

# Gestión de Órdenes de Transferencia de Recursos

GOTE

Documento de Especificaciones Técnicas del Servicio Web

VERSION 1.3

## Tabla de Contenido

1.	Introducción .....	3
a)	Propósito .....	3
b)	Ámbito.....	3
2.	Generalidades .....	3
a)	Glosario .....	3
b)	Suposiciones.....	3
3.	Definición del Servicio.....	4
a)	Atributos XML .....	4
ORDENES DE TRANSFERENCIA .....	4	
CUENTA CRÉDITO .....	4	
FORMATO MENSAJE .....	4	
b)	Definición de Formatos.....	6
FECHAS .....	6	
FECHAS/HORAS .....	6	
NUMÉRICOS CON DECIMALES .....	6	
CÓDIGOS DE BANCOS DESTINO .....	7	
4.	Servicio Web .....	8
a)	Servicio Firma de Ordenes de Transferencia .....	8
b)	Métodos Necesarios .....	8
SOLICITUD NUEVA ORDEN DE TRANSFERENCIA {newTransact}.....	8	
CONSULTA DE ESTADO ORDEN DE TRANSFERENCIA {transactStatus} .....	9	
SOLICITUD CÓDIGOS DE BANCO {bankList} .....	10	
5.	Códigos de Retorno.....	11
6.	Entornos de Ejecución.....	12
a)	Servidor de Pruebas .....	12
b)	Servidor de Producción .....	12
c)	Encriptación .....	12
ENCRIPCIÓN SIMÉTRICA: .....	12	
CIFRADO DE LA CLAVE SECRETA ASIMÉTRICA.....	12	
LLAMADA AL SERVICIO:.....	12	
FLUJO:.....	12	
d)	Firma .....	12

## Revisiones

FECHA	VERSIÓN	DESCRIPCIÓN	AUTOR
23/01/2017	1.0	Creación del documento	Dalia Ramírez
05/05/2017	1.1	Actualización del ejemplo de xml	Dalia Ramírez
10/082017	1.2	Actualización de mensaje de respuesta (página 9)	Dalia Ramírez
26/09/2019	1.3	Actualización de Glosario ( <a href="https">https</a> ), y sección 6 protocolos de publicación de servicios.	Dalia Ramírez

## 1. Introducción

El presente documento tiene como objetivo describir el servicio web para la interconexión entre la Dirección Nacional de Aduanas y los Bancos Interconectados a ella en el marco del proyecto de Firma Digital de Ordenes de Transferencia de Recursos.

### a) Propósito

El proyecto denominado “Firma Digital de Ordenes de Transferencias de Recursos” tiene como principal objetivo substituir la gestión de las transferencias bancarias de la DNA a terceros que actualmente se realiza de forma manual mediante soporte físico papel, por transferencias bancarias electrónicas con servicios web con firma digital.

### b) Ámbito

Este documento que establece las especificaciones técnicas del servicio web para el desarrollo por parte de las entidades bancarias para la recepción de las órdenes de transferencia firmadas por la DNA digitalmente.

## 2. Generalidades

### a) Glosario

SIGLAS	DESCRIPCIÓN
SICA	Sistema Integrado de Contabilidad Aduanera
DNA	Dirección Nacional de Aduanas
WS	Web Service
Web Service	Servicio Web
Servicio Web	Tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones
VPN	Virtual Private Network
Virtual Private Network	Tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet
SOAP	Simple Object Access Protocol
Simple Object Access Protocol	Protocolo estándar que define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML
WSDL	Web Services Description Language
Web Services Description Language	Formato XML que se utiliza para describir servicios Web
https	Protocolo seguro de transferencia de hipertexto. Utiliza un cifrado basado en la seguridad de textos SSL/TLS para crear un canal cifrado

### b) Suposiciones

Conocimiento acabado de los estándares SSL y Web Services.

### 3. Definición del Servicio

#### a) Atributos XML

##### ORDENES DE TRANSFERENCIA

Las órdenes de transferencia incluirán toda la información necesaria para poder realizar la operación de transferencia bancaria entre cuentas de forma satisfactoria.

A continuación se detalla la estructura y definición de las órdenes de transferencia:

TAG	DESCRIPCIÓN	TIPO DATO	LONGITUD
idSofiaOrden	ID único transacción SOFIA	String	16
fechaLiquidacion	Fecha en la cual se realizará la transferencia bancaria	String	
cuentaDebito	Nº Cuenta de la DNA desde la que se realizará el débito	String	20
tipoDocEmisor	Tipo Documento del Emisor	String	
numDocEmisor	Número de Documento del Emisor	String	
cuentaCredito	Datos referentes a las cuentas destino de los Beneficiarios.	String	

##### CUENTA CRÉDITO

A continuación se describe el contenido del array para el TAG {cuentaCredito}:

TAG	DESCRIPCIÓN	TIPO DATO	LONGITUD
idItem	ID único del ítem de transferencia	Integer	4
idCuentaCredito	Nº Cuenta Crédito	string	20
nombreBenef	Nombre del Beneficiario	String	80
tipoDocBenef	Tipo Documento del Beneficiario	String	3
numDocBenef	Número de Documento del Beneficiario	String	16
impTrans	Importe de la Transacción	BigDecimal	
concepto	Texto de concepto de la transacción	String	80
bancoRecp	Código del Banco Receptor de la transacción	Integer	4

##### FORMATO MENSAJE

Las órdenes de transferencia estarán formateadas en formato XML y éste XML estará firmado digitalmente por los firmantes autorizados para la cuenta de débito.

Los datos deberán estar incluidos en un TAG Root denominado {gote}

Ejemplo estructura tipo XML:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<gote-firmado>
<gote>
  <idSofiaOrden>BQ030121/2016</idSofiaOrden>
  <fechaLiquidacion>20160621</fechaLiquidacion>
  <cuentaDebito>147000365</cuentaDebito>
  <tipoDocEmisor>RUC</tipoDocEmisor>
  <numDocEmisor>800015</numDocEmisor>
  <cuentaCredito>
    <item>
      <idItem>1</idItem>
      <idCuentaCredito>430</idCuentaCredito>
      <nombreBenef>Banco Central del Paraguay</nombreBenef>
    </item>
  </cuentaCredito>
</gote>
</gote-firmado>
```

```

        <tipoDocBenef>RUC</tipoDocBenef>
        <numDocBenef>80044332-3</numDocBenef>
        <impTrans>295152878.000</impTrans>
        <concepto>Transferencia a BCP</concepto>
        <bancoRecp>1001</bancoRecp>
    </item>
    <item>
        <idItem>2</idItem>
        <idCuentaCredito>3789684000</idCuentaCredito>
        <nombreBenef>CENTRO DESPACHANTES DE ADUANA DEL</nombreBenef>
        <tipoDocBenef>RUC</tipoDocBenef>
        <numDocBenef>60023332-5</numDocBenef>
        <impTrans>63429.000</impTrans>
        <concepto>Transferencia a CDA</concepto>
        <bancoRecp>1020</bancoRecp>
    </item>
</cuentaCredito>
</gote>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://xxx/REC-xml-c14n-
20010315"/>
            <ds:SignatureMethod Algorithm="http://xxx/xmldsig#dsa-sha1"/>
            <ds:Reference URI="">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://xxx/xmldsig#enveloped-
signature"/>
                    <ds:Transform Algorithm="http://xxx/REC-xml-c14n-
20010315"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://xxx/xmldsig#sha1"/>
                <ds:DigestValue>5mfi7ac9VeIzSzoOONqNMCaWt8k=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>YeL8n8vssSd...ICaJ22GDAGA==</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyValue>
                <ds:DSAKeyValue>
                    <ds:P>X9T...Acc=</ds:P>
                    <ds:Q>l2BQjxU...C/BYHPU=</ds:Q>
                    <ds:G>9+...PSSo=</ds:G>
                    <ds:Y>KjHl...9Q=</ds:Y>
                </ds:DSAKeyValue>
            </ds:KeyValue>
            <ds:X509Data>
                <ds:X509Certificate>MIIEHgAwIBAg...YHEHYW</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
</gote-firmado>

```

## b) Definición de Formatos

A continuación se detallan los formatos de normalización para los datos sensibles:

### FECHAS

Para la normalización de los datos que contengan fechas, se describe la siguiente composición:

- **Formato: YYYYMMDD:**
  - 4 dígitos para el Año
  - 2 dígitos para el Mes
  - 2 dígitos para el Día

### FECHAS/HORAS

Para la normalización de los datos que contengan fechas y horas, se describe la siguiente composición:

- **Formato: YYYYMMDDHHMMSS:**
  - 4 dígitos para el Año
  - 2 dígitos para el Mes
  - 2 dígitos para el Día
  - 2 dígitos para las Horas
  - 2 dígitos para los Minutos
  - 2 dígitos para los Segundos

### NUMÉRICOS CON DECIMALES

Para la normalización de los datos que contengan numéricos con decimales, se describe la siguiente composición:

- **Formato: DDDDDDDDD.DDD:**
  - Precisión: 3 decimales
  - Separador Miles y Millones: Sin carácter separador
  - Separador Decimales: Un punto (.)

## CÓDIGOS DE BANCOS DESTINO

A continuación se detalla la lista de los códigos y nombre de los bancos destino posibles:

Código	Nombre o Descripción
1001	BANCO CENTRAL DEL PARAGUAY
1002	BANCO NACIONAL DE FOMENTO
1003	BANCO NACION ARGENTINA
1004	BANCO GNB
1005	BANCO DO BRASIL
1006	CITIBANK N.A.
1007	BBVA BANCO S.A.
1008	BANCO SUDAMERIS PARAGUAY S.A.
1017	ITAU S.A.
1020	BANCO CONTINENTAL S.A.
1028	BANCO REGIONAL S.A.I.F.
1030	BANCO AMAMBAY S.A.
1033	BANCO
1040	BANCO ITAPUA SAECA
1039	Banco Visión S.A.
1041	BANCO FAMILIAR
3520	BANCOS DEL EXTERIOR
1011	COMPRA CHEQUE EUROS
1042	BANCO ATLAS SAECA
1043	BANCOP S.A.
1044	INTERFISA BANCO



## 4. Servicio Web

La transmisión de las órdenes de transferencia se realizará mediante medios telemáticos a través de Internet. En la actualidad, la DNA y la entidad bancaria poseen una conexión entre ellos con túnel VPN. Dicha conexión será usada en este proyecto.

La tecnología elegida para el intercambio de datos es Web Service o Servicio Web.

El protocolo de comunicación WS será SOAP.

### a) Servicio Firma de Ordenes de Transferencia

A continuación se detalla y describe el servicio web a desarrollar por la entidad bancaria para la gestión de órdenes de transferencia.

### b) Métodos Necesarios

El servicio web GOTE deberá poseer tres métodos de acceso:

- **newTransact** → Solicitud de registro de nueva orden de transferencia
- **transactStatus** → Solicitud consulta de estado de una orden de transferencia ya solicitada
- **bankList** → Solicitud listado de bancos

### SOLICITUD NUEVA ORDEN DE TRANSFERENCIA {newTransact}

Mediante este método del servicio GoteWS, la DNA podrá registrar una nueva solicitud de orden de transferencia electrónica.

#### Parámetros de entrada:

Nombre	Tipo Dato	Descripción
<b>transactXML</b>	String	Contendrá la orden de transferencia formateada en XML, codificada en BASE64 y cifrada con algoritmo RSA y con el certificado que el Banco suministrará.

#### Retorno:

Nombre	Tipo Dato	Descripción
responseGote	String	Contendrá la información de retorno de la solicitud en formato JSON con estándar RF4627

La composición de la información contenida en “responseGote” en formato JSON RF4627 es la siguiente:

Nombre	Tipo Dato	Descripción
<b>transactId</b>	Void	
<b>responseCode</b>	Integer	Identificador del Retorno
<b>responseDescription</b>	String	Texto Descriptivo del Retorno

## CONSULTA DE ESTADO ORDEN DE TRANSFERENCIA {transactStatus}

Este método habilitará a la DNA a realizar una consulta de estado sobre una Orden de Transferencia ya registrada con anterioridad.

### **Parámetros de entrada:**

Nombre	Tipo Dato	Descripción
transactId	String	Contendrá el ID único transacción SOFIA

### **Retorno:**

Nombre	Tipo Dato	Descripción
responseGote	String	Contendrá la información de retorno de la solicitud en formato JSON con estándar RF4627

La composición de la información contenida en “**responseGote**” en formato JSON RF4627 es la siguiente:

Nombre	Tipo Dato	Descripción
transactId	String	ID único transacción SOFIA Solicitado
responseCode	Integer	Código de respuesta General
responseDescription	String	Descripción de respuesta General
items	Array	Array de Items del transactId

La composición del array de “**items**” es la siguiente:

Nombre	Tipo Dato	Descripción
itemId	Integer	ID único del Item de transferencia Solicitado
responseCode	Integer	Identificador del Retorno
responseDescription	String	Texto Descriptivo del Retorno

### **Ejemplo:**

```
{ "transactId": "BQ02130/2016", "items": [ { "itemId": 1, "responseCode": 50, "responseDescription": "La Orden de Transferencia está pendiente de procesamiento" }, { "itemId": 2, "responseCode": 50, "responseDescription": "La Orden de Transferencia está pendiente de procesamiento" } ] }
```

Jerárquicamente, quedaría así:

```
{
  "transactId": "BQ02130/2016",
  "items": [
    {
      "itemId": 1,
      "responseCode": 50,
      "responseDescription": "La Orden de Transferencia está pendiente de procesamiento"
    },
    {
      "itemId": 1,
      "responseCode": 50,
      "responseDescription": "La Orden de Transferencia está pendiente de procesamiento"
    }
  ]
}
```

## SOLICITUD CÓDIGOS DE BANCO {bankList}

Mediante este método del servicio GoteWS, la DNA podrá obtener una lista de todos los bancos existentes con sus códigos registrados en el Banco.

### **Parámetros de entrada:**

*No se esperan parámetros de entrada*

### **Retorno:**

Nombre	Tipo Dato	Descripción
responseGote	String	Contendrá la información de retorno de la solicitud en formato JSON con estándar RF4627

La composición de la información contenida en "responseGote" en formato JSON RF4627 es la siguiente:

Nombre	Tipo Dato	Descripción
Codigobanco	String	Código del Banco
Descripcion	String	Descripción

### **Ejemplo:**

```
{"responseGote":[{"Codigobanco":"2112","Descripcion":"Banco Amambay"}, {"Codigobanco":"2113","Descripcion":"Banco Atlas"},...]}
```

Jerárquicamente quedaría así:

```
{
  "responseGote": [
    {
      "Codigobanco": "2112",
      "Descripcion": "Banco Amambay"
    },
    {
      "Codigobanco": "2113",
      "Descripcion": "Banco Atlas"
    },
    . . .
  ]
}
```

## 5. Códigos de Retorno

A continuación se detallan los códigos y descripciones de los posibles retornos sobre los métodos implementados en el servicio web GoteWS:

Código	Descripción
0	Orden de Transferencia completada correctamente
1	Petición registrada correctamente y pendiente de procesamiento
2	Faltan parámetros o son incorrectos
3	Error registrando transacción. Intentelo más tarde
4	Orden de Transferencia ya registrada previamente
5	transactId inexistente
6	Error de seguridad. No se ha podido descryptar la clave y/o el mensaje.
10	La cuenta origen es incorrecta
11	La cuenta destino es incorrecta
12	El código de banco destino es incorrecto
13	En Proceso
14	Pendiente de Verificar Firmas
15	Error en Firmantes
16	Transferencia Rechazada
17	Transferencia Realizada
18	Consulta realizada correctamente
19	Fecha de Operación de la cuenta es menor a la Apertura
20	La operación no puede realizarse , Existe un Bloqueo Total de la Cuenta
21	Cuenta Cancelada
22	La Cuenta Débito no pose Fondos Suficientes
23	Bloqueo al Crédito
24	Pendiente Activación de Cuenta
25	Bloqueo al Débito
26	Cuenta Crédito Pendiente de Envío
27	Cuenta Crédito Anulada
28	Cuenta Crédito Rechazada
29	Cuenta Crédito Enviada
30	El formato XML es incorrecto
31	El XML no está firmado
32	Alguna de las firmas del XML no son correctas
33	Error de integridad de los datos
34	La/s Autoridad de Certificación de algún/os firmante/s no es reconocida
35	Alguno/s certificado/s ha/n sido revocado/s
36	No se ha podido comprobar la revocación de algún/os certificado/s
50	La Orden de Transferencia está pendiente de procesamiento
51	No se ha podido procesar la transacción por falta de fondos en cuenta origen

Se han definido franjas numéricas para los retornos dependiendo de su ámbito:

- **Primera decena:** Retornos generales o de ámbito general
- **Del 10 al 29:** Retorno de validación en entorno bancario
- **Del 30-49:** Retorno para el ámbito de Firma Digital e Integridad de la información
- **Del 50-9999:** Retorno en el ámbito del procesamiento bancario de la solicitud

## 6. Entornos de Ejecución

El Banco debe preparar dos entornos de ejecución para el servicio web GOTE:

- Servidor de Pruebas
- Servidor de Producción

Tanto para el servidor de pruebas como el de producción las URLs deben estar publicadas bajo el protocolo HTTPS (Protocolo **SEGURO** de transferencia de hipertexto).

### a) Servidor de Pruebas

Con el objetivo de que la aduana pueda realizar la homologación del servicio web, la entidad deberá disponer de un ambiente de pruebas sin afectación real en los servicios productivos del banco ni de la DNA.

### b) Servidor de Producción

Una vez todas las partes del proyecto aprueben el correcto funcionamiento del mismo, el servicio web GoteWS será publicado en el entorno productivo. La dirección de acceso y consumo del servicio, será publicado en el momento correspondiente al inicio del servicio.

Como se ha anotado en el punto anterior, el servidor de producción no publicará la definición del servicio web (WSDL) por motivos de seguridad.

### c) Encriptación

#### ENCRIPCIÓN SIMÉTRICA:

El XML será cifrado simétricamente con el siguiente algoritmo:

- AES / ECB / PKCS5Padding

Para cifrar simétricamente se debe de incorporar una frase o clave secreta de encriptación.

#### CIFRADO DE LA CLAVE SECRETA ASIMÉTRICA

La clave secreta se encriptará con clave asimétrica con la clave pública del certificado del banco suministrado ya.

#### LLAMADA AL SERVICIO:

Incorporaremos al WS un parámetro más que será el parámetro de la clave secreta. Al estar encriptada con el certificado del banco, sólo nosotros podremos descifrar la clave secreta y una vez realizado, podremos descifrar el XML.

#### FLUJO:

1. Se obtiene el XML firmado
2. Se cifra con la clave simétrica
3. Se codifica a BASE64 el XML
4. Se cifra la clave secreta con la clave pública del certificado del banco
5. Se codifica a BASE64 la clave secreta ya cifrada
5. Se llama al WS con:
  - Parámetro 1: XML firmado + Cifrado + Codificado
  - Parámetro 2: Clave Secreta + Cifrado + Codificado

### d) Firma

Múltiples firmantes

Cuando un mismo documento es firmado por varios firmantes, en el que los mismos están al mismo nivel y en el que no importa el orden en el que se firma, se produce una operación de co-firma en paralelo. Es decir, en estos casos, dos firmas de un mismo documento se encuentran a un mismo nivel,

ninguna envuelve a la otra ni una prevalece sobre la otra. Es claro que la primera firma no se modifica ni se incluye en la segunda firma.