TPV-Virtual

Manual de Integración - WebService

Versión: 3.0.1
Fecha: 26/11/2020
Referencia: RS.TE.CEL.MAN.0038

Redsys, Servicios de Procesamiento, S.L. – c/ Francisco Sancha, 12 – 28034 Madrid (España)

www.redsys.es

Control de versión

Versión	Fecha	Afecta	Breve descripción del cambio
1.0	01/06/2018	TODO	Versión Inicial
1.1	24/09/2018	Punto 8.1	Código ASCII del Ds_Merchant_Order
1.2	26/09/2018	Punto 8.1	Dato opcional Ds_Merchant_Cvv2
1.3	27/09/2018	Punto 8.4	Dato opcional Ds_CardNumber y Ds_ExpiryDate
1.4	29/01/2019	Punto 8.3	Se añade en el parámetro Ds_Merchant_TransactionType el tipo de Anulación de Autorización
1.5	14/03/2019	Punto 8,9,10,11	Se rehace el punto 8, eliminando los puntos de Monedas e Idiomas y se creando un punto 9. Se añaden los puntos 10 y 11
2.0	27/03/2019	Varios puntos	Añadida la información sobre EMV3DS y PSD2. Cambios en el apartado de transacciones con DCC. Añadida la información sobre Autenticaciones con DCC. Añadido apartado Timeout. Añadida referencia a los nuevos documentos TPV-Virtual GuiaErroresSIS.xlsx y TPV-Virtual Parámetros Entrada-Salida.xlsx
2.1	12/04/2019	Puntos 5, 9,10.	Nota importante sobre integración EMV3DS Añadidas tarjetas de pruebas para EMV3DS La hoja de cálculo de los errores SIS, se modifica para incluirla en la hoja de cálculo Parámetros de entrada-salida

2.2	25/07/2019	PSD2 y MIT	Operaciones COF y MIT Cálculo Firma de ChallengeRequest Parámetro creq
2.3	04/10/2019	Todo el documento	Se añaden adaptaciones para EVM3DS 2.2
2.4	12/11/2019	5.1, 5.2, 8, 9	Se marcan los avances para las funcionalidades EMV 3DS
2.5	24/01/2020	Puntos 5,6,8,9,10	PUNTOS 5, 6 añadido el parámetro Ds_Card_PSD2 PUNTOS 5, MIT y tokenización Peticiones con EXENCIONES. Aclaración y ejemplos para funcionalidades de avances EMV3DS. Modificación tarjetas de pruebas para los avances EMV3DS.
2.5.1	07/0/2020	Puntos 14	Se añade error por no utilizar sección CDATA
2.6	10/02/2020	Puntos 6,7	Definición de nuevos parámetros opcionales “cambioBCE” y “porcentajeSobreBCE” para operaciones DCC con monedas de la Unión Europea. Se modifica la estructura del punto 11
3.0	01/10/2020	Todo el documento	Se elimina la marca “avance” en las funcionalidades afectadas por PSD2. Las librerías de ayuda a la integración se incluyen en Anexo 2. El punto 9 queda pendiente de especificaciones de las marcas. En el apartado de pruebas, se incluyen tarjetas de las distintas marcas.
3.0.1	26/11/2020	Punto 6	Se incluye nota IMPORTANTE: operación que inicia flujo en versión 2 y en el proceso de autenticación cambia el flujo a versión 1. Se añade tarjeta de prueba para este caso

ÍNDICE

1. Introducción

1.1 Objetivo

Este documento recoge los aspectos técnicos necesarios para que un comercio realice la integración con el TPV Virtual mediante conexión Web Service SOAP.

Esta forma de conexión permite a los comercios tener integrado el TPV Virtual dentro de su propia aplicación Web. Además, este modo de conexión ofrece la posibilidad de autenticar al titular mediante el protocolo 3DS, el proceso de autenticación del titular se realiza directamente con el banco emisor de su tarjeta en el momento de realizar la transacción y dota de mayor seguridad a las compras.

NOTA IMPORTANTE: Con motivo de la entrada en pleno vigor de la directiva de Europea de Pagos PSD2 a lo largo de 2020, se incluyen en esta guía algunas nuevas características y especificaciones técnicas que estarán disponibles a lo largo del 2020, para facilitar la preparación de los trabajos en aquellos casos de comercios que deseen incorporar ciertas posibilidades a su operativa de pago, especialmente en lo referente a la gestión de las autenticaciones y exenciones a la autenticación que la PSD2 contempla.

1.2 Definiciones, siglas y abreviaturas

- **SIS**. Servidor Integrado de Redsys (Servidor del TPV Virtual).
- **SCA**. Strong Customer Authentication. Autenticación reforzada del titular.
- **Frictionless**. Autenticación sin intervención del titular.
- **Challenge**. Autenticación reforzada del titular (mediante OTP, contraseña estática, biometría, etc).
- **PSD2**. Payment Service Providers. Regulación europea en los servicios de pagos digitales.
- **3DSecure**: Sistema de seguridad para los pagos online. En adelante EMV3DS.
- **EMV3DS**: Siglas para identificar la nueva versión de 3DSecure en el TPV-Virtual.
- **MIT**. Merchant Initiated Transaction. Se refiere a las transacciones iniciadas directamente por el comercio sin que el titular esté presente como por ejemplo en el caso de pagos recurrentes.
- **COF**. Credentials On File. Se refiere a la operativa en la que se almacenan los datos de tarjeta para futuros usos.

- **DCC.** Dynamic Currency Conversion. Permite que el titular realice el pago en su propia moneda en lugar de la definida en el terminal.

1.3 Referencias

- Documentación de Integración con el SIS
- TPV-Virtual Guía SIS.
- Guía Especificaciones COF Ecom.
- TPV-Virtual Parámetros Entrada-Salida.xlsx

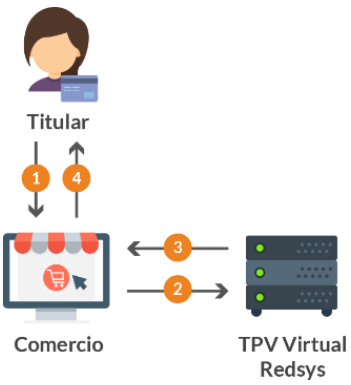
2. Envío de petición de pago Web Service

Esta forma de conexión permite a los comercios tener integrado el TPV Virtual dentro de su propia aplicación Web, así todo el proceso de pago se realiza en la misma web del comercio y el cliente no abandona en ningún momento este entono web. Este modo de conexión también ofrece la posibilidad de autenticar al titular mediante el protocolo 3DSecure, que dota de mayor seguridad a las compras.

Es importante tener en cuenta que en este tipo de integración es el comercio el que recoge los datos de tarjeta del cliente para procesar el pago y, por tanto, tiene afectación en su cumplimiento de PCI-DSS.

Los comercios también pueden utilizar este modo de conexión para integrar el TPV Virtual con su backoffice y realizar operaciones asociadas como devoluciones o confirmaciones de Preautorización. En este caso, no es necesario que el comercio maneje los datos de tarjeta, por lo que si sólo utiliza la integración REST para este tipo de operaciones no tendría afectación de cara a cumplimiento de PCI-DSS.

El esquema básico de un pago mediante integración Web service sería el siguiente:



1. El titular selecciona los productos que desea comprar e introduce los datos de tarjeta en un formulario mostrado por el comercio.
2. El comercio envía los datos al pago al TPV virtual.
3. Una vez realizado el pago, el TPV virtual informa del resultado de la operación al comercio.
4. El comercio devuelve la información del resultado del pago al titular.

3. Estructura de una petición Web Service

El comercio debe enviar al TPV Virtual los datos de la petición de pago vía Web Service con codificación UTF-8. 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>1444904795</DS_MERCHANT_ORDER>
            <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
            <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
            <DS_MERCHANT_PAN>XXXXXXXXXXXXXXXX</DS_MERCHANT_PAN>
            <DS_MERCHANT_CVV2>XXX</DS_MERCHANT_CVV2>
            <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
            <DS_MERCHANT_TERMINAL>871</DS_MERCHANT_TERMINAL>
            <DS_MERCHANT_EXPIRYDATE>XXXX</DS_MERCHANT_EXPIRYDATE>
    </DATOSENTRADA>
    <DS_SIGNATUREVERSION>HMAC_SHA256_V1</DS_SIGNATUREVERSION>
    <DS_SIGNATURE>
            VV3acxBgABrS5VYcLyJD1KqIsa2pPdvajPBG510lFfg=
    </DS_SIGNATURE>
</REQUEST>
```

NOTA: la conexión requiere del uso de un sistema de firma basado en HMAC SHA-256, que autentica entre sí al servidor del comercio y al TPV Virtual. Para desarrollar el cálculo de este tipo de firma, el comercio puede realizar el desarrollo por sí mismo utilizando las funciones estándar de los diferentes entornos de desarrollo, si bien para facilitar los desarrollos ponemos a su disposición librerías (PHP, JAVA y .NET). Ver Anexos. Estas librerías también están disponibles en la siguiente dirección:

https://pagosonline.redsys.es/descargas.html

3.1 Identificar la versión de algoritmo de firma a utilizar (Ds_SignatureVersion)

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 3.

3.2 Montar la cadena de datos de la petición (DATOSENTRADA)

Se debe montar una cadena con todos los datos de la petición en formato XML dando como resultado el elemento **<DATOSENTRADA>**.

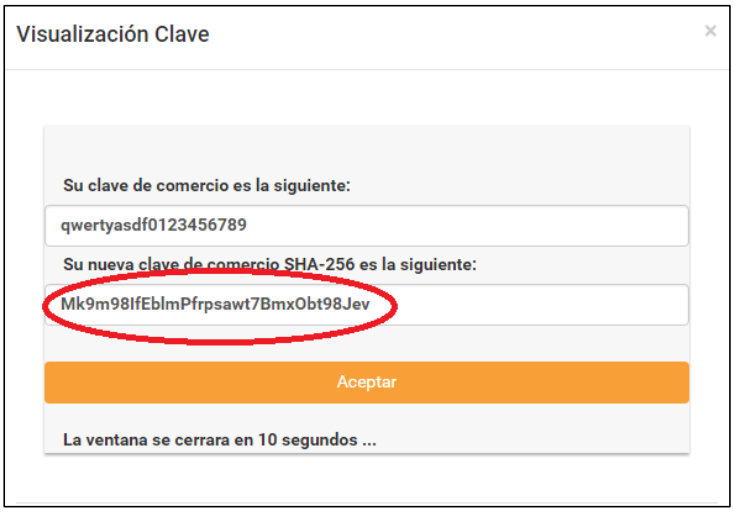
Se debe tener en cuenta que existen varios tipos de peticiones y según el tipo varía la estructura del mensaje y los parámetros que se envían y reciben.

Podemos diferenciar tres tipos de peticiones:

- Peticiones de pago (con envío de datos de tarjeta). Ver *guía Tpv-Virtual. Parámetros Entrada-salida.xlsx.*
- Peticiones de Confirmación/Devolución. Ver *guía Tpv-Virtual. Parámetros Entrada-salida.xlsx.*
- Peticiones de pagos recurrentes (con envío referencia. Ver *guía Tpv-Virtual. Parámetros Entrada-salida.xlsx.*

3.3 Firmar los datos de la petición (Ds_Signature)

Para calcular la firma es necesario utilizar una clave específica para cada terminal. Para obtener esta clave tiene que acceder al Portal de Administración, opción Consulta datos de Comercio, en el apartado "Ver clave", puede consultar esta clave, tal y como se muestra en la siguiente imagen:



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.***

Una vez se tiene montado 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 3.

NOTA: Puede utilizar las librerías de ayuda para generar la firma, ver Anexo 2. Punto 1

4. Estructura de respuesta Web Service

Una vez enviada la petición el TPV Virtual, la interpretará y realizará las validaciones necesarias para, a continuación, procesar la operación. Dependiendo del resultado de la operación, se construye mensaje en formato XML de respuesta con el resultado de la misma con codificación UTF-8. En él se incluirán los siguientes campos:

- RETORNOXML: Elemento raíz del mensaje de respuesta.
- CODIGO: Elemento que indica si la transacción se ha procesado correctamente.
- OPERACION: Elemento con los parámetros de respuesta de la transacción. Entre sus parámetros se encentra el elemento Ds_Signature, que incluye la firma de los datos enviados.

Ejemplo de respuesta de pago **(comercio configurado sin envío de datos de tarjeta):**


```
<RETORNOXML>
        <CODIGO>0</CODIGO>
        <OPERACION>
                <Ds_Amount>145</Ds_Amount>
                <Ds_Currency>978</Ds_Currency>
                <Ds_Order>1444912789</Ds_Order>
                <Ds_Signature>
                        bAuiQOymGvYzqHi7dEeuWrRYFeUjtFH6NyOoWSl0vHU=
                </Ds_Signature>
                <Ds_MerchantCode>999008881</Ds_MerchantCode>
                <Ds_Terminal>871</Ds_Terminal>
                <Ds_Response>0000</Ds_Response>
                <Ds_AuthorisationCode>050372</Ds_AuthorisationCode>
                <Ds_TransactionType>0</Ds_TransactionType>
                <Ds_SecurePayment>0</Ds_SecurePayment>
                <Ds_Language>1</Ds_Language>
                <Ds_Card_Type>D</Ds_Card_Type>
                <Ds_MerchantData></Ds_MerchantData>
                <Ds_Card_Country>724</Ds_Card_Country>
                <Ds_Card_Brand>1</Ds_Card_Brand>
        </OPERACION>
</RETORNOXML>
```


Ejemplo de respuesta de pago **(comercio configurado con envío de datos de tarjeta):**


```
<RETORNOXML>
        <CODIGO>0</CODIGO>
        <OPERACION>
                <Ds_Amount>145</Ds_Amount>
                <Ds_Currency>978</Ds_Currency>
                <Ds_Order>1449821545</Ds_Order>
                <Ds_Signature>
                        6quLImPCOSTFpwhC7+ai1L+SPdKbcGx2sgC2A/1hwQo=
                </Ds_Signature>
                <Ds_MerchantCode>999008881</Ds_MerchantCode>
                <Ds_Terminal>871</Ds_Terminal>
                <Ds_Response>0000</Ds_Response>
                <Ds_AuthorisationCode>109761</Ds_AuthorisationCode>
                <Ds_TransactionType>0</Ds_TransactionType>
                <Ds_SecurePayment>0</Ds_SecurePayment>
                <Ds_Language>1</Ds_Language>
                <Ds_CardNumber>454881********04</Ds_CardNumber>
                <Ds_MerchantData></Ds_MerchantData>
                <Ds_Card_Country>724</Ds_Card_Country>
                <Ds_Card_Brand>1</Ds_Card_Brand>
        </OPERACION>
</RETORNOXML>
```


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

- Código **(<CODIGO>)**: Indica si la operación se ha procesado correctamente o no, (no indica si ha sido autorizada, solo si se ha procesado). Un valor 0 en esta respuesta, indica que la operación ha sido correcta, cualquier otro valor distinto de 0 se trata de un error en el

procesamiento de la operación (ver códigos de error en la *guía "TPV-Virtual Parámetros Entrada-Salida.xlsx". aptdo códigos de error)*

- 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 revisando el valor del campo Ds_Response.

Valor de Ds_Response	Descripción
Valor de 0 a 100	Operación autorizada en pagos y preautorizaciones.
Valor 900	Operación autorizada en devoluciones, confirmaciones y autenticación PUCE
Valor 400	Operación autorizada en anulaciones
Cualquier otro valor	Revisar listado detallado en "*TPV-Virtual Parámetros Entrada-Salida.xlsx*"

NOTA: La relación de parámetros que forman parte de la respuesta están disponibles en la guía "TPV-Virtual Parámetros Entrada-Salida.xlsx"

4.1 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. **El comercio es responsable de validar el HMAC enviado por el TPV Virtual para asegurarse de la validez de la respuesta. Esta validación es necesaria para garantizar que los datos no han sido manipulados y que el origen es realmente el TPV Virtual.**

Para realizar el cálculo de la firma de respuesta se deben seguir 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_ORDER).

2. Se calcula el HMAC SHA256 de la cadena formada por la concatenación del valor de los siguientes campos:

- Si está usando el método "iniciaPeticion" con resultado de Ds_EMV3DS y threeDSInfo="CardConfiguration":

Cadena = CODIGO + Ds_MerchantCode + Ds_Terminal + Ds_Order + Ds_TransactionType

- Si está usando el método "trataPetición" con resultado de Ds_EMV3DS y threeDSInfo="**ChallengeRequest**":

Cadena = Ds_Amount + Ds_Order + Ds_MerchantCode + Ds_Currency+ Ds_TransactionType + MD

- Si está usando el método "**trataPeticion**" con campo Ds_response:

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 = 1451444912789999008881978000000

Si el comercio tiene configurado envío de tarjeta en la respuesta, se debe calcular 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_CardNumber + Ds_TransactionType + Ds_SecurePayment

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

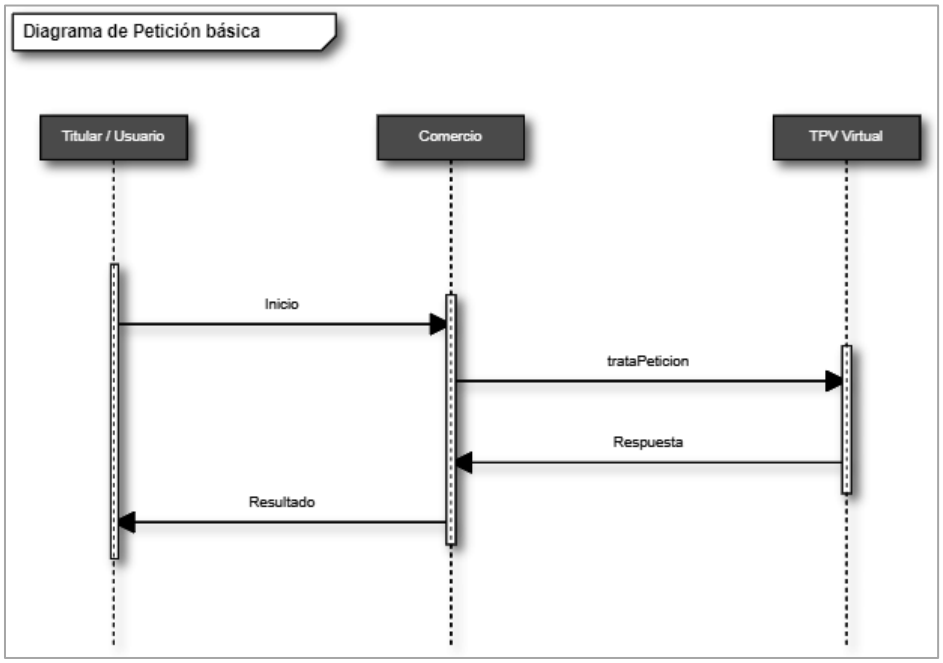
Cadena = 1451449821545999008881978000045488120494000040 0

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: Puede utilizar las librerías de ayuda para validar la firma, ver Anexo 2. Punto 2

5. Transacciones Directas (Sin Autenticación)

El siguiente esquema presenta el flujo general de una operación realizada mediante conexión Web Service de Redsys, sin autenticación del titular:



Para realizar una petición en la que no es necesario autenticar al titular (ej: pago sin autenticación, devolución, confirmación de preautorización, etc.), el comercio deberá preparar la petición con los parámetros necesarios según se ha indicado en el punto 3 y enviarla a los siguientes endpoints, dependiendo de si se quiere realizar una petición en el entorno de prueba u operaciones reales:

URL Conexión	Método	Entorno
https://sis-t.redsys.es:25443/sis/services/SerClsWSEntradaV2	trataPeticion	Pruebas
https://sis.redsys.es/sis/services/SerClsWSEntradaV2	trataPeticion	Real

- El método "**trataPeticion**", permite la realización del procesamiento de la operación indicada a través del Web Service.

La descripción exacta de este tipo de peticiones XML se presenta mediante el fichero WSDL de Anexo 1: Web Service de petición de pago y autenticación – WSDL

6. Transacciones con Autenticación 3DSecure 1.0 y EMV3DS

6.1 Pasos para realizar una transacción con autenticación

La integración mediante una conexión Web service permite realizar pagos con autenticación del titular utilizando el protocolo 3DSecure definido por las marcas. Este modo de conexión está preparado para utilizar las diferentes versiones de dicho protocolo, tanto la versión 3DS 1 como la EMV 3DS 2.

Para realizar la autenticación es necesario incorporar en el flujo de pago varios pasos adicionales, que se explican a continuación. Dependiendo de la versión del protocolo 3DS utilizado, este flujo puede variar ligeramente, aunque los pasos principales se mantienen.

Es importante tener en cuenta que aquel comercio que quiera realizar autenticaciones mediante una conexión Web service, tiene que estar adaptado a las dos versiones de protocolo 3DS, puesto que la versión utilizada en cada operación dependerá de la versión de protocolo 3DS de la tarjeta implicada en la misma.

Los pagos con autenticación EMV3DS en la conexión Web service sigue los siguientes pasos:

- **Paso 1: Iniciar petición**

El comercio deberá hacer una petición al TPV Virtual para obtener información sobre las posibilidades de la tarjeta en cuanto a autenticación (versión protocolo 3DS), posibilidad de aplicación de exenciones, operativas especiales (por ej. si permite DCC) y por tanto como deben gestionarse los siguientes pasos.

- **Paso 2: 3DSMethod (Si está incluida en protocolo EMV3DS)**

El comercio ejecuta el 3DSMethod para que el emisor capture la información del dispositivo utilizado por el titular: User-Agent, modelo de dispositivo, etc. Más información sobre este paso en los apartados posteriores.

- **Paso 3: Solicitud de autorización**

El comercio enviará la solicitud de autorización de la operación incluyendo el resultado del 3DSMethod y otros datos adicionales del protocolo EMV3DS, así como una posible solicitud de exención SCA dentro del marco de la PSD2.

El TPV Virtual iniciará la autenticación, donde se podrá obtener como resultado:

a. Autenticación OK (Frictionless): la operación ha sido autenticada sin necesidad de solicitar ninguna acción al titular de la tarjeta y el TPV Virtual continuará el proceso de autorización.

b. Challenge Required: La entidad emisora requiere verificar la autenticidad del cliente mediante una autenticación explícita o reto (challenge).

c. Otro resultado: autenticación no disponible, autenticación rechazada, error en la autenticación, etc.

El TPV Virtual decidirá, según el caso, autorizar o rechazar la operación.

- **Paso 4: Autenticación (Si procede)**

En este paso la Entidad emisora verifica la autenticidad del titular de la tarjeta mediante una autenticación con participación del titular de la tarjeta (challenge) como OTP por SMS (One Time Password), contraseña estática, biometría, combinación de los anteriores, etc.

- **Paso 5: Confirmación de autorización**

El comercio enviará la autorización, con el resultado del challenge, al TPV Virtual para finalizar el proceso de autorización.

***NOTA IMPORTANTE*: El comercio debe estar preparado para realizar cualquiera de los flujos que se muestran en los siguientes apartados, puesto que en función de la respuesta obtenida en el paso "Iniciar Petición" se deberá utilizar el flujo del protocolo 3DSecure 1.0 o EMV3DS.**

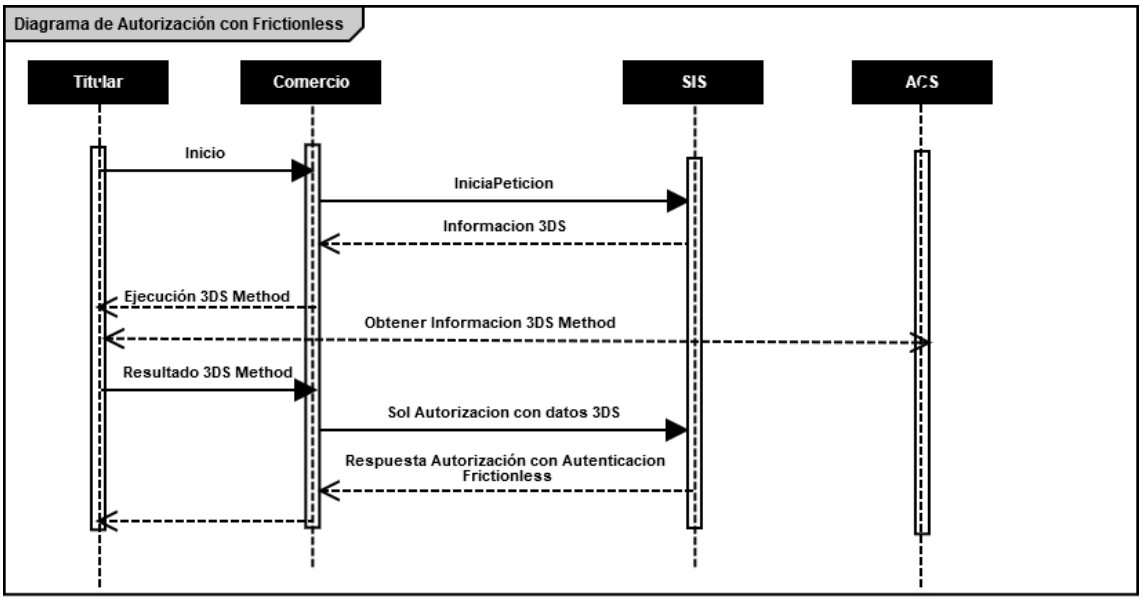
Además, en el caso del protocolo EMV3DS, el comercio también deberá estar preparado para soportar ambos procesos de Autenticación: Challenge (con intervención del titular) o Frictionless (sin intervención del titular). El emisor de la tarjeta será el encargado de determinar el proceso de Autenticación que se deberá llevar a cabo.

NOTA: Recomendamos que en el paso 3 el comercio proporcione toda la información adicional posible para ayudar al emisor a identificar que la operación se está realizando por el auténtico titular de la tarjeta. Esta información adicional aumentará la probabilidad de un flujo frictionless (autenticación sin intervención del titular, ayudando así a reducir la tasa de abandono

El tiempo máximo desde el inicio de la petición y la solicitud de autorización es de 1 hora. Pasado este tiempo la petición se da como perdida y se deberá volver a realizar el flujo desde el principio.

Ejemplo del flujo de una Autorización con autenticación EMV3DS Frictionless

El siguiente esquema presenta el flujo general de una operación con autenticación frictionless realizada a través del TPV Virtual.



1. El titular selecciona los productos que desea comprar e introduce los datos de tarjeta en un formulario mostrado por el comercio.
2. El comercio realiza un inicia petición enviando los datos al TPV Virtual.
3. El TPV Virtual comprueba la configuración de la tarjeta, y en la respuesta informará si la tarjeta soporta autenticación EMV3DS y la versión de protocolo EMV3DS que se aplica.

   3.1 Si la tarjeta lo requiere ejecutar el 3DSMethod: se inicia conexión desde el browser con el ACS y este devuelve el resultado de la ejecución al comercio

4. El comercio envía la solicitud de autorización con tarjeta que soporta EMV3DS. Además de los datos de pago es necesario enviar el resultado del 3DSMethod y los datos adicionales para la autenticación.

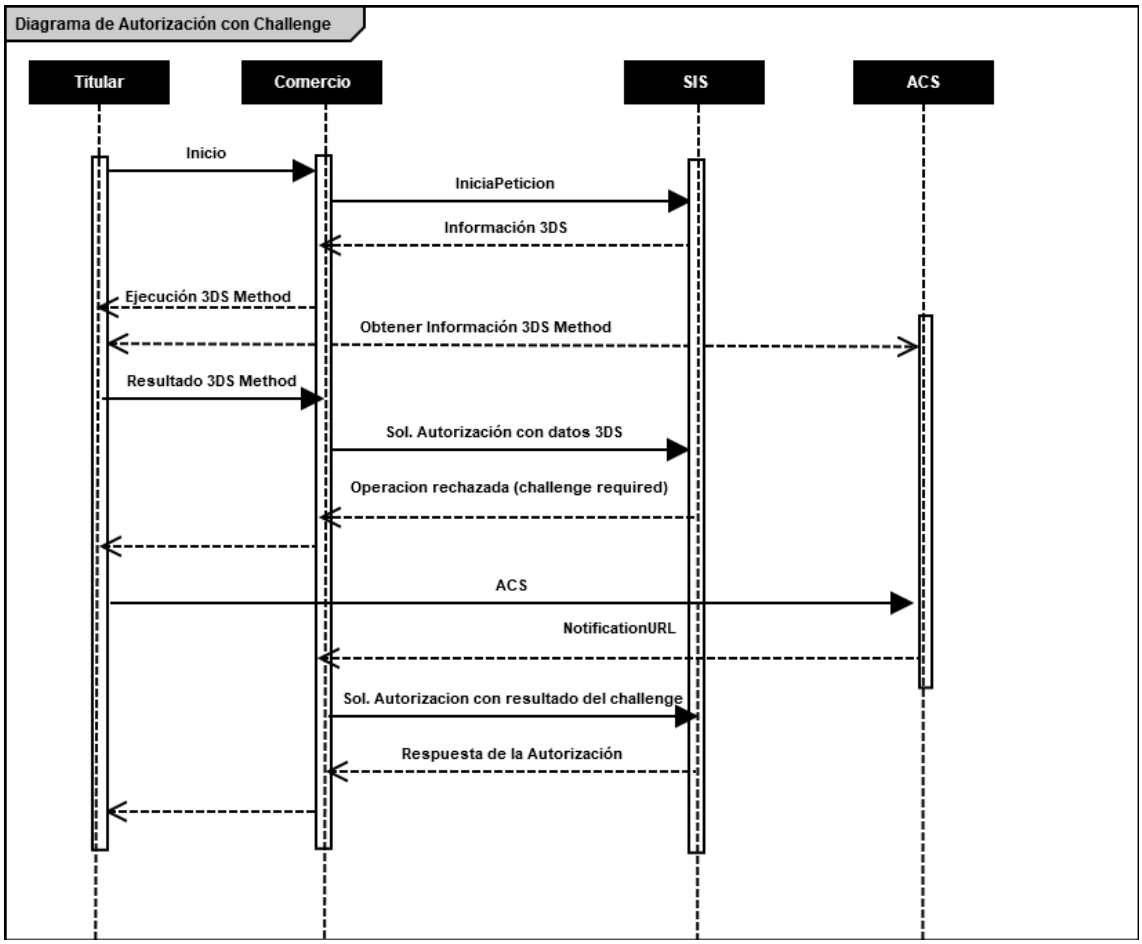
   El TPV Virtual inicia la autenticación, y el emisor, en base a los datos recibidos, autentica la operación sin necesidad de intervención del titular. A continuación, el TPV Virtual procesará la autorización

5. Una vez realizado el pago, el TPV virtual informa del resultado de la operación.
6. El comercio devuelve la información del resultado del pago al titular.

NOTA: en los diagramas solo se tienen en cuenta los flujos del comercio y los actores con lo que interviene en contacto directo.

Ejemplo del flujo de una Autorización con autenticación EMV3DS Challenge

El siguiente esquema presenta el flujo general de una operación con autenticación por challenge realizada a través del TPV Virtual.



1. El titular selecciona los productos que desea comprar e introduce los datos de tarjeta en un formulario mostrado por el comercio.
2. El comercio realiza un inicia petición enviando los datos al TPV Virtual.
3. El TPV Virtual comprueba la configuración de la tarjeta, y en la respuesta informará si la tarjeta soporta autenticación EMV3DS y la versión de protocolo EMV3DS que se aplica.

   3.1 Si la tarjeta lo requiere ejecutar el 3DSMethod: se inicia conexión desde el browser con el ACS y este devuelve el resultado de la ejecución al comercio

4. El comercio envía la solicitud de autorización con tarjeta que soporta EMV3DS. Además de los datos de pago es necesario enviar el resultado del 3DSMethod y los datos adicionales para la autenticación.

   El TPV Virtual inicia la autenticación, y el emisor en base a los datos recibidos decide que el titular debe verificar su autenticidad (challenge)

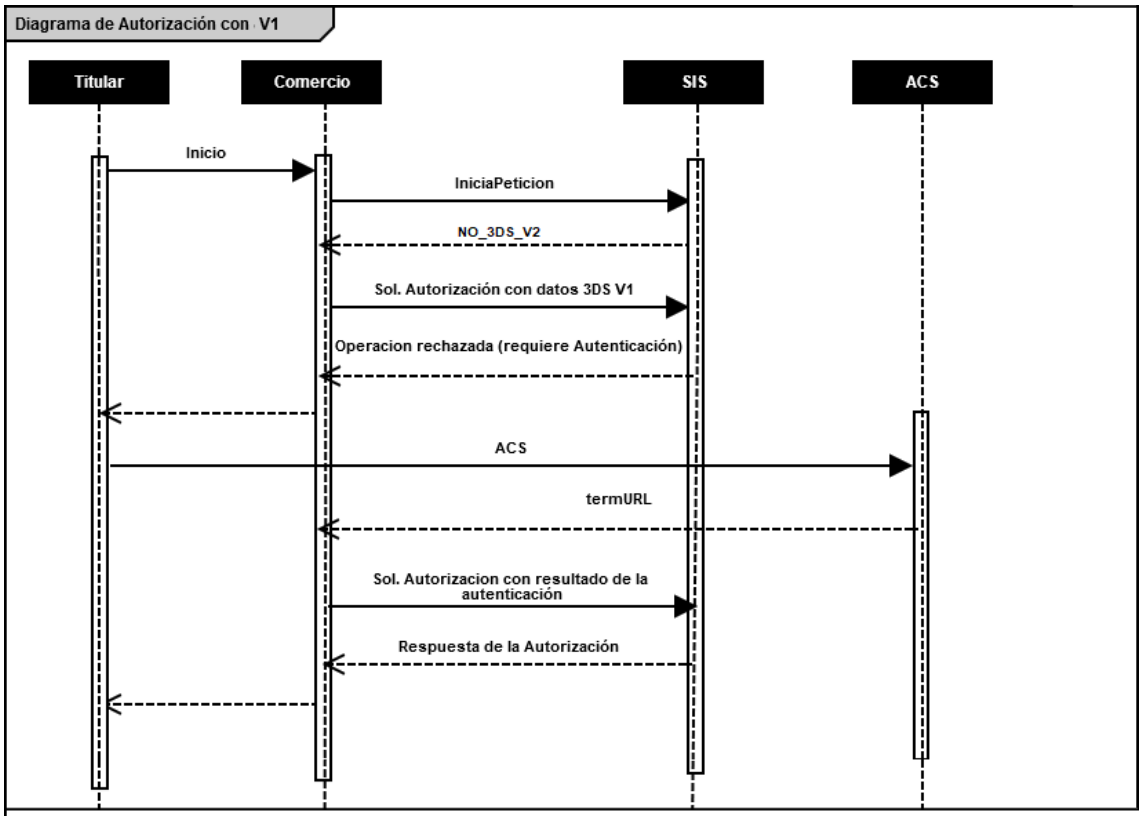
5. El TPV Virtual devuelve la información para que el titular pueda realizar el challenge con su banco emisor. En este momento, y hasta que se reciba la respuesta de la autenticación en el paso 9, las peticiones quedarán marcadas en el Portal de administración como "Sin Finalizar" con el código = 8210.
6. El comercio redirige al titular vía browser para que conecte con su emisor
7. El titular completa el challenge (autenticación)
8. La entidad emisora devuelve el resultado del challenge (autenticación) a la url indicada por el comercio
9. El comercio envía el resultado del challenge (autenticación) al TPV Virtual para finalizar el proceso de autorización
10. Una vez realizado el pago, el TPV virtual responde con el resultado de la operación.
11. El comercio responde con la información del resultado del pago al titular

NOTA: en los diagramas solo se tienen en cuenta los flujos del comercio y los actores con lo que interviene en contacto directo.

IMPORTANTE : Hay transacciones en las que en la respuesta del InicaPetición se informa que la versión de la tarjeta es EMV 3DS y **el comercio envía la petición con datos EMV 3DS**, posteriormente, **en el proceso de la autenticación, la marca puede indicarnos que no es posible completar la autenticación con versión 2**. En este caso **el flujo de la operación continuará en versión 1.0** (en la respuesta el comercio espera recibir datos Creq, pero recibe un Pareq, en este caso el proceso de autenticación tiene que realizarse en versión 1). Por lo tanto **es necesario** que, para poder tratar correctamente este tipo de situaciones, **el comercio esté preparado para realizar el flujo de la operación tanto en versión EMV 3DS como en versión 3DS v1.0.**

Ejemplo del flujo de una Autorización con autenticación 3DSecure 1.0

El siguiente esquema presenta el flujo general de una operación con autenticación EMV3DS v1, en la que se ha determinado que es necesario realizar la autenticación del titular.



1. El titular selecciona los productos que desea comprar e introduce los datos de tarjeta en un formulario mostrado por el comercio.
2. El comercio realiza un inicia petición enviando los datos al TPV Virtual.
3. El TPV Virtual comprueba la configuración de la tarjeta, y en la respuesta informará de la versión de protocolo de autenticación que soporta la operación.

   3.1 Si la tarjeta no permite EMV3DS el comercio puede solicitar la autenticación con los datos de 3DSecure 1.0. Se recibirá un valor de protocolo NO_3DS_V2

4. El comercio envía la solicitud de autorización al TPV Virtual indicando que está preparado para3DSecure 1.0.
5. El TPV Virtual devolverá la información necesaria para que el titular pueda realizar la autenticación con su banco emisor. En este momento, y hasta que se reciba la respuesta de la autenticación en el paso 9, las peticiones quedarán marcadas en el Portal de administración como “Sin Finalizar” con el código = 8102.
6. El comercio redirige al titular vía browser para que conecte con su emisor.

7. El titular completa la autenticación.
8. La entidad emisora devuelve el resultado de la autenticación a la URL indicada facilitada por el comercio.
9. El comercio envía el resultado de la autenticación al TPV Virtual para finalizar el proceso de autorización.
10. Una vez realizado el pago, el TPV virtual responde con el resultado de la operación.
11. El comercio responde con la información del resultado del pago al titular

NOTA: en los diagramas solo se tienen en cuenta los flujos del comercio y los actores con lo que interviene en contacto directo.

6.2 Ejemplos de peticiones para realizar una transacción con autenticación EMV3DS

Iniciar Petición

Esta petición permite obtener el tipo de autenticación 3D Secure que se puede realizar, además de la URL del 3DSMethod en caso de que exista.

El inicia petición se hace a través de una petición Webservice SOAP al TPV Virtual. En dicha petición deberá incluir los siguientes parámetros:

- <DS_SIGNATUREVERSION>: Constante que indica la versión de firma que se está utilizando.
- <DATOSENTRADA>: Datos de la petición de pago. Ver guía *Tpv-Virtual. Parámetros Entrada-salida.xlsx*
- <DS_SIGNATURE>.: Firma de los datos enviados.

Dichos parámetros deben enviarse a los siguientes URL dependiendo de si se quiere realizar una petición en el entorno de prueba u operaciones reales, llamando al método "***iniciaPeticion***":

URL Conexión	Método	Entorno
https://sis-t.redsys.es:25443/sis/services/SerClsWSEntradaV2	iniciaPeticion	Pruebas
https://sis.redsys.es/sis/services/SerClsWSEntradaV2	iniciaPeticion	Real

Una vez gestionada la petición, el TPV Virtual informará al servidor del comercio del resultado de la misma con la información del resultado incluida en un fichero XML (RETORNOXML). En él se incluirán los siguientes campos:

- CODIGO: Código de respuesta o error SIS
- OPERACION: Datos de respuesta de la operación. En este campo se incluirá el parámetro de salida *Ds_Signature* con la firma de la petición de respuesta.

A continuación, se describen los datos que debe incluir el DATOSENTRADA para enviar un inicia petición:

```
<DATOSENTRADA>
 <DS_MERCHANT_AMOUNT>1000</DS_MERCHANT_AMOUNT>
 <DS_MERCHANT_ORDER>1552571678</DS_MERCHANT_ORDER>
 <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
 <DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
 <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
 <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
 <DS_MERCHANT_PAN> XXXXXXXXXXXXXXXXXX </DS_MERCHANT_PAN>
 <DS_MERCHANT_EMV3DS>{'threeDSInfo':'CardData'}</DS_MERCHANT_EMV3DS>
</DATOSENTRADA>
```

Como respuesta se obtendrá lo siguiente:

```
<RETORNOXML>
 <CODIGO>0</CODIGO>
 <INFOTARJETA>
  <Ds_Order>1553155286</Ds_Order>
  <Ds_MerchantCode>999008881</Ds_MerchantCode>
  <Ds_Terminal>2</Ds_Terminal>
  <Ds_TransactionType>0</Ds_TransactionType>
  <Ds_EMV3DS>{"protocolVersion":"2.1.0",
          "threeDSServerTransID":"8de84430-3336-4ff4-b18d-f073b546ccea",
          "threeDSInfo":"CardConfiguration",
          "threeDSMethodURL":"https://sis.redsys.es/sis-simulador-web/threeDsMethod.jsp"}</Ds_EMV3DS>
  <Ds_Card_PSD2>Y</Ds_Card_PSD2>
  <Ds_Signature>7155jJYTzqeO/FoKjIQwUrjRJU7CxiOLHlC00d5c/RU=</Ds_Signature>
 </INFOTARJETA>
</RETORNOXML>
```

El parámetro **Ds_EMV3DS** estará compuesto por los siguientes campos:

- **protocolVersion**: siempre indicará el número de versión mayor permitido en la operación. El comercio será responsable de utilizar el número de versión para el cual esté preparado.
- **threeDSServerTransID**: identificador de la transacción EMV3DS.
- **threeDSInfo**: CardConfiguration.
- **threeDSMethodURL**: URL del 3DSMethod.

El parámetro **Ds_Card_PSD2** informará al comercio si la tarjeta informada en la petición está afectada o no por PSD2. Los valores posibles serán "Y" para indicar que la tarjeta está afectada por PSD2, o "N" para indicar lo contrario.

Ejecución del 3DSMethod

El 3DSMethod es un proceso que permite a la entidad emisora capturar la información del dispositivo que está utilizando el titular. Esta información, junto con los datos EMV3DS que son enviados en la autorización, será utilizada por la entidad para hacer una evaluación del riesgo de la transacción. En base a esto, el emisor puede determinar que la transacción es confiable y por lo tanto no requerir la intervención del titular para verificar su autenticidad (frictionless).

La captura de datos del dispositivo se realiza mediante un iframe oculto en el navegador del cliente, que establecerá conexión directamente con la entidad emisora de forma transparente para el usuario. El comercio recibirá una notificación cuanto haya terminado la captura de información y en el siguiente paso, al realizar la petición de autorización al TPV Virtual el comercio deberá enviar el parámetro threeDSCompInd indicando la ejecución del 3DSMethod.

Pasos para la ejecución del 3DSMethod:

1. En la respuesta recibida con la configuración de la tarjeta (iniciaPeticion) se recibe los datos siguientes para ejecutar el 3DSMethod:
    a. threeDSMethodURL: url del 3DSMethod
    b. threeDSServerTransID: Identificador de transacción EMV3DS

    Si en la respuesta no se recibe threeDSMethodURL el proceso finaliza. En la autorización enviar threeDSCompInd = N
2. Construir el JSON Object con los parámetros:
    a. threeDSServerTransID: valor recibido en la respuesta de consulta de tarjeta
    b. threeDSMethodNotificationURL: url del comercio a la que será notificada la finalización del 3DSMethod desde la entidad
3. Codificar el JSON anterior en Base64url encode
4. Debe incluirse un iframe oculto en el navegador del cliente, y enviar un campo **threeDSMethodData** con el valor del objecto json anterior, en un formulario http post a la url obtenida en la consulta inicial **threeDSMethodURL**
5. La entidad emisora interactúa con el browser para proceder a la captura de información. Al finalizar enviará el campo **threeDSMethodData** en el iframe html del navegador por http post a la url **threeDSMethodNotificationURL** (indicada en el paso 2), y el 3DSMethod termina.
6. Si el 3DSMethod se ha completado en menos de 10 segundos se enviará **threeDSCompInd = Y** en la autorización. Si no se ha completado en 10 segundos debe detener la espera y enviar la autorización con **threeDSCompInd = N**

Petición de autorización con datos EMV3DS

La petición de autorización se hace a través de una petición al TPV Virtual En dicha petición deberá incluir los siguientes parámetros:

- <DS_SIGNATUREVERSION>: Constante que indica la versión de firma que se está utilizando.
- <DATOSENTRADA>: Datos de la petición de pago. Ver guía *Tpv-Virtual. Parámetros Entrada-salida.xlsx*

- <DS_SIGNATURE>.: Firma de los datos enviados.

Dichos parámetros deben enviarse a los siguientes URL dependiendo de si se quiere realizar una petición en el entorno de prueba u operaciones reales, llamando al método "***trataPeticion***":

URL Conexión	Método	Entorno
https://sis-t.redsys.es:25443/sis/services/SerClsWSEntradaV2	trataPeticion	Pruebas
https://sis.redsys.es/sis/services/SerClsWSEntradaV2	trataPeticion	Real

Una vez gestionada la petición, el TPV Virtual informará al servidor del comercio del resultado de la misma con la información del resultado incluida en un fichero XML (RETORNOXML). En él se incluirán los siguientes campos:

- CODIGO: Código de respuesta o error SIS
- OPERACION: Datos de respuesta de la operación. En este campo se incluirá el parámetro de salida *Ds_Signature* con la firma de la petición de respuesta.

A continuación, se describen los datos de debe incluir el DATOSENTRADA para enviar una petición de autorización con autenticación EMV3DS:

```
<DATOSENTRADA>
 <DS_MERCHANT_AMOUNT>1000</DS_MERCHANT_AMOUNT>
 <DS_MERCHANT_ORDER>1552572812</DS_MERCHANT_ORDER>
 <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
 <DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
 <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
 <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
 <DS_MERCHANT_PAN> XXXXXXXXXXXXXXXXXX </DS_MERCHANT_PAN>
 <DS_MERCHANT_EXPIRYDATE  >XXXX</ DS_MERCHANT_EXPIRYDATE>
 <DS_MERCHANT_CVV2>XXX</ DS_MERCHANT_CVV2>
 <DS_MERCHANT_EMV3DS>{
                    "threeDSInfo":"AuthenticationData",
                    "protocolVersion":"2.1.0",
                    "browserAcceptHeader":"text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8,ap
          plication/json",
                    "browserUserAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36",
                    "browserJavaEnabled":"false",
                    "browserLanguage":"ES-es",
                    "browserColorDepth":"24",
                    "browserScreenHeight":"1250",
                    "browserScreenWidth":"1320",
                    "browserTZ":"52",
                    "threeDSServerTransID":"8de84430-3336-4ff4-b18d-f073b546ccea",
                    "notificationURL":" https://comercio-inventado.es/recibe-respuesta-autenticacion",
                    "threeDSCompInd":"Y"
          }</DS_MERCHANT_EMV3DS>
</DATOSENTRADA>
```

Como respuesta se obtendrá:

- Si se hace un ***Frictionless***, se obtendrá directamente el resultado final de la operación:

```
<RETORNOXML>
 <CODIGO>0</CODIGO>
 <OPERACION>
  <Ds_Amount>1000</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>
  <Ds_Order>1552572812</Ds_Order>
  <Ds_Signature>B4Ok6jJAEOWFE6XT1nvLvUMM1kwt9CAkkLJkCHFBrso=</Ds_Signature>
  <Ds_MerchantCode>999008881</Ds_MerchantCode>
  <Ds_Terminal>2</Ds_Terminal>
  <Ds_TransactionType>0</Ds_TransactionType>
  <Ds_Response>0000</Ds_Response>
  <Ds_AuthorisationCode >694432</Ds_AuthorisationCode>
  <Ds_SecurePayment>1</Ds_SecurePayment>
  <Ds_Language >1</Ds_Language>
  <Ds_CardNumber>454881******0004</Ds_CardNumber>
  <Ds_Card_Type>C</Ds_Card_Type>
 <Ds_MerchantData ></Ds_MerchantData>
 <Ds_Card_Country>724</Ds_Card_Country>
 <Ds_Card_Brand>1</Ds_Card_Brand>
 </OPERACION>
</RETORNOXML>
```


- Si se requiere ***Challenge***, se obtendrán los datos para realizar el Challenge:


```
<RETORNOXML>
 <CODIGO>0</CODIGO>
 <OPERACION>
  <Ds_Amount>1000</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>
  <Ds_Order>1552572812</Ds_Order>
  <Ds_Signature>B4Ok6jJAEOWFE6XT1nvLvUMM1kwt9CAkkLJkCHFBrso=</Ds_Signature>
  <Ds_MerchantCode>999008881</Ds_MerchantCode>
  <Ds_Terminal>2</Ds_Terminal>
  <Ds_TransactionType>0</Ds_TransactionType>
  <Ds_EMV3DS>{"threeDSInfo":"ChallengeRequest",
          "protocolVersion":"2.1.0",
          "acsURL":"https://sis.redsys.es/sis-simulador-web/authenticationRequest.jsp",
          "creq":"eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6ImU5OWMzYzI2LTFiZWItNGY4NS05ZmE3LTI3OTJiZjE5NDZl
MiIsImFjc1RyYW5zSUQiOiIyMTQzNDFhYi0wMjlhLTRmMGEtOTEyNi1iMDFkYmE5OTc2MTkiLCJtZXNzYWdlVHlwZSI6Ik
NSZXEiLCJtZXNzYWdlVmVyc2lvbiI6IjIuMS4wIiwiY2hhbGxlbmdlV2luZG93U2l6ZSI6IjA1In0"}</Ds_EMV3DS>
 </OPERACION>
</RETORNOXML>
```


Ejecución del Challenge

Describimos este proceso en 3 pasos:

Paso 1.- Conexión desde el comercio el ACS del banco emisor

El siguiente paso consiste en conectar desde el comercio con la entidad emisora para que el cliente se pueda autenticar. Esta conexión se hace enviando un formulario http POST a la url del ACS del banco. Para esta conexión utilizamos los datos recibidos en el parámetro <Ds_EMV3DS> del paso anterior (parámetros acsURL y creq):


```
<Ds_EMV3DS>{"threeDSInfo":"ChallengeRequest",
          "protocolVersion":"2.1.0",
          "acsURL":"https://sis.redsys.es/sis-simulador-web/authenticationRequest.jsp",
```

"creq":"eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6ImU5OWMzYzI2LTFiZWItNGY4NS05ZmE3LTI3OTJiZjE5NDZlMiIsImFjc1RyYW5zSUQiOiIyMTQzNDFhYi0wMjlhLTRmMGEtOTEyNi1iMDFkYmE5OTc2MTkiLCJtZXNzYWdlVHlwZSI6IkNSZXEiLCJtZXNzYWdlVmVyc2lvbiI6IjIuMS4wIiwiY2hhbGxlbmdlV2luZG93U2l6ZSI6IjA1In0"}
</Ds_EMV3DS>

Ejemplo:
<form action="{acsURL}" method="POST" enctype = "application/x-www-form-urlencoded">
<input type="hidden" name="creq" value="{creq}" ">
</form>

Con los datos recibidos en <Ds_EMV3DS> sería:

<form action="https://sis.redsys.es/sis-simulador-web/authenticationRequest.jsp" method="POST" enctype = "application/x-www-form-urlencoded">

<input type="hidden" name="creq"
value="eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6ImU5OWMzYzI2LTFiZWItNGY4NS05ZmE3LTI3OTJiZjE5NDZlMiIsImFjc1RyYW5zSUQiOiIyMTQzNDFhYi0wMjlhLTRmMGEtOTEyNi1iMDFkYmE5OTc2MTkiLCJtZXNzYWdlVHlwZSI6IkNSZXEiLCJtZXNzYWdlVmVyc2lvbiI6IjIuMS4wIiwiY2hhbGxlbmdlV2luZG93U2l6ZSI6IjA1In0">
</form>

Paso 2.- Ejecución del challenge

El titular se autentica por los métodos que le exija su entidad emisora: OTP, contraseña estática, biometría, etc.

Paso 3.- Recepción del resultado de la autenticación

Una vez finalizado el challenge la entidad emisora enviará el resultado al comercio, haciendo un http POST a la url del parámetro *notificationURL* que el comercio envió previamente en la petición de autorización:

"notificationURL":" https://comercio-inventado.es/recibe-respuesta-autenticacion"

El comercio recibirá el parámetro "cres" que utlizará en la petición de autorización final que vemos en el siguiente apartado.

Confirmación de autorización EMV3DS posterior al Challenge

A continuación, se describen los datos de debe incluir DATOSENTRADA para enviar una petición de confirmación de autorización EMV3DS:

<DATOSENTRADA>
<DS_MERCHANT_AMOUNT>1000</DS_MERCHANT_AMOUNT>
<DS_MERCHANT_ORDER>1552572812</DS_MERCHANT_ORDER>
<DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
<DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
<DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
<DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
<DS_MERCHANT_PAN> XXXXXXXXXXXXXXXXXX </DS_MERCHANT_PAN>
<DS_MERCHANT_EXPIRYDATE >XXXX</ DS_MERCHANT_EXPIRYDATE>
<DS_MERCHANT_CVV2>XXX</ DS_MERCHANT_CVV2>
<DS_MERCHANT_EMV3DS>{"threeDSInfo":"ChallengeResponse",
"protocolVersion":"2.1.0",
"cres":"eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6IjhkZTg0NDMwLTMzMzYtNGZmNC1iMThkLWYwNzNiNTQ2Y2NlYSIsImFjc1RyYW5zSUQiOiJkYjVjOTljNC1hMmZkLTQ3ZWUtOTI2Zi1mYTBiMDk0MzUyYTAiLCJtZXNzYWdlVHlwZSI6IkNSZXMiLCJtZXNzYWdlVmVyc2lvbiI6IjIuMS4wIiwidHJhbnNTdGF0dXMiOiJZIn0="}
</DS_MERCHANT_EMV3DS>
</DATOSENTRADA>

*NOTA: el contenido del parámetro **cres** debe enviarse como una cadena continua sin retornos de carro ni saltos de línea*

Como respuesta se obtendrá el resultado final de la operación:


```
<RETORNOXML>
 <CODIGO>0</CODIGO>
 <OPERACION>
  <Ds_Amount>1000</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>
  <Ds_Order>1552572812</Ds_Order>
  <Ds_Signature>B4Ok6jJAEOWFE6XT1nvLvUMM1kwt9CAkkLJkCHFBrso=</Ds_Signature>
  <Ds_MerchantCode>999008881</Ds_MerchantCode>
  <Ds_Terminal>2</Ds_Terminal>
  <Ds_TransactionType>0</Ds_TransactionType>
  <Ds_Response>0000</Ds_Response>
  <Ds_AuthorisationCode >694432</Ds_AuthorisationCode>
  <Ds_SecurePayment>1</Ds_SecurePayment>
  <Ds_Language >1</Ds_Language>
  <Ds_CardNumber>454881******0004</Ds_CardNumber>
  <Ds_Card_Type>C</Ds_Card_Type>
 <Ds_MerchantData ></Ds_MerchantData>
 <Ds_Card_Country>724</Ds_Card_Country>
 <Ds_Card_Brand>1</Ds_Card_Brand>
 </OPERACION>
</RETORNOXML>
```

6.3 Ejemplo de peticiones para realizar una transacción con autenticación 3DSecure 1.0

Iniciar Petición

Esta petición permite obtener el tipo de autenticación 3D Secure que se puede realizar, además de la URL del 3DSMethod en caso de que exista.

El inicia petición se hace a través de una petición Webservice SOAP al TPV Virtual. En dicha petición deberá incluir los siguientes parámetros:

- <DS_SIGNATUREVERSION>: Constante que indica la versión de firma que se está utilizando.
- <DATOSENTRADA>: Datos de la petición de pago. Ver guía *Tpv-Virtual. Parámetros Entrada-salida.xlsx*
- <DS_SIGNATURE>.: Firma de los datos enviados.

Dichos parámetros deben enviarse a los siguientes URL dependiendo de si se quiere realizar una petición en el entorno de prueba u operaciones reales, llamando al método "***iniciaPeticion***":

URL Conexión	Método	Entorno
https://sis-t.redsys.es:25443/sis/services/SerClsWSEntradaV2	iniciaPeticion	Pruebas
https://sis.redsys.es/sis/services/SerClsWSEntradaV2	iniciaPeticion	Real

Una vez gestionada la petición, el TPV Virtual informará al servidor del comercio del resultado de la misma con la información del resultado incluida en un fichero XML (RETORNOXML). En él se incluirán los siguientes campos:

- CODIGO: Código de respuesta o error SIS
- OPERACION: Datos de respuesta de la operación. En este campo se incluirá el parámetro de salida *Ds_Signature* con la firma de la petición de respuesta.

A continuación, se describen los datos de debe incluir el DATOSENTRADA para enviar un inicia petición:

```
<DATOSENTRADA>
 <DS_MERCHANT_AMOUNT>1000</DS_MERCHANT_AMOUNT>
 <DS_MERCHANT_ORDER>1552571678</DS_MERCHANT_ORDER>
 <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
 <DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
 <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
 <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
 <DS_MERCHANT_PAN> XXXXXXXXXXXXXXXXXX </DS_MERCHANT_PAN>
 <DS_MERCHANT_EMV3DS>{'threeDSInfo':'CardData'}</DS_MERCHANT_EMV3DS>
 <Ds_Card_PSD2>Y</Ds_Card_PSD2>
</DATOSENTRADA>
```

Como respuesta se obtendrá lo siguiente:

```
<RETORNOXML>
 <CODIGO>0</CODIGO>
 <INFOTARJETA>
```

```
<Ds_Order>1553155286</Ds_Order>
<Ds_MerchantCode>999008881</Ds_MerchantCode>
<Ds_Terminal>2</Ds_Terminal>
<Ds_TransactionType>0</Ds_TransactionType>
<Ds_EMV3DS>{"protocolVersion":"NO_3DS_V2"}</Ds_EMV3DS>
<Ds_Card_PSD2>Y</Ds_Card_PSD2>
<Ds_Signature>7155jJYTzqeO/FoKjIQwUrjRJU7CxiOLHlC00d5c/RU=</Ds_Signature>
</INFOTARJETA>
```


El parámetro **Ds_EMV3DS** estará compuesto únicamente por el siguiente campo:

- **protocolVersion**: siempre indicará el número de versión mayor permitido en la operación. En el caso de que la versión exija realizar autenticación con 3DSecure 1.0 se indicará el valor "NO_3DS_V2".

El parámetro **Ds_Card_PSD2** informará al comercio si la tarjeta informada en la petición está afectada o no por PSD2. Los valores posibles serán "Y" para indicar que la tarjeta está afectada por PSD2, o "N" para indicar lo contrario.

Solicitar autorización

Esta petición permite indicar al comercio que quiere solicitar una transacción realizando la autenticación 3DSecure 1.0 si procede.

La petición de autorización se hace a través de una petición al TPV Virtual. En dicha petición deberá incluir los siguientes parámetros:

- <DS_SIGNATUREVERSION>: Constante que indica la versión de firma que se está utilizando.
- <DATOSENTRADA>: Datos de la petición de pago. Ver guía *Tpv-Virtual. Parámetros Entrada-salida.xlsx*
- <DS_SIGNATURE>.: Firma de los datos enviados.

Dichos parámetros deben enviarse a los siguientes URL dependiendo de si se quiere realizar una petición en el entorno de prueba u operaciones reales, llamando al método "***trataPeticion***":

URL Conexión	Método	Entorno
https://sis-t.redsys.es:25443/sis/services/SerClsWSEntradaV2	trataPeticion	Pruebas
https://sis.redsys.es/sis/services/SerClsWSEntradaV2	trataPeticion	Real

Una vez gestionada la petición, el TPV Virtual informará al servidor del comercio del resultado de la misma con la información del resultado incluida en un fichero XML (RETORNOXML). En él se incluirán los siguientes campos:

- CODIGO: Código de respuesta o error SIS

- OPERACION: Datos de respuesta de la operación. En este campo se incluirá el parámetro de salida *Ds_Signature* con la firma de la petición de respuesta.

A continuación, se describen los datos que debe incluir el DATOSENTRADA para enviar un inicia petición:


```
<DATOSENTRADA>
 <DS_MERCHANT_AMOUNT>1000</DS_MERCHANT_AMOUNT>
 <DS_MERCHANT_ORDER>1552572812</DS_MERCHANT_ORDER>
 <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
 <DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
 <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
 <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
 <DS_MERCHANT_PAN> XXXXXXXXXXXXXXXXXX </DS_MERCHANT_PAN>
 <DS_MERCHANT_EXPIRYDATE  >XXXX</ DS_MERCHANT_EXPIRYDATE>
 <DS_MERCHANT_CVV2>XXX</ DS_MERCHANT_CVV2>
 <DS_MERCHANT_EMV3DS>{
        "threeDSInfo":"AuthenticationData",
                "protocolVersion":"1.0.2",
                "browserAcceptHeader":"text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8,ap
        plication/json",
                "browserUserAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
        (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36"}</DS_MERCHANT_EMV3DS>
</DATOSENTRADA>
```


Como respuesta se obtendrá lo siguiente:


```
<RETORNOXML>
 <CODIGO>0</CODIGO>
 <OPERACION>
  <Ds_Amount>1000</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>
  <Ds_Order>1552572812</Ds_Order>
  <Ds_Signature>B4Ok6jJAEOWFE6XT1nvLvUMM1kwt9CAkkLJkCHFBrso=</Ds_Signature>
  <Ds_MerchantCode>999008881</Ds_MerchantCode>
  <Ds_Terminal>2</Ds_Terminal>
  <Ds_TransactionType>0</Ds_TransactionType>
  <Ds_EMV3DS>{"threeDSInfo":"ChallengeRequest",
        "protocolVersion":"1.0.2",
        "acsURL": "https://sis.redsys.es/sis-simulador-web/authenticationRequest.jsp",
        "PAReq":"eJxVUttygjAQ/RWG95KEooKzpkPVjj7QOpZ+QBp2KlYuDVDx77tRqS0zmdmzJ+zlnMBDXxycbzRNX
pUzV3jcdbDUVZaXHzP3LX26C90HCenOIC5eUXcGJSTYNOoDnTybuU1Rq7zPsFGlFmIU+mOfi4j7vrAfn3DOw9HYlbCJt/gl
4dpKUifPBzZAqmn0TpWtBKW/HtfPMhgFYSiAXSEUaNYL+brcJstNnCy381X8nAK7pKFUBcp5RUjnlZOhU5sO35XzZFSXIb
AzD7rqytac5MQPgA0AOnOQu7atp4wdj0fPYNacGk9XBTBLAbvNtuls1FCpPs9kso/7lzQ+JftIn6R09p88WcRHOjNg9gZkqk
U5KOIIPhVi6kfAznlQhZ1BintPcNr0gqC2TeKBsszfDJAHhiw6yWgS0hYDAuzrqkS6QbL+xkDOaEY73Cafr6zGuiXZ/loloIEYW
LnPjK2WkzhBJC7lLABm/2VXJ9n1GVD073n8AOa7wW0=",
        "MD":"cd164a6d0b77c96f7ef476121acfa987a0edf602"}</Ds_EMV3DS>
 </OPERACION>
</RETORNOXML>
```


Ejecución de la autenticación

El comercio deberá montar un formulario que envíe un POST a la URL del parámetro *acsURL* obtenido en la respuesta de la petición de autorización anterior. Dicho formulario envía 3 parámetros necesarios para la autenticación:

- *PaReq*, cuyo valor se obtiene del parámetro *PAReq* obtenido en la respuesta de la petición de autorización anterior.
- *MD*, cuyo valor se obtiene del parámetro *MD* obtenido en la respuesta de la petición de autorización anterior.

- *TermUrl*, que identifica la URL a la que entidad Emisora hará un POST con el resultado de autenticación. Dicho formulario enviará un único parámetro *PARes*, que contiene el resultado de la autenticación y que deberá ser recogido por el comercio para su posterior envío en la petición de confirmación de autorización.

Confirmación de autorización 3DSecure 1.0 posterior al Challenge

A continuación, se describen los datos que debe incluir el DATOSENTRADA para enviar una petición de confirmación de autorización 3DSecure 1.0 al Servicio SOAP:

```
<DATOSENTRADA>
  <DS_MERCHANT_AMOUNT>1000</DS_MERCHANT_AMOUNT>
  <DS_MERCHANT_ORDER>1552572812</DS_MERCHANT_ORDER>
  <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
  <DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
  <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
  <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
  <DS_MERCHANT_PAN> XXXXXXXXXXXXXXXXXX </DS_MERCHANT_PAN>
  <DS_MERCHANT_EXPIRYDATE  >XXXX</ DS_MERCHANT_EXPIRYDATE>
  <DS_MERCHANT_CVV2>XXX</  DS_MERCHANT_CVV2>
  <DS_MERCHANT_EMV3DS>{"threeDSInfo":"ChallengeResponse",
          "protocolVersion":"1.0.2",
          "PARes":"eJzFWNmSo0iyfecrymoeNVVsWqBNmWPBKlaJVcAbmwBJLALE9vWDlJVZWT3VNn3vw70yyRR4u
Dvu ESeOu8X2X0N+/dLFdZOVxctX9Dvy9UtchGWUFcnLV8vkvhFf//W6NdM6jhkjDu91/LpV4qbxk/hL  …..",
          "MD":"035535127d549298f11d7d2fc1b0d4e9300f93f1"}
</DS_MERCHANT_EMV3DS>
 </DATOSENTRADA>
```

Como respuesta se obtendrá el resultado final de la operación:

```
<RETORNOXML>
 <CODIGO>0</CODIGO>
 <OPERACION>
  <Ds_Amount>1000</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>
  <Ds_Order>1552572812</Ds_Order>
  <Ds_Signature>B4Ok6jJAEOWFE6XT1nvLvUMM1kwt9CAkkLJkCHFBrso=</Ds_Signature>
  <Ds_MerchantCode>999008881</Ds_MerchantCode>
  <Ds_Terminal>2</Ds_Terminal>
  <Ds_TransactionType>0</Ds_TransactionType>
  <Ds_Response>0000</Ds_Response>
  <Ds_AuthorisationCode >694432</Ds_AuthorisationCode>
  <Ds_SecurePayment>1</Ds_SecurePayment>
  <Ds_Language >1</Ds_Language>
  <Ds_CardNumber>454881******0004</Ds_CardNumber>
  <Ds_Card_Type>C</Ds_Card_Type>
 <Ds_MerchantData ></Ds_MerchantData>
 <Ds_Card_Country>724</Ds_Card_Country>
 <Ds_Card_Brand>1</Ds_Card_Brand>
 </OPERACION>
</RETORNOXML>
```

7. Transacciones con DCC

7.1 Pasos para realizar una transacción con DCC

A continuación, se detallarán todas aquellas características adicionales de la operativa DCC en los comercios que utilicen la interfaz SOAP. El comercio tiene que estar configurado para realizar este tipo de operativa.

Los pagos con DCC en la conexión SOAP sigue los siguientes pasos:

- **Paso 1: Iniciar petición**

El comercio deberá hacer una consulta al TPV Virtual para saber si la tarjeta ofrece DCC y la información de DCC asociada a la transacción que se ha indicado.

- **Paso 2: Solicitud de autorización**

El comercio enviará la solicitud de autorización de la operación incluyendo la información de DCC obtenida en el paso anterior.

El tiempo máximo desde el inicio de la petición y la solicitud de autorización es de 1 hora. Pasado este tiempo la petición se da como perdida y se deberá volver a realizar el flujo desde el principio.

7.2 Pasos para realizar una transacción con DCC

Iniciar Petición

Esta petición permite obtener el tipo de autenticación 3D Secure y DCC que se puede realizar.

El inicia petición se hace a través de una petición Webservice SOAP al TPV Virtual. En dicha petición deberá incluir los siguientes parámetros:

- <DS_SIGNATUREVERSION>: Constante que indica la versión de firma que se está utilizando.
- <DATOSENTRADA>: Datos de la petición de pago. Ver guía *Tpv-Virtual. Parámetros Entrada-salida.xlsx*
- <DS_SIGNATURE>.: Firma de los datos enviados.

Dichos parámetros deben enviarse a los siguientes URL dependiendo de si se quiere realizar una petición en el entorno de prueba u operaciones reales, llamando al método "***iniciaPeticion***":

URL Conexión	Método	Entorno
https://sis-t.redsys.es:25443/sis/services/SerClsWSEntradaV2	iniciaPetcion	Pruebas
https://sis.redsys.es/sis/services/SerClsWSEntradaV2	iniciaPeticion	Real

Una vez gestionada la petición, el TPV Virtual informará al servidor del comercio del resultado de la misma con la información del resultado incluida en un fichero XML (RETORNOXML). En él se incluirán los siguientes campos:

- CODIGO: Código de respuesta o error SIS
- OPERACION: Datos de respuesta de la operación. En este campo se incluirá el parámetro de salida *Ds_Signature* con la firma de la petición de respuesta.

NOTA: *En esta operativa DCC hay que tener en cuenta que, por normativa del Banco Central Europeo (BCE), en las operaciones en las que intervengan las siguientes monedas: Lev, Kuna croata, Corona danesa, Florín húngaro (forinto), Zloty, Corona Checa, Leu rumano, Corona sueca, Libra, es necesario informar al cliente del % de incremento entre el cambio aplicado y el cambio del BCE. Esta información se devolverá, en las operaciones en estas monedas, en los parámetros* <cambioBCE> *y* <porcentajeSobreBCE>.

A continuación, se describen los datos de debe incluir el DATOSENTRADA para enviar un inicia petición:

```
<DATOSENTRADA>
 <DS_MERCHANT_AMOUNT>5785</DS_MERCHANT_AMOUNT>
 <DS_MERCHANT_ORDER>1552571678</DS_MERCHANT_ORDER>
 <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
 <DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
 <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
 <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
 <DS_MERCHANT_PAN>XXXXXXXXXXXXXXXXXX</DS_MERCHANT_PAN>
 < DS_MERCHANT_DCC  >Y</DS_MERCHANT_EMV3DS>
 <Ds_Card_PSD2>Y</Ds_Card_PSD2>
</DATOSENTRADA>
```

Como respuesta se obtendrá lo siguiente:

```
<RETORNOXML>
 <CODIGO>0</CODIGO>
 <INFOTARJETA>
  <Ds_Order>1553159610</Ds_Order>
  <Ds_MerchantCode>999008881</Ds_MerchantCode>
  <Ds_Terminal>2</Ds_Terminal>
  <Ds_TransactionType>0</Ds_TransactionType>
  <Ds_DCC>{
          "InfoMonedaTarjeta":{
                  "monedaDCC":"826",
                  "litMonedaDCC":"POUND STERLING.",
                  "litMonedaRDCC":"GBP",
                  "importeDCC":"53.60",
                  "cambioDCC":"1.079288",
                  "fechaCambioDCC":"2019-01-16",
                  "markUp":"0.03",
                  "cambioBCE":"1.136092"
                  "porcentajeSobreBCE":"0.05”
                  },
          "InfoMonedaComercio":{
                  "monedaCome":"978",
                  "litMonedaCome":"EUR",
                  "importeCome":"57.85"}
  }</Ds_DCC>
  <Ds_Signature>chhx3Pg3/TpNGcj4whDJkZ0KfQMImi/4ga6BwyfPnDw=</Ds_Signature>
 </INFOTARJETA>
```

```
</RETORNOXML>
```

Petición de autorización con DCC

Esta petición permite indicar al comercio que quiere iniciar una transacción con los datos de DCC obtenidos anteriormente.

El inicia petición se hace a través de una petición Webservice SOAP al TPV Virtual. En dicha petición deberá incluir los siguientes parámetros:

- <DS_SIGNATUREVERSION>: Constante que indica la versión de firma que se está utilizando.
- <DATOSENTRADA>: Datos de la petición de pago. Ver guía *Tpv-Virtual. Parámetros Entrada-salida.xlsx*
- <DS_SIGNATURE>.: Firma de los datos enviados.

Dichos parámetros deben enviarse a los siguientes URL dependiendo de si se quiere realizar una petición en el entorno de prueba u operaciones reales, llamando al método "***trataPeticion***":

URL Conexión	Método	Entorno
https://sis-t.redsys.es:25443/sis/services/SerClsWSEntradaV2	trataPeticion	Pruebas
https://sis.redsys.es/sis/services/SerClsWSEntradaV2	trataPeticion	Real

Una vez gestionada la petición, el TPV Virtual informará al servidor del comercio del resultado de la misma, con la información incluida en un fichero XML (RETORNOXML). En él se incluirán los siguientes campos:

- CODIGO: Código de respuesta o error SIS
- OPERACION: Datos de respuesta de la operación. En este campo se incluirá el parámetro de salida *Ds_Signature* con la firma de la petición de respuesta.

A continuación, se describen los datos a incluir para enviar una petición de autorización con DCC al Servicio SOAP:

```
<DATOSENTRADA>
 <DS_MERCHANT_AMOUNT>1000</DS_MERCHANT_AMOUNT>
 <DS_MERCHANT_ORDER>1552572812</DS_MERCHANT_ORDER>
 <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
 <DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
 <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
 <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
 <DS_MERCHANT_PAN>XXXXXXXXXXXXXXXXXX</DS_MERCHANT_PAN>
 <DS_MERCHANT_EXPIRYDATE  >XXXX</ DS_MERCHANT_EXPIRYDATE>
 <DS_MERCHANT_CVV2>XXX</ DS_MERCHANT_CVV2>
 <DS_MERCHANT_DCC>{
```

"monedaDCC":"840",
"importeDCC":"11.50"}</DS_MERCHANT_DCC>
</DATOSENTRADA>

Como respuesta se obtendrá el resultado final de la operación:

<RETORNOXML>
<CODIGO>0</CODIGO>
<OPERACION>
<Ds_Amount>1000</Ds_Amount>
<Ds_Currency>978</Ds_Currency>
<Ds_Order>1552572812</Ds_Order>
<Ds_Signature>B4Ok6jJAEOWFE6XT1nvLvUMM1kwt9CAkkLJkCHFBrso=</Ds_Signature>
<Ds_MerchantCode>999008881</Ds_MerchantCode>
<Ds_Terminal>2</Ds_Terminal>
<Ds_TransactionType>0</Ds_TransactionType>
<Ds_Response>0000</Ds_Response>
<Ds_AuthorisationCode >694432</Ds_AuthorisationCode>
<Ds_SecurePayment>1</Ds_SecurePayment>
<Ds_Language >1</Ds_Language>
<Ds_CardNumber>454881******0004</Ds_CardNumber>
<Ds_Card_Type>C</Ds_Card_Type>
<Ds_MerchantData ></Ds_MerchantData>
<Ds_Card_Country>724</Ds_Card_Country>
<Ds_Card_Brand>1</Ds_Card_Brand>
</OPERACION>
</RETORNOXML>

8. Transacciones Autenticadas con DCC

8.1 Pasos para realizar una transacción con autenticación y DCC

A continuación, se detallarán todas aquellas características adicionales para una transacción con autenticación en la que se desee utilizar la operativa DCC para comercios que utilicen la interfaz SOAP. El comercio tiene que estar configurado para hacer este tipo de operativa.

Partiendo de los pasos necesarios para la realización de una transacción con autenticación, incluiremos la parte especifica de una operativa con:

- **Paso 1: Iniciar petición**

El comercio deberá hacer una consulta al TPV Virtual para saber si la tarjeta está inscrita en EMV3DS y poder iniciar el proceso de autenticación y si está tarjeta ofrece **DCC**.

- **Paso 2: 3DSMethod (Si procede)**

El comercio ejecuta el 3DSMethod para que el emisor capture la información del dispositivo.

- **Paso 3: Solicitud de autorización**

El comercio enviará la solicitud de autorización de la operación incluyendo el resultado del 3DSMethod y otros datos adicionales del protocolo EMV3DS. Además, incluyendo la información de **DCC** obtenida en el paso 1.

El TPV Virtual iniciará la autenticación, donde se podrá obtener como resultado:

a. Autenticación OK (Frictionless): la operación ha sido autenticada y el TPV Virtual continuará el proceso de autorización.

b. Challenge Required: La entidad emisora requiere verificar la autenticidad del cliente

c. Otro resultado: autenticación no disponible, autenticación rechazada, error en la autenticación, etc.

   El TPV Virtual decidirá según el caso autorizar o rechazar la operación.

- **Paso 4: Autenticación (Si procede)**

La entidad emisora requiere que el titular verifique su autenticidad (mediante OTP, contraseña estática, biometría, etc).

- **Paso 5: Confirmación de autorización**

El comercio enviará la autorización con el resultado del challenge al TPV Virtual para finalizar el proceso de autorización.

Recomendamos que en el paso 3 el comercio proporcione toda la información adicional para aumentar la probabilidad de flujo frictionless y una mayor tasa de autorización.

8.2 Pasos para realizar una transacción autenticada con DCC

A continuación, se detallan solamente aquellos pasos que cambiar con respecto a una autorización sin DCC.

Iniciar Petición

Para iniciar la petición de una operación con autenticación y 3DS se deberán seguir el apartado Iniciar Petición añadiendo los datos de DCC.

A continuación, se describen los datos a incluir para enviar una petición de inicia petición al Servicio SOAP con autenticación y 3DS:

```
<DATOSENTRADA>
 <DS_MERCHANT_AMOUNT>1000</DS_MERCHANT_AMOUNT>
 <DS_MERCHANT_ORDER>1552571678</DS_MERCHANT_ORDER>
 <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
 <DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
 <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
 <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
 <DS_MERCHANT_PAN> XXXXXXXXXXXXXXXXXX </DS_MERCHANT_PAN>
 <DS_MERCHANT_DCC>Y</DS_MERCHANT_DCC>
 <DS_MERCHANT_EMV3DS>{'threeDSInfo':'CardData'}</DS_MERCHANT_EMV3DS>
 <Ds_Card_PSD2>Y</Ds_Card_PSD2>
</DATOSENTRADA>
```

Como respuesta se obtendrá lo siguiente:

```
<RETORNOXML>
 <CODIGO>0</CODIGO>
 <INFOTARJETA>
  <Ds_Order>1552571678</Ds_Order>
  <Ds_MerchantCode>999008881</Ds_MerchantCode>
  <Ds_Terminal>2</Ds_Terminal>
  <Ds_TransactionType>0</Ds_TransactionType>
  <Ds_DCC>{
        "InfoMonedaTarjeta":{
              "monedaDCC":"840",
              "litMonedaDCC":"DOLAR U.S.A.",
              "litMonedaRDCC":"USD",
              "importeDCC":"11.50",
              "cambioDCC":"0.869841",
              "fechaCambioDCC":"2019-01-16",
              "markUp":"0.03"
              "cambioBCE":"0.869835"},
        "InfoMonedaComercio":{
              "monedaCome":"978",
              "litMonedaCome":"EUR",
              "importeCome":"10.00"}
  }</Ds_DCC>
  <Ds_EMV3DS>{"protocolVersion":"2.1.0",
        "threeDSServerTransID":"8de84430-3336-4ff4-b18d-f073b546ccea",
        "threeDSInfo":"CardConfiguration",
        "threeDSMethodURL":"https://sis.redsys.es/sis-simulador-web/threeDsMethod.jsp"}
 </Ds_EMV3DS>
  <Ds_Card_PSD2>N</Ds_Card_PSD2>
  <Ds_Signature>7155jJYTzqeO/FoKjIQwUrjRJU7CxiOLHlC00d5c/RU=</Ds_Signature>
 </INFOTARJETA>
</RETORNOXML>
```

Petición de autorización con DCC

A continuación, se describen los datos a incluir en una petición de autorización con DCC al Servicio SOAP:

```
<DATOSENTRADA>
 <DS_MERCHANT_AMOUNT>1000</DS_MERCHANT_AMOUNT>
 <DS_MERCHANT_ORDER>1552572812</DS_MERCHANT_ORDER>
 <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
 <DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
 <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
 <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
 <DS_MERCHANT_PAN>XXXXXXXXXXXXXXXXXX</DS_MERCHANT_PAN>
 <DS_MERCHANT_EXPIRYDATE  >XXXX</ DS_MERCHANT_EXPIRYDATE>
 <DS_MERCHANT_CVV2>XXX</  DS_MERCHANT_CVV2>
 <DS_MERCHANT_DCC>{
                    "monedaDCC":"840",
                    "importeDCC":"11.50"}</DS_MERCHANT_DCC>
 <DS_MERCHANT_EMV3DS>{
                    "threeDSInfo":"AuthenticationData",
                    "protocolVersion":"2.1.0",
                    "browserAcceptHeader":"text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8,ap
          plication/json",
                    "browserUserAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36",
                    "browserJavaEnabled":"false",
                    "browserJavascriptEnabled":"false",
                    "browserLanguage":"ES-es",
                    "browserColorDepth":"24",
                    "browserScreenHeight":"1250",
                    "browserScreenWidth":"1320",
                    "browserTZ":"52",
                    "threeDSServerTransID":"8de84430-3336-4ff4-b18d-f073b546ccea",
                    "notificationURL":"https://sis.redsys.es/sis-simulador-web/SisRESTCreqCres_3DSecureV2.jsp",
                    "threeDSCompInd":"Y"
          }</DS_MERCHANT_EMV3DS>
</DATOSENTRADA>
```

9. Adaptaciones PSD2

De acuerdo a la norma de PSD2 (entrada en vigor el 14 de septiembre de 2019), directiva europea que tiene como objetivo mejorar la seguridad y reforzar la autenticación del cliente en las operaciones de comercio electrónico. Como norma básica se exige la autenticación del titular en todas las operaciones, sin embargo, también se define la posibilidad de que el comercio, en la petición de pago solicite una exención para evitar dicha autenticación. Para solicitar una exención el comercio deberá incluir el siguiente parámetro en sus peticiones.

PARÁMETRO	VALORES POSIBLES
DS_MERCHANT_EXCEP_SCA	LWV, TRA, MIT, COR, ATD

- LWV (Low value transaction): exención por bajo importe (hasta 30 €, con máx. 5 ops. o 100 € acumulado por tarjeta, estos contadores son controlados a nivel de entidad emisora de la tarjeta)
- TRA (Análisis de riesgo de la operación): esta exención se basa en un análisis de riesgo de la operación por parte del adquirente/comercio.
- MIT (Merchant Initiated Transaction): operación iniciada por el comercio sin estar asociada a una acción o evento del cliente, es decir, sin que haya interacción posible con el cliente. Estas operaciones están fuera del alcance de la PSD2. Este es el caso de las operativas de pagos de subscripciones, recurrentes, etc. y, en general, casi todas las que requieren el almacenamiento de las credenciales de pago del cliente (COF) o su equivalente "pago por referencia". Toda operativa de pago iniciada por el comercio (MIT) requiere que la operación inicial, cuando el cliente concede el permiso al comercio de uso de sus credenciales de pago, se haga mediante operación autenticada con SCA.
- COR (Secure Corporate Payment): exención restringida al caso de operaciones entre empresas, no a consumidores.
- ATD : exención de autenticación delegada. Autenticación Delegada es un programa específico de las marcas. (para más información, consultar con la documentación de las marcas sobre este tema)

NOTA: Se deberá tener en cuenta que para las exenciones LWV, TRA y COR la primera opción será marcar la exención en el paso de la autenticación, para mejorar la experiencia de usuario. Esto permite que si el emisor no acepta la propuesta de exención y requiere SCA pueda solicitar la autenticación en el mismo momento sin necesidad de rechazar la operación (challenge required EMV3DS).

Ejemplos de peticiones con exenciones.

9.1 Ejemplos de peticiones con exenciones.

Como se indica en el punto anterior la normativa contempla diferentes exenciones que se pueden marcar para no autenticar algunas de las operaciones de comercio electrónico. Hay que tener en cuenta que al marcar exenciones la responsabilidad al fraude de la operación recae en el comercio.

Se contemplan dos tipos de mensajes donde podemos marcar una exención:

- **Petición con datos EMV3DS**. Las exenciones marcadas en peticiones con envió de datos EMV3DS, se marcarán en la autenticación. Si esta exención no es aceptada se devolverá una petición de CHALLENGE para que el titular se autentiqué con SCA. De esta forma la petición no se pierde y continuará el flujo habitual, sin que el titular se vea afectado. SE RECOMIENDA ESTA OPCIÓN.
- **Petición sin datos EMV3DS.** Las exenciones marcadas en las peticiones en las que no se han informado los datos EMV3DS, se marcarán en la autorización. Si esta exención no es aceptada se procederá a una denegación con **Ds_Response = 0195** (Requiere SCA). Si se quiere volver a hacer la petición con datos EMV3DS se deberá enviar otra petición completamente nueva.

Mensaje Inicia Petición (Conocer mis exenciones permitidas)

Las exenciones dependen de la configuración y la activación por parte de la entidad, para conocer que exenciones podemos aplicar deberemos mandar el parámetro DS_MERCHANT_EXCEP_SCA con el valor "Y" y como respuesta obtendremos las posibles exenciones a marcar.

Nota: Para la exención TRA, se establece un máximo de importe que vendrá también informado.

EJEMPLO DE INICIA PETICIÓN

```
<DATOSENTRADA>
 <DS_MERCHANT_AMOUNT>1000</DS_MERCHANT_AMOUNT>
 <DS_MERCHANT_ORDER>1552571678</DS_MERCHANT_ORDER>
 <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
 <DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
 <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
 <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
 <DS_MERCHANT_PAN>  XXXXXXXXXXXXXXXXXX </DS_MERCHANT_PAN>
 <DS_MERCHANT_EMV3DS>{'threeDSInfo':'CardData'}</DS_MERCHANT_EMV3DS>
 <DS_MERCHANT_EXCEP_SCA>Y</DS_MERCHANT_EXCEP_SCA>
 <Ds_Card_PSD2>Y</Ds_Card_PSD2>
</DATOSENTRADA>
```

Como respuesta se obtendrá lo siguiente:

```
<RETORNOXML>
 <CODIGO>0</CODIGO>
 <INFOTARJETA>
  <Ds_Order>1553155286</Ds_Order>
  <Ds_MerchantCode>999008881</Ds_MerchantCode>
  <Ds_Terminal>2</Ds_Terminal>
  <Ds_TransactionType>0</Ds_TransactionType>
  <Ds_EMV3DS>{"protocolVersion":"2.1.0",
          "threeDSServerTransID":"8de84430-3336-4ff4-b18d-f073b546ccea",
          "threeDSInfo":"CardConfiguration",
          "threeDSMethodURL":"https://sis.redsys.es/sis-simulador-web/threeDsMethod.jsp"}</Ds_EMV3DS>
  <Ds_Excep_SCA>LWV;TRA[30.0];COR;MIT</Ds_Excep_SCA>
```

```
    <Ds_Card_PSD2>Y</Ds_Card_PSD2>

    <Ds_Signature>7155jJYTzqeO/FoKjIQwUrjRJU7CxiOLHlC00d5c/RU=</Ds_Signature>
  </INFOTARJETA>
</RETORNOXML>
```

Mensaje Trata Petición (Con EMV3DS)


```
<DATOSENTRADA>
 <DS_MERCHANT_AMOUNT>1000</DS_MERCHANT_AMOUNT>
 <DS_MERCHANT_ORDER>1552572812</DS_MERCHANT_ORDER>
 <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
 <DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
 <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
 <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
 <DS_MERCHANT_PAN> XXXXXXXXXXXXXXXXXX </DS_MERCHANT_PAN>
 <DS_MERCHANT_EXPIRYDATE >XXXX</ DS_MERCHANT_EXPIRYDATE>
 <DS_MERCHANT_CVV2>XXX</ DS_MERCHANT_CVV2>
 <DS_MERCHANT_EXCEP_SCA>LWV</DS_MERCHANT_EXCEP_SCA>
 <DS_MERCHANT_EMV3DS>{
                "threeDSInfo":"AuthenticationData",
                "protocolVersion":"2.1.0",
                "browserAcceptHeader":"text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8,appli
        cation/json",
                "browserUserAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/71.0.3578.98 Safari/537.36",
                "browserJavaEnabled":"false",
                "browserLanguage":"ES-es",
                "browserColorDepth":"24",
                "browserScreenHeight":"1250",
                "browserScreenWidth":"1320",
                "browserTZ":"52",
                "threeDSServerTransID":"8de84430-3336-4ff4-b18d-f073b546ccea",
                "notificationURL":" https://comercio-inventado.es/recibe-respuesta-autenticacion",
                "threeDSCompInd":"Y"
        }</DS_MERCHANT_EMV3DS>
</DATOSENTRADA>
```


Mensaje Trata Petición (Sin EMV3DS)

Se incluye el parámetro DS_MERCHANT_EXCEP_SCA con el valor de la excepción propuesta. Como no se informan los campos de EMV3DS, la exención se solicitará directamente en la petición de autorización por lo que si el emisor no la acepta podrá denegar con un 0195 “soft-decline” para indicar que requiere autenticación. Si el terminal tiene configurados métodos de pago seguros, se deberá añadir también el parámetro DS_MERCHANT_DIRECTPAYMENT con el valor true.


```
<DATOSENTRADA>
 <DS_MERCHANT_AMOUNT>1000</DS_MERCHANT_AMOUNT>
 <DS_MERCHANT_ORDER>1552572812</DS_MERCHANT_ORDER>
 <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
 <DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
 <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
 <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
 <DS_MERCHANT_PAN> XXXXXXXXXXXXXXXXXX </DS_MERCHANT_PAN>
 <DS_MERCHANT_EXPIRYDATE >XXXX</ DS_MERCHANT_EXPIRYDATE>
 <DS_MERCHANT_CVV2>XXX</ DS_MERCHANT_CVV2>
 <DS_MERCHANT_EXCEP_SCA>LWV</DS_MERCHANT_EXCEP_SCA>
</DATOSENTRADA>
```

9.2 Transacciones iniciadas por el comercio (MIT)

Una transacción MIT es aquella que es iniciada por el propio comercio sin que haya interacción posible con el cliente. Por ejemplo, pago mensual de un recibo o cuota de subscripción. Este tipo de operaciones, al no estar el cliente presente y no ser posible su autenticación, no requerirán de autenticación del titular (SCA).

Para identificar correctamente este tipo de transacción, el comercio debe incluir en la petición de pago, el parámetro **DS_MERCHANT_EXCEP_SCA** con el valor **MIT** y, además, enviar el parámetro **DS_MERCHANT_DIRECTPAYMENT** con el valor **true**.

Estas transacciones MIT, pueden estar asociadas a una petición inicial de pago (**Operación COF inicia**l) en la que el titular está presente y concede el permiso al comercio para que use sus datos de pago en cargos posteriores, de acuerdo a un servicio prestado de forma continuada en el tiempo. Esta operación inicial deberá ser autenticada con SCA y debe marcarse siguiendo las especificaciones COF. La operación MIT también requiere que se marque correctamente el indicador de COF, de acuerdo al uso concreto que se esté haciendo de las credenciales almacenadas.

Hay que tener en cuenta que no todas las operativas en las que se utilizan datos de tarjeta/credenciales almacenadas (COF) pueden ser consideradas MIT. Por ejemplo, la operativa de **pago en 1 clic**, donde las credenciales del cliente están almacenadas o tokenizadas (pago por referencia), **NO** se pueden considerar transacciones iniciadas por el comercio las peticiones de pago que se realizan utilizando las credenciales almacenadas ya que el titular está presente y por lo tanto puede autenticarse. En este caso, según la normativa PSD2, y mientras no se aplique otra exención, se requiere el uso de autenticación reforzada (SCA).

NOTA 1: Para más información sobre especificaciones de Credentials on File (COF) ver Guía Especificaciones COF Ecom.

NOTA2: El listado completo de todos los parámetros de entrada del SIS está disponible en el doc. "TPV-Virtual Parámetros Entrada-Salida.xlsx".

10. Funcionalidades Avanzadas EMV3DS

En cuando a este punto de operaciones R3I, las especificaciones todavía no están cerradas por parte de las marcas. Este punto se suprime, temporalmente, hasta que dispongamos de los requisitos de las marcas que nos permitan implementar la solución definitiva para este tipo de transacciones

11. Parámetros de Entrada y Salida (ejemplos de petición Web service)

11.1 Parámetros de la solicitud

En la petición de pago hacia el TPV Virtual SIS se tendrán que enviar una serie de parámetros obligatorios y otros opcionales, que irán en función del tipo de operación y operativa que se desee realizar.

NOTA: El listado completo de todos los errores del SIS está disponible en el documento "TPV-Virtual Parámetros Entrada-Salida.xlsx".

En los siguientes puntos se mostrarán algunos ejemplos de peticiones WebService SOAP:

Petición de pago/preautorización (con envío de datos de tarjeta)

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

```
<DATOSENTRADA>
        <DS_MERCHANT_AMOUNT>145</DS_MERCHANT_AMOUNT>
        <DS_MERCHANT_ORDER>050911523002</DS_MERCHANT_ORDER>
        <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
        <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
        <DS_MERCHANT_PAN>XXXXXXXXXXXXXX</DS_MERCHANT_PAN>
        <DS_MERCHANT_CVV2>XXX</DS_MERCHANT_CVV2>
        <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
        <DS_MERCHANT_TERMINAL>999</DS_MERCHANT_TERMINAL>
        <DS_MERCHANT_EXPIRYDATE>XXXX</DS_MERCHANT_EXPIRYDATE>
</DATOSENTRADA>

*<DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>  para PAGO
*<DS_MERCHANT_TRANSACTIONTYPE>1</DS_MERCHANT_TRANSACTIONTYPE>  para PREAUTORIZACIÓN
```

Petición de Confirmación/Devolución/Anulación

A continuación, se muestra un ejemplo de un mensaje de devolución:

```
<DATOSENTRADA>
        <DS_MERCHANT_AMOUNT>145</DS_MERCHANT_AMOUNT>
        <DS_MERCHANT_ORDER>050911523002</DS_MERCHANT_ORDER>
        <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
        <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
        <DS_MERCHANT_TRANSACTIONTYPE>3</DS_MERCHANT_TRANSACTIONTYPE>
        <DS_MERCHANT_TERMINAL>999</DS_MERCHANT_TERMINAL>
</DATOSENTRADA>

*<DS_MERCHANT_TRANSACTIONTYPE>2</DS_MERCHANT_TRANSACTIONTYPE>  para CONFIRMACIÓN de preautorización
*<DS_MERCHANT_TRANSACTIONTYPE>3</DS_MERCHANT_TRANSACTIONTYPE>  para DEVOLUCIÓN
*<DS_MERCHANT_TRANSACTIONTYPE>9</DS_MERCHANT_TRANSACTIONTYPE>  para ANULACIÓN de preautorización
```

Uso de Tokenización en transacción MIT (Pago por Referencia)

A continuación, se muestra un ejemplo de un mensaje de petición de pago utilizando una referencia con una transacción iniciada por el comercio (MIT):

```
<DATOSENTRADA>
        <DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
        <DS_MERCHANT_TERMINAL>999</DS_MERCHANT_TERMINAL>
        <DS_MERCHANT_ORDER>050911523002</DS_MERCHANT_ORDER>
        <DS_MERCHANT_AMOUNT>145</DS_MERCHANT_AMOUNT>
        <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
        <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
        <DS_MERCHANT_IDENTIFIER>XXXXXXXXXXXXXXXXXXX</ DS_MERCHANT_IDENTIFIER>
        <DS_MERCHANT_DIRECTPAYMENT>true<DS_MERCHANT_DIRECTPAYMENT>
        <DS_MERCHANT_EXCEP_SCA>MIT</ DS_MERCHANT_EXCEP_SCA>
</DATOSENTRADA>
```

Nota: Por PSD2 la solicitud de generación de referencia deberá realizarse siempre con autenticación del titular.

12. Entorno de Pruebas

El comercio puede utilizar el entorno de test para realizar las pruebas que necesite para verificar el correcto funcionamiento de su integración antes de hacer la implantación en el entorno real.

En esta guía se facilitan datos genéricos de prueba que pueden ser utilizados por cualquier cliente, si el comercio está interesado en realizar estas pruebas con los datos de su comercio, deberá dirigirse a su Entidad bancaría para que le facilite los datos de acceso.

Las URLs de acceso al entorno de pruebas son:

URL Conexión inicia petición
https://sis-t.redsys.es:25443/sis/services/SerClsWSEntradaV2
URL Conexión trata petición
https://sis-t.redsys.es:25443/sis/services/SerClsWSEntradaV2
URL acceso al Portal de Administración
https://sis-t.redsys.es:25443/canales/portal

NOTA: El flujo de las operaciones en el entorno de pruebas en el mismo que en el entorno de producción, con la única diferencia que los pagos realizados en este entorno no tendrán validez contable.

DATOS GENÉRICOS DE PRUEBA

- Número de comercio (DS_MERCHANT_MERCHANTCODE): Aquí se deberá poner el número facilitado por su entidad (ejemplo 999008881)
- Terminal (DS_MERCHANT_TERMINAL): Aquí se deberá poner el número facilitado por su entidad (ejemplo 01)
- Clave de firma: sq7HjrUOBfKmC576ILgskD5srU870gJ7

NOTA: Estos son datos genéricos, que puede utilizar cualquier comercio. Si el cliente quiere hacer pruebas con operativas específicas de funcionamiento de su propio comercio, deberá contactar con su entidad bancaria para que le facilite los datos para realizar estas pruebas.

Tarjeta de pruebas	Descripción
4548812049400004 Caducidad: no se valida CVV2: distinto de 999	Tarjeta que permite realizar operaciones con autenticación en versión 1.0.2
4918019160034602 Caducidad: no se valida CVV2: distinto de 999	EMV3DS 2.1 con *threeDSMethodURL y* autenticación Frictionless
4548814479727229 Caducidad: no se valida CVV2: distinto de 999	EMV3DS 2.1 sin *threeDSMethodURL y* autenticación Frictionless
4918019199883839 Caducidad: no se valida CVV2: distinto de 999	EMV3DS 2.1 con *threeDSMethodURL y* autenticación Challenge
4548817212493017 Caducidad: no se valida CVV2: distinto de 999	EMV3DS 2.1 sin *threeDSMethodURL y* autenticación Challenge
Operaciones denegadas	
Cualquier operación con valor de CVV2 = 999 o importe terminado en 96	
Pruebas PSD2	
4548816134581156 Caducidad: no se valida CVV2: distinto de 999	EMV3DS 2.2 *sin threeDSMethodURL con autenticación Frictionless*
4548816131164386 Caducidad: no se valida CVV2: distinto de 999	EMV3DS 2.2 *sin threeDSMethodURL con autenticación Challenge*
4548815324058868 Caducidad: no se valida CVV2: distinto de 999	EMV3DS 2.2 *sin threeDSMethodURL. Si se envía una exención se realizará autenticación Frictionless. Si no se envía exenciones pedirá Challenge*
4548815374025114 Caducidad: no se valida CVV2: distinto de 999	EMV3DS 2.2 *sin threeDSMethodURL. Si se envía MIT devolverá Frictionless, en cualquier otro caso pedirá Challenge*
5576441563045037 Caducidad: no se valida CVV2: distinto de 999	EMV3DS 2.2 *sin threeDSMethodUR. Acepta solo pagos 3RI-OTA*
4548817212493017 Caducidad: no se valida CVV2: distinto de 999	Tarjeta con soft decline. Denegación 195 si la autorización no va como autenticada.
Pruebas DCC	

4137360000000006 Caducidad: no se valida CVV2: distinto de 999	Tarjeta Visa con DCC y 3DS V1
5424180805648190 Caducidad: no se valida CVV2: distinto de 999	Tarjeta Master con DCC y EMV3DS 2 Frictionless
4117731234567891 Caducidad: no se valida CVV2: distinto de 999	Tarjeta Visa con DCC y EMV3DS 2 Challenge
5409960031405146 Caducidad: no se valida CVV2: distinto de 999	Tarjeta Master con moneda Korona Noruega y EMV3DS 2 Challenge
Otras marcas	
36849800000018 Caducidad: no se valida CVV2: distinto de 999	Tarjeta Diners
36849800000000 Caducidad: no se valida CVV2: distinto de 999	Tarjeta Diners
376674000000008 Caducidad: no se valida CVV2: distinto de 999	Tarjeta Amex
376674000000016 Caducidad: no se valida CVV2: distinto de 999	Tarjeta Amex
3587870000000001 Caducidad: no se valida CVV2: distinto de 999	Tarjeta JCB
3587870000000019 Caducidad: no se valida CVV2: distinto de 999	Tarjeta JCB

13. Timeout

Que hacer en el caso de que el TPV Virtual no responda a una petición solicitada.

Este problema puede tener dos posibles causas:

- No se ha recibido la petición, con lo que TPV Virtual no responderá al mensaje de petición.
- TPV Virtual ha recibido el mensaje de petición, pero no puede contactar con el Centro Autorizador. Esta conexión tiene definido un timeout de 30 segundos, por lo que si transcurrido ese tiempo, no se recibe respuesta del Centro Autorizador, se devolverá un mensaje de respuesta con código 9912/912 "Emisor no disponible". La aplicación cliente deberá por tanto establecer un timeout mayor (unos 40 o 50 segundos), para asegurar que TPV Virtual siempre le va a responder.

13.1 Que hacer en caso de timeout del TPV Virtual

Para las peticiones de un pago, preautorización o confirmación se deberá mandar su operación de anulación correspondiente.

En el caso de operaciones de devoluciones u operaciones de anulaciones se podrá volver a realizar la petición.

14. Errores frecuentes

Error de firma (SIS0042)

Cuando hay un error de firma el comercio ha de verificar:

- Que los datos que se han utilizado para hacer la firma son iguales a los que se envían en el formulario, teniendo en cuenta, que cualquier modificación del valor o formato de un campo posterior al cálculo de la firma, hace que ésta sea incorrecta.
- Que la clave secreta empleada por el comercio coincide con la clave que tiene cargada el comercio en el módulo de administración (apartado comercios).
- Se debe revisar que los comercios no están enviando espacios en blanco en la firma. Si la petición se hace mediante cURL o mediante el navegador Safari, puede que se conviertan los símbolos "+" en espacio en blanco. Para que esto no ocurra se deben sustituir los símbolos "+" de la firma por "%2B" (Valor URL encoded).
- Si el comercio no consigue localizar qué parámetro es el erróneo, debe contactar con el Centro de Atención al Cliente de Redsys, o con el departamento de Soporte a la Integración de Redsys, si su entidad le ha facilitado el contacto.

Tengo en mi comercio denegaciones por número de repetido (SIS0051), pero no tengo constancia de haberlos repetido.

Esto ocurre habitualmente porque la plataforma del comercio está generando números de pedido repetido únicamente cuando recibe denegaciones o autorizaciones, pero los está repitiendo cuando las transacciones se quedan a medias. Ante esto hay dos opciones:

- Solicitar al servicio de Soporte que el TPV se configure para que pueda repetir números de pedidos. Máximo de una operación autorizada al día y sin límite para las denegadas.
- Generar siempre números de pedido distintos, no solo para las operaciones autorizadas y denegadas, sino para aquellas que no hayan finalizado trascurrido un tiempo.

Necesito hacer una devolución de una operación, pero no me aparece la opción de devolución en el módulo de administración.

Se debe a que el usuario con el que se está accediendo a Canales no tiene permiso para hacer devoluciones. Si necesita este permiso debe ponerse en contacto con su entidad.

Lanzo mis operaciones con SOAP y el TPV-Virtual nos devuelve siempre "Internal Error".

El parámetro que se envía en las peticiones vía SOAP es en formato XML y debe cerciorarse si está incluyendo el parámetro de envío dentro de una sección CDATA.

15. Preguntas Frecuentes

Soy un comercio y necesito conocer la clave de encriptación de mi TPV Virtual

En el punto 3 de este mismo documento se indica cómo acceder al valor de clave.

Mi usuario de comercio de acceso al módulo de administración del Canales está bloqueado. ¿Cómo puedo desbloquearlo?

Bajo las casillas de usuario y contraseña existe un link de "He olvidado mi contraseña". Tras pulsarlo deberá escribir su usuario y confirmar la dirección de envío de la nueva contraseña.

ANEXOS

1. Web Service de petición de pago y autenticación – WSDL

WSDL: https://sis.redsys.es /sis/services/SerClsWSEntradaV2/wsdl/SerClsWSEntradaV2.wsdl

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:apachesoap="http://xml.apache.org/xml-soap"
xmlns:impl="http://webservice.sis.sermepa.es"
xmlns:intf="http://webservice.sis.sermepa.es"
xmlns:wsdlsoap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://webservice.sis.sermepa.es">
        <wsdl:types>
                <schema xmlns="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified" 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/">
                        <element name="trataPeticion">
                                <complexType>
                                        <sequence>
                                                <element name="datoEntrada" nillable="true"
                                                type="xsd:string"/>
                                        </sequence>
                                </complexType>
                        </element>
                        <element name="trataPeticionResponse">
                                <complexType>
                                        <sequence>
                                                <element name="trataPeticionReturn"
                                                nillable="true" type="xsd:string"/>
                                        </sequence>
                                </complexType>
                        </element>
                        <element name="trataPeticion3DES">
                                <complexType>
                                        <sequence>
                                                <element name="datoEntrada" nillable="true"
                                                type="xsd:string"/>
                                        </sequence>
                                </complexType>
                        </element>
                        <element name="trataPeticionResponse3DES">
                                <complexType>
                                        <sequence>
                                                <element name="trataPeticionReturn"
                                                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>
        <element name="consultaBIN">
                <complexType>
                        <sequence>
                                <element name="datoEntrada" nillable="true"
                                type="xsd:string"/>
                        </sequence>
                </complexType>
        </element>
        <element name="consultaBINResponse">
                <complexType>
                        <sequence>
                                <element name="consultaBINReturn"
                                nillable="true" type="xsd:string"/>
                        </sequence>
                </complexType>
        </element>
        <element name="iniciaPeticion">
                <complexType>
                        <sequence>
                                <element name="datoEntrada" nillable="true"
                        type="xsd:string"/>
                        </sequence>
                </complexType>
        </element>
        <element name="iniciaPeticionResponse">
                <complexType>
                        <sequence>
                                <element name="iniciaPeticionReturn"
                                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="consultaDCCResponse">
    <wsdl:part element="intf:consultaDCCResponse" name="parameters"/>
</wsdl:message>
<wsdl:message name="trataPeticionRequest">
    <wsdl:part element="intf:trataPeticion" name="parameters"/>
</wsdl:message>
<wsdl:message name="trataPeticionResponse">
    <wsdl:part element="intf:trataPeticionResponse" name="parameters"/>
</wsdl:message>
<wsdl:message name="trataPeticionRequest3DES">
    <wsdl:part element="intf:trataPeticion3DES" name="parameters"/>
</wsdl:message>
<wsdl:message name="trataPeticionResponse3DES">
    <wsdl:part element="intf:trataPeticionResponse3DES" name="parameters"/>
</wsdl:message>
<wsdl:message name="consultaBINRequest">
    <wsdl:part element="intf:consultaBIN" name="parameters"/>
</wsdl:message>
<wsdl:message name="consultaBINResponse">
    <wsdl:part element="intf:consultaBINResponse" name="parameters"/>
</wsdl:message>
<wsdl:message name="iniciaPeticionRequest">
    <wsdl:part element="intf:iniciaPeticion" name="parameters"/>
</wsdl:message>
<wsdl:message name="iniciaPeticionResponse">
    <wsdl:part element="intf:iniciaPeticionResponse" name="parameters"/>
```

```
</wsdl:message>
<wsdl:portType name="SerClsWSEntrada">
        <wsdl:operation name="trataPeticion">
                <wsdl:input message="intf:trataPeticionRequest"
                name="trataPeticionRequest"/>
                <wsdl:output message="intf:trataPeticionResponse"
                name="trataPeticionResponse"/>
        </wsdl:operation>
        <wsdl:operation name="trataPeticion3DES">
                <wsdl:input message="intf:trataPeticionRequest3DES"
                name="trataPeticionRequest3DES"/>
                <wsdl:output message="intf:trataPeticionResponse3DES"
                name="trataPeticionResponse3DES"/>
        </wsdl:operation>
        <wsdl:operation name="consultaDCC">
                <wsdl:input message="intf:consultaDCCRequest"
                name="consultaDCCRequest"/>
                <wsdl:output message="intf:consultaDCCResponse"
                name="consultaDCCResponse"/>
        </wsdl:operation>
        <wsdl:operation name="consultaBIN">
                <wsdl:input message="intf:consultaBINRequest"
                name="consultaBINRequest"/>
                <wsdl:output message="intf:consultaBINResponse"
                name="consultaBINResponse"/>
        </wsdl:operation>
        <wsdl:operation name="iniciaPeticion">
                <wsdl:input message="intf:iniciaPeticionRequest"
        name="iniciaPeticionRequest"/>
                <wsdl:output message="intf:iniciaPeticionResponse"
        name="iniciaPeticionResponse"/>
        </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="trataPeticion">
                <wsdlsoap:operation soapAction=""/>
                <wsdl:input name="trataPeticionRequest">
                        <wsdlsoap:body use="literal"/>
                </wsdl:input>
                <wsdl:output name="trataPeticionResponse">
                        <wsdlsoap:body use="literal"/>
                </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="trataPeticion3DES">
                <wsdlsoap:operation soapAction=""/>
                <wsdl:input name="trataPeticionRequest3DES">
                        <wsdlsoap:body use="literal"/>
                </wsdl:input>
                <wsdl:output name="trataPeticionResponse3DES">
                        <wsdlsoap:body use="literal"/>
                </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="consultaDCC">
                <wsdlsoap:operation soapAction=""/>
                <wsdl:input name="consultaDCCRequest">
                        <wsdlsoap:body use="literal"/>
                </wsdl:input>
                <wsdl:output name="consultaDCCResponse">
                        <wsdlsoap:body use="literal"/>
                </wsdl:output>
        </wsdl:operation>
        <wsdl:operation name="consultaBIN">
                <wsdlsoap:operation soapAction=""/>
                <wsdl:input name="consultaBINRequest">
                        <wsdlsoap:body use="literal"/>
                </wsdl:input>
                <wsdl:output name="consultaBINResponse">
```

```
                        <wsdlsoap:body use="literal"/>
                    </wsdl:output>
                </wsdl:operation>
                <wsdl:operation name="iniciaPeticion">
                    <wsdlsoap:operation soapAction=""/>
                    <wsdl:input name="iniciaPeticionRequest">
                        <wsdlsoap:body use="literal"/>
                    </wsdl:input>
                    <wsdl:output name="iniciaPeticionResponse">
                        <wsdlsoap:body use="literal"/>
                    </wsdl:output>
                </wsdl:operation>
        </wsdl:binding>
        <wsdl:service name="SerClsWSEntradaService">
                <wsdl:port binding="intf:SerClsWSEntradaSoapBinding"
                name="SerClsWSEntrada">
                    <wsdlsoap:address
location="https://sis.redsys.es/sis/services/SerClsWSEntrada"/>
                </wsdl:port>
        </wsdl:service>
</wsdl:definitions>
```

2. Librerías de ayuda

2.1. Librerías de ayuda para el cálculo de la firma

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

2.1.1 Librería PHP

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

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

```
include_once 'redsysHMAC256_API_WS_PHP_4.0.2/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

obtenida del módulo de administración y el elemento con los datos de la petición de pago (<DATOSENTRADA>), tal y como se muestra a continuación:

```
$datosEntrada="<DATOSENTRADA><DS_MERCHANT_AMOUNT>200</DS_MERCHANT_AMOUNT><DS_MERCHANT_CURRENCY>978
$claveModuloAdmin = 'Mk9m98IfEblmPfrpsawt7BmxObt98Jev';
$signature = $miObj->createMerchantSignatureHostToHost($claveModuloAdmin, $datosEntrada);
```

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

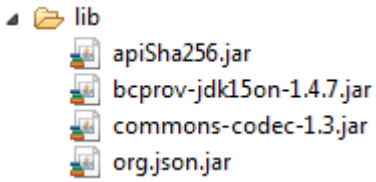
2.1.2 Librería JAVA

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

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

```
ApiWsMacSha256 apiWsMacSha256 = new ApiWsMacSha256();
```

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 obtenida del módulo de administración 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><DS_MERCHANT_CURRENCY>978
String claveModuloAdmin = "Mk9m98IfEblmPfrpsawt7BmxObt98Jev";
String signature = apiWsMacSha256.createMerchantSignatureHostToHost(claveModuloAdmin, datosEntrada);
```

Una vez obtenido el valor del elemento <DS_SIGNATURE>, ya se puedo completar el mensaje de petición de pago y realizar la llamada Web Service.

2.1.3 Librería .NET

A continuación, se presentan los pasos que debe seguir un comercio para la utilización de la librería .NET proporcionada por Redsys:

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

```
using RedsysAPIPrj;
```

2. Crear un objeto de la clase del Web Service de Redsys. Para poder realizar esto es necesario añadir una nueva referencia web con el fichero SerClsWSEntrada.wsdl.

```
WebRedsysWs.SerClsWSEntradaService s = new WebRedsysWs.SerClsWSEntradaService();
```

Nota: En el atributo location de la etiqueta <wsdlsoap:address> Del fichero SerClsWSEntrada.wsdl, indicar si se trata del entorno real o pruebas:

https://sis-t.redsys.es:25443/sis/services/SerClsWSEntrada (Pruebas)

https://sis.redsys.es/sis/services/SerClsWSEntrada (Real)

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

```
RedsysAPIWs r = new RedsysAPIWs();
```

Al realizar este paso se inicializan los atributos diccionario clave/valor m_keyvalues y cryp de la clase Cryptogra (Clase auxiliar para realizar las operaciones criptográficas necesarias)

4. Generar parametros de DATOSENTRADA (Modalidad Petición de Pago con envío de datos de tarjeta) mediante la función:

```
string dataEntrada = r.GenerateDatoEntradaXML(amount, fuc, currency, pan, cvv2, trans, terminal, expire);
```

5. 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 obtenida del módulo de administración y el elemento con los datos de la petición de pago (<DATOSENTRADA>), tal y como se muestra a continuación:

```
string signature = r.createMerchantSignatureHostToHost(kc, dataEntrada);
```

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

string XML final de petición de pago con DATOSENTRADA, DS_SIGNATUREVERSION y DS_SIGNATURE calculado en punto 5.

```
string requestXML = r.GenerateRequestXML(dataEntrada, signature);
```

Después se llama al método trataPeticion del Web service de Redsys pasándole como parámetro el string XML final calculado con el método GenerateRequestXML.

```
string result = s.trataPeticion(requestXML);
```

2.2. Librerías de ayuda respuesta Web service

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

2.2.1 Librería PHP

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

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

```
include_once 'redsysHMAC256_API_WS_PHP_4.0.2/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 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 obtenida del módulo de administración, la cadena que se desea firmar(concatenación de campos descrita en el punto 2 del apartado 4.1 del presente documento) y el número de pedido.

```
$cadenaConcatenada="1451444912789999008881978000000";
$numPedido="1444912789";
$claveModuloAdmin = 'Mk9m98IfEblmPfrpsawt7BmxObt98Jev';
$signature = $miObj->createSignatureResponseHostToHost($claveModuloAdmin,
                                                       $cadenaConcatenada,
                                                       $numPedido);
```

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

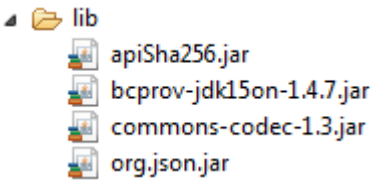
2.2.2 Librería JAVA

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

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

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

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



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

```
ApiWsMacSha256 apiWsMacSha256 = new ApiWsMacSha256();
```

4. 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 obtenida del módulo de administración, la cadena que se desea firmar(concatenación de campos descrita en el punto 2 del apartado 4.1 del presente documento) y el número de pedido.

```
String cadenaConcatenada="145144491278999900888197800000";
String numPedido="1444912789";
String claveModuloAdmin = "Mk9m98IfEblmPfrpsawt7BmxObt98Jev";
String signature = apiWsMacSha256.createSignatureResponseHostToHost(claveModuloAdmin,
                                                                    cadenaConcatenada,
                                                                    numPedido);
```

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

2.2.3 Librería .NET

A continuación, se presentan los pasos que debe seguir un comercio para la utilización de la librería .NET proporcionada por Redsys:

1. Convertir la cadena respuesta XML al atributo diccionario m_keyvalues de la clave RedsysAPIWs:

```
r.XMLToDiccionary(result);
```

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 obtenida del módulo de administración, 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 cadena = r.GenerateCadena(result);
string numOrder = r.GetDictionary("Ds_Order");
string signatureCalculate = r.createSignatureResponseHostToHost(kc, cadena, numOrder);
```

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