



**Guía de migración a firma HMAC SHA256
Conexión por Web Service**

SERVICIO TECNICO TPV VIRTUAL

Teléfono: 902 365 650 opción 2

tpvvirtual@bancsabadell.com

Atención especial para migración SHA1 a SHA2: Lunes a
Viernes de 10h a 19h

ÍNDICE DE CONTENIDO

1. Introducción	4
1.1 Objetivo	4
2. Resumen de las diferencias del nuevo modelo (HMAC SHA-256) respecto del modelo anterior (SHA-1).....	5
3. Descripción general del flujo.....	6
3.1 Envío de petición al TPV Virtual	6
3.1.1 Entrada WS.....	6
3.1.2 Entrada Operaciones	6
4. Mensaje de petición de pago Host to Host.....	8
4.1 Montar la cadena de datos de la petición	9
4.2 Identificar la versión de algoritmo de firma a utilizar.....	9
4.3 Identificar la clave a utilizar para la firma	9
4.4 Firmar los datos de la petición.....	10
4.5 Utilización de librerías de ayuda	10
4.5.1 Librería PHP	10
4.5.2 Librería JAVA.....	11
5. Respuesta de petición Host to Host.....	12
5.1 Firma del mensaje de respuesta	13
5.2 Utilización de librerías de ayuda	13
5.2.1 Librería PHP	14
5.2.2 Librería JAVA.....	14
6. Entorno de pruebas.....	16
7. Códigos de error.....	17
8. ANEXOS.....	21
8.1 Peticiones de pago (con envío de datos de tarjeta)	21
8.2 Peticiones de Confirmación/Devolución.....	23
8.3 Respuesta Host to Host	24

8.4	Web Service de petición de pago - WSDL.....	27
-----	---	----

1. Introducción

1.1 Objetivo

Este documento recoge los aspectos técnicos necesarios para que un comercio, que actualmente esté operando en el SIS, realice la migración con el TPV Virtual utilizando el nuevo sistema de firma basado en HMAC SHA256.

El algoritmo actual (SHA-1) en el que se basa la seguridad de la conexión de la tienda con el tpv virtual (y viceversa) es un algoritmo obsoleto según los estándares de seguridad, y podría ser objeto de ataques. Para garantizar la mayor seguridad en la conexión con el TPV Virtual SIS los métodos anteriores deben actualizarse al nuevo sistema de firma basado en HMAC SHA256.

Esta documentación aplica a los comercios que acceden al SIS vía Host to Host, es decir, comercios que acceden vía Web Service o mediante la entrada "Operaciones".

Para desarrollar el cálculo de este nuevo tipo de firma, el comercio puede realizar el desarrollo por sí mismo utilizando las funciones estándar o utilizar las librerías suministradas (PHP y JAVA).

2. **Resumen de las diferencias del nuevo modelo (HMAC SHA-256) respecto del modelo anterior (SHA-1)**

Las diferencias del nuevo modelo de conexión basado en HMAC SHA-256 respecto al modelo anterior en uso (basado en SHA-1) se pueden resumir en los siguientes 3 puntos:

1. Formato del parámetro enviado.
 - **ANTES:** Se enviaba un único parámetro cuyo elemento raíz era <DATOSENTRADA>. Este elemento raíz contenía todos los campos de la petición de pago.
 - **AHORA:** Se envía un único parámetro cuyo elemento raíz es <REQUEST>. El elemento <DATOSENTRADA> forma parte del elemento raíz <REQUEST>, junto con dos nuevos campos que se describirán en detalle en este documento.

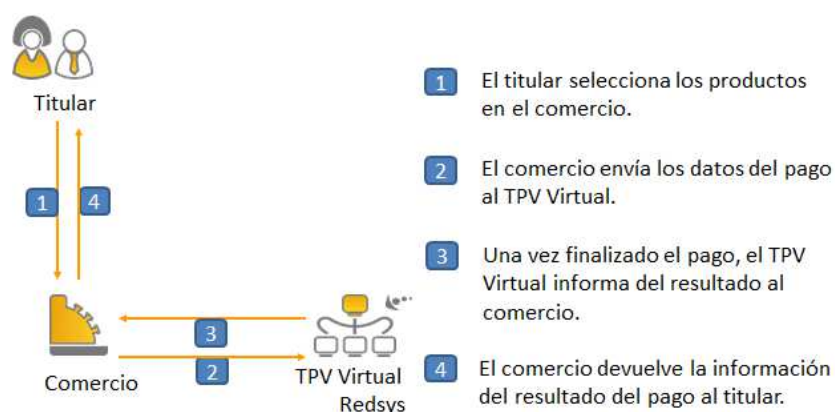
2. Cálculo de la firma enviada por el comercio.
 - **ANTES:** La firma se calculaba como un SHA-1 sobre la concatenación de los campos enviados y se enviaba como un campo del elemento <DATOSENTRADA>. No se enviaba ningún parámetro indicador de la versión de firma utilizada.
 - **AHORA:** La firma se calcula con una nueva clave diversificada por operación, y un nuevo algoritmo (HMAC SHA256). La firma se envía en un nuevo campo que forma parte del elemento raíz <REQUEST>. Además se incluye un campo nuevo que indica la versión de firma utilizada que forma parte del elemento raíz <REQUEST>.

3. Cálculo de la firma de respuesta.
 - **ANTES:** La firma se calculaba como un SHA-1 sobre la concatenación de los campos recibidos.
 - **AHORA:** La firma se calcula con una nueva clave diversificada por operación, y un nuevo algoritmo (HMAC SHA256) sobre la concatenación de los campos recibidos.

NOTA: No es necesario modificar ningún parámetro dentro del módulo de administración del comercio. El TPV Virtual aceptará de forma automática las conexiones basadas en HMAC SHA-256, una vez que la tienda online empiece a enviarlas al TPV Virtual. De igual forma, el TPV Virtual utilizará el formato HMAC SHA-256 para confirmar dichas operaciones al servidor de la tienda (notificaciones y retorno de la navegación del cliente).

3. Descripción general del flujo

El siguiente esquema presenta el flujo general de una operación realizada vía Host to Host.



3.1 Envío de petición al TPV Virtual

3.1.1 Entrada WS

Como se muestra en el paso 2 del esquema anterior, el comercio debe enviar al TPV Virtual los datos de la petición de pago vía Web Service con codificación UTF-8. Para ello el Web Service tiene publicados varios métodos sobre los cuales operan los TPV Virtuales. El método "**trataPetición**", permite la realización de operaciones a través del Web Service, para lo cual se debe construir un XML que incluye los datos de la petición de pago. La descripción exacta de esta petición XML se presenta mediante el fichero WSDL en el Anexo 5 (Web Service de petición de pago - WSDL) del apartado Anexos del presente documento.

Esta petición de pago debe enviarse a las siguientes URLs dependiendo de si se quiere realizar una petición de pruebas u operaciones reales:

URL Conexión	Entorno
https://sis-t.redsys.es:25443/sis/services/SerClsWSEntrada	Pruebas
https://sis.redsys.es/sis/services/SerClsWSEntrada	Real

Una vez enviada la petición el TPV Virtual la interpretará y realizará las validaciones necesarias para, a continuación, procesar la operación, tal y como se muestra en el paso 3 del esquema anterior. Dependiendo del resultado de la operación, se construye un documento XML de respuesta con el resultado de la misma con codificación UTF-8.

3.1.2 Entrada Operaciones

Como se muestra en el paso 2 del esquema anterior, el comercio debe enviar al TPV Virtual los datos de la petición de pago mediante la entrada "Operaciones" con codificación UTF-8. Para ello deberá preparar un formulario de un único parámetro de nombre "entrada" y cuyo valor es el XML construido que incluye los datos de la petición de pago.

Esta petición de pago debe enviarse a las siguientes URLs dependiendo de si se quiere realizar una petición de pruebas u operaciones reales:

URL Conexión	Entorno
https://sis-t.redsys.es:25443/sis/operaciones	Pruebas
https://sis.redsys.es/sis/operaciones	Real

Una vez enviada la petición el TPV Virtual la interpretará y realizará las validaciones necesarias para, a continuación, procesar la operación, tal y como se muestra en el paso 3 del esquema anterior. Dependiendo del resultado de la operación, se construye un documento XML de respuesta con el resultado de la misma con codificación UTF-8.

NOTA: Todo lo relacionado con la respuesta del acceso Host to Host se expone en el apartado 5.

4. Mensaje de petición de pago Host to Host

Para que el comercio pueda realizar la petición a través del Web Service de Banco Sabadell, es necesario intercambiar una serie de datos, tanto en los mensajes de petición como en los mensajes de respuesta.

La estructura del mensaje siempre será la misma, estableciendo como raíz del mismo el elemento **<REQUEST>**. En su interior siempre deben encontrarse tres elementos que hacen referencia a:

- Datos de la petición de pago. Elemento identificado por la etiqueta **<DATOSENTRADA>**.
- Versión del algoritmo de firma. Elemento identificado por la etiqueta **<DS_SIGNATUREVERSION>**.
- Firma de los datos de la petición de pago. Elemento identificado por la etiqueta **<DS_SIGNATURE>**.

A continuación se muestra un ejemplo de un mensaje de petición de pago:

```
<REQUEST>
  <DATOSENTRADA>
    <DS_MERCHANT_AMOUNT>145</DS_MERCHANT_AMOUNT>
    <DS_MERCHANT_ORDER>151029142229</DS_MERCHANT_ORDER>
    <DS_MERCHANT_MERCHANTCODE>327234688</DS_MERCHANT_MERCHANTCODE>
    <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
    <DS_MERCHANT_PAN>4548812049400004</DS_MERCHANT_PAN>
    <DS_MERCHANT_EXPIRYDATE>1512</DS_MERCHANT_EXPIRYDATE>
    <DS_MERCHANT_CVV2>285</DS_MERCHANT_CVV2>
    <DS_MERCHANT_TRANSACTIONTYPE>A</DS_MERCHANT_TRANSACTIONTYPE>
    <DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
  </DATOSENTRADA>
  <DS_SIGNATUREVERSION>HMAC_SHA256_V1</DS_SIGNATUREVERSION>
  <DS_SIGNATURE>2YW19YQ8rb/0LLav79Y5L24Yw045KxN5hme27605WxY=</DS_SIGNATURE>
</REQUEST>
```

Para facilitar la integración del comercio, a continuación se explica de forma detallada los pasos a seguir para montar el mensaje de petición de pago.

4.1 Montar la cadena de datos de la petición

Se debe montar una cadena con todos los datos de la petición en formato XML dando como resultado el elemento **<DATOSENTRADA>**. Cabe destacar que ya no formará parte de este elemento el parámetro **<DS_MERCHANT_MERCHANTSIGNATURE>**.

Se debe tener en cuenta que existen varios tipos de peticiones y según el tipo varía la estructura del mensaje y los parámetros que se envían y reciben.

Podemos diferenciar tres tipos de peticiones:

- Peticiones de pago (con envío de datos de tarjeta). En el Anexo 1 (Peticiones de pago) del apartado Anexos del presente documento, se presentan los parámetros necesarios para este tipo de petición incluyendo un ejemplo.
- Peticiones de Confirmación/Devolución. En el Anexo 3 (Peticiones de Confirmación/Devolución) del apartado Anexos del presente documento, se presentan los parámetros necesarios para este tipo de petición incluyendo un ejemplo.

4.2 Identificar la versión de algoritmo de firma a utilizar

En la petición se debe identificar la versión concreta de algoritmo que se está utilizando para la firma. Actualmente se utiliza el valor **HMAC_SHA256_V1** para identificar la versión de todas las peticiones, por lo que este será el valor del elemento **<DS_SIGNATUREVERSION>**, tal y como se puede observar en el ejemplo de mensaje mostrado al inicio del apartado 4.

4.3 Identificar la clave a utilizar para la firma

Para calcular la firma es necesario utilizar una clave específica para cada terminal. La clave de comercio que debe utilizar es la que recibió a través de SMS desde Banco Sabadell.

NOTA IMPORTANTE: Esta clave debe ser almacenada en el servidor del comercio de la forma más segura posible para evitar un uso fraudulento de la misma. El comercio es responsable de la adecuada custodia y mantenimiento en secreto de dicha clave.

4.4 Firmar los datos de la petición

Una vez se tiene montada el elemento con los datos de la petición de pago (<DATOSENTRADA>) y la clave específica del terminal se debe calcular la firma siguiendo los siguientes pasos:

1. Se genera una clave específica por operación. Para obtener la clave derivada a utilizar en una operación se debe realizar un cifrado 3DES entre la clave del comercio, la cual debe ser previamente decodificada en BASE 64, y el valor del número de pedido de la operación (DS_MERCHANT_ORDER).
2. Se calcula el HMAC SHA256 del elemento <DATOSENTRADA>.
3. El resultado obtenido se codifica en BASE 64, y el resultado de la codificación será el valor del elemento **<DS_SIGNATURE>**, tal y como se puede observar en el ejemplo de formulario mostrado al inicio del apartado 4.

NOTA: La utilización de las librerías de ayuda proporcionadas por Banco Sabadell para la generación de este campo, se expone en el apartado 4.5.

4.5 Utilización de librerías de ayuda

En los apartados anteriores se ha descrito la forma de acceso al SIS utilizando conexión vía Host to Host y el sistema de firma basado en HMAC SHA256. En este apartado se explica cómo se utilizan las librerías disponibles en PHP y JAVA para facilitar los desarrollos y la generación de la firma. El uso de las librerías suministradas por Banco Sabadell es opcional, si bien simplifican los desarrollos a realizar por el comercio.

4.5.1 Librería PHP

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería PHP proporcionada por Banco Sabadell:

1. Importar el fichero principal de la librería, tal y como se muestra a continuación:

```
include './apiRedsysWs.php';
```

El comercio debe decidir si la importación desea hacerla con la función "include" o "required", según los desarrollos realizados.

2. Definir un objeto de la clase principal de la librería, tal y como se muestra a continuación:

```
$miObj = new RedsysAPIWs;
```

3. Calcular el elemento **<DS_SIGNATURE>**. Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería "createMerchantSignatureHostToHost()" con la clave de comercio facilitada y el elemento con los datos de la petición de pago (**<DATOSENTRADA>**), tal y como se muestra a continuación:

```
$datoEntrada='<DATOSENTRADA><DS_MERCHANT_AMOUNT>'.importe.'</DS_MERCHANT_AMOUNT><DS_MERCHANT_ORDER>'.  
$clave = 'sq7HjrU0BfKmc576ILgskD5srU870gJ7';  
$signature = $miObj->createMerchantSignatureHostToHost($clave, $datoEntrada);
```

Una vez obtenido el valor del elemento **<DS_SIGNATURE>**, ya se puede completar el mensaje de petición de pago y realizar la llamada Host to Host.

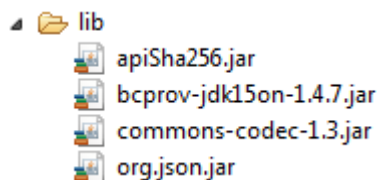
4.5.2 Librería JAVA

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería JAVA proporcionada por Banco Sabadell:

1. Importar la librería, tal y como se muestra a continuación:

```
<%@page import="sis.redsys.api.ApiWsMacSha256"%>
```

El comercio debe incluir en la vía de construcción del proyecto todas las librerías (JARs) que se proporcionan:



2. Calcular el elemento **<DS_SIGNATURE>**. Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería "createMerchantSignatureHostToHost()" con la clave de comercio facilitada y el elemento con los datos de la petición de pago (**<DATOSENTRADA>**), tal y como se muestra a continuación:

```
String datosEntrada="<DATOSENTRADA><DS_MERCHANT_AMOUNT>200</DS_MERCHANT_AMOUNT>..."  
String clave = "sq7HjrU0BfKmc576ILgskD5srU870gJ7";  
String signature = ApiMacSha256.createMerchantSignatureHostToHost(clave, datosEntrada);
```

Una vez obtenido el valor del elemento **<DS_SIGNATURE>**, ya se puede completar el mensaje de petición de pago y realizar la llamada Host to Host.

5. Respuesta de petición Host to Host

En el presente apartado se describen los datos que forman parte del mensaje de respuesta de una petición vía Host to Host. Este mensaje se genera en formato XML y a continuación se muestra un ejemplo del mismo:

```
<RETORNOXML>
  <CODIGO>0</CODIGO>
  <OPERACION>
    <Ds_Amount>145</Ds_Amount>
    <Ds_Currency>978</Ds_Currency>
    <Ds_Order>151029142229</Ds_Order>
    <Ds_Signature>
      MRvyhuDEpg4BmzfTdgHKrI5qQ9U5UD2Qe8eDadIZtyE=
    </Ds_Signature>
    <Ds_MerchantCode>327234688</Ds_MerchantCode>
    <Ds_Terminal>2</Ds_Terminal>
    <Ds_Response>0000</Ds_Response>
    <Ds_AuthorisationCode>185714</Ds_AuthorisationCode>
    <Ds_TransactionType>A</Ds_TransactionType>
    <Ds_SecurePayment>0</Ds_SecurePayment>
    <Ds_Language>1</Ds_Language>
    <Ds_MerchantData></Ds_MerchantData>
    <Ds_Card_Country>724</Ds_Card_Country>
  </OPERACION>
</RETORNOXML>
```

Como se puede observar en el ejemplo anterior, la respuesta está formada por dos elementos principales:

- Código (**<CODIGO>**): Indica si la operación ha sido correcta o no, (no indica si ha sido autorizada, solo si se ha procesado). Un 0 indica que la operación ha sido correcta. En el caso de que sea distinto de 0, tendrá un código. (Ver códigos de error en apartado 6 de esta Guía)
- Datos de la operación (**<OPERACION>**): Recoge toda la información necesaria sobre la operación que se ha realizado. Mediante este elemento se determina si la operación ha sido autorizada o no.

NOTA: La relación de parámetros que forman parte de la respuesta se describe en el Anexo 4 (Respuesta Host to Host) del apartado Anexos del presente documento.

5.1 Firma del mensaje de respuesta

Una vez se ha obtenido el mensaje de respuesta y la clave específica del terminal, siempre y cuando la operación se autorice, se debe comprobar la firma de la respuesta siguiendo los siguientes pasos:

1. Se genera una clave específica por operación. Para obtener la clave derivada a utilizar en una operación se debe realizar un cifrado 3DES entre la clave del comercio y el valor del número de pedido de la operación (DS_MERCHANT_ORDER).
2. Se calcula el HMAC SHA256 de la cadena formada por la concatenación del valor de los siguientes campos:

Cadena = Ds_Amount + Ds_Order + Ds_MerchantCode + Ds_Currency + Ds_Response + Ds_TransactionType + Ds_SecurePayment

Si tomamos como ejemplo la respuesta que se presenta al inicio de este apartado la cadena resultante sería:

Cadena = 1451510291422293272346889780000A0

3. El resultado obtenido se codifica en BASE 64, y el resultado de la codificación debe ser el mismo que el valor del parámetro **<Ds_Signature>** obtenido en la respuesta.

NOTA: La utilización de las librerías de ayuda proporcionadas por Banco Sabadell para la generación de este parámetro, se expone en el apartado 5.2.

5.2 Utilización de librerías de ayuda

En este apartado se explica cómo se utilizan las librerías disponibles en PHP y JAVA para facilitar los desarrollos y la generación de la firma de respuesta. El uso de las librerías suministradas por Banco Sabadell es opcional, si bien simplifican los desarrollos a realizar por el comercio.

5.2.1 Librería PHP

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería PHP proporcionada por Banco Sabadell:

1. Importar el fichero principal de la librería, tal y como se muestra a continuación:

```
include './apiRedsysWs.php';
```

El comercio debe decidir si la importación desea hacerla con la función "include" o "required", según los desarrollos realizados.

2. Definir un objeto de la clase principal de la librería, tal y como se muestra a continuación:

```
$miObj = new RedsysAPI;
```

3. Calcular el parámetro **<Ds_Signature>**. Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería "createSignatureResponseHostToHost()" con la clave de comercio facilitada, la cadena que se desea firmar (concatenación de campos descrita en el punto 2 del apartado 5.1 del presente documento) y el número de pedido.

```
$cadenaConcatenada = "145151029142229327234688978000A0";  
$numPedido = "151029142229";  
$clave = 'sq7HjrUOBfKmC576ILgskD5srU870gJ7';  
$signature = $miObj->createMerchantSignatureResponseHostToHost($clave,  
                                                                $cadenaConcatenada,  
                                                                $numPedido);
```

El resultado obtenido debe ser el mismo que el valor del parámetro **<Ds_Signature>** obtenido en la respuesta.

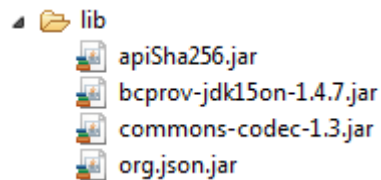
5.2.2 Librería JAVA

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería JAVA proporcionada por Banco Sabadell:

1. Importar la librería, tal y como se muestra a continuación:

```
<%@page import="sis.redsys.api.ApiWsMacSha256"%>
```

El comercio debe incluir en la vía de construcción del proyecto todas las librerías(JARs) que se proporcionan:



2. Calcular el parámetro **<Ds_Signature>**. Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería "createSignatureResponseHostToHost()" con la clave de comercio facilitada, la cadena que se desea firmar (concatenación de campos descrita en el punto 2 del apartado 5.1 del presente documento) y el número de pedido.

```
String cadenaConcatenada = "145151029142229327234688978000A0";  
String numPedido = "145151029142229327234688978000A0";  
String clave = "sq7HjrU0BfKmc576ILgskD5srU870gJ7";  
String signature = ApiMacSha256.createMerchantSignatureResponseHostToHost(clave,  
cadenaConcatenada,  
numPedido);
```

El resultado obtenido debe ser el mismo que el valor del parámetro **<Ds_Signature>** obtenido en la respuesta.

6. Entorno de pruebas

El entorno de pruebas permite realizar las pruebas necesarias para verificar el correcto funcionamiento del sistema antes de la utilización en real del TPV Virtual del comercio. Dicho entorno es idéntico al real, pero sin que los pagos realizados tengan una validez contable.

Las claves del entorno de pruebas que le facilitamos a continuación son comunes para otros clientes de Banco Sabadell. También puede utilizar el entorno de pruebas de su comercio para realizar todas las pruebas que necesite. En caso de que no disponga de los datos de configuración, comuníquese con el Servicio Técnico en el teléfono 902 365 650 o el buzón tpvvirtual@bancsabadell.com.

Los parámetros del entorno de prueba son los que se describen a continuación.

1. URL para el envío de las órdenes de pago:

Entrada Web Service:

<https://sis-t.redsys.es:25443/sis/services/SerClsWSEntrada>

2. Número de comercio (Ds_Merchant_MerchantCode): 327234688

3. Clave secreta: qwertyasdf0123456789

4. Terminal (Ds_Merchant_Terminal):

- Terminal 002 - Para pagos en EUROS (Ds_MerchantCurrency = 978) de comercios bajo protocolo No-CES (pagos considerados NO seguros)

5. Tarjeta aceptada:

- Numeración: 4548 8120 4940 0004
- Caducidad 12/17
- Código CVV2: 123.

En modo de compra segura (CES), en la que se requiera autenticación del comprador, el código de identificación personal (CIP) es: 123456

6. URL módulo de administración:

<https://sis-t.redsys.es:25443/canales/bsabadell>

7. Acceso al módulo de administración:

- Terminal 002 (NO CES):

- Usuario: 327234688-002
- Password: 123456a

7. Códigos de error

En este apartado se presenta un glosario de los errores que se pueden producir en el proceso de integración.

Glosario de errores del SIS

ERROR	DESCRIPCIÓN	MENSAJE (ANEXO VI)
SIS0007	Error al desmontar el XML de entrada o error producido al acceder mediante un sistema de firma antiguo teniendo configurado el tipo de clave HMAC SHA256	MSG0008
SIS0008	Error falta Ds_Merchant_MerchantCode	MSG0008
SIS0009	Error de formato en Ds_Merchant_MerchantCode	MSG0008
SIS0010	Error falta Ds_Merchant_Terminal	MSG0008
SIS0011	Error de formato en Ds_Merchant_Terminal	MSG0008
SIS0014	Error de formato en Ds_Merchant_Order	MSG0008
SIS0015	Error falta Ds_Merchant_Currency	MSG0008
SIS0016	Error de formato en Ds_Merchant_Currency	MSG0008
SIS0017	Error no se admiten operaciones en pesetas	MSG0008
SIS0018	Error falta Ds_Merchant_Amount	MSG0008
SIS0019	Error de formato en Ds_Merchant_Amount	MSG0008
SIS0020	Error falta Ds_Merchant_MerchantSignature	MSG0008
SIS0021	Error la Ds_Merchant_MerchantSignaturevienevacía	MSG0008
SIS0022	Error de formato en Ds_Merchant_TransactionType	MSG0008
SIS0023	Error Ds_Merchant_TransactionType desconocido	MSG0008
SIS0024	Error Ds_Merchant_ConsumerLanguage tiene más de 3 posiciones	MSG0008
SIS0025	Error de formato en Ds_Merchant_ConsumerLanguage	MSG0008
SIS0026	Error No existe el comercio / terminal enviado	MSG0008
SIS0027	Error Moneda enviada por el comercio es diferente a la que tiene asignada para ese terminal	MSG0008
SIS0028	Error Comercio / terminal está dado de baja	MSG0008
SIS0030	Error en un pago con tarjeta ha llegado un tipo de operación que no es ni pago ni preautorización	MSG0000
SIS0031	Método de pago no definido	MSG0000
SIS0033	Error en un pago con móvil ha llegado un tipo de operación que no es ni pago ni preautorización	MSG0000
SIS0034	Error de acceso a la Base de Datos	MSG0000
SIS0037	El número de teléfono no es válido	MSG0000
SIS0038	Error en java	MSG0000
SIS0040	Error el comercio / terminal no tiene ningún método de pago asignado	MSG0008
SIS0041	Error en el cálculo de la HASH de datos del comercio.	MSG0008
SIS0042	La firma enviada no es correcta	MSG0008
SIS0043	Error al realizar la notificación on-line	MSG0008

ERROR	DESCRIPCIÓN	MENSAJE (ANEXO VI)
SIS0046	El bin de la tarjeta no está dado de alta	MSG0002
SIS0051	Error número de pedido repetido	MSG0001
SIS0054	Error no existe operación sobre la que realizar la devolución	MSG0008
SIS0055	Error existe más de un pago con el mismo número de pedido	MSG0008
SIS0056	La operación sobre la que se desea devolver no está autorizada	MSG0008
SIS0057	El importe a devolver supera el permitido	MSG0008
SIS0058	Inconsistencia de datos, en la validación de una confirmación	MSG0008
SIS0059	Error no existe operación sobre la que realizar la confirmación	MSG0008
SIS0060	Ya existe una confirmación asociada a la preautorización	MSG0008
SIS0061	La preautorización sobre la que se desea confirmar no está autorizada	MSG0008
SIS0062	El importe a confirmar supera el permitido	MSG0008
SIS0063	Error. Número de tarjeta no disponible	MSG0008
SIS0064	Error. El número de tarjeta no puede tener más de 19 posiciones	MSG0008
SIS0065	Error. El número de tarjeta no es numérico	MSG0008
SIS0066	Error. Mes de caducidad no disponible	MSG0008
SIS0067	Error. El mes de la caducidad no es numérico	MSG0008
SIS0068	Error. El mes de la caducidad no es válido	MSG0008
SIS0069	Error. Año de caducidad no disponible	MSG0008
SIS0070	Error. El Año de la caducidad no es numérico	MSG0008
SIS0071	Tarjeta caducada	MSG0000
SIS0072	Operación no anulable	MSG0000
SIS0074	Error falta Ds_Merchant_Order	MSG0008
SIS0075	Error el Ds_Merchant_Order tiene menos de 4 posiciones o más de 12	MSG0008
SIS0076	Error el Ds_Merchant_Order no tiene las cuatro primeras posiciones numéricas	MSG0008
SIS0077	Error el Ds_Merchant_Order no tiene las cuatro primeras posiciones numéricas. No se utiliza	MSG0000
SIS0078	Método de pago no disponible	MSG0005
SIS0079	Error al realizar el pago con tarjeta	MSG0000
SIS0081	La sesión es nueva, se han perdido los datos almacenados	MSG0007
SIS0084	El valor de Ds_Merchant_Conciliation es nulo	MSG0008
SIS0085	El valor de Ds_Merchant_Conciliation no es numérico	MSG0008
SIS0086	El valor de Ds_Merchant_Conciliation no ocupa 6 posiciones	MSG0008
SIS0089	El valor de Ds_Merchant_ExpiryDate no ocupa 4 posiciones	MSG0008
SIS0092	El valor de Ds_Merchant_ExpiryDate es nulo	MSG0008
SIS0093	Tarjeta no encontrada en la tabla de rangos	MSG0006
SIS0094	La tarjeta no fue autenticada como 3D Secure	MSG0004
SIS0097	Valor del campo Ds_Merchant_CComercio no válido	MSG0008
SIS0098	Valor del campo Ds_Merchant_CVentana no válido	MSG0008

ERROR	DESCRIPCIÓN	MENSAJE (ANEXO VI)
SIS0112	Error El tipo de transacción especificado en Ds_Merchant_Transaction_Type no esta permitido	MSG0008
SIS0113	Excepción producida en el servlet de operaciones	MSG0008
SIS0114	Error, se ha llamado con un GET en lugar de un POST	MSG0000
SIS0115	Error no existe operación sobre la que realizar el pago de la cuota	MSG0008
SIS0116	La operación sobre la que se desea pagar una cuota no es una operación válida	MSG0008
SIS0117	La operación sobre la que se desea pagar una cuota no está autorizada	MSG0008
SIS0118	Se ha excedido el importe total de las cuotas	MSG0008
SIS0119	Valor del campo Ds_Merchant_DateFrecuency no válido	MSG0008
SIS0120	Valor del campo Ds_Merchant_ChargeExpiryDate no válido	MSG0008
SIS0121	Valor del campo Ds_Merchant_SumTotal no válido	MSG0008
SIS0122	Valor del campo Ds_Merchant_DateFrecuency o no Ds_Merchant_SumTotal tiene formato incorrecto	MSG0008
SIS0123	Se ha excedido la fecha tope para realizar transacciones	MSG0008
SIS0124	No ha transcurrido la frecuencia mínima en un pago recurrente sucesivo	MSG0008
SIS0132	La fecha de Confirmación de Autorización no puede superar en más de 7 días a la de Preautorización.	MSG0008
SIS0133	La fecha de Confirmación de Autenticación no puede superar en más de 45 días a la de Autenticación Previa.	MSG0008
SIS0139	Error el pago recurrente inicial está duplicado	MSG0008
SIS0142	Tiempo excedido para el pago	MSG0000
SIS0197	Error al obtener los datos de cesta de la compra en operación tipo pasarela	MSG0000
SIS0198	Error el importe supera el límite permitido para el comercio	MSG0000
SIS0199	Error el número de operaciones supera el límite permitido para el comercio	MSG0008
SIS0200	Error el importe acumulado supera el límite permitido para el comercio	MSG0008
SIS0214	El comercio no admite devoluciones	MSG0008
SIS0216	Error Ds_Merchant_CVV2 tiene más de 3 posiciones	MSG0008
SIS0217	Error de formato en Ds_Merchant_CVV2	MSG0008
SIS0218	El comercio no permite operaciones seguras por la entrada /operaciones	MSG0008
SIS0219	Error el número de operaciones de la tarjeta supera el límite permitido para el comercio	MSG0008
SIS0220	Error el importe acumulado de la tarjeta supera el límite permitido para el comercio	MSG0008
SIS0221	Error el CVV2 es obligatorio	MSG0008
SIS0222	Ya existe una anulación asociada a la preautorización	MSG0008
SIS0223	La preautorización que se desea anular no está autorizada	MSG0008
SIS0224	El comercio no permite anulaciones por no tener firma ampliada	MSG0008
SIS0225	Error no existe operación sobre la que realizar la anulación	MSG0008
SIS0226	Inconsistencia de datos, en la validación de una anulación	MSG0008
SIS0227	Valor del campo Ds_Merchant_TransactionDate no válido	MSG0008
SIS0229	No existe el código de pago aplazado solicitado	MSG0008
SIS0252	El comercio no permite el envío de tarjeta	MSG0008

ERROR	DESCRIPCIÓN	MENSAJE (ANEXO VI)
SIS0253	La tarjeta no cumple el check-digit	MSG0006
SIS0254	El número de operaciones de la IP supera el límite permitido por el comercio	MSG0008
SIS0255	El importe acumulado por la IP supera el límite permitido por el comercio	MSG0008
SIS0256	El comercio no puede realizar preautorizaciones	MSG0008
SIS0257	Esta tarjeta no permite operativa de preautorizaciones	MSG0008
SIS0258	Inconsistencia de datos, en la validación de una confirmación	MSG0008
SIS0261	Operación detenida por superar el control de restricciones en la entrada al SIS	MSG0008
SIS0270	El comercio no puede realizar autorizaciones en diferido	MSG0008
SIS0274	Tipo de operación desconocida o no permitida por esta entrada al SIS	MSG0008
SIS0429	Error en la versión enviada por el comercio en el parámetro Ds_SignatureVersion	MSG0008
SIS0432	Error FUC del comercio erróneo	MSG0008
SIS0433	Error Terminal del comercio erróneo	MSG0008
SIS0434	Error ausencia de número de pedido en la operación enviada por el comercio	MSG0008
SIS0435	Error en el cálculo de la firma	MSG0008
SIS0436	Error en la construcción del elemento padre <REQUEST>	MSG0008
SIS0437	Error en la construcción del elemento <DS_SIGNATUREVERSION>	MSG0008
SIS0438	Error en la construcción del elemento <DATOSENTRADA>	MSG0008
SIS0439	Error en la construcción del elemento <DS_SIGNATURE>	MSG0008

8. ANEXOS

8.1 Peticiones de pago (con envío de datos de tarjeta)

En el presente anexo se describen los datos necesarios y sus características, para enviar una petición Host to Host en formato XML. Así mismo se incluye un ejemplo de cómo utilizar esos datos en los mensajes de petición de pago.

Nombre del dato	Long. / Tipo	Descripción
<i>DS_MERCHANT_AMOUNT</i>	12 / N	Obligatorio. Las dos últimas posiciones se consideran decimales, salvo en el caso de los Yenes que no tienen.
<i>DS_MERCHANT_ORDER</i>	12 / A-N	Obligatorio. Número de pedido. Los 4 primeros dígitos deben ser numéricos. Cada pedido es único, no puede repetirse.
<i>DS_MERCHANT_MERCHANTCODE</i>	9 / N	Obligatorio. Código FUC asignado al comercio.
<i>DS_MERCHANT_TERMINAL</i>	3 / N	Obligatorio. Número de Terminal que le asignará su banco. Por defecto valor "001".3 se considera su longitud máxima.
<i>DS_MERCHANT_CURRENCY</i>	4 / N	Obligatorio. Moneda del comercio. Tiene que ser la contratada para el Terminal. Valor 978 para Euros, 840 para Dólares, 826 para Libras esterlinas y 392 para Yenes.
<i>DS_MERCHANT_PAN</i>	19 / N	Obligatorio. Tarjeta. Su longitud depende del tipo de tarjeta.
<i>DS_MERCHANT_EXPIRYDATE</i>	4 / N	Obligatorio. Caducidad de la tarjeta. Su formato es AAMM, siendo AA los dos últimos dígitos del año y MM los dos dígitos del mes.
<i>DS_MERCHANT_CVV2</i>	3-4 / N	Obligatorio. Código CVV2 de la tarjeta.
<i>DS_MERCHANT_TRANSACTIONTYPE</i>	1 / A-N	Obligatorio. Campo para el comercio para indicar qué tipo de transacción es. Los posibles valores son: A – Pago tradicional 1 – Preautorización O – Autorización en diferido

Tipo A: caracteres ASCII del 65 = **A** al 90 = **Z** y del 97 = **a** al 122 = **z**.
Tipo N: caracteres ASCII del 30 = **0** al 39 = **9**.

A continuación se muestra un ejemplo de un mensaje de petición de pago:

```
<REQUEST>
  <DATOSENTRADA>
    <DS_MERCHANT_AMOUNT>145</DS_MERCHANT_AMOUNT>
    <DS_MERCHANT_ORDER>151029142229</DS_MERCHANT_ORDER>
    <DS_MERCHANT_MERCHANTCODE>327234688</DS_MERCHANT_MERCHANTCODE>
    <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
    <DS_MERCHANT_PAN>4548812049400004</DS_MERCHANT_PAN>
    <DS_MERCHANT_EXPIRYDATE>1512</DS_MERCHANT_EXPIRYDATE>
    <DS_MERCHANT_CVV2>285</DS_MERCHANT_CVV2>
    <DS_MERCHANT_TRANSACTIONTYPE>A</DS_MERCHANT_TRANSACTIONTYPE>
    <DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
  </DATOSENTRADA>
  <DS_SIGNATUREVERSION>HMAC_SHA256_V1</DS_SIGNATUREVERSION>
  <DS_SIGNATURE>2YW19YQ8rb/0LLav79Y5L24Yw045KxN5hme27605WxY=</DS_SIGNATURE>
</REQUEST>
```

8.2 Peticiones de Confirmación/Devolución

En el presente anexo se describen los datos necesarios y sus características, para enviar una petición Host to Host en formato XML. Así mismo se incluye un ejemplo de cómo utilizar esos datos en los mensajes de petición de pago.

Nombre del dato	Long. / Tipo	Descripción
<i>DS_MERCHANT_AMOUNT</i>	12 / N	Obligatorio. Las dos últimas posiciones se consideran decimales, salvo en el caso de los Yenes que no tienen.
<i>DS_MERCHANT_ORDER</i>	12 / A-N	Obligatorio. Número de pedido. Los 4 primeros dígitos deben ser numéricos. Cada pedido es único, no puede repetirse.
<i>DS_MERCHANT_MERCHANTCODE</i>	9 / N	Obligatorio. Código FUC asignado al comercio.
<i>DS_MERCHANT_TERMINAL</i>	3 / N	Obligatorio. Número de Terminal que le asignará su banco. Por defecto valor "001".3 se considera su longitud máxima.
<i>DS_MERCHANT_CURRENCY</i>	4 / N	Obligatorio. Moneda del comercio. Tiene que ser la contratada para el Terminal. Valor 978 para Euros, 840 para Dólares, 826 para Libras esterlinas y 392 para Yenes.
<i>DS_MERCHANT_TRANSACTIONTYPE</i>	1 / A-N	Obligatorio. Campo para el comercio para indicar qué tipo de transacción es. Los posibles valores son: 2 – Confirmación 3 – Devolución Automática 6 – Transacción Sucesiva 9 – Anulación de Preautorización P - Confirmación de autorización en diferido Q - Anulación de autorización en diferido S – Autorización recurrente sucesiva diferido
<i>DS_MERCHANT_AUTHORIZATIONCODE</i>	6 / Num	Opcional. Representa el código de autorización necesario para identificar una transacción recurrente sucesiva en las devoluciones de operaciones recurrentes sucesivas. Obligatorio en devoluciones de operaciones recurrentes.

Tipo A: caracteres ASCII del 65 = **A** al 90 = **Z** y del 97 = **a** al 122 = **z**.
Tipo N: caracteres ASCII del 30 = **0** al 39 = **9**.

A continuación se muestra un ejemplo de un mensaje de petición de pago recurrente:

```
<REQUEST>
  <DATOSENTRADA>
    <DS_MERCHANT_AMOUNT>145</DS_MERCHANT_AMOUNT>
    <DS_MERCHANT_ORDER>151029150450</DS_MERCHANT_ORDER>
    <DS_MERCHANT_MERCHANTCODE>327234688</DS_MERCHANT_MERCHANTCODE>
    <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
    <DS_MERCHANT_TRANSACTIONTYPE>3</DS_MERCHANT_TRANSACTIONTYPE>
    <DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
  </DATOSENTRADA>
  <DS_SIGNATUREVERSION>HMAC_SHA256_V1</DS_SIGNATUREVERSION>
  <DS_SIGNATURE>uegr2AawcuVR4pK1KN5KiOI7Kzj6Y+8z4HgHRFTYgIw=</DS_SIGNATURE>
</REQUEST>
```

8.3 Respuesta Host to Host

A continuación se presenta una tabla que recoge todos los parámetros que forman parte de la respuesta Host to Host.


Nombre del dato	Long. / Tipo	Descripción
<i>CODIGO</i>		Obligatorio. Indica si la operación ha sido correcta o no, (no indica si ha sido autorizada, solo si se ha procesado). Un 0 indica que la operación ha sido correcta. En el caso de que sea distinto de 0, tendrá un código. (Ver códigos de error en apartado 6 de esta Guía)
<i>Ds_Amount</i>	12 / A-N	Obligatorio. Para Euros las dos últimas posiciones se consideran decimales, salvo en el caso de los Yenes que no tienen.
<i>Ds_Currency</i>	4 / N	Obligatorio. Moneda del comercio.
<i>Ds_Order</i>	12 / A-N	Obligatorio. Número de pedido.
<i>Ds_Signature</i>	40 / A-N	Obligatorio. Firma del comercio.
<i>Ds_MerchantCode</i>	9 / N	Obligatorio. Código FUC asociado al comercio.
<i>Ds_Terminal</i>	3 / N	Obligatorio. Número de Terminal del comercio.
<i>Ds_Response</i>	4 / N	Obligatorio. Valor que indica el resultado de la operación. Indicará si ha sido autorizada o no. Los posibles valores de este campo se describen en la siguiente tabla.
<i>Ds_AuthorisationCode</i>	6 / N	Optativo. Código de autorización en caso de existir para las operaciones autorizadas.
<i>Ds_TransactionType</i>	1 / A-N	Obligatorio. Indica qué tipo de transacción se ha realizado. Los posibles valores son: A – Pago tradicional 1 – Preautorización 2 – Confirmación 3 – Devolución Automática 5 – Transacción Recurrente 6 – Transacción Sucesiva 9 – Anulación de Preautorización O – Autorización en diferido P - Confirmación de autorización en diferido Q - Anulación de autorización en diferido R – Autorización recurrente inicial diferido S – Autorización recurrente sucesiva diferido
<i>Ds_SecurePayment</i>		Obligatorio. Indica si el pago ha sido seguro o no: <ul style="list-style-type: none"> • 0: seguro (no se aplica) • 1: no seguro.
<i>Ds_Language</i>	1 / N	Obligatorio. Idioma.

Tipo A: caracteres ASCII del 65 = **A** al 90 = **Z** y del 97 = **a** al 122 = **z**.
Tipo N: caracteres ASCII del 30 = **0** al 39 = **9**.

Estos son los posibles valores del Ds_Response o "Código de respuesta":

CÓDIGO	SIGNIFICADO
0000 a 0099	Transacción autorizada para pagos y preautorizaciones
900	Transacción autorizada para devoluciones y confirmaciones
101	Tarjeta caducada
102	Tarjeta en excepción transitoria o bajo sospecha de fraude
106	Intentos de PIN excedidos
125	Tarjeta no efectiva
129	Código de seguridad (CVV2/CVC2) incorrecto
180	Tarjeta ajena al servicio
184	Error en la autenticación del titular
190	Denegación del emisor sin especificar motivo
191	Fecha de caducidad errónea
202	Tarjeta en excepción transitoria o bajo sospecha de fraude con retirada de tarjeta
904	Comercio no registrado en FUC
909	Error de sistema
913	Pedido repetido
944	Sesión Incorrecta
950	Operación de devolución no permitida
9912/912	Emisor no disponible
9064	Número de posiciones de la tarjeta incorrecto
9078	Tipo de operación no permitida para esa tarjeta
9093	Tarjeta no existente
9094	Rechazo servidores internacionales
9104	Comercio con "titular seguro" y titular sin clave de compra segura
9218	El comercio no permite op. seguras por entrada /operaciones
9253	Tarjeta no cumple el check-digit
9256	El comercio no puede realizar preautorizaciones
9257	Esta tarjeta no permite operativa de preautorizaciones
9261	Operación detenida por superar el control de restricciones en la entrada al SIS
9913	Error en la confirmación que el comercio envía al TPV Virtual (solo aplicable en la opción de sincronización SOAP)
9914	Confirmación "KO" del comercio (solo aplicable en la opción de sincronización SOAP)
9915	A petición del usuario se ha cancelado el pago
9928	Anulación de autorización en diferido realizada por el SIS (proceso batch)
9929	Anulación de autorización en diferido realizada por el comercio
9997	Se está procesando otra transacción en SIS con la misma tarjeta
9998	Operación en proceso de solicitud de datos de tarjeta
9999	Operación que ha sido redirigida al emisor a autenticar

Estos códigos de respuesta, además de en la propia respuesta Host to Host, se muestran en el campo "Código de respuesta" de la consulta de operaciones, siempre y cuando la operación no está autorizada, tal y como se muestra en la siguiente imagen:

Sesión / Fecha Totales	Fecha Hora	Tipo Operación Num. Pedido	Resultado NºAutorización o Cod.Respuesta	Importe	Neto Lote/Cajón
01-10-15	01-10-2015 16:50:16	Autorización Tradicional 151001165015	Sin Finalizar 9997		
01-10-15	01-10-2015 16:50:23	Autorización Tradicional 151001165022	Autorizada 581956	1,00 EUR	2 /

8.4 Web Service de petición de pago - WSDL

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definition targetNamespace="http://webservice.sis.sermepa.es"
xmlns:apachesoap="http://xml.apache.org/xml-soap"
xmlns:impl="http://webservice.sis.sermepa.es"
xmlns:intf="http://webservice.sis.sermepa.es"
xmlns:wSDL="http://schemas.xmlsoap.org/wsdl/"
xmlns:wSDLsoap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<wsdl:types>
<schema elementFormDefault="qualified"
targetNamespace="http://webservice.sis.sermepa.es"
xmlns="http://www.w3.org/2001/XMLSchema" xmlns:apachesoap="http://xml.apache.org/xml-
soap" xmlns:impl="http://webservice.sis.sermepa.es"
xmlns:intf="http://webservice.sis.sermepa.es"
xmlns:wSDL="http://schemas.xmlsoap.org/wsdl/">
<element name="trataPetición">
<complexType>
<sequence>
<element name="datoEntrada" nillable="true" type="xsd:string"/>
</sequence>
</complexType>
</element>
<element name="trataPeticiónResponse">
<complexType>
<sequence>
<element name="trataPeticiónReturn" nillable="true" type="xsd:string"/>
</sequence>
</complexType>
</element>
<element name="consultaDCC">
<complexType>
<sequence>
<element name="datoEntrada" nillable="true" type="xsd:string"/>
</sequence>
</complexType>
</element>
<element name="consultaDCCResponse">
<complexType>
<sequence>
<element name="consultaDCCReturn" nillable="true" type="xsd:string"/>
</sequence>
</complexType>
</element>
</schema>
</wsdl:types>
<wsdl:message name="consultaDCCRequest">
<wsdl:part element="intf:consultaDCC" name="parameters"/>
</wsdl:message>
<wsdl:message name="trataPeticiónResponse">
<wsdl:part element="intf:trataPeticiónResponse" name="parameters"/>
</wsdl:message>
<wsdl:message name="trataPeticiónRequest">
<wsdl:part element="intf:trataPetición" name="parameters"/>
</wsdl:message>
<wsdl:message name="consultaDCCResponse">
<wsdl:part element="intf:consultaDCCResponse" name="parameters"/>
</wsdl:message>
<wsdl:portType name="SerClsWSEntrada">
<wsdl:operation name="trataPetición">
<wsdl:input message="intf:trataPeticiónRequest" name="trataPeticiónRequest"/>
<wsdl:output message="intf:trataPeticiónResponse" name="trataPeticiónResponse"/>
</wsdl:operation>
<wsdl:operation name="consultaDCC">
<wsdl:input message="intf:consultaDCCRequest" name="consultaDCCRequest"/>
<wsdl:output message="intf:consultaDCCResponse" name="consultaDCCResponse"/>
</wsdl:operation>
</wsdl:portType>
<wsdl:binding name="SerClsWSEntradaSoapBinding" type="intf:SerClsWSEntrada">
<wsdlsoap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
<wsdl:operation name="trataPetición">
<wsdlsoap:operation soapAction="" />
<wsdl:input name="trataPeticiónRequest">
```

```
<wsdlsoap:bodyuse="literal"/>
</wsdl:input>
<wsdl:outputname="trataPeticionResponse">
<wsdlsoap:bodyuse="literal"/>
</wsdl:output>
</wsdl:operation>
<wsdl:operationname="consultaDCC">
<wsdlsoap:operationsoapAction=""/>
<wsdl:inputname="consultaDCCRequest">
<wsdlsoap:bodyuse="literal"/>
</wsdl:input>
<wsdl:outputname="consultaDCCResponse">
<wsdlsoap:bodyuse="literal"/>
</wsdl:output>
</wsdl:operation>
</wsdl:binding>
<wsdl:serviceName="SerClsWSEntradaService">
<wsdl:portbinding="intf:SerClsWSEntradaSoapBinding" name="SerClsWSEntrada">
<wsdlsoap:addresslocation="https://sis.redsys.es/sis/services/SerClsWSEntrada"/>
</wsdl:port>
</wsdl:service>
</wsdl:definitions>
```