Tabla de contenido

[Documento técnico 2](#_Toc483227881)

[Propuesta Intercambio de información 2](#_Toc483227882)

[Personas Acreditadas 2](#_Toc483227883)

[INTRODUCCIÓN 2](#_Toc483227884)

[Objetivo: 2](#_Toc483227885)

[Alcance: 2](#_Toc483227886)

[Alcance: 2](#_Toc483227887)

[Seguridad: 3](#_Toc483227888)

[Proceso 3](#_Toc483227889)

[Generación de Llave privada y pública “openssl” PKCS8 3](#_Toc483227890)

[Ejemplo código Java 4](#_Toc483227891)

[Lectura de la llave privada. 4](#_Toc483227892)

[Lectura de la llave pública. 4](#_Toc483227893)

[Cifrar 4](#_Toc483227894)

[Descifrar 5](#_Toc483227895)

[Métodos: 6](#_Toc483227896)

[Método “actualizacionPersonaSICOPEA” 6](#_Toc483227897)

[Métodos: 8](#_Toc483227898)

[Método “actualizacionEntidadSICOPEA” 8](#_Toc483227899)

# **Documento técnico**

# **Propuesta Intercambio de información**

# **Personas Acreditadas**

# 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:

## Alcance:

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

-     **ActualizacionPersonaSICOPEA,** 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 referentes a la información de las personas acreditadas ante Cancillería, como respuesta devuelve el resultado de la operación, caso contrario las excepciones producidas.

-     **ActualizacionEntidadSICOPEA,** 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 referentes a la información de las Entidades registradas ante Cancillería (Embajadas, Consulados, ONG’s), como respuesta devuelve el resultado de la operación, caso contrario las excepciones producidas.

## **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 “actualizacionPersonaSICOPEA”

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 la información de la Persona Acreditada, 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 | **wsSicopea** | | | | | |
| NameSpace |  | | | | | |
| Ubicación | Testing |  | | | | |
| Producción |  | | | | |
| WebMethod | **ActualizacionPersonaSICOPEA** | Descripción | Actualizar Informacion de Personas Acreditadas en el sistema SICOPEA | | | |
| Parámetros de Entrada | Parámetro | | Descripción | Tipo |
| informacionIntercambio | ClasePasaporte | Código del Tipo de Pasaporte Los valores permitidos son:  - Diplomatico - Oficial - Servicio - Corriente - Especial  Obligatorio. | String |
| NroPasaporte | Número de Pasaporte de la Persona Acreditada. Ejemplo: G53812417 Longitud máxima de 30 caracteres.  Obligatorio. | String |
| TipoDiplomatico | Tipo de personal Diplomatico. Los valores permitidos son:  - Normal - Ley617  Obligatorio | String |
| CodEntidad | Codigo de la Entidad a al que pertenece el personal Diplomatico.  Obligatorio | int |
| NombreCompleto | Nombre Completo de la Persona Acreditada.  Longitud máxima de 200 caracteres.  Obligatorio | String |
| Nombres | Nombre de la Persona Acreditada. Longitud máxima de 100 caracteres.  Obligatorio | String |
| Paterno | Apellido Paterno de la Persona Acreditada. Longitud máxima de 50 caracteres.  No obligatorio. | String |
| Materno | Apellido Materno de la Persona Acreditada. Longitud máxima de 50 caracteres.  No obligatorio. | String |
| CargoPersona | Cargo de la Persona Acreditada. Longitud máxima de 300 caracteres.  Obligatorio. | String |
| Categoria | Código del Tipo de Pasaporte Los valores permitidos son:  - Primera Categoria - Segunda Categoria - Tercera Categoria - Cuarta Categoria - Quinta Categoria - Sexta Categoria - Ninguna - Otros  Obligatorio. | String |
| CiteSolAcreditacion | Número Cite de la Carta de Solicitud de Acreditación. Longitud máxima de 150 caracteres.  Obligatorio. | String |
| FechaCiteSol | Fecha de la Carta de Solicitud de Acreditación. Formato Permitido: dd/mm/aaa  Obligatorio. | String |
| FechaLlegadaAlPais | Fecha de la Llegada al País de la Persona Acreditada. Formato Permitido: dd/mm/aaa  Obligatorio. | String |
| Fechacese | Fecha de Case de la Persona Acreditada. Formato Permitido: dd/mm/aaa  Obligatorio. | String |
| Proyecto | Nombre del Proyecto al que pertenece la persona acreditada. Longitud máxima de 150 caracteres.  No obligatorio | String |
| Parámetros de Salida | estadoSolicitud | | Igual a “OK” en caso de ser exitosa la recepción. | String |
| descripcion | | En caso de producirse un error, se despliega el mensaje del error. | String |

|  |  |  |
| --- | --- | --- |
| |  | | --- | | EJEMPLO:  **Solicitud**  <?xml version="1.0" encoding="UTF-8" standalone="no"?>  <datosPersonaAcreditada>  <clasePasaporte>Oficial</clasePasaporte>  <nroPasaporte>G53812417</nroPasaporte>  <tipoDiplomatico>Ley617</tipoDiplomatico>  <codEntidad>3125</codEntidad>  <nombres>CARLOS</nombres>  <paterno>BERGER</paterno>  <materno>ANDREU</materno>  <cargoPersona>AYUDANTE ADMINISTRATIVO AGREGARIA MILITAR, NAVAL, AEREA DE ECUADOR</cargoPersona>  <categoria>Primera Categoria</categoria>  <citeSolAcreditacion>N. V. Nº 449/2016</citeSolAcreditacion>  <fechaCiteSol>30/08/2016</fechaCiteSol>  <fechaLlegadaAlPais>01/09/2016</fechaLlegadaAlPais>  <fechacese>05/05/2020</fechacese>  </ datosPersonaAcreditada >  **Respuesta**  <?xml version="1.0" encoding="UTF-8" standalone="no"?>  < remiteSolicitud>  <estado>OK</estado>  <descripcion> </ descripcion >  </ remiteSolicitud> | |  | |

Métodos:

Método “actualizacionEntidadSICOPEA”

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 la información de una Entidad (Embajadas, Consulados, ONG’s), 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** | **wsSicopea** | | | | | |
| **NameSpace** |  | | | | | |
| **Ubicación** | Testing |  | | | | |
| Producción |  | | | | |
| **WebMethod** | **ActualizacionEntidadSICOPEA** | Descripción | Actualizar Informacion de las Entidades en el sistema SICOPEA | | | |
| Parámetros de Entrada | Parámetro | | Descripción | Tipo |
| informacionIntercambio | CodEntidad | Codigo de la Entidad a al que pertenece el personal Diplomatico.  Obligatorio. | int |
| NombreEntidad | Nombre de la Entidad a al que pertenece el personal Diplomatico. Longitud máxima de 200 caracteres.  Obligatorio. | String |
| Direccion | Dirección de la Entidad. Longitud máxima de 200 caracteres.  No obligatorio. | String |
| Telefono | Numeros de Telefono de la Entidad. Longitud máxima de 50 caracteres.  No obligatorio. | String |
| Fax | Números de Fax de la Entidad. Longitud máxima de 50 caracteres.  No obligatorio. | String |
| Correo | Correo electronico de la Entidad. Longitud máxima de 200 caracteres.  No obligatorio. | String |
| TipoEntidad | Tipo de la Entidad  Los valores permitidos son: - Embajada - Institucion  Obligatorio. | String |
| Parámetros de Salida | estadoSolicitud | | Igual a “OK” en caso de ser exitosa la recepción. | String |
| descripcion | | En caso de producirse un error, se despliega el mensaje del error. | String |

|  |  |  |
| --- | --- | --- |
| |  | | --- | | EJEMPLO:  **Solicitud**  <?xml version="1.0" encoding="UTF-8" standalone="no"?>  <datosEntidad>  <codEntidad>3125</codEntidad>  <nombreEntidad>EMBAJADA DE ECUADOR</nombreEntidad>  <direccion>CALACOTO CALLE 10 NRO 8054</direccion>  <telefono>2784422</telefono>  <fax>2771043</fax>  <correo>EECUBOLIVIA@MMRREE.GOV.S</correo>  <tipoEntidad>Embajada</tipoEntidad>  </ datosEntidad >  **Respuesta**  <?xml version="1.0" encoding="UTF-8" standalone="no"?>  < remiteSolicitud>  <estado>OK</estado>  <descripcion> </ descripcion >  </ remiteSolicitud> | |  | |