|  |
| --- |
|  |
| Red VUCE |
| Grupo Tecnológico |
|  |
| **PROTOCOLOS DE COMUNICACIÓN Y SEGURIDAD** |
| **05/11/2013** |

|  |
| --- |
|  |

Contenido

[1. Introducción 4](#_Toc373142514)

[2. Modelo VUCE 5](#_Toc373142515)

[2.1 Modelo de Interoperabilidad VUCE 6](#_Toc373142516)

[2.2 Interacción Punto a Punto 7](#_Toc373142517)

[2.3 Modelo de Interoperabilidad VUCE 8](#_Toc373142518)

[2.4 Diagrama de Contexto Red VUCE 10](#_Toc373142519)

[3. Marco Teórico 11](#_Toc373142520)

[3.1 SOAP 13](#_Toc373142521)

[3.1.1 Esquemas, estilo y codificación (Encoding, XML) 14](#_Toc373142522)

[3.1.2 Archivos o datos binarios (XOP) 16](#_Toc373142523)

[3.2 Seguridad 17](#_Toc373142524)

[3.2.1 Túnel Seguro 17](#_Toc373142525)

[3.2.2 (WS-Security) 17](#_Toc373142526)

[4. Estándares y Protocolos de Comunicación a utilizar en la RED VUCE 20](#_Toc373142527)

[4.1 Servicios 20](#_Toc373142528)

[4.2 Flujo de Interoperación 21](#_Toc373142529)

[4.2.1 Notificar Inicio del Proceso de Exportación 22](#_Toc373142530)

[4.2.2 Notificar de Respuesta al Proceso de Exportación 22](#_Toc373142531)

[4.3 Log de servicios 23](#_Toc373142532)

[4.4 Flujo de Interacción de los Servicios 23](#_Toc373142533)

[4.5 Manejo de errores 25](#_Toc373142534)

[5. Pasos para integración a la red VUCE 26](#_Toc373142535)

[5.1 Análisis funcional de esquemas y armonización de datos. 26](#_Toc373142536)

[5.2 Implementación de Servicios 27](#_Toc373142537)

[5.3 Implementación de Clientes 27](#_Toc373142538)

[5.4 Pruebas. 27](#_Toc373142539)

[6. Referencias 29](#_Toc373142540)

# Introducción

El presente documento tiene como objetivo dar apoyo en la definición del modelo tecnológico que permita el intercambio de información entre las ventanillas únicas de comercio exterior de los países de la región.

El modelo tecnológico de la red VUCE tiene como fin proponer estándares de arquitectura e intercambio de información y protocolos teniendo presente la seguridad de los datos, generando un modelo tecnológico como recomendación para la construcción de un sistema que pueda ser parte de la red VUCE.

En modelo tecnológico estará compuesto de los siguientes elementos:

* Definiciones conceptuales de protocolos de comunicación (referencias capítulo 6).
* Estándares y protocolos de comunicación.
* Protocolo de seguridad.
* Modelo VUCE SOA

La red VUCE contempla la interoperabilidad entre países que deberán interactuar entre sus procesos de importación y exportación de mercancías o productos, por lo que es relevante la definición de un único modelo de interacción entre un país de origen y otro de destino.

Los elementos mencionados comparten el mismo objetivo que es definir el modelo tecnológico. La definición de los protocolos y estándares de comunicación para interoperabilidad entre países, están soportados por las interacciones definidas en el proceso general de comercio exterior. Y a su vez, estos protocolos son parte fundamental para la implementación de la Arquitectura Orientada a Servicios que esta consultoría propone.

Los protocolos y estándares de comunicación se definen en base a los puntos de interacción identificados en el análisis de los procesos.

# Modelo VUCE

Con el objetivo de entender las necesidades de la Red VUCE, se define el modelo VUCE, que se componen de un conjunto de macroprocesos considerados como transversales en los procesos de comercio exterior de los países de la región, los cuales se toman como base para definir los puntos de interoperabilidad que son la base para el intercambio electrónico de información entre los países miembros.

Los macroprocesos definidos son los siguientes:

* Proceso de exportación, importación.
* Proceso de ingreso y revisión zona primaria o zona aduanera.

Cada proceso define interacciones entre los países que interactúan en un proceso de exportación e importación, origen y destino respectivamente.

En la siguiente ilustración se pueden visualizar los macroprocesos mencionados y su interacción (Ilustración 1, Modelo de Interoperabilidad VUCE).

## Modelo de Interoperabilidad VUCE

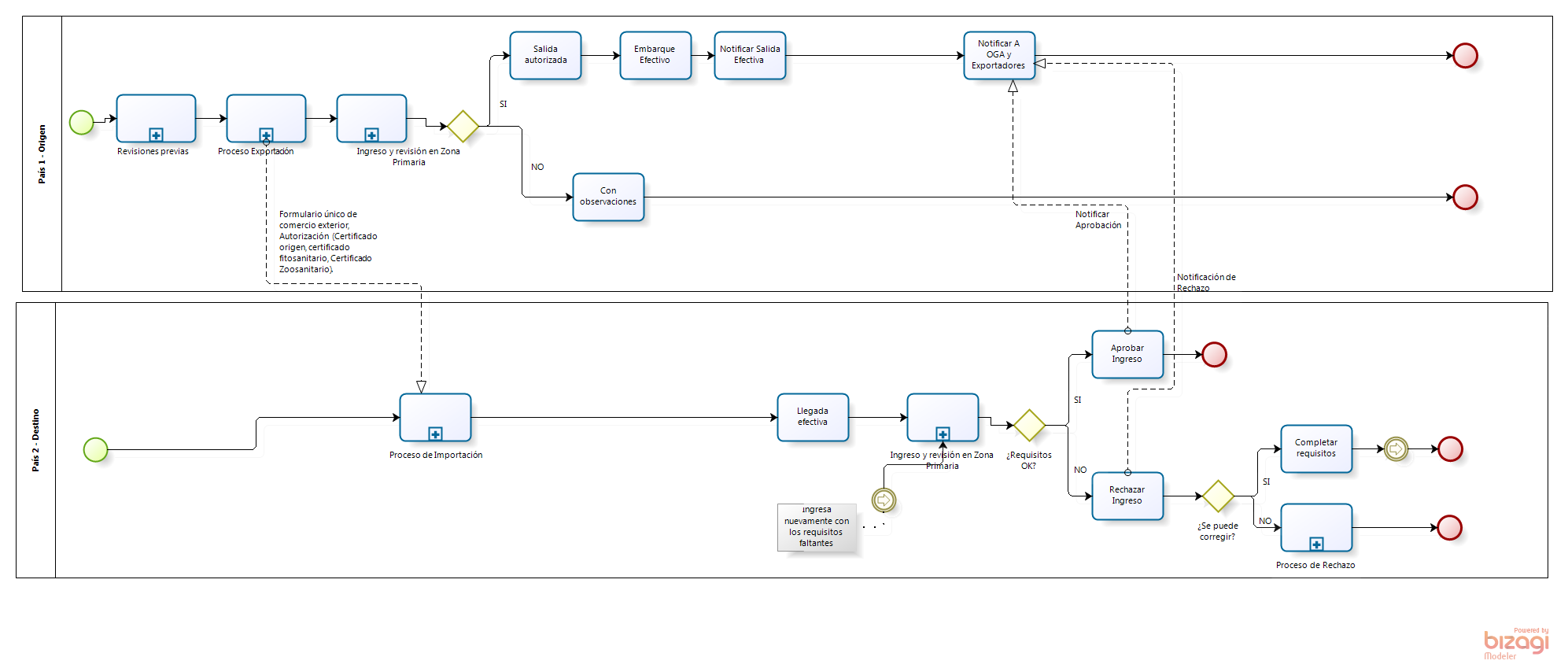


Ilustración 1, Modelo de Interoperabilidad VUCE

Los puntos de interacción mencionados en el diagrama de contexto son dos, inicio de proceso, aprobación y rechazo:

| **#** | **Interoperabilidad** | **Desde** | **Hacia** | **Información** |
| --- | --- | --- | --- | --- |
| 1 | Notificación inicio de proceso | Proceso de exportación | Proceso de importación | Formulario único de comercio exterior documentación requerida. |
| 2 | Notificación aprobación de ingreso y distribución | Proceso Ingreso y revisión zona primaria | Proceso exportación | Identificador del formulario único con fecha, hora y folio de autorización. |
|  | Notificación rechazo | Proceso Ingreso y revisión zona primaria | Proceso exportación | Identificador del formulario único con fecha, hora, folio de rechazo y listado de observaciones. |

Tabla 1, Descripción de interacciones de la Red VUCE

El segundo punto de notificación se divide en dos tipos de respuesta, la aprobación del proceso de exportación, según la información enviada y el rechazo con sus respectivas observaciones.

## Interacción Punto a Punto

La interacción en entre los países miembros de la red VUCE, se implementara en un sistema punto a punto. Esto implica que cada país deberá establecer un canal de comunicación con los países de la red o con el país que deba iniciar un proceso de comercio exterior.

Para estandarizar la forma en que los países se comunican, se propone la utilización de mecanismos y protocolos estándar, para que el proceso de integración sea fluido y amigable.

## Modelo de Interoperabilidad VUCE

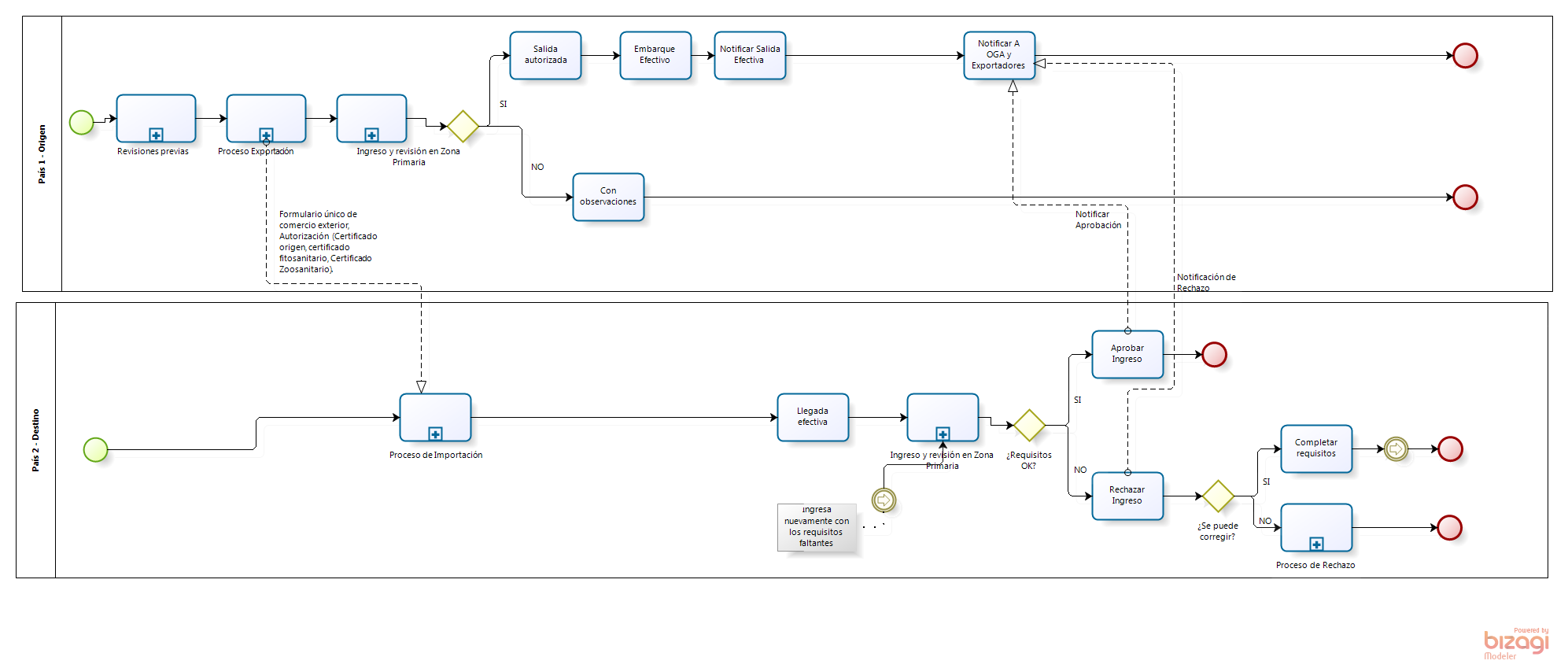


Ilustración 1, Modelo de Interoperabilidad VUCE

Los puntos de interacción mencionados en el diagrama de contexto son dos, inicio de proceso, aprobación y rechazo:

| **#** | **Interoperabilidad** | **Desde** | **Hacia** | **Información** |
| --- | --- | --- | --- | --- |
| 1 | Notificación inicio de proceso | Proceso de exportación | Proceso de importación | Formulario único de comercio exterior documentación requerida. |
| 2 | Notificación aprobación de ingreso y distribución | Proceso Ingreso y revisión zona primaria | Proceso exportación | Identificador del formulario único con fecha, hora y folio de autorización. |
|  | Notificación rechazo | Proceso Ingreso y revisión zona primaria | Proceso exportación | Identificador del formulario único con fecha, hora, folio de rechazo y listado de observaciones. |

Tabla 1, Descripción de interacciones de la Red VUCE

El segundo punto de notificación se divide en dos tipos de respuesta, la aprobación del proceso de exportación, según la información enviada y el rechazo con sus respectivas observaciones.

## Diagrama de Contexto Red VUCE

En el siguiente diagrama se presenta el modelo de contexto de las interacciones de los países de origen y destino de la Red VUCE.

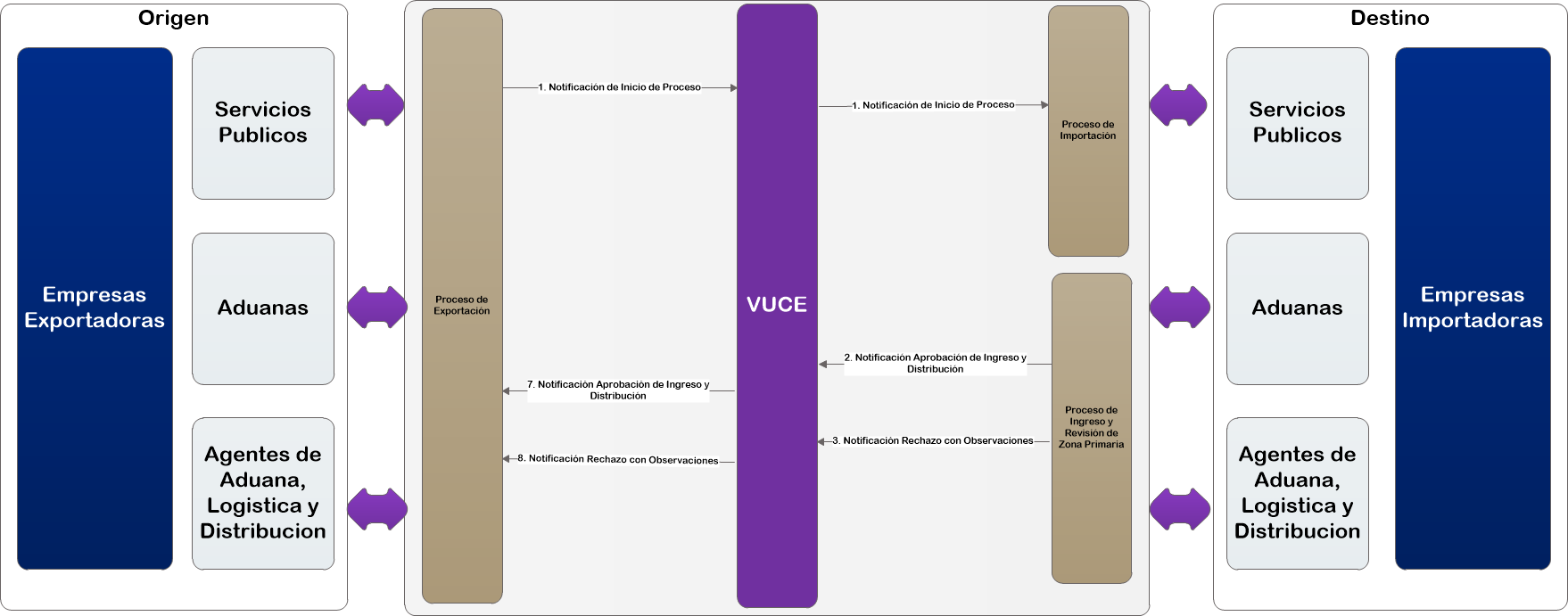


Ilustración 2, Diagrama de Contexto Red VUCE

# Marco Teórico

La definición de protocolos de comunicación se elabora en base a la propuesta y recomendaciones para la interoperabilidad de la red VUCE y las mejores prácticas disponibles en el mercado tecnológico.

Una premisa importante para definir los protocolos y una arquitectura Orientada a Servicios, es seguir un estándar que sea transversal a los proveedores de lenguajes o tecnologías que permitan lograr el objetivo, que es contar con una plataforma de interoperabilidad para la der VUCE.

No obstante, los estándares propuestos han sido creados por proveedores de tecnología de clase mundial, para resolver las necesidades en esta materia tecnológica. Estos han sido adoptados por organismos que se encargan que estas definiciones sean estándares transversales para todos los proveedores.

Para la definición de los protocolos se proponen los siguientes estándares que dan cabida a una arquitectura SOA.

* BPEL
* UDDI
* WSDL
* SOAP
* XML
* HTTP
* WS-Security

A continuación se presenta una ilustración de interacción de componentes y estándares que componen la arquitectura SOA.

En este capítulo solo revisaremos los estándares referentes a los protocolos de comunicación.

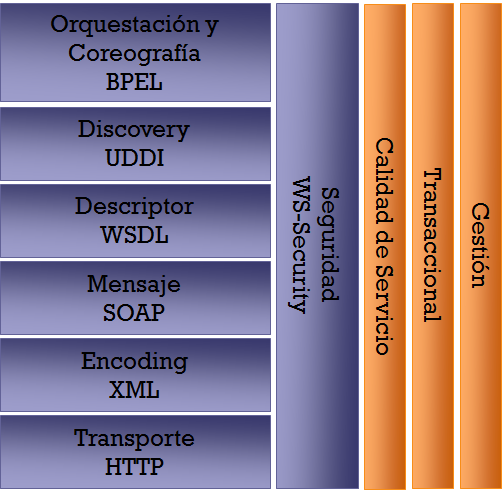


Ilustración 3, Estándares de Servicios Web

En la siguiente tabla se describen los estándares propuestos.

| **Nombre** | **Descripción** |
| --- | --- |
| Orquestación y Coreografía  **BPEL** | La orquestación y coreografía de servicios se propone realizarla mediante el Lenguaje BPEL (Business Process Execution Lenguege). BPEL, permite la interacción de varios servicios, mediante un solo servicios de entrada. |
| Discovery  **UDDI** | UDDI (Universal Description Discovery and Integration), es un contenedor del catálogo de servicios empresarial y es el encargado de llevar el registro de la vida de un servicio. |
| Descriptor  **WSDL** | WSDL (Web Services Description Language), es el estándar que describe un servicio web. Por ejemplo, donde está publicado, y sus parámetros de entrada y salida. |
| Mensaje  **SOAP** | SOAP (Simple Object Access Protocol), es el protocolo estándar que define los mensajes de los Servicios Web |
| Encoding  **XML** | XML (eXtensible Markup Language), es un lenguaje estándar interpretado por diversas tecnologías y base de otros estándares como WSDL, SOAP, UDDI, entre otros. |
| Transporte  **HTTP** | HTTP (Hypertext Transfer Protocol), es el lenguaje estándar para el transporte de la información entre los distintos puntos de interoperabilidad, no obstante en el presente documento se propone su utilización de manera segura HTTPS. |
| Seguridad  **WS-Security** | WS-Security, protocolo estándar define la seguridad a nivel de servicios, resguardando la integridad y seguridad en mensajería que viaja en los servicios web. |

Tabla 2, Descripción de Estándares de Servicios Web

## SOAP

Es el protocolo estándar que define los mensajes que viajan en los servicios WEB. Este protocolo regula la manera en que se comunicar los servicios de manera estructurada.

A este protocolo se incorporan mecanismos para proteger la integridad y confidencialidad en los mensajes mediante el uso de WS-Security, que utiliza SAML, Kerberos, tokens o los certificados X.509, encriptación y firmas XML.

Un mensaje SOAP se compone de dos estructuras principales, el encabezado y el cuerpo, como se muestra en la siguiente figura.

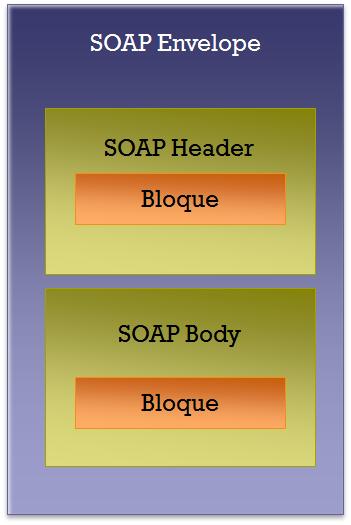


Ilustración 4, Estructura del Protocolo SOAP

En la siguiente tabla se describen las estructuras del estándar SOAP.

| **Nombre** | **Descripción** |
| --- | --- |
| Envelope | Es el elemento raíz del mensaje o sobre que contiene la definición de todo el mensaje del servicio. |
| Header | El encabezado del mensaje contiene información específica del contenido del mensaje. Por ejemplo información de enrutador, seguridad, etc. |
| Body | El cuerpo contiene la información más relevante del mensaje, es decir es información que se utiliza para el procesamiento del negocio del mensaje. |
| Bloque | En el mensaje puede estar agrupado por bloques dentro de la cabecera o cuerpo del mensaje. Estos bloques son representados por esquemas que detallan y especifican el mensaje.  Para escribir y definir el mensaje existen estilos y tipos de codificación, que describen un mensaje en el protocolo SOAP. |

Tabla 3, Descripción de estructura SOAP

### Esquemas, estilo y codificación (Encoding, XML)

Los esquemas son la definición de los parámetros de entrada y salida de los servicios, éstos en la estructura SOAP, está representada por los Bloques.

El mensaje SOAP, se puede escribir utilizando dos estilos de programación.

#### Estilo RPC/literal

Este estilo se basa en usar mensajes SOAP para crear llamadas a procedimientos remotos (Remote Procedure Calls).

Esta alternativa indica que el mensaje tiene los datos como contenido del cuerpo SOAP, e incluye la información relativa al procedimiento o función a la que ésta pertenece en el ruteo del mensaje por parte del servidor de aplicaciones.

|  |
| --- |
| **Ejemplo RPC/literal** |
| <env:Envelope xmlns:env="http://www.w3.org/2003/05/SOAP-envelope">  <env:Header/>  <env:Body>  <cex:notificacion xmlns:cex="http://www.comercioexterior.cl/cex ">  <cex:categoria>EXPORTACION</ cex:categoria>  < cex:subcategoria>ADUANA</ cex:subcategoria>  < cex:estado>APROBADO</ cex:estado>  < cex:observacion></cex:observacion>  </ cex:notificacion>  </env:Body>  </env:Envelope> |

#### Estilo RPC/encoded

El estilo RPC/encoded, a diferencia de RPC/literal, el mensaje incluye información de tipo de dato que debe contener los atributos del mensaje.

|  |
| --- |
| **Ejemplo RPC/encoded** |
| <env:Envelope xmlns:env="http://www.w3.org/2003/05/SOAP-envelope">  <env:Header>  </env:Header>  <env:Body>  <cex:notificacion xmlns:cex="http://www.comercioexterior.cl/cex">  <cex:categoria xsi:type="xsd:string">EXPORTACION</cex:categoria>  <cex:subcategoria xsi:type="xsd:string">ADUANA</ cex:subcategoria>  <cex:estado xsi:type="xsd:string">APROBADO</cex:estado>  <cex:observacion xsi:type="xsd:string"></cex:observacion>  </cex:notificacion>  </env:Body>  </env:Envelope> |

#### Estilo Document/literal

Éste estilo implica únicamente la incorporación de los datos apropiados en el mensaje, no definiendo el procedimiento a realizar como es el caso de RPC.

|  |
| --- |
| **Ejemplo Document/literal** |
| <env:Envelope xmlns:env="http://www.w3.org/2003/05/SOAP-envelope">  <env:Header>  </env:Header>  <env:Body>  <categoria>EXPORTACION</categoria>  <subcategoria>ADUANA</subcategoria>  <estado>APROBADO</estado>  <observacion></observacion>  </env:Body>  </env:Envelope> |

Como se mencionó, el mensaje no incluye información acerca del proceso del destino o el destino que se deben enviar los datos, sino es el software el encargado de direccionar la información.

### Archivos o datos binarios (XOP)

XOP es un protocolo proporciona una formar de referenciar de manera fiable los datos externos desde un documento XML, mediante el suministro de un mecanismo por el cual se puede extraer selectivamente la información mediante un mensaje MIME (Multipurpose Internet Mail Extensions) que también es incluido en el mensaje SOAP, y hace una referencia directa a al documento.

|  |
| --- |
| **Ejemplo XOP** |
| MIME-Version: 1.0  Content-Type: Multipart/Related;boundary=MIME\_boundary;  type="application/xop+xml";  start="<soapmsg.xml@daily-moon.com>";  start-info="text/xml"  Content-Description: An XML document with binary data in it    --MIME\_boundary  Content-Type: application/xop+xml;  charset=UTF-8;  type="text/xml"  Content-Transfer-Encoding: 8bit  Content-ID: <soapmsg.xml@comercioexterios.ccl>    <env:Envelope xmlns:env="http://www.w3.org/2003/05/SOAP-envelope">  <env:Header>  </env:Header>  <env:Body>  <cex:notificacion xmlns:cms="http://www.comercioexterior.com/cex">  <cex:categoria>EXPORTACION</categoria>  <cex:subcategoria>ADUANA</cex:subcategoria>  <cex:estado>REQUEST<cex:estado>  <cex:certificado><xop:Include  xmlns:xop='http://www.w3.org/2004/08/xop/include'  href='cid:http://comercioexterior.cl/certificadozoosanitario.pdf'  /></cex:certificado>  </cex:notificacion>  </env:Body>  </env:Envelope>    --MIME\_boundary  Content-Type: application/vnd.openoffice  Content-Transfer-Encoding: binary  Content-ID: <http:// comercioexterior.cl/certificadozoosanitario.pdf >    // binary octets for the word processing file    --MIME\_boundary-- |

## Seguridad

La seguridad entre un emisor y un receptor es de suma importancia para garantizar que el mensaje enviado no sea distorsionado en el camino o simplemente evitar que sea leído por quien no corresponda. Por esta razón hay dos formas de asegurar la comunicación, la primera es asegurar el canal de y la segunda es asegurar el mensaje.

### Túnel Seguro

El aseguramiento del canal de comunicación, indica que toda la información trasmitida viaja cifrada por un túnel virtual, donde el emisor y el receptor tienen la clave para poder leer la información trasmitida.

SSL VPN es la aplicación del protocolo de protección Transport Layer Security (TLS), conocido generalmente como SSL, en una red que utiliza infraestructura pública de telecomunicaciones, como Internet, para proporcionar a las oficinas remotas o usuarios individuales acceso seguro a las redes de las organizaciones. Y en este caso de los miembros de la red VUCE.

En términos sencillos, una red privada virtual (VPN) proporciona un mecanismo de comunicación de datos entre dos extremos.

Un servidor SSL VPN funciona mediante la creación de un canal virtual a través de Internet público utilizando el cifrado simétrico. Ambos lados del canal tienen las llaves que se utilizan para cifrar y descifrar el tráfico.

### (WS-Security)

El protocolo WS-Security (WSS) es una extensión del protocolo SOAP que define mecanismos para proteger la integridad y confidencialidad en los mensajes mediante estándares como: SAML, Kerberos, tokens o los certificados X.509, encriptación y las firmas XML.

WS-Security define como utilizar mecanismos existentes para proporcionar autenticación, confidencialidad e integridad a los Web Service, incorporando los anteriores estándares en el mensaje de tipo SOAP de modo que se pueda aplicar seguridad a una parte del mensaje o a su totalidad, separando de esta definición a los protocolos de transporte.

En la cabecera del mensaje SOAP se almacena la información de seguridad de tal modo que si se implementa una firma digital, en este segmento incluirá la información asociada a la firma.

En la siguiente figura se muestra como es el flujo de mensajes utilizando este protocolo de seguridad.

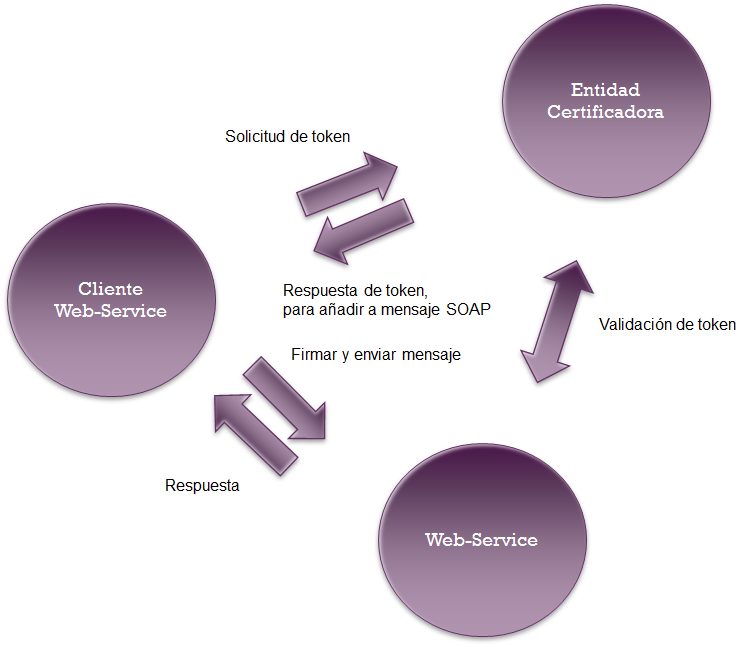


Ilustración 4, Flujo de interacción WS-Security.

La entidad certificadora es el servicio de validación que autoriza las credenciales user/password. Éste procedimiento consiste en un cliente que solicita los tokens necesarios para dar seguridad a la transmisión, añadiendo a éste al mensaje para luego enviarlo al servidor. A su vez el servidor es capaz de validar la integridad, confidencialidad y no repudio del mensaje.

#### Autenticación

Token: se utiliza un usuario junto con una contraseña para validar al cliente. En este caso, el cliente debe firmar el mensaje y el servidor puede comprobar la veracidad, calculando la firma del mensaje recibido y comparándola con el valor recibido.

En el caso de utilizar certificados X.509, el mensaje puede ser firmado utilizando una clave privada. Entonces, el mensaje debe contener el certificado en un BinarySecurityToken. Es recomendable firmar también el certificado con la clave privada.

#### Encriptación

Como se ha mencionado WS-Security no define nuevos estándares para la encriptación, por esta razón se puede usar criptografía de clave pública o privada, simétrica o asimétrica. Usualmente la encriptación se realiza a través del XML Encription, que permite cifrar tanto partes de un documento como su totalidad.

#### Firma

Para firmar documentos se pueden utilizar los métodos de autenticación mencionados. Sin embargo, también se ofrece la posibilidad de aplicar la XML Signature, la cual define la sintaxis adecuada para las firmas digitales que se pueden implementar.

# Estándares y Protocolos de Comunicación a utilizar en la RED VUCE

En el presente apartado se definirá los protocolos a utilizar para establecer la comunicación punto a punto por los países miembros de la red VUCE en el proceso de comercio exterior.

En el apartado Marco Teórico se muestran los protocolos y mecanismos estándares de comunicación y seguridad, que se deben utilizar para establecer un canal efectivo entre los miembros de la red.

Los protocolos y estándares considerados son los siguientes:

|  |  |
| --- | --- |
| Mensaje | SOAP 1.2 |
|  | RPC/literal |
|  | XOP – Envió de Archivos |
| Seguridad | WS-Security |
|  | SSL |
|  | Certificados (X.509-RSA). |

A continuación se definen los servicios y el flujo de para establecer la comunicación entre ambos extremos.

## Servicios

De la definición del proceso de la red VUCE, se identifican dos servicios síncronos:

**Notificación de Inicio de Proceso de Exportación**, este servicio recibe el formulario único de comercio exterior documentación requerida, enviada desde el país de origen.

**Notificación de Respuesta al Proceso de Exportación**, servicio para recibir la respuesta del proceso de importación del país de destino. Esta respuesta puede ser una aprobación o un rechazo.

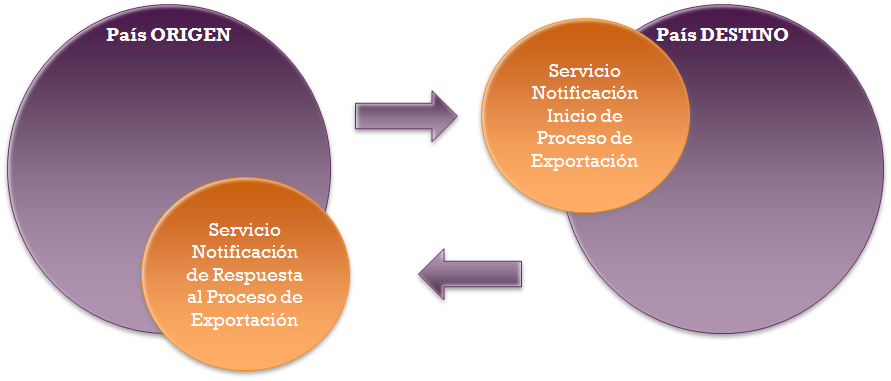


Ilustración 4, Servicios del Notificación del Proceso de Exportación.

Todos los países miembros de la red VUCE deben implementar los dos servicios definidos en el proceso de comercio exterior. El país de destino deberá proporcionar el servicio de inicio de proceso y el país de origen el que recibe la respuesta.

## Flujo de Interoperación

El flujo de interoperación comienza cuando un país de origen inicia el proceso de importación enviando al país de destino la notificación de inicio..

El segundo paso es cuando el país de destino notifica el resultado del proceso de revisión de las mercancías recibidas, según la documentación enviada por el país de origen. Éste resultado puede ser una aprobación al proceso de exportación e importación enviando los parámetros de aprobación, o el rechazo junto con los motivos de éste. Una vez notificado el país de origen puede volver a enviar el formulario con la información requerida o faltante según los motivos del rechazo.

En caso de que el proceso finalice en un rechazo, el proceso debe volver a iniciar, enviando la información requerida inicialmente y con las observaciones informadas.

A continuación se describen los dos servicios que representan a los puntos de notificación definidos.

### Notificar Inicio del Proceso de Exportación

Para dar inicio al proceso se debe enviar una notificación que contendrá los siguientes datos de entrada:

**Datos de Entrada**

1. Formulario único de comercio exterior, este formulario contendrá la información indispensable para que el proceso se lleve a cabo. El cual debe incluir la identificación de la transacción del proceso de comercio exterior, teniendo en cuenta lo siguiente:

* Nombre de Campo: Código único de transacción de un proceso de comercio exterior.
* Tipo de campo: Alfanumérico, 14 dígitos.
* Code Remarks: 2 dígitos por código de país (ISO 3166), 6 dígitos para la fecha (UNTDID 2379 = 2 DDMMYY), Secuencial de 6 dígitos (se debe rellenar con ceros a la derecha).  Las comas es solo para separar, no son parte del código.

Ejemplo1: CO191113000001

Ejemplo2: CO191113000002

1. Documentos de acompañamiento al proceso (Certificados), esta documentación será trasmitida como metadata y la referencia del documento físico en formato binario.

**Datos de Salida**

1. Confirmación de la recepción del mensaje.
2. Mensaje de error, para aplicar reintentos.

Este servicio deberá ser sincrónico, enviando el acuse de recibo hacia el cliente quien lo invoca (País de origen), con el fin de notificar de manera oportuna si hubo algún error en el mensaje, o en su recepción para que puede reintentar su envío o incorporar mejoras. Esto es de suma importancia para almacenar un log el resultado a las llamadas al servicio.

### Notificar de Respuesta al Proceso de Exportación

Como resultado del proceso de revisión de los antecedentes y las mercancías recibidas por el país de origen, se finaliza el ciclo o proceso enviando la notificación de respuesta con el fin de informar en el estado que ha terminado.

Para este servicio a dos tipos de mensaje:

1. El mensaje de aprobación, que enviara el estado del término del proceso, con información relevante para que se pueda dar termino a dicho proceso por el país de origen.
2. El mensaje de rechazo, que enviara el estado del término del proceso y las observaciones o motivos del rechazo para que puedan ser subsanados por el país de origen. Además de una fecha límite para subsanar las observaciones.

**Datos de Entrada**

1. Respuesta del término del proceso e información relevante para el cierre de este en el país de origen. O respuesta de rechazo y observaciones o motivos para poder ser subsanados por el país de origen. Además de la fecha límite para el reenvió de la información.

**Datos de Salida**

1. Confirmación de la recepción del mensaje.
2. Mensaje de error, para aplicar reintentos.

Este servicio deberá ser sincrónico, enviando el acuse de recibo hacia el cliente quien lo invoca (País de destino), con el fin de notificar de manera oportuna si hubo algún error en el mensaje, o en su recepción para que puede reintentar su envío o incorporar mejoras. Esto es de suma importancia para almacenar un log el resultado a las llamadas al servicio.

## Log de servicios

Es recomendable que en ambos extremos (servidor y cliente) se almacene el log con el resultado del procesamiento de las notificaciones, para detectar de manera oportuna errores que puedan interrumpir el correcto flujo del proceso definido.

## Flujo de Interacción de los Servicios

Para iniciar la comunicación entre ambos puntos de la red, el país de origen y destino deben realizar los siguientes pasos:

**Origen y Destino**

1. Se debe autenticar con el sistema del país destino.
2. Aseguramiento del canal, el canal de comunicación debe estar asegurado, debe ser establecerse un canal SSL, entre el origen y destino.

**Origen**

1. Creación del mensaje
2. Se debe anexar la clave pública del certificado.
3. Enviar el mensaje al receptor.

**Destino**

1. Se recibe el mensaje.
2. Se valida, la autenticidad, comprobando con el certificado.
3. Se procesa el mensaje.
4. Se prepara la respuesta.
5. Se debe autenticar con el sistema del país origen.
6. Aseguramiento del canal, el canal de comunicación debe estar asegurado, debe ser establecerse un canal SSL, entre el origen y destino.
7. Se anexa clave pública.
8. Se envía la respuesta.

**Origen**

1. Se recibe la respuesta
2. Se valida la clave pública de la respuesta.
3. Se procesa la respuesta.

## Manejo de errores

Se debe implementar una codificación de los errores de los servicios con el fin de informar, de manera correcta una anomalía en el proceso. Con esta información el cliente puede tomar las medidas evolutivas y correctivas.

Una vez terminado el proceso de armonización de datos se debe codificar los errores posibles, para establecer una lista de errores conocidos con los que se pueda tomar decisiones, en el proceso de comercio exterior.

El mensaje de respuesta debe entregar una lista de errores, por ejemplo:

|  |
| --- |
| **Ejemplo Errores** |
| <Respuesta>  <estado>ERROR</estado> (APROBADO, RECHAZADO, ERROR)  <errores>  <error>  <código>00111</código>  <descripción>El formulario de comercio…</descripción>  </error>  <error>  <código>00112</código>  <descripción>El certificado…</descripción>  </error>  …  </errores>  </Respuesta> |

# Pasos para integración a la red VUCE

Para facilitar y generar una comunicación robusta se recomienda el uso de un Service Bus.

Para que un país pueda subirse a la red debe realizar los siguientes pasos, se categorizan en cuatro:

1. Intercambiar certificados (X.509-RSA).
2. Publicar e intercambiar web service de autenticación (SSL), WS de inicio de un proceso de comercio exterior, como también El WS para la notificación de aceptación o rechazo. Para este caso se recomienda utilizar un service bus, considerando crear los proxy y bussines correspondientes para publicar o consumir web service.
   * Construir los proxy para publicar los Web service de su propiedad. Es recomendable establecer un dominio y no publicar los WS directamente con IP.
   * Construir los clientes de cada Web service a consumir de los demás países de la red. Puede priorizar por los países con los que hoy día tiene intercambio comercial.
3. Análisis funcional de esquemas y armonización de datos.
4. Implementación de Servicios
5. Implementación de Clientes
6. Pruebas.

## Análisis funcional de esquemas y armonización de datos.

Del proceso de armonización de datos entre países de la red, se analizan y defines los datos que se deben trasmitir entre los países, para los dos servicios definidos.

Para el proceso de análisis se debe realizar lo siguiente:

1. Analizar los datos definidos por el proceso de armonización.
2. Homologar la información armonizada de la red VUCE, con la información que cuenta el país que se incorpora a la Red.
3. Analizar y revisar los contratos de los servicios definidos en el proceso de armonización, donde se defines los tipos de datos y estrategia tecnológica para su implementación.

Una vez terminado los procesos anteriores se puede proceder a implementar los servicios.

## Implementación de Servicios

Una vez analizado y homologados los datos con los definidos por el proceso de armonización, se debe proceder a implementar los servicios, siguiendo los siguientes pasos.

1. Crear las interfaces de los servicios (Web Servicie), según la definición de las firmas de los contratos definidos.
2. Intercambiar certificados (X.509-RSA).
3. Intercambiar user y password para poder establecer la autenticación y levantar el canal seguro.
4. Crear el usuario y asignar la clave del sistema en cada service bus.
5. Implementar lógica de procesamiento del mensaje.
6. Implementar la lógica para añadir la clave pública de su certificado.
7. Implementar lógica de armado de respuesta.
8. Implementar lógica de manejo de errores.
9. Construir los Web service de su propiedad. Es recomendable establecer un dominio y no publicar los WS directamente con IP.
10. Publicar los Web service como Proxy en el service bus.

## Implementación de Clientes

Para implementar el cliente se debe analizar los siguientes pasos:

1. Crear las interfaces para el cliente Web Service, según la definición del servicio expuesto en el país de destino. El contrato del servicio no debe ser distinto para cada país. El objetivo es poder reutilizar este cliente independiente a la plataforma tecnológica usada por el origen.
2. Publicar el cliente en el service bus como business.
3. Implementar la lógica para validar la clave pública enviada en el mensaje vs la contenida en el certificado.
4. Implementar lógica para construir el mensaje de respuesta.

## Pruebas.

El proceso de integración debe pasar por un periodo de pruebas con el fin de certificar que la integración se ha realizado de manera satisfactoria. Para esto se recomienda lo siguiente:

* + - Construir test de los Web service publicados.
    - Construir test de los Web service a consumir.
    - Contar con una herramienta para probar Web Service. Además, de las pruebas de test que pueden realizarse directamente en el Service Bus.
    - Diseñar un plan de pruebas, considerando el flujo básico y los flujos alternativos (catálogo de errores).
    - Definir una herramienta y contratar un servicio para publicar las incidencias reportadas de cada país en base al consumo de servicios.
    - Definir un SLA de tiempo de respuesta por cada servicio.

# Referencias

El presente documento se ha realizado basado en las siguientes referencias.

1. Comprender las especificaciones de los servicios web, Parte 1, 2, 3, 4, 5, <http://www.ibm.com/developerworks/ssa/webservices/tutorials/ws-understand-web-services1/index.html>
2. W3C – Recursos de Seguridad, <http://www.w3.org/Security/>

<http://www.w3c.es/Divulgacion/GuiasBreves/Seguridad>

<http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/Overview>

<http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/Overview>

1. Networking and Internet Technologies – WS-Security, <http://blogs.salleurl.edu/networking-and-internet-technologies/ws-security-wss/>
2. Web Services Security Specifications, <http://msdn.microsoft.com/en-us/library/ms951273.aspx>
3. SOA Security, Ramarao Kenneganti,- 2008
4. W3C – SOAP, <http://www.w3.org/TR/soap/>