSocialEmisor>IMPORTADORA Y EXPORTADORA ALMATE</nombreRazonSocialEmisor>  <numeroDocumento>674532</numeroDocumento>  <fechaEmision>15/01/2014</fechaEmision>  <importe>600.00</importe>  <tipoMoneda>USD</tipoMoneda>  <tipoDeCambio>1</tipoDeCambio>  </datoDocumentoAdicional>  <datoDocumentoAdicional>  <numeroDocumento>2</numeroDocumento>  <documentoSoporte>740</documentoSoporte>  <nombreRazonSocialEmisor>IMPORTADORA Y EXPORTADORA RAKTIS</nombreRazonSocialEmisor>  <numeroDocumento>000764</numeroDocumento>  <fechaEmision>20/01/2014</fechaEmision>  <importe>450.00</importe>  <tipoMoneda>AUD</tipoMoneda>  <tipoDeCambio>3.4565</tipoDeCambio>  </datoDocumentoAdicional>  </documentosAdicionales>  </datosCertificado>  **Respuesta**  <?xml version="1.0" encoding="UTF-8" standalone="no"?>  < remiteSolicitud>  <numeroTramite>2013-258</numeroTramite>  <estado>OK</estado>  </ remiteSolicitud> | | | | | | | |

ANEXO 1. LISTADO DE MATERIAL PARA USO AERONÁUTICO

|  |
| --- |
| D E S C R I P C I Ó N |
|  |