BBVA
Creando Oportunidades

TPV VIRTUAL

Manual de instalación para el desarrollador

Entrada REST

Versión 1.0

BBVA
Creando Oportunidades

Índice

1. INTRODUCCIÓN

1.1. Objetivo

Este documento recoge los aspectos técnicos necesarios para que un comercio realice la integración con el TPV Virtual utilizando un interfaz REST.

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, que permite autenticar al titular directamente con el banco emisor de su tarjeta en el momento de realizar la transacción que 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 avanzan en esta guía algunas nuevas características y especificaciones técnicas que estarán disponibles a futuro (en 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. Dichos epígrafes están marcados en su caso como "AVANCE".

Estas nuevas funcionalidades marcadas como "AVANCE", ya están disponibles en el entorno de Test.

1.2. Definiciones, siglas y abreviaturas

- SIS. 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 3DSecure en la nueva versión del TPV-Virtual

2. ENVÍO DE PETICIÓN

Para que el comercio pueda realizar la petición a través del método “trataPeticionREST” del interfaz REST, es necesario intercambiar una serie de datos, tanto en los mensajes de petición como en los mensajes de respuesta.

El comercio debe hacer llegar al TPV Virtual una petición POST mediante la interfaz REST. En dicha petición se enviará un JSON que incluya los siguientes parámetros:

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la petición codificada en Base 64 y sin retornos de carro (En la sección de anexos se incluye la lista de parámetros que se pueden enviar en una solicitud de pago).
- Ds_Signature: Firma de los datos enviados. Es el resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior.

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) cuya utilización se presenta en detalle en esta guía en los siguientes apartados y que están a su disposición en la siguiente dirección:

http://www.redsys.es/wps/portal/redsys/publica/areadeserviciosweb/descargaDeDocumentacion YEjecutables/

2.1. Identificar la versión de algoritmode 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 parámetro **Ds_SignatureVersion**.

2.2. Montar la cadena de datos de la petición (Ds_MerchantParameters)

En la petición se deben enviar todos los parámetros necesarios para identificar el tipo de operación que se desea realizar. Todos los parámetros se montarán en formato JSON, y el nombre de cada parámetro deberá indicarse en mayúsculas o con estructura “CamelCase” (Por ejemplo: DS_MERCHANT_AMOUNT o Ds_Merchant_Amount).

A continuación, se muestran un ejemplo del objeto JSON de una petición:

*{"DS_MERCHANT_AMOUNT":"145","DS_MERCHANT_ORDER":"1446068581","DS_MERCHANT_MERCHANTC ODE":"999008881","DS_MERCHANT_CURRENCY":"978","DS_MERCHANT_TRANSACTIONTYPE":"0","DS_MER CHANT_TERMINAL":"1","DS_MERCHANT_MERCHANTURL":"http:\/\/www.prueba.com\/urlNotificacion.php" ,"DS_MERCHANT_PAN":"454881*******04","DS_MERCHANT_EXPIRYDATE":"1512","DS_MERCHANT_CVV2 ":"123"}*

Una vez montada la cadena JSON con todos los campos, es necesario codificarla en BASE64 sin retornos de carro para asegurarnos de que se mantiene constante y no es alterada en el proceso de envío.

A continuación, se muestra el objeto JSON codificado en BASE64:

eyJEU19NRVJDSEFOVF9BTU9VTlQiOiIxNDUiLCJEU19NRVJDSEFOVF9PUkRFUiI6IjE0NDYwNjg1ODEiLCJEU1
9NRVJDSEFOVF9NRVJDSEFOVENPREUiOiI5OTkwMDg4ODEiLCJEU19NRVJDSEFOVF9DVVJSRU5DWSI6Ijk3
OCIsIkRTX01FUkNIQU5UX1RSQU5TQUNUSU9OVFlQRSI6IjAiLCJEU19NRVJDSEFOVF9URVJNSU5BTCI6IjEiL
CJEU19NRVJDSEFOVF9NRVJDSEFOVFVSTCI6Imh0dHA6XC9cL3d3dy5wcnVlYmEuY29tXC91cmxOb3RpZmlj
YWNpb24ucGhwIiwiRFNfTUVSQ0hBTlRfUEFOIjoiNDU0ODgxMjA0OTQwMDAwNCIsIkRTX01FUkNIQU5UX
0VYUElSWURBVEUiOiIxNTEyIiwiRFNfTUVSQ0hBTlRfQ1ZWMiI6IjEyMyJ9

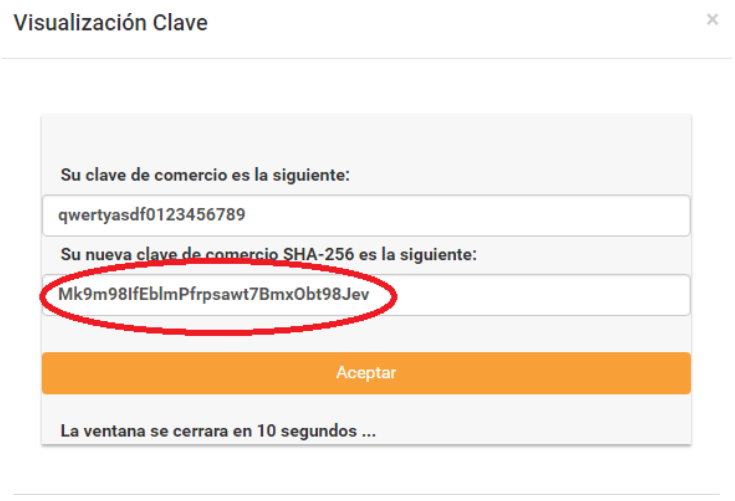
La cadena resultante de la codificación en BASE64 será el valor del parámetro **Ds_MerchantParameters**.

NOTA: La utilización de las librerías de ayuda proporcionadas para la generación de este campo, se expone en el apartado 2.4.

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

2.3. Firmar los datos de la petición (Ds_Signature)

Para calcular la firma es necesario utilizar una clave específica para cada terminal. Se puede obtener la clave accediendo al Portal de Administración, opción Consulta datos de Comercio, en el apartado "Ver 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 montada la cadena de datos a firmar (Ds_MerchantParameters) 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 valor del parámetro Ds_MerchantParameters y la clave obtenida en el paso anterior.
3. El resultado obtenido se codifica en BASE 64, y el resultado de la codificación será el valor del parámetro **Ds_Signature**.

NOTA: La utilización de las librerías de ayuda proporcionadas para la generación de este campo, se expone en el apartado 3.5.

2.4. Utilización de librerías de ayuda

En los apartados anteriores se ha descrito la forma de acceso al TPV Virtual utilizando la entrada REST y el sistema de firma basado en HMAC SHA256. En este apartado se explica como se utilizan las librerías disponibles en PHP, JAVA y .NET para facilitar los desarrollos y la generación de los campos del formulario de pago. El uso de las librerías suministradas es opcional, si bien simplifican los desarrollos a realizar por el comercio.

Librería PHP

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

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

```
include_once 'redsysHMAC256_API_PHP_4.0.2/apiRedsys.php';
```

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

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

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

3. Calcular el parámetro Ds_MerchantParameters. Para llevar a cabo el cálculo de este parámetro, inicialmente se deben añadir todos los parámetros de la petición de pago que se desea enviar, tal y como se muestra a continuación:

```
$miObj->setParameter("DS_MERCHANT_AMOUNT",$amount);
$miObj->setParameter("DS_MERCHANT_ORDER",$id);
$miObj->setParameter("DS_MERCHANT_MERCHANTCODE",$fuc);
$miObj->setParameter("DS_MERCHANT_CURRENCY",$moneda);
$miObj->setParameter("DS_MERCHANT_TRANSACTIONTYPE",$trans);
$miObj->setParameter("DS_MERCHANT_TERMINAL",$terminal);
$miObj->setParameter("DS_MERCHANT_MERCHANTURL",$url);
```

Por último, para calcular el parámetro Ds_MerchantParameters, se debe llamar a la función de la librería “createMerchantParameters()”, tal y como se muestra a continuación:

```
$params = $miObj->createMerchantParameters();
```

1. Calcular el parámetro Ds_Signature. Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería “createMerchantSignature()” con la clave obtenida del módulo de administración, tal y como se muestra a continuación:

```
$claveModuloAdmin = 'Mk9m98IfEblmPfrpsawt7BmxObt98Jev';
$signature = $miObj->createMerchantSignature($claveModuloAdmin);
```

2. Una vez obtenidos los valores de los parámetros Ds_MerchantParameters y Ds_Signature, se debe rellenar la petición REST con dichos valores y el parámetro Ds_SignatureVersion.

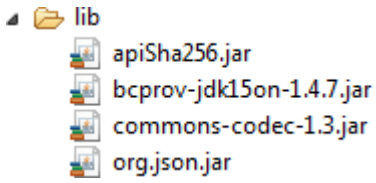
Librería JAVA

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

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

```
<%@page import="sis.redsys.api.ApiMacSha256"%>
```

   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:

```
ApiMacSha256 apiMacSha256 = new ApiMacSha256();
```

3. Calcular el parámetro Ds_MerchantParameters. Para llevar a cabo el cálculo de este

parámetro, inicialmente se deben añadir todos los parámetros de la petición de pago

```
apiMacSha256.setParameter("DS_MERCHANT_AMOUNT", amount);
apiMacSha256.setParameter("DS_MERCHANT_ORDER", id);
apiMacSha256.setParameter("DS_MERCHANT_MERCHANTCODE", fuc);
apiMacSha256.setParameter("DS_MERCHANT_CURRENCY", moneda);
apiMacSha256.setParameter("DS_MERCHANT_TRANSACTIONTYPE", trans);
apiMacSha256.setParameter("DS_MERCHANT_TERMINAL", terminal);
apiMacSha256.setParameter("DS_MERCHANT_MERCHANTURL", url);
```

que se desea enviar, tal y como se muestra a continuación:

Por último se debe llamar a la función de la librería “createMerchantParameters()”, tal y como se muestra a continuación:

```
String params = apiMacSha256.createMerchantParameters();
```

4. Calcular el parámetro Ds_Signature. Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería “createMerchantSignature()” con la clave obtenida del módulo de administración, tal y como se muestra a continuación:

```
String claveModuloAdmin = "Mk9m98IfEblmPfrpsawt7BmxObt98Jev";
String signature = apiMacSha256.createMerchantSignature(claveModuloAdmin);
```

5. Una vez obtenidos los valores de los parámetros Ds_MerchantParameters y Ds_Signature, se debe rellenar la petición REST con dichos valores y el parámetro Ds_SignatureVersion

Librería .NET

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

1. Importar la librería RedsysAPI y Newronsoft.Json en su proyecto.
2. Calcular el parámetro **Ds_MerchantParameters**. Para llevar a cabo el cálculo de este parámetro, inicialmente se deben añadir todos los parámetros de la petición de pago que se desea enviar, tal y como se muestra a continuación:

```
// New instance of RedysAPI
RedsysAPI r = new RedsysAPI();

// Fill Ds_MerchantParameters parameters
r.SetParameter("DS_MERCHANT_AMOUNT", amount);
r.SetParameter("DS_MERCHANT_ORDER", id);
r.SetParameter("DS_MERCHANT_MERCHANTCODE", fuc);
r.SetParameter("DS_MERCHANT_CURRENCY", currency);
r.SetParameter("DS_MERCHANT_TRANSACTIONTYPE", trans);
r.SetParameter("DS_MERCHANT_TERMINAL", terminal);
r.SetParameter("DS_MERCHANT_MERCHANTURL", url);
```

Por último se debe llamar a la función de la librería “createMerchantParameters()”, tal y como se muestra a continuación:

```
string parms = r.createMerchantParameters();
Ds_MerchantParameters.Value = parms;
```

1. Calcular el parámetro **Ds_Signature**. Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería “createMerchantSignature()” con la clave obtenida del módulo de administración, tal y como se muestra a continuación:

```
string sig = r.createMerchantSignature(kc);
Ds_Signature.Value = sig;
```

2. Una vez obtenidos los valores de los parámetros Ds_MerchantParameters y Ds_Signature, se debe rellenar la petición REST con dichos valores y el parámetro Ds_SignatureVersion.

3. RESPUESTA DE PETICIÓN

En función de si la respuesta se ha procesado correctamente o no, se recibirán dos tipos de respuesta:

1. **Respuesta de una operación procesada correctamente**

   Cuando una petición se ha procesado correctamente, una vez recibida la respuesta de la petición al TPV Virtual, el comercio debe capturar y validar los parámetros de retorno para conocer el resultado de la operación.

   Cualquier respuesta del TPV-Virtual será un JSON que incluirá los siguientes parámetros:

   - Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
   - Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la respuesta codificada en Base 64 y sin retornos de carro (En la sección de anexos se incluye la lista de parámetros que se pueden enviar en una solicitud de pago).
   - Ds_Signature: Firma de los datos recibidos. Es el resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior. **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.**

     Se posibilita la utilización de las librerías de ayuda para la captura y validación de los parámetros del retorno. En el siguiente apartado se muestra la utilización de las librerías de ayuda.

2. **Respuesta de una operación No procesada correctamente**

   Cuando una petición no se ha procesado correctamente, se informará en un JSON el código de error que identificará el motivo por el cual la petición no se ha podido procesar.

   El error que se ha producido se informará en el parámetro *errorCode*, tal y como se muestra a continuación:

   {"errorCode":"SIS0042"}

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

3.1 Utilización de librerías de ayuda

En los apartados anteriores se ha descrito la forma de acceso al TPV Virtual utilizando conexión REST. En este apartado se explica cómo se utilizan las librerías disponibles PHP, JAVA y .NET para facilitar los desarrollos para la recepción de los parámetros en la respuesta del servicio REST. El uso de las librerías es opcional, si bien simplifican los desarrollos a realizar por el comercio.

Librería PHP

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

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

```
include_once 'redsysHMAC256_API_PHP_4.0.2/apiRedsys.php';
```

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

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

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

2. Capturar los parámetros de la respuesta:

```
$version = $_GET["Ds_SignatureVersion"];
$params = $_GET["Ds_MerchantParameters"];
$signatureRecibida = $_GET["Ds_Signature"];
```

3. Decodificar el parámetro **Ds_MerchantParameters**. Para llevar a cabo la decodificación de este parámetro, se debe llamar a la función de la librería “decodeMerchantParameters()”, tal y como se muestra a continuación:

```
$decodec = $miObj->decodeMerchantParameters($params);
```

4. Una vez se ha realizado la llamada a la función “decodeMerchantParameters()”, se puede obtener el valor de cualquier parámetro que sea susceptible de incluirse en la respuesta. Para llevar a cabo la obtención del valor de un parámetro se debe llamar a la función “getParameter()” de la librería con el nombre de parámetro, tal y como se muestra a continuación para obtener el código de respuesta:

```
$codigoRespuesta = $miObj->getParameter("Ds_Response");
```

   NOTA IMPORTANTE: Es importante llevar a cabo la validación de todos los parámetros que se envían

en la comunicación.

5. Validar el parámetro **Ds_Signature**. Para llevar a cabo la validación de este parámetro se debe calcular la firma y compararla con el parámetro **Ds_Signature** capturado. Para ello se debe llamar a la función de la librería "createMerchantSignatureNotif()" con la clave obtenida del módulo de administración y el parámetro **Ds_MerchantParameters** capturado, tal y como se muestra a continuación:

```
$claveModuloAdmin = 'Mk9m98IfEblmPfrpsawt7BmxObt98Jev';
$signatureCalculada = $miObj->createMerchantSignatureNotif($claveModuloAdmin,
                                                           $params);
```

6. Una vez hecho esto, ya se puede validar si el valor de la firma enviada coincide con el valor de la firma calculada, tal y como se muestra a continuación:

```
if ($signatureCalculada === $signatureRecibida){
    echo "FIRMA OK. Realizar tareas en el servidor";
} else {
    echo "FIRMA KO. Error, firma inválida";
}
```

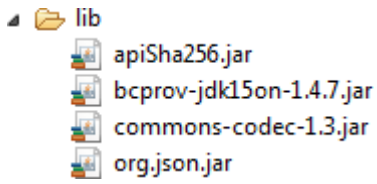
Librería JAVA

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

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

```
<%@page import="sis.redsys.api.ApiMacSha256"%>
```

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:

```
ApiMacSha256 apiMacSha256 = new ApiMacSha256();
```

3. Capturar los parámetros del retorno de la petición:

```
String version = request.getParameter("Ds_SignatureVersion");
String params = request.getParameter("Ds_MerchantParameters");
String signatureRecibida = request.getParameter("Ds_Signature");
```

Decodificar el parámetro **Ds_MerchantParameters**. Para llevar a cabo la decodificación de este parámetro, se debe llamar a la función de la librería "decodeMerchantParameters()", tal y como se muestra a continuación:

```
String decodec = apiMacSha256.decodeMerchantParameters(params);
```

Una vez se ha realizado la llamada a la función "decodeMerchantParameters()", se puede obtener el valor de cualquier parámetro que sea susceptible de incluirse en la respuesta (Anexo **¡Error! No se encuentra el origen de la referencia.**). Para llevar a cabo la obtención d el valor de un parámetro se debe llamar a la función "getParameter()" de la librería con el nombre de parámetro, tal y como se muestra a continuación para obtener el código de respuesta:

```
String codigoRespuesta = apiMacSha256.getParameter("Ds_Response");
```

NOTA IMPORTANTE: Es importante llevar a cabo la validación de todos los parámetros que se envían en la comunicación.

4. Validar el parámetro **Ds_Signature**. Para llevar a cabo la validación de este parámetro se debe calcular la firma y compararla con el parámetro **Ds_Signature** capturado. Para ello se debe llamar a la función de la librería "createMerchantSignatureNotif()" con la clave obtenida del módulo de administración y el parámetro **Ds_MerchantParameters** capturado, tal y como se muestra a continuación:

```
String claveModuloAdmin = "Mk9m98IfEblmPfrpsawt7BmxObt98Jev";
String signatureCalculada = apiMacSha256.createMerchantSignatureNotif(claveModuloAdmin,
                                                                      params);
```

Una vez hecho esto, ya se puede validar si el valor de la firma enviada coincide con el valor de la firma calculada, tal y como se muestra a continuación:

```
if (signatureCalculada.equals(signatureRecibida)) {
    System.out.println("FIRMA OK. Realizar tareas en el servidor");
} else {
    System.out.println("FIRMA KO. Error, firma inválida");
}
```

Librería .NET

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

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

```
using RedsysAPIPrj;
```

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

```
RedsysAPI r = new RedsysAPI();
```

c. Capturar los parámetros del retorno:

```
string version = Request.QueryString["Ds_SignatureVersion"];

string parms = Request.QueryString["Ds_MerchantParameters"];

string signatureRecibida = Request.QueryString["Ds_Signature"];
```

NOTA IMPORTANTE: Es importante llevar a cabo la validación de todos los parámetros que se envían en la comunicación.

d. Validar el parámetro **Ds_Signature**. Para llevar a cabo la validación de este parámetro se debe calcular la firma y compararla con el parámetro **Ds_Signature** capturado. Para ello se debe llamar a la función de la librería “createMerchantSignatureNotif()” con la clave obtenida del módulo de administración y el parámetro **Ds_MerchantParameters** capturado, tal y como se muestra a continuación:

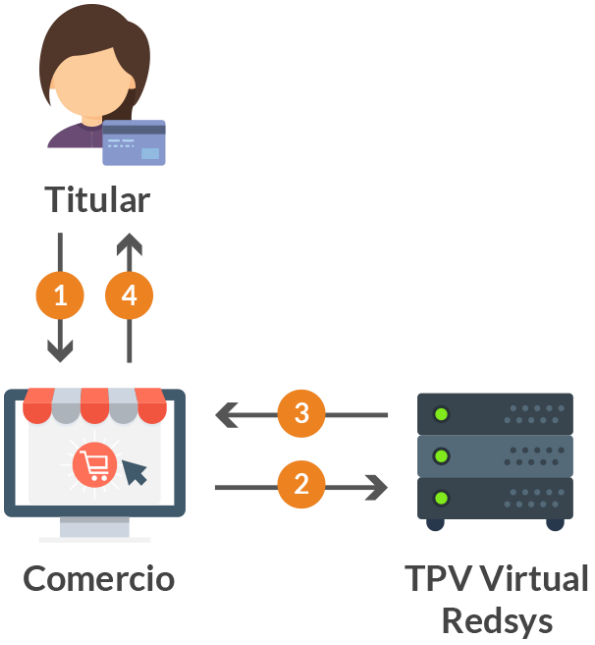
```
var kc = "sq7HjrUOBfKmC576ILgskD5srU870gJ7";

string signatureCalculada =  r.createMerchantSignatureNotif(kc, parms);
```

Una vez hecho esto, ya se puede validar si el valor de la firma enviada coincide con el valor de la firma calculada, tal y como se muestra a continuación:

```
if (signatureRecibida == signatureCalculada)
{
    result.InnerHtml = "FIRMA OK. Realizar tareas en el servidor";
}
else
{
    result.InnerHtml = "FIRMA KO. Error, firma invalida";
}
```

4. TRANSACCIONES DIRECTAS (Sin Autenticación)

El siguiente esquema presenta el flujo general de una operación realizada a través de la entrada REST del TPV Virtual sin 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 envía los datos del pago al TPV virtual.
3. Una vez realizado el pago, el TPV virtual informa del resultado de la operación.
4. El comercio devuelve la información del resultado del pago al titular.

4.1. Envío de petición al TPV Virtual

Como se muestra en el paso 2 del esquema anterior, el comercio debe enviar al TPV Virtual los datos de la petición de pago en una petición REST. En dicha petición deberá incluir los siguientes parámetros:

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la petición codificada en Base 64 y sin retornos de carro (En la sección de anexos se incluye la lista de parámetros que se pueden enviar en una solicitud de pago).
- Ds_Signature: Firma de los datos enviados. Es el resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior.

Dichos parámetros deben enviarse a los siguientes endpoints, dependiendo de si se quiere realizar una petición en el entorno de prueba u operaciones reales:

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

4.2. Recepción del resultado

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

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la respuesta codificada en Base 64 y sin retornos de carro.
- Ds_Signature: Firma de los datos enviados. Resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior.

NOTA: El TPV Virtual envía la notificación on-line a la URL informada por el comercio en el parámetro Ds_Merchant_MerchantURL.

5. Transacciones con Autenticación 3DSecure 1.0 y EMV3DS

5.1. Pasos para realizar una transacción con autenticación EMV3DS (Avance)

Los pagos con autenticación EMV3DS en la conexión REST 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.**

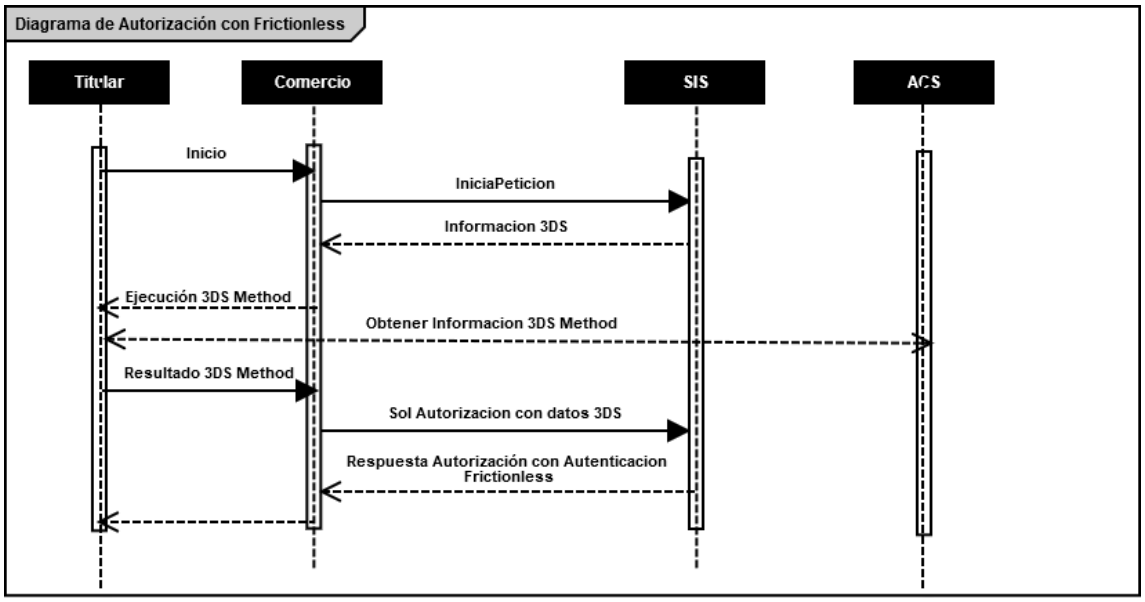
Además, en el caso del protocolo EMV3DS, el comercio también deberá estar preparado para soportar ambos procesos de Autenticación: Challenge (con intervención del titular) o Frictionless (sin intervención del titular). El emisor de la tarjeta será el encargado de determinar el proceso de Autenticación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

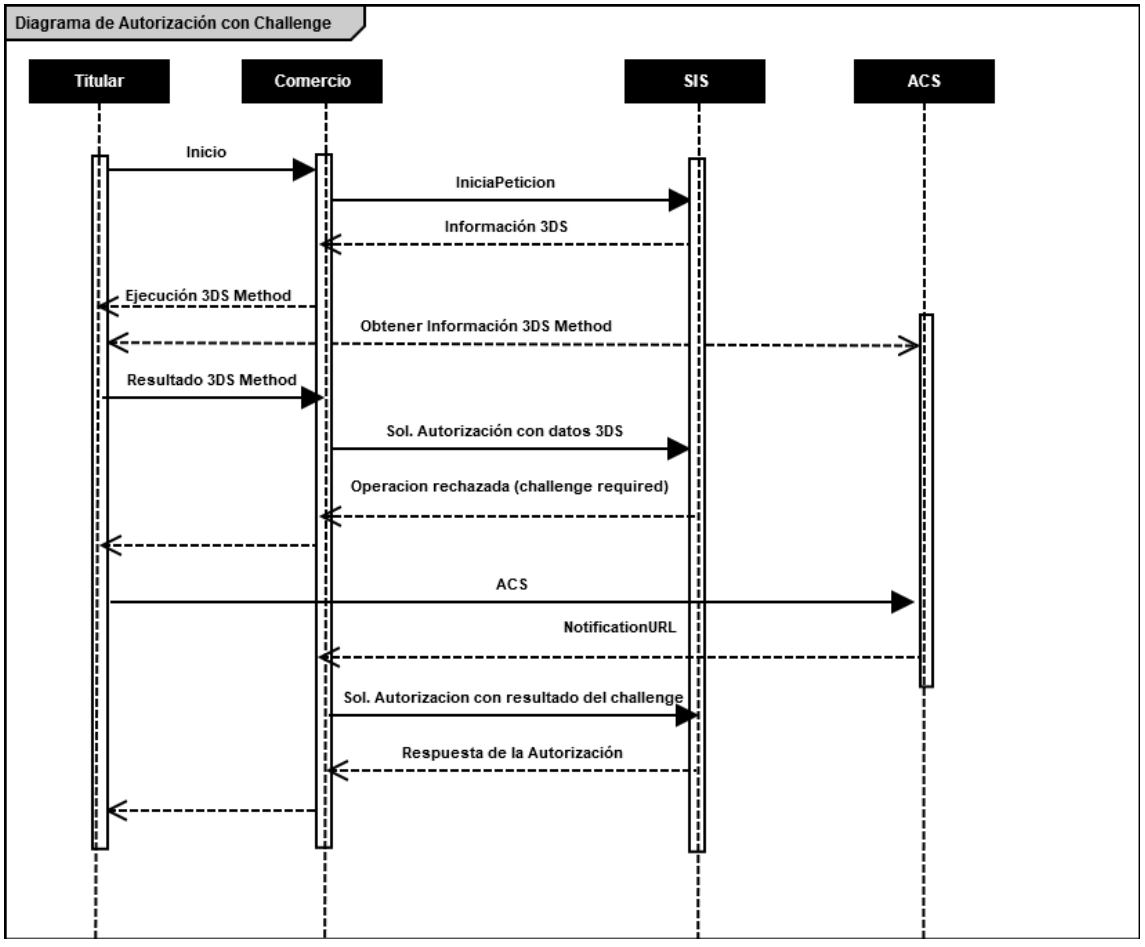
   El TPV Virtual inicia la autenticación, y el emisor, en base a los datos recibidos, autentica la operación sin necesidad de intervención del titular. A continuación, el TPV Virtual procesará la autorización

5. Una vez realizado el pago, el TPV virtual informa del resultado de la operación.
6. El comercio muestra el 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.

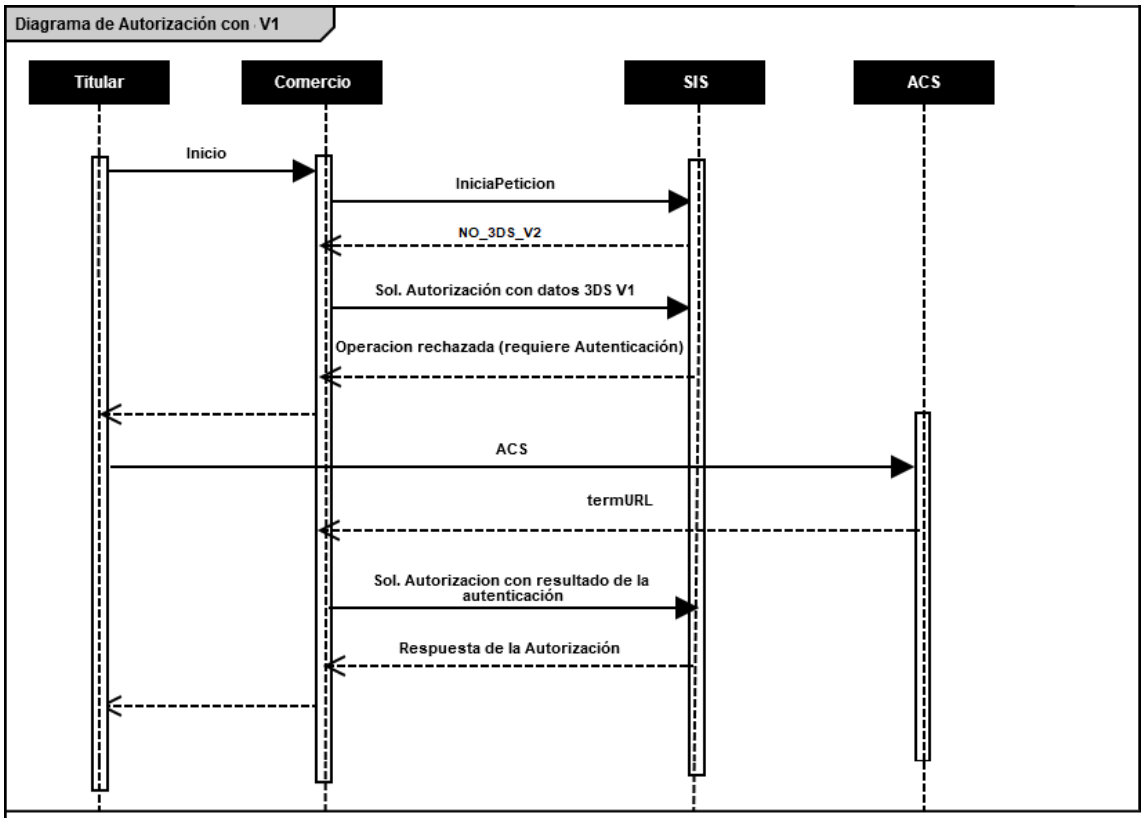
    El TPV Virtual inicia la autenticación, y el emisor en base a los datos recibidos decide que el titular debe verificar su autenticidad (challenge)

5. El TPV Virtual devuelve la información para que el titular pueda realizar el challenge (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 = 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.

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 al comercio informará de la versión de protocolo de autenticación que soporta la operación.

    3.1. Si la tarjeta no permite EMV3DS, se recibirá un valor protocolo **NO_3DS_v2**. En este caso el comercio puede solicitar la autenticación mediante protocolo 3DSecure 1.0.

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.

5.2. Peticiones para realizar una transacción con autenticación EMV3DS (Avance)

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 REST al TPV Virtual En dicha petición deberá incluir los siguientes parámetros:

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la petición codificada en Base 64 y sin retornos de carro (Consultar Parámetros de entrada y salida).
- Ds_Signature: Firma de los datos enviados. Es el resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior

Dichos parámetros deben enviarse a los siguientes endpoints dependiendo de si se quiere realizar una petición en el entorno de prueba u operaciones reales:

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

Una vez gestionada la petición, el TPV Virtual informará al servidor del comercio el resultado

de la misma, con la información del resultado incluida en un fichero JSON. En él se incluirán los siguientes campos:

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la respuesta codificada en Base 64 y sin retornos de carro.
- Ds_Signature: Firma de los datos enviados. Resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior. **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.**

A continuación, se describen los datos que debe incluir el Ds_MerchantParameters para enviar un inicia petición al Servicio REST:


```
{
  "DS_MERCHANT_ORDER":"1552571678",
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"999",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX ",
  "DS_MERCHANT_EMV3DS": {"threeDSInfo":"CardData"}
}
```


Como respuesta se obtendrá lo siguiente:


```
{
  "Ds_Order":"1552571678",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_TransactionType":"0",
  "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_Card_PSD2":"Y"
}
```


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 REST al TPV Virtual En dicha petición deberá incluir los siguientes parámetros:

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la petición codificada en Base 64 y sin retornos de carro (Consultar Parámetros de entrada y salida).
- Ds_Signature: Firma de los datos enviados. Es el resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior

Dichos parámetros deben enviarse a los siguientes endpoints dependiendo de si se quiere realizar una petición en el entorno de prueba u operaciones reales:

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

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

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la respuesta codificada en Base 64 y sin retornos de carro.
- Ds_Signature: Firma de los datos enviados. Resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior. **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.**

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

```
{
  "DS_MERCHANT_ORDER":1552572812,
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"2",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
```

```
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX ",
  "DS_MERCHANT_EXPIRYDATE":"XXXX",
  "DS_MERCHANT_CVV2":"XXX", "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://comercio-inventado.es/recibe-respuesta-autenticacion",
                  "threeDSCompInd":"Y"
          }
}
```


Como respuesta se obtendrá:

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


```
{
  "Ds_Amount":"1000",
  "Ds_Currency":"978",
  "Ds_Order":"1552572812",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_Response":"0000",
  "Ds_AuthorisationCode":"694432",
  "Ds_TransactionType":"0",
  "Ds_SecurePayment":"1",
  "Ds_Language":"1",
  "Ds_CardNumber":"454881******0004",
  "Ds_Card_Type":"C",
  "Ds_MerchantData":"",
  "Ds_Card_Country":"724",
  "Ds_Card_Brand":"1"
}
```


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


```
{
  "Ds_Amount":"1000",
  "Ds_Currency":"978",
  "Ds_Order":"1552572812",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_TransactionType":"0",
  "Ds_EMV3DS":{
          "threeDSInfo":"ChallengeRequest",
          "protocolVersion":"2.1.0",
           "acsURL":"https://sis.redsys.es/sis-simulador-web/authenticationRequest.jsp",
            "creq":"eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6IjhkZTg0NDMwLTMzMzYtNGZmNC1iMThkLWYwNzNiNTQ
2Y2NlYSIsImFjc1RyYW5zSUQiOiJkYjVjOTljNC1hMmZkLTQ3ZWUtOTI2Zi1mYTBiMDk0MzUyYTAiLCJtZXNzYWdlVHlwZSI
6IkNSZXEiLCJtZXNzYWdlVmVyc2lvbiI6IjIuMS4wIiwiY2hhbGxlbmdlV2luZG93U2l6ZSI6IjA1In0"
  }
}
```

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="eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6ImU5OWMzYzI2LTFiZWItNGY4NS05ZmE3LTI3OTJiZjE5NDZlMiIsImFjc1Ry
YW5zSUQiOiIyMTQzNDFhYi0wMjlhLTRmMGEtOTEyNi1iMDFkYmE5OTc2MTkiLCJtZXNzYWdlVHlwZSI6IkNSZXEiLCJtZXNzY
WdlVmVyc2lvbiI6IjIuMS4wIiwiY2hhbGxlbmdlV2luZG93U2l6ZSI6IjA1In0">
</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 el Ds_MerchantParameters para enviar una petición de confirmación de autorización EMV3DS al Servicio REST:

```
{
  "DS_MERCHANT_ORDER":1552577128, "DS_MERCHANT_MERCHANTCODE":"999008881", "DS_MERCHANT_TERMINAL":"2",
  "DS_MERCHANT_CURRENCY":"978", "DS_MERCHANT_TRANSACTIONTYPE":"0", "DS_MERCHANT_AMOUNT":"1000",
```

"DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX ", "DS_MERCHANT_EXPIRYDATE":"XXXX", "DS_MERCHANT_CVV2":"XXX",
"DS_MERCHANT_EMV3DS":{
"threeDSInfo":"ChallengeResponse", "protocolVersion":"2.1.0",
"cres":"eyJ0aHJlZURTU2VydmVyVHJhbnNJRCI6IjhkZTg0NDMwLTMzMzYtNGZmNC1iMThkLWYw
NzNiNTQ2Y2NlYSIsImFjc1RyYW5zSUQiOiJkYjVjOTljNC1hMmZkLTQ3ZWUtOTI2Zi1mYTBiMDk0MzUyYTAiLCJ
tZXNzYWdlVHlwZSI6IkNSZXMiLCJtZXNzYWdlVmVyc2lvbiI6IjIuMS4wIiwidHJhbnNTdGF0dXMiOiJZIn0="
}
}

Como respuesta se obtendrá el resultado final de la operación:

{
"Ds_Amount":"1000",
"Ds_Currency":"978",
"Ds_Order":"1552572812",
"Ds_MerchantCode":"999008881",
"Ds_Terminal":"2",
"Ds_Response":"0000",
"Ds_AuthorisationCode":"694432",
"Ds_TransactionType":"0",
"Ds_SecurePayment":"1",
"Ds_Language":"1",
"Ds_CardNumber":"454881******0004",
"Ds_Card_Type":"C",
"Ds_MerchantData":"",
"Ds_Card_Country":"724",
"Ds_Card_Brand":"1"
}

5.3. 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.

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

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la petición codificada en Base 64 y sin retornos de carro (Consultar Parámetros de entrada y salida).
- Ds_Signature: Firma de los datos enviados. Es el resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior

Dichos parámetros deben enviarse a los siguientes endpoints dependiendo de si se quiere realizar una petición en el entorno de prueba u operaciones reales:

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

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

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la respuesta codificada en Base 64 y sin retornos de carro.
- Ds_Signature: Firma de los datos enviados. Resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior. **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.**

A continuación, se describen los datos de debe incluir el Ds_MerchantParameters para enviar un inicia petición al Servicio REST:

```
{
  "DS_MERCHANT_ORDER":"1552571678",
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"999",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX ",
  "DS_MERCHANT_EMV3DS": {"threeDSInfo":"CardData"}
}
```

Como respuesta se obtendrá lo siguiente:

```
{
  "Ds_Order":"1552571678",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_TransactionType":"0",
  "Ds_EMV3DS": {
    "protocolVersion":"NO_3DS_V2"
  },
   "Ds_Card_PSD2":"Y"
}
```

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

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la petición codificada en Base 64 y sin retornos de carro (Consultar Parámetros de entrada y salida).
- Ds_Signature: Firma de los datos enviados. Es el resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior

Dichos parámetros deben enviarse a los siguientes endpoints dependiendo de si se quiere realizar una petición en el entorno de prueba u operaciones reales:

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

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

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la respuesta codificada en Base 64 y sin retornos de carro.
- Ds_Signature: Firma de los datos enviados. Resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior. **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.**

A continuación, se describen los datos que debe incluir el Ds_MerchantParameters para enviar una petición de autenticación al Servicio REST:

```
{
  "DS_MERCHANT_ORDER":1552642885,
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"2",
```

```
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX ",
  "DS_MERCHANT_EXPIRYDATE":"XXXX",
  "DS_MERCHANT_CVV2":"XXX", "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"
                        }
}
```


Como respuesta se obtendrá lo siguiente:


```
{
  "Ds_Order":"1552642885",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_Currency":"978",
  "Ds_Amount":"1000",
  "Ds_TransactionType":"0",
  "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+Jftln6R09p88WcRHOjNg9gZkqk
U5KOIIPhVi6kfAznlQhZ1BintPcNr0gqC2TeKBsszfDJAHhiw6yWgS0hYDAuzrqkS6QbL+xkDOaEY73Cafr6zGuiXZ/lololEYW
LnPjK2WkzhBJC7lLABm/2VXJ9n1GVD073n8AOa7wW0=",
            "MD":"cd164a6d0b77c96f7ef476121acfa987a0edf602"
  }
}
```


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 Ds_MerchantParameters para enviar una petición de confirmación de autorización 3DSecure 1.0 al Servicio REST:


```
{
```

```
  "DS_MERCHANT_ORDER":1552642885,
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"2",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX ",
  "DS_MERCHANT_EXPIRYDATE":"XXXX",
  "DS_MERCHANT_CVV2":"XXX",
  "DS_MERCHANT_EMV3DS":{
            "threeDSInfo":"ChallengeResponse",
            "protocolVersion":"1.0.2",
            "PARes":"eJzFWNmSo0iyfecrymoeNVVsWqBNmWPBKlaJVcAbmwBJLALE9vWDlJVZWT3VNn3vw70yyRR4u
 Dvu ESeOu8X2X0N+/dLFdZOVxctX9Dvy9UtchGWUFcnLV8vkvhFf//W6NdM6jhkjDu91/LpV4qbxk/hL …..",
            "MD":"035535127d549298f11d7d2fc1b0d4e9300f93f1"
            }
}
```


Como respuesta se obtendrá el resultado final de la operación:


```
{
  "Ds_Amount":"1000",
  "Ds_Currency":"978",
  "Ds_Order":"1552642885",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_Response":"0000",
  "Ds_AuthorisationCode":"694432",
  "Ds_TransactionType":"0",
  "Ds_SecurePayment":"1",
  "Ds_Language":"1",
  "Ds_CardNumber":"454881******0004",
  "Ds_Card_Type":"C",
  "Ds_Card_Country":"724",
  "Ds_Card_Brand":"1"
}
```

6. Transacciones con DCC

6.1. 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 REST. El comercio tiene que estar configurado para realizar este tipo de operativa.

Los pagos con DCC en la conexión Rest 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.

NOTA: 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.

6.2. Pasos para realizar una transacción con DCC

Iniciar Petición

Esta petición permite obtener los datos de DCC para la petición solicitada.

El inicio de petición se hace a través de una petición REST al TPV Virtual En dicha petición deberá incluir los siguientes parámetros:

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la petición codificada en Base 64 y sin retornos de carro (Consultar Parámetros de entrada y salida).
- Ds_Signature: Firma de los datos enviados. Es el resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior

Dichos parámetros deben enviarse a los siguientes endpoints dependiendo de si se quiere realizar una petición en el entorno de prueba u operaciones reales:

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

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

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la respuesta codificada en Base 64 y sin retornos de carro.
- Ds_Signature: Firma de los datos enviados. Resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior. **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.**

A continuación, se describen los datos de debe incluir el Ds_MerchantParameters para enviar una petición de inicia peticion al Servicio REST:


```
{
  "DS_MERCHANT_ORDER":1552580496,
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"2",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_PAN":"XXXXXXXXXXXXXXXXXX",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_DCC":"Y"
}
```


Como respuesta se obtendrá lo siguiente:


```
{
  "Ds_Order":"1552580496",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_TransactionType":"0",
  "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"
    },
    "InfoMonedaTitular":{
      "monedaCome":"978",
      "litMonedaCome":"EUR",
      "importeCome":"10.00"
```

```
    }
  }
  "Ds_Card_PSD2":"Y"
}
```

Petición de autorización con DCC

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

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

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la petición codificada en Base 64 y sin retornos de carro (Consultar Parámetros de entrada y salida).
- Ds_Signature: Firma de los datos enviados. Es el resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior

Dichos parámetros deben enviarse a los siguientes endpoints dependiendo de si se quiere realizar una petición en el entorno de prueba u operaciones reales:

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

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

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando.
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la respuesta codificada en Base 64 y sin retornos de carro.
- Ds_Signature: Firma de los datos enviados. Resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior. **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.**

A continuación, se describen los datos de debe incluir el Ds_MerchantParameters para enviar una petición de autorización con DCC al Servicio REST:


```
{
  "DS_MERCHANT_ORDER":1552581014,
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"2",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":"XXXXXXXXXXXXXXXXXX",
  "DS_MERCHANT_EXPIRYDATE":"XXXX",
  "DS_MERCHANT_CVV2":"XXX",
  "DS_MERCHANT_DCC":{
                    "monedaDCC":"840",
                    "importeDCC":"11.50"
                    }
}
```


Como respuesta se obtendrá el resultado final de la operación:


```
{
  "Ds_Amount":"1000",
  "Ds_Currency":"978",
  "Ds_Order":"1552572812",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_Response":"0000",
  "Ds_AuthorisationCode":"694432",
  "Ds_TransactionType":"0",
  "Ds_SecurePayment":"1",
  "Ds_Language":"1",
  "Ds_CardNumber":"454881******0004",
  "Ds_Card_Type":"C",
  "Ds_MerchantData":"",
  "Ds_Card_Country":"724",
  "Ds_Card_Brand":"1"
}
```

7. Transacciones Autenticadas con DCC

7.1. 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 REST. 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 específica 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.

NOTA: 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.

7.2. Pasos para realizar una transacción 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 EMV3DS se deberán seguir el apartado
Iniciar Petición añadiendo los datos de DCC.

A continuación, se describen los datos que debe incluir el Ds_MerchantParameters para enviar una petición de inicia petición al Servicio REST con autenticación y 3DS:


```
{
  "DS_MERCHANT_ORDER":1552580496,
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"2",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_PAN":"XXXXXXXXXXXXXXXXXX",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_DCC":"Y"
   "DS_MERCHANT_EMV3DS": {"threeDSInfo":"CardData"}
 }
```


Como respuesta se obtendrá lo siguiente:


```
{
  "Ds_Order":"1552580496",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_TransactionType":"0",
  "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"
    },
    "InfoMonedaTitular":{
      "monedaCome":"978",
      "litMonedaCome":"EUR",
      "importeCome":"10.00"
    }
   },
   "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_Card_PSD2":"N"

}
```

Petición de autorización con DCC

A continuación, se describen los datos de debe incluir el Ds_MerchantParameters para enviar una petición de autorización con DCC al Servicio REST:


```
{
  "DS_MERCHANT_ORDER":1552581014,
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"2",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":"XXXXXXXXXXXXXXXXXX",
  "DS_MERCHANT_EXPIRYDATE":"XXXX",
  "DS_MERCHANT_CVV2":"XXX",
  "DS_MERCHANT_DCC":{
                        "monedaDCC":"840",
                        "importeDCC":"11.50"
                                },
   "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://sis-d.redsys.es/sis-simulador-
 web/SisRESTCreqCres_3DSecureV2.jsp",
                        "threeDSCompInd":"Y"
            }

}
```

8. Adaptaciones PSD2 (Avance)

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 se definen una serie de exenciones al uso de SCA que podrán venir marcadas en la petición de autorización.

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

- LWV: 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: exención por utilizarse un sistema de análisis de riesgo (y considerarse bajo riesgo) por parte de BBVA/comercio.
- MIT: operación iniciada por el comercio (sin estar asociada a una acción o evento del cliente) que están fuera del alcance de la PSD2. Este es el caso de las operativas de pagos de subscripciones, recurrentes, etc. todas las que requieren el almacenamiento de las credenciales de pago del cliente (COF) o su equivalente mediante operativas de pagos programados tokenizados (uso funcionalidad “pago por referencia” en pagos iniciados por el comercio). Toda operativa de pago iniciada por el comercio (MIT) requiere que inicialmente cuando el cliente concede el permiso al comercio de uso de sus credenciales de pago, dicho “permiso o mandato” se haga mediante operación autenticada con SCA.
- COR: exención restringida a los casos de uso de un protocolo pago corporativo seguro.
- ATD: exención de autenticación delegada.

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 quiere aceptar la propuesta de exención y requiere SCA pueda solicitar la autenticación en el mismo momento sin necesidad de rechazar la operación (challenge required EMV3DS).

8.1. Ejemplos de peticiones con exenciones.

Como anteriormente podemos observar la normativa contemplan diferentes exenciones que se pueden marcar para no autenticar algunas de las operaciones de comercio electrónico. 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 BBVA, 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.

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

EJEMPLO DE INICIA PETICIÓN


```
{
  "DS_MERCHANT_ORDER":"1552571678",
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"999",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_EXCEP_SCA":"Y",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX ",
  "DS_MERCHANT_EMV3DS": {"threeDSInfo":"CardData"}
}
```


Como respuesta se obtendrá lo siguiente:


```
{
  "Ds_Order":"1552571678",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_TransactionType":"0",
  "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_Excep_SCA":"LWV;TRA[30.0];COR;MIT;ATD;WHL",
   "Ds_Card_PSD2":"Y"
}
```

Mensaje Trata Petición (Con EMV3DS)


```
{
  "DS_MERCHANT_ORDER":1552572812,
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"2",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"100",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX ",
  "DS_MERCHANT_EXPIRYDATE":"XXXX",
  "DS_MERCHANT_CVV2":"XXX",
  "DS_MERCHANT_EXCEP_SCA:"LWV",
  "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",
                  "browserJavaScriptEnabled":"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"
          }
}
```


Mensaje Trata Petición (Sin EMV3DS)


```
{
  "DS_MERCHANT_ORDER":1552572812,
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"2",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"100",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX ",
  "DS_MERCHANT_EXPIRYDATE":"XXXX",
  "DS_MERCHANT_CVV2":"XXX",
  "DS_MERCHANT_EXCEP_SCA:"LWV"
}
```


8.2. Transacciones iniciadas por el comercio (MIT)

¿Qué se considera una transacción MIT?

Las transacciones iniciadas por el comercio, sin que haya interacción posible con el cliente. Por ejemplo, pago mensual de un recibo o cuota de subscripción. Este tipo de exención requiere el marcaje de la operativa como COF (Credencial on File) de acuerdo al uso concreto que se esté haciendo de las credenciales almacenadas.

MIT inicial: Esta operación deberá ser autenticada con SCA. El titular está presente y es aquella en la que concede el permiso y acuerda con el comercio las condiciones para que se usen sus datos de pago para cargos posteriores de acuerdo a un servicio prestado continuado en el tiempo. Esta operativa debe marcarse debidamente siguiendo la especificación Card-on-file (COF) para indicar que los datos de tarjeta se están almacenando para pagos posteriores.

MIT posteriores: En estas operaciones MIT el titular no está presente y no puede ser autenticado. Esta operativa debe también marcarse debidamente siguiendo la especificación Card-on-file (COF) para indicar que se está realizando una operación recurrente sobre una inicial MIT que sí fue autenticada.

¿Cómo afecta PSD2 al pago 1 click?

No todas las operativas en las que se utilizan datos de tarjeta/credenciales almacenadas (COF) son consideradas MIT. Por ejemplo, la operativa de pago en 1 clic, donde las credenciales del cliente están almacenadas o tokenizadas (pago por referencia) con el objetivo de facilitar al máximo el momento del pago sin tener que solicitarlas de nuevo al cliente, **NO** se puede considerar una transacción iniciada por el comercio ya que, en el momento de la compra, el titular está presente. En tal caso según PSD2, y mientras no se aplique otra exención, se requiere el uso de autenticación reforzada (SCA).

NOTA: El listado completo de todos los parámetros de entrada del TPV Virtual se presenta en la hoja de cálculo "TPV-Virtual Parámetros Entrada-Salida.xlsx".

NOTA2: Acceder a la Guía COF para más información "Especificaciones COF ECom v1.1.pdf".

Transacciones MIT y uso de tokenización (pago por referencia)

En muchos casos se suele utilizar la tokenización de las credenciales de pago del cliente para que el TPV Virtual se encargue del almacenamiento seguro de los mismos y asegurar el cumplimiento de los estándares de seguridad de PCI DSS, con el objetivo de generar más tarde pagos iniciados por el comercio sin estar presente el titular de la tarjeta.

En estos casos, en la transacción inicial en la que se solicitar el token o referencia, bajo PSD2 se debe utilizar 3D Secure para aplicar autenticación reforzada y además se debe marcar adecuadamente mediante los parámetros COF el uso que se dará a la misma, de forma que en usos posteriores iniciados por el comercio con el token/referencia, el propio tpv virtual incorpore de forma automática la información de marcaje de uso adecuada e información adicional requerida según la marca de la tarjeta (pej: id transacción original requerido para los pagos COF en Visa "DS_MERCHANT_COF_TXNID")

1. Uso de tokenización y MIT

En algunos casos se utiliza el pago por referencia o tokenización para realizar operaciones sucesivas sin que el titular esté presente. Para estos casos el comercio deberá enviar los parámetros COF y la solicitud de generación de referencia y en los pagos posteriores solo deberá marcar la exención MIT y la referencia a utilizar.

1) En la primera operación deberá enviar los parámetros COF (DS_MERCHANT_COF_INI, DS_MERCHANT_COF_TYPE) y la solicitud de generación de referencia.
2) Pagos sucesivos deberá marcar DS_MERCHANT_COF_INI (N) , DS_MERCHANT_EXCEP_SCA como MIT y la referencia a utilizar.

9. Funcionalidades Avanzadas EMV3DS (Avance)

De cara a la normativa PSD2 en la que se obliga a la autenticación de todas las operaciones de comercio electrónico, el protocolo ofrece la posibilidad de autenticar también esas operaciones en las que el titular no está presente. Se distingues dos casos diferenciados

- Operaciones Recurrentes: que ofrecen al comercio la posibilidad de realizar posteriores transacciones recurrentes autenticadas.
- Operaciones OTA: que ofrecen al comercio la posibilidad de realizar una única transacción de autenticación por el importe íntegro y, asociados a la misma, efectuar los cargos parciales en los diferentes comercios que formen parte de la transacción en momentos posteriores a la autenticación.

Estas operaciones se distingues en dos partes.

- Petición inicial con autenticación del titular. En esta petición el titular está presente y se autentica SCA, al solicitar que será una operación 3RI, se devolverán los datos necesarios para realizar las operaciones posteriores.
- Peticiones posteriores. Con los datos obtenidos en la operación inicial de autenticación se realizan las sucesivas operaciones de autorización.

NOTA: para realizar esta integración se requiere activación por parte de BBVA y solo estará disponible con la versión del protocolo 2.2. de EMV3DS.

NOTA2: estas funcionalidades están sujetas a posibles modificaciones exigidas por las marcas, por lo que en los siguientes apartados se muestra una aproximación con los detalles conocidos actualmente.

9.1. Pagos recurrentes EMV3DS ("3RI-Recurring")

Este tipo de operativa ofrece al comercio la posibilidad de autenticar los pagos recurrentes, de forma que se ejerce el cambio de responsabilidad y el comercio estará protegido en caso de fraude en estos pagos.

El primer pago recurrente siempre deberá ser autenticado por el titular. Los pagos sucesivos serán autenticados (3RI) sin intervención del titular, pero será necesario que el comercio proporcione al TPV Virtual los datos necesarios para la autenticación que se verán a continuación:

Pago recurrente inicial

El primer pago se procesará como una transacción autenticada EMV 3DS (frictionless o challenge) siguiendo los pasos habituales. Para solicitar que será una operación recurrente

se tendrán que marcar los parámetros COF.

- Inicia petición

EJEMPLO DE PETICIÓN:


```
{
  "DS_MERCHANT_ORDER":"1552571678",
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"999",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX ",
  "DS_MERCHANT_EMV3DS": {"threeDSInfo":"CardData"}
}
```


Como respuesta se obtendrá lo siguiente:


```
{
  "Ds_Order":"1552571678",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_TransactionType":"0",
  "Ds_EMV3DS": {
    "protocolVersion":"2.2.0",
    "threeDSServerTransID":"8de84430-3336-4ff4-b18d-f073b546ccea",
    "threeDSInfo":"CardConfiguration",
    "threeDSMethodURL":https://sis.redsys.es/sis-simulador-web/threeDsMethod.jsp
  },
    "Ds_Card_PSD2":"Y"
}
```


- Ejecución del 3DSMethod
- Trata petición

  En la Petición de Autorización al “tratapeticion” debe marcarse la operación como COF Inicial Recurrente:

  - DS_MERCHANT_COF_INI = “S” ⟶ OPERACIÓN COF INICIAL SI
  - DS_MERCHANT_COF_TYPE = “R” ⟶ OPERACIÓN COF RECURRENTE

EJEMPLO DE PETICIÓN:


```
    {
  "DS_MERCHANT_ORDER":1552572812,
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"2",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX ",
  "DS_MERCHANT_EXPIRYDATE":"XXXX",
  "DS_MERCHANT_CVV2":"XXX",
  “DS_MERCHANT_COF_INI” : “S”,
  “DS_MERCHANT_COF_TYPE” :“R”,
  "DS_MERCHANT_EMV3DS":
        {
```

```
                    "threeDSInfo":"AuthenticationData",
                    "protocolVersion":"2.2.0",
                    "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",
                    "browserJavaScriptEnabled":"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"
          }
}
```


- Respuesta final de la petición

  Se devolverán los siguientes parámetros necesarios para poder hacer operaciones sucesivas 3RI- Recurring:

  - Ds_Merchant_Cof_Txnid: CAMPO OPCIONAL, IdTransaccion inicial para enviar en autorizaciones sucesivas
  - Ds_EMV3DS: estará compuesto por los siguientes campos:

    - Eci: indicador del tipo de autenticación
    - traceId: Identificador de las referencias 3RI
    - threeDSRequestorPriorAuthenticationInfo:
      - threeDSReqPriorRef: {referencia de la autenticación inicial}
      - threeDSReqPriorAuthMethod: {método de autenticación inicial
      - threeDSReqPriorAuthTimestamp: {timestamp de la autenticación inicial}
      - threeDSReqPriorAuthData: {datos adicionales}

EJEMPLO DE RESPUESTA:


```
{
  "Ds_Amount":"1000",
  "Ds_Currency":"978",
  "Ds_Order":"1552572812",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_Response":"0000",
  "Ds_AuthorisationCode":"694432",
  "Ds_TransactionType":"0",
  "Ds_SecurePayment":"1",
  "Ds_Language":"1",
  "Ds_CardNumber":"****************",
  "Ds_Card_Type":"C",
  "Ds_MerchantData":"",
  "Ds_Card_Country":"724",
  "Ds_Card_Brand":"1",
  "Ds_Merchant_Cof_Txnid": "IdTransaccion inicial para enviar en autorizaciones sucesivas",
  "DS_EMV3DS" : {
                    "Eci":"05",
                    "traceId":"0100000000000000",
                    "threeDSRequestorPriorAuthenticationInfo":{
                              "threeDSReqPriorRef":"5a31771c-6e88-4378-9f99-b114d90f8040",
```

```
                    "threeDSReqPriorAuthMethod":"01",
                    "threeDSReqPriorAuthTimestamp":"201912051020"
                }
            }
```

Pago recurrente sucesivo

Los pagos sucesivos se procesarán como transacciones autenticadas (3RI). Puesto que el titular no está presente las autenticaciones serán frintionless y no se aplicará 3DS Method.

En los pasos a seguir para una recurrente sucesiva segura serán los mismos que una transacción autenticada EMV3DS con las siguientes particularidades:

- Inicia petición: Se deberá marcar el valor de 3RI-Recurring.

EJEMPLO DE PETICIÓN:

```
{
  "DS_MERCHANT_ORDER":"1552571678",
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"999",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX",
  "DS_MERCHANT_EMV3DS": {"threeDSInfo":"3RI-Recurring"}
}
```

Como respuesta se obtendrá lo siguiente:

```
{
  "Ds_Order":"1552571678",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_TransactionType":"0",
  "Ds_EMV3DS": {
    "protocolVersion":"2.2.0",
    "threeDSServerTransID":"8de84430-3336-4ff4-b18d-f073b546ccea",
    "threeDSInfo":"CardConfiguration"
  },
    "Ds_Card_PSD2":"Y"
}
```

- Trata petición. Deberá marcarse con los parámetros COF que corresponda y enviar el Json de EMV3DS incluyendo los parámetros que se devolvieron la petición de autenticación.
  - DS_MERCHANT_COF_INI = “N” ⟶ OPERACIÓN COF INICIAL NO
  - DS_MERCHANT_COF_TYPE = “R” ⟶ OPERACIÓN COF RECURRENTE
  - DS_MERCHANT_COF_TXID ⟶ CAMPO OPCIONAL, identificador de la transacción
  - DS_MERCHANT_EMV3DS ⟶ Valores de tratapeticion + los valores devueltos en la petición inicial

EJEMPLO DE PETICIÓN:


```
{
  "DS_MERCHANT_ORDER":1552572812,
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"2",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX ",
  "DS_MERCHANT_EXPIRYDATE":"XXXX",
  "DS_MERCHANT_CVV2":"XXX",
  "DS_MERCHANT_COF_INI" : "N",
  "DS_MERCHANT_COF_TYPE" :"R",
  "DS_MERCHANT_COF_TXNID": "IdTransaccion inicial",
  "DS_MERCHANT_EMV3DS":
            {
            "threeDSInfo":"AuthenticationData",
            "protocolVersion":"2.2.0",
            "browserAcceptHeader":"text/html,application/xhtml+xml,application/xml;q=0.9 ",
            "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://comercio-inventado.es/recibe-respuesta-autenticacion",
            "threeDSCompInd":"Y",
             "Eci":"05",
            "traceId":"0100000000000000",
            "threeDSRequestorPriorAuthenticationInfo":{
                        "threeDSReqPriorRef":"5a31771c-6e88-4378-9f99-b114d90f8040",
                        "threeDSReqPriorAuthMethod":"01",
                        "threeDSReqPriorAuthTimestamp":"201912051020"
                  }
            }
}
```


9.2. Pagos autenticados de diferentes comercios (“3RI-OTA”)

Este tipo de operativa ofrece al comercio la posibilidad de realizar una única transacción de autenticación por el importe íntegro y, asociados a la misma, efectuar los cargos parciales en los diferentes comercios que formen parte de la transacción.

NOTA: Esta solución es extensible a agencias de viajes online o a soluciones como MarketPlace.

Pago OTA inicial

El primer pago se procesará como una transacción autenticada EMV 3DS (frintionless o challenge) siguiendo los pasos habituales. Para solicitar que será una operación de solo autenticación se tendrán que marcar los siguientes parámetros.

- Inicia petición.

EJEMPLO DE PETICIÓN:

```
{
  "DS_MERCHANT_ORDER":"1552571678",
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"999",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXXX",
  "DS_MERCHANT_EMV3DS": {"threeDSInfo":"CardData"}
}
```

Como respuesta se obtendrá lo siguiente:

```
{
  "Ds_Order":"1552571678",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_TransactionType":"0",
  "Ds_EMV3DS": {
    "protocolVersion":"2.2.0",
    "threeDSServerTransID":"8de84430-3336-4ff4-b18d-f073b546ccea",
    "threeDSInfo":"CardConfiguration"
  },
    "Ds_Card_PSD2":"Y"
}
```

- Ejecución del 3DSMethod
- Trata petición

  En la Petición de Autorización al “tratapeticion” debe marcarse que vamos a solicitar una autenticación OTA y el tipo de transacción de autenticación:

  - DS_MERCHANT_OTA = “S” ⟶ OPERACIÓN OTA INICIAL SI
  - DS_TRANSACTION_TYPE = “7” ⟶ PETICIÓN DE AUTENTICACIÓN

EJEMPLO DE PETICIÓN:

```
{
  "DS_MERCHANT_ORDER":1552572812,
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"2",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"7",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXXX ",
```

```
  "DS_MERCHANT_EXPIRYDATE":"XXXX",
  "DS_MERCHANT_CVV2":"XXX",
  “DS_MERCHANT_OTA” : “S”,
  "DS_MERCHANT_EMV3DS":
        {
              "threeDSInfo":"AuthenticationData",
              "protocolVersion":"2.2.0",
              "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",
              "browserJavaScriptEnabled":"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"
        }
}
```


- Respuesta final de la petición

  Se devolverán los parámetros necesarios para poder hacer operaciones sucesivas 3RI-OTA.

  - authenticationValue: CAMPO OPCIONAL con el valor de autenticación
  - Eci: indicador del tipo de autenticación
  - traceId:Identificador de las referencias 3RI
  - threeDSRequestorPriorAuthenticationInfo : threeDSReqPriorRef: {referencia de la autenticación inicial } threeDSReqPriorAuthMethod: {método de autenticación inicial threeDSReqPriorAuthTimestamp: {timestamp de la autenticación inicial} threeDSReqPriorAuthData: {datos adicionales}

EJEMPLO DE RESPUESTA:


```
{
  "Ds_Amount":"1000",
  "Ds_Currency":"978",
  "Ds_Order":"1552572812",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_Response":"0000",
  "Ds_AuthorisationCode":"694432",
  "Ds_TransactionType":"7",
  "Ds_SecurePayment":"1",
  "Ds_Language":"1",

  "Ds_CardNumber":"**********",
  "Ds_Card_Type":"C",
  "Ds_MerchantData":"",
  "Ds_Card_Country":"724",
  "Ds_Card_Brand":"1",
  “DS_EMV3DS” : {
        "Eci":"05",
        "traceId":"0100000000000000",
```

```
        "authenticationValue": "AJkBAoIpI5dGUThEhSkjAAAAAAA=",
        "threeDSRequestorPriorAuthenticationInfo":{
                "threeDSReqPriorRef":"5a31771c-6e88-4378-9f99-b114d90f8040",
                "threeDSReqPriorAuthMethod":"01",
                "threeDSReqPriorAuthTimestamp":"201912051020"
        }
}
```

Pago OTA

El comercio interesado, una vez que el comercio autenticador le haya facilitado los datos de la autenticación, deberá realizar las peticiones de 3RI-OTA con los campos obtenidos anteriormente, de la siguiente forma:

- Inicia petición. Se deberá marcar el valor de 3RI-OTA.

EJEMPLO DE PETICIÓN:

```
{
  "DS_MERCHANT_ORDER":"1552571678",
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"999",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX",
  "DS_MERCHANT_EMV3DS": {"threeDSInfo":"3RI-OTA"}
}
```

Como respuesta se obtendrá lo siguiente:

```
{
  "Ds_Order":"1552571678",
  "Ds_MerchantCode":"999008881",
  "Ds_Terminal":"2",
  "Ds_TransactionType":"0",
  "Ds_EMV3DS": {
    "protocolVersion":"2.2.0",
    "threeDSServerTransID":"8de84430-3336-4ff4-b18d-f073b546ccea",
    "threeDSInfo":"CardConfiguration"
  },
    "Ds_Card_PSD2":"Y"
}
```

- Trata Petición. Se deberán mandar los datos EMV3DS que se han obtenido en la petición inicial.

EJEMPLO DE PETICIÓN:

```
{
  "DS_MERCHANT_ORDER":1552572812,
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"2",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"1000",
```

```
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX ",
  "DS_MERCHANT_EXPIRYDATE":"XXXX",
  "DS_MERCHANT_CVV2":"XXX",
  "DS_MERCHANT_EMV3DS":
{
            "threeDSInfo":"AuthenticationData",
            "protocolVersion":"2.2.0",
            "browserAcceptHeader":"text/html,application/xhtml+xml,application/xml;q=0.9 ",
            "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://comercio-inventado.es/recibe-respuesta-autenticacion",
            "threeDSCompInd":"Y",
            "authenticationValue": "AJkBAoIpI5dGUThEhSkjAAAAAAA=",
             "Eci":"05",
            "traceId":"0100000000000000",
            "threeDSRequestorPriorAuthenticationInfo":{
                        "threeDSReqPriorRef":"5a31771c-6e88-4378-9f99-b114d90f8040",
                        "threeDSReqPriorAuthMethod":"01",
                        "threeDSReqPriorAuthTimestamp":"201912051020"
                  }
}
}
```


NOTA: Se debe tener en cuenta que en el caso del pago OTA existen diferencias en función de la marca de la tarjeta (Visa y Mastercard). Estas diferencias hacen referencia a la posibilidad de reutilizar el dato authenticacionValue en una compra que agrega varios servicios o productos, siendo la marca Mastercard permisiva a la reutilización del authenticacionValue al contrario que Visa.

Por esto motivo el mensaje Trata Petición de los diversos pagos OTA realizados con una tarjeta Mastercard permitirá la reutilización del authenticacionValue obtenido en el pago OTA inicial, realizando el proceso de autorización sin pasar por la autenticación. Por el contrario, VISA no permite su reutilización y por lo tanto se deberá pasar por el proceso de autenticación previo a la autorización en cada uno de los diversos pagos OTA.

Pago OTA Delegado

Si la autorización la va a realizar un comercio diferente al interesado, se deberá seguir los protocolos del apartado Integración para PSP para envió de peticiones a otros FUC y seguir el apartado Pagos autenticados de diferentes comercios (“3RI-OTA”)

10. Otras Integraciones REST

10.1. Integración para PSP

Si eres un agregador de comercio o PSPs hay una integración específica para que, de esta forma, con clave secreta para PSP puedan operar en nombre de los comercios a nivel de terminal.

Para estas peticiones los parámetros a enviar son los mismos que en la petición habitual de comercios, pero estos tendrán una versión de firma y firma en ANSI X9.19.

No se definen flujos específicos para PSP. Los parámetros de entrada y salida así como los códigos de error se podrán ver en Parámetros de entrada y salida y Códigos de error.

NOTA: para realizar esta integración se requiere activación por parte de BBVA.

Configuración

Los comercios-terminales deberán estar asociados y configurados para poder enviar peticiones desde un PSP. Esta configuración debe solicitársela el comercio a BBVA.

Solicitud y recepción de claves

Se recibirán dos claves privadas con el protocolo establecido.

- Clave para realizar cifrado 3DES del campo DS_MERCHANT_PAN
- Clave para firmar la petición (DS_MERCHANTPARAMETERS) según la normal X9.19

Envío de petición al TPV Virtual

Al igual que en la petición de pago enviada por un comercio, el PSP tiene los campos siguientes variando como hemos comentado antes la firma y su versión de firma.

- Ds_SignatureVersion: Constante que indica la versión de firma que se está utilizando. Para esta integración de PSP el valor a utilizar será **T25V1.**
- Ds_MerchantParameters: Cadena en formato JSON con todos los parámetros de la petición codificada en Base 64 y sin retornos de carro (En la sección de anexos se incluye la lista de parámetros que se pueden enviar en una solicitud de pago). Si se envía el campo DS_MERCHANT_PAN este debe estar firmado con 3DES.
- Ds_Signature: Firma de los datos enviados. Es el resultado del Mac X9.19 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior. El valor a enviar en el campo Ds_Signature se obtiene convirtiendo a hexadecimal la Mac obtenida en el paso anterior y cogiendo los 4 primeros bytes (8 caracteres) iniciando por la izquierda del

resultado.

Dichos parámetros deben enviarse a los siguientes endpoints dependiendo de si se quiere realizar una petición en el entorno de prueba u operaciones reales:

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

Recepción del resultado

La recepción del resultado será firmada de la misma forma que la petición de envío, según la norma ANSI x9.19

Ejemplo de peticiones

Cadena en JSON

*{"DS_MERCHANT_AMOUNT":"145","DS_MERCHANT_ORDER":"1446068581","DS_MERCHANT_MERCHANTCODE":"999008881","DS_MERCHANT_CURRENCY":"978","DS_MERCHANT_TRANSACTIONTYPE":"0","DS_MERCHANT_TERMINAL":"1","DS_MERCHANT_MERCHANTURL":"http:\/\/www.prueba.com\/urlNotificacion.php","DS_MERCHANT_PAN":"454881********04","DS_MERCHANT_EXPIRYDATE":"1512","DS_MERCHANT_CVV2":"123"}*

Ciframos en 3DES el parámetro DS_MERCHANT_PAN

Número de tarjeta	*454881********04*
Número de tarjeta hexadecimal cifrado en 3DES modo CBC sin vector, clave F180E06B7A89A88F4A2A52C8EC1C5D1C	*377f34989cf0ae79857a70aa45f3e4c3*

Cadena en JSON con PAN cifrado:

{"DS_MERCHANT_AMOUNT":"145","DS_MERCHANT_ORDER":"1446068581","DS_MERCHANT_MERCHANTCODE":"999008881","DS_MERCHANT_CURRENCY":"978","DS_MERCHANT_TRANSACTIONTYPE":"0","DS_MERCHANT_TERMINAL":"1","DS_MERCHANT_MERCHANTURL":"http:\/\/www.prueba.com\/urlNotificacion.php","DS_MERCHANT_PAN":"377f34989cf0ae79857a70aa45f3e4c3","DS_MERCHANT_EXPIRYDATE":"1512","DS_MERCHANT_CVV2":"123"}

A continuación, se muestra el objeto JSON codificado en BASE64, campo DS_MERCHANT_PARAMETERS:

eyJEU19NRVJDSEFOVF9BTU9VTlQiOiIxNDUiLCJEU19NRVJDSEFOVF9PUkRFUiI6IjE0NDYwNjg1ODEiLCJEU19NRVJDSEFOVF9NRVJDSEFOVENPREUiOiI5OTkwMDg4ODEiLCJEU19NRVJDSEFOVF9DVVJSRU5DWSI6Ijk3OCIsIkRTX01FUkNIQU5UX1RSQU5TQUNUSU9OVFlQRSI6IjAiLCJEU19NRVJDSEFOVF9URVJNSU5BTCI6IjEiLCJEU19NRVJDSEFOVF9NRVJDSEFOVFVSTCI6Imh0dHA6XC9cL3d3dy5wcnVlYmEuY29tXC91cmxOb3RpZmljYWNpb24ucGhwIiwiRFNfTUVSQ0hBTlRfUEFOIjoiMzc3ZjM0OTg5Y2YwYWU3OTg1N2E3MGFhNDVmM2U0YzMiLCJEU19NRVJDSEFOVF9FWFBJUllEQVRFIjoiMTUxMiIsIkRTX01FUkNIQU5UX0NWVjIiOiIxMjMifQ==

Firmar los datos de la petición

Sobre toda la cadena obtenida en el paso anterior (DS_MERCHANT_PARAMETERS) se calcula la firma completa en base a la norma x9.19.

Obtenemos la MAC 5D823A402DE70705 con la clave de cifrado

269289DA6EAD0B20928C8F2F2F6BC752 y el ds_merchant_parameters.

El campo ds_signature será cogiendo los 4 primeros bytes (8 caracteres) iniciando por la izquierda del resultado del MAC del paso anterior ***5D823A40***

Formar el mensaje de la petición

- *Ds_SignatureVersion: T25V1*
- *Ds_MerchantParameters:*
  eyJEU19NRVJDSEFOVF9BTU9VTlQiOiIxNDUiLCJEU19NRVJDSEFOVF9PUkRFUiI6IjE0NDYwNjg1ODEiLCJEU19NRVJD
  SEFOVF9NRVJDSEFOVENPREUiOiI5OTkwMDg4ODEiLCJEU19NRVJDSEFOVF9DVVJSRU5DWSI6Ijk3OCIsIkRTX01FUk
  NIQU5UX1RSQU5TQUNUSU9OVFlQRSI6IjAiLCJEU19NRVJDSEFOVF9URVJNSU5BTCI6IjEiLCJEU19NRVJDSEFOVF9NR
  VJDSEFOVFVSTCI6Imh0dHA6XC9cL3d3dy5wcnVlYmEuY29tXC91cmxOb3RpZmljYWNpb24ucGhwIiwiRFNfTUVSQ0h
  BTlRfUEFOIjoiMzc3ZjM0OTg5Y2YwYWU3OTg1N2E3MGFhNDVmM2U0YzMiLCJEU19NRVJDSEFOVF9FWFBJUllEQV
  RFIjoiMTUxMiIsIkRTX01FUkNIQU5UX0NWVjliOiIxMjMifQ==
- *Ds_Signature: 5D823A40*

10.2. ¿Operas por PUCE? Protocolo unificado de comercios

Para comercios/integradores que envían las autorizaciones de comercio electrónico por protocolo PUC (también conocida como PRICE Comercios) y además desean poder aplicar autenticación EMV3DS pueden:

1. Utilizar el protocolo REST descrito en esta guía para gestionar la autenticación 3D Secure del titular (3DSecure 1.0 y EMV3DS)
2. Posteriormente enviar la autorización por una conexión PUC/PRICE existente. El envío de la autorización financiera a través de PUC no es estrictamente necesario (ya que con este mismo REST es posible realizar también este paso) pero está disponible para los comercios/instalaciones que ya tienen este protocolo implantado en sus sistemas contables.

En este punto se detallan las particularidades (ej: envío del dato de case) a incorporar en el mensaje de solicitud de autenticación REST para el envío con control de clave de PSP y poder utilizar los datos de la autenticación 3DS obtenida para ligarlos a una autorización enviada por la conexión PUCE

NOTA: Al operar con protocolo PUCE/PUC solo se realizará por el TPV-Virtual la autenticación (EMV3DS), teniendo que usar el PUC para DCC, tokenización, COF y la exencion(MIT) de PSD que van en los mensajes de autorización.

NOTA2: para realizar esta integración se requiere activación por parte de BBVA.

Mensaje de solicitud de autenticación

El mensaje de solicitud de autenticación seguirá la misma estructura que los mensajes definidos en este documento. Los parámetros de entrada se definen en el siguiente apartado Parámetros de entrada y salida.

A continuación, se describen los datos de debe incluir el Ds_MerchantParameters para enviar una petición de autenticación PUCE al Servicio REST:

```
{
  "DS_MERCHANT_ORDER":1552572812,
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"2",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"17",
  "DS_MERCHANT_MATCHINGDATA ":" 35VSTCh0dHA6XC9cL3d3d",
  "DS_ACQUIRER_IDENTIFIER ":"185187",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXX ",
  "DS_MERCHANT_EXPIRYDATE":"XXXX",
  "DS_MERCHANT_CVV2":"XXX
}
```

Para las operaciones con autenticación EMV3DS se tendrán en cuenta las peticiones descritas en el apartado Transacciones con Autenticación EMV3DS. Los diagramas serán simulares a los expuestos, teniendo en cuenta no se realiza la autorización por el TPV-Virtual, en los casos de Frictionless se deberá realizar una petición más con la autorización al PUC y en los casos de Challenge la autorización final no se deberá enviar al TPV-Virtual si no al PUC.

Mensaje de respuesta a solicitud de autenticación

El mensaje de respuesta de autenticación seguirá la misma estructura que los mensajes definidos en este documento. Los parámetros se definen en apartado Parámetros de entrada y salida.

Mensaje de solicitud de autorización existente por protocolo PUC

Este mensaje no sufrirá cambios. Revisar la Guía de PUCE.

10.3. MPI Externo EMV3DS

En el caso de que se disponga de un MPI certificado propio, se podrán mandar las peticiones y en estas indicar que la operación viene autenticada. Este MPI, para poder

realizar operaciones EMV3DS, deberá estar certificado con EMVCO y con las diversas marcas.

Las peticiones se realizarán de la misma forma que se ha explicado en el documento y añadiendo en el campo DS_MERCHANT_PARAMETERS el parámetro DS_MERCHANT_MPIEXTERNAL, del tipo JSON Object. Acceder al apartado Parámetros de entrada y salida para conocer el detalle del parámetro y de los campos que lo componen.

A continuación, se describen los datos de debe incluir el Ds_MerchantParameters para enviar una petición de autenticación con MPI en versión 1.0.2 al Servicio REST:

```
{
  "DS_MERCHANT_ORDER":1552572812,
 "DS_MERCHANT_MERCHANTCODE":"999008881",
 "DS_MERCHANT_TERMINAL":"2",
 "DS_MERCHANT_CURRENCY":"978",
 "DS_MERCHANT_TRANSACTIONTYPE":"0",
 "DS_MERCHANT_AMOUNT":"1000",
 "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXXX ",
 "DS_MERCHANT_EXPIRYDATE":"XXXX",
 "DS_MERCHANT_CVV2":"XXX",
 " DS_MERCHANT_MPIEXTERNAL ":{
   "TXID”:” VFVSTCI6Imh0dHA6XC9cL3d3dy5wcnVlYmEuY23456gh67j789”,
   "CAVV”:” Y23456gh67j7Imh0dHA6XC9cL3d3dy5VlYmEu89VFVSTCI6wcn” ,
   "ECI”:”5”
   }
}
```

A continuación, se describen los datos de debe incluir el Ds_MerchantParameters para enviar una petición de autenticación con MPI en versión 2 al Servicio REST:

```
{
  "DS_MERCHANT_ORDER":1552572812,
 "DS_MERCHANT_MERCHANTCODE":"999008881",
 "DS_MERCHANT_TERMINAL":"2",
 "DS_MERCHANT_CURRENCY":"978",
 "DS_MERCHANT_TRANSACTIONTYPE":"0",
 "DS_MERCHANT_AMOUNT":"1000",
 "DS_MERCHANT_PAN":" XXXXXXXXXXXXXXXXXX ",
 "DS_MERCHANT_EXPIRYDATE":"XXXX",
 "DS_MERCHANT_CVV2":"XXX"",
 " DS_MERCHANT_MPIEXTERNAL ":{
   "threeDSServerTransID”:” FVSTCI6Imh0A6XC9cL3d3dy5wcnVlYmEuY23”,
   "authenticacionValue”:” 7Imh0dHA6XC9cL3d3dy5VlYmEu81” ,
   "protocolVersion”:”2.1.0”
   }
}
```

NOTA: para realizar esta integración se requiere activación por parte de BBVA.

11. Entorno de pruebas

Existe un entorno de test que permite realizar las pruebas necesarias para verificar el correcto funcionamiento del sistema antes de hacer la implantación en el entorno real.

A continuación, se proporcionarán las URL de acceso al portal de administración en endpoint del servicio para realizar las pruebas. Para obtener los datos de acceso, deberán dirigirse a BBVA para que ésta les proporcione los datos de acceso.

La URL para iniciar las operaciones (Autenticaciones o DCC):

https://sis-t.redsys.es:25443/sis/rest/iniciaPeticionREST

La URL para el envío de las órdenes de pago es la siguiente:

https://sis-t.redsys.es:25443/sis/rest/trataPeticionREST

Adicionalmente, la URL para el acceso al módulo de administración es la siguiente:

https://sis-t.redsys.es:25443/canales

NOTA: El entorno de pruebas será idéntico al entorno real, con la única diferencia que los pagos realizados en este entorno no tendrán validez contable.

NOTA2: Desde BBVA se proporcionan unos datos genéricos de prueba para todos los clientes. Como ya se ha indicado, para obtener los datos de su comercio, deberá contactar con su gestor.

DATOS GENÉRICOS DE PRUEBA

- Número de comercio (Ds_Merchant_MerchantCode): Aquí se deberá poner el número facilitado por BBVA (ejemplo 999008881)
- Terminal (Ds_Merchant_Terminal): Aquí se deberá poner el número facilitado por BBVA (ejemplo 01)
- Clave secreta: sq7HjrUOBfKmC576ILgskD5srU870gJ7

Tarjetas Autorizadas:

- Tarjeta autorizada 1:
  - Numeración: 4548812049400004
  - Caducidad: 12/20
  - Código CVV2: 123
  - Para compras seguras, en la que se requiere la autenticación del titular, el código de autenticación personal (CIP) es 123456.

- Tarjeta aceptada 2 (3DSecure 1.0 *con "iniciapeticion"* NO_3DS_V2):
  - Numeración: 4548812049400004
  - Caducidad: 12/20
  - Código CVV2: 123
  - Para compras seguras, en la que se requiere la autenticación del titular, el código de autenticación personal (CIP) es 123456.
- Tarjeta aceptada 3 (EMV3DS 2.1 *con "iniciapeticion" con threeDSMethodURL con autenticación FRICTIONLESS)*
  - Numeración: 4918019160034602
  - Caducidad: 12/20
  - Código CVV2: 123

    Para compras seguras, en la que se requiere la autenticación del titular, el código de autenticación personal (CIP) es 123456.
- Tarjeta aceptada 4 (EMV3DS *2.1 con "iniciapeticion" sin threeDSMethodURL con autenticación FRICTIONLESS)*
  - Numeración: 4548814479727229
  - Caducidad: 12/20
  - Código CVV2: 123
  - Para compras seguras, en la que se requiere la autenticación del titular, el código de autenticación personal (CIP) es 123456.
- Tarjeta aceptada 5 (EMV3DS 2.1 *con "iniciapeticion" con threeDSMethodURL con autenticación CHALLENGE)*
  - Numeración: 4918019199883839
  - Caducidad: 12/20
  - Código CVV2: 123

    Para compras seguras, en la que se requiere la autenticación del titular, el código de autenticación personal (CIP) es 123456.
- Tarjeta aceptada 6 (EMV3DS 2.1 *con "iniciapeticion" sin threeDSMethodURL con autenticación CHALLENGE)*
  - Numeración: 4548817212493017

- Caducidad: 12/20
- Código CVV2: 123
- Para compras seguras, en la que se requiere la autenticación del titular, el código de autenticación personal (CIP) es 123456.

Tarjetas Denegadas (Código de respuesta 190):

- Tarjeta denegada 1:
  - Numeración: 5576440022788500
  - Caducidad: 12/20
  - Código CVV2: 123
  - Para compras seguras, en la que se requiere la autenticación del titular, el código de autenticación personal (CIP) es 123456.

- Tarjeta denegada 2 (EMV3DS *2.1 con "iniciapeticion" con threeDSMethodURL con autenticación FRICTIONLESS)*
  - Numeración: 4907277775205123
  - Caducidad: 12/20
  - Código CVV2: 123
  - Para compras seguras, en la que se requiere la autenticación del titular, el código de autenticación personal (CIP) es 123456.

- Tarjeta denegada 3 (EMV3DS 2.1 *con "iniciapeticion" con threeDSMethodURL con autenticación CHALLENGE)*
  - Numeración: 4907271141151707
  - Caducidad: 12/20
  - Código CVV2: 123
  - Para compras seguras, en la que se requiere la autenticación del titular, el código de autenticación personal (CIP) es 123456.

11.1. Tarjetas de pruebas versión 2.2 (Avance)

DATOS GENÉRICOS DE PRUEBA

- Número de comercio (Ds_Merchant_MerchantCode): Aquí se deberá poner el número facilitado por BBVA (ejemplo 999008881)

- Terminal (Ds_Merchant_Terminal): Aquí se deberá poner el número facilitado por BBVA (ejemplo 01)
- Clave secreta: sq7HjrUOBfKmC576ILgskD5srU870gJ7

Tarjetas Autorizadas:

- Tarjeta aceptada 7 (3DSecure 2.2 *con "iniciapeticion" sin threeDSMethodURL con autenticación FRICTIONLESS)*:
  - Numeración: 4548816134581156
  - Caducidad: 12/20
  - Código CVV2: 123
  - Para compras seguras, en la que se requiere la autenticación del titular, el código de autenticación personal (CIP) es 123456.
- Tarjeta aceptada 8 (3DSecure 2.2 *con "iniciapeticion" sin threeDSMethodURL con autenticación CHALLENGE)*:
  - Numeración: 4548816131164386
  - Caducidad: 12/20
  - Código CVV2: 123
  - Para compras seguras, en la que se requiere la autenticación del titular, el código de autenticación personal (CIP) es 123456.
- Tarjeta aceptada 9 (3DSecure 2.2 *con "iniciapeticion" sin threeDSMethodURL acepta exenciones con FRICTIONLESS sin exenciones CHALLENGE)*:
  - Numeración: 4548815324058868
  - Caducidad: 12/20
  - Código CVV2: 123
  - Para compras seguras, en la que se requiere la autenticación del titular, el código de autenticación personal (CIP) es 123456.
- Tarjeta aceptada 10 (3DSecure 2.2 *con "iniciapeticion" sin threeDSMethodURL acepta solo exencion MIT con FRICTIONLESS sin exenciones o otras exenciones CHALLENGE)*:
  - Numeración: 4548815374025114
  - Caducidad: 12/20
  - Código CVV2: 123
  - Para compras seguras, en la que se requiere la autenticación del titular, el código de autenticación personal (CIP) es 123456.

- Tarjeta aceptada 11 (3DSecure 2.2 *con "iniciapeticion" sin threeDSMethodURL acepta solo pagos 3RI-OTA)*:
    - Numeración: 5576441563045037
    - Caducidad: 12/20
    - Código CVV2: 123
    - Para compras seguras, en la que se requiere la autenticación del titular, el código de autenticación personal (CIP) es 123456.

12. Parámetros de entrada y salida

12.1. Parámetros de la solicitud

En la petición de pago hacia el TPV Virtual se tendrán que enviar una serie de datos 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 parámetros de entrada del TPV Virtual se presenta en la hoja de cálculo "TPV-Virtual Parámetros Entrada-Salida.xlsx".

En los siguientes puntos se mostrarán algunos ejemplos de peticiones:

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

A continuación, se muestra un ejemplo del parámetro Ds_Merchant_Parameters, previo a ser codificado en Base 64:

```
{ "DS_MERCHANT_ORDER":"1552565870",
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"999",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"0",
  "DS_MERCHANT_AMOUNT":"1000",
  "DS_MERCHANT_PAN":"XXXXXXXXXXXXX",
  "DS_MERCHANT_EXPIRYDATE":"XXXX",
  "DS_MERCHANT_CVV2":"XXX"}

* DS_MERCHANT_TRANSACTIONTYPE":"0" para PAGO
* DS_MERCHANT_TRANSACTIONTYPE":"1" para PREAUTORIZACIÓN
```

Petición de Confirmación/Devolución/Anulación

A continuación, se muestra un ejemplo del parámetro Ds_Merchant_Parameters, previo a ser codificado en Base 64:

```
{ "DS_MERCHANT_ORDER":"1552565870",
  "DS_MERCHANT_MERCHANTCODE":"999008881",
  "DS_MERCHANT_TERMINAL":"999",
  "DS_MERCHANT_CURRENCY":"978",
  "DS_MERCHANT_TRANSACTIONTYPE":"3",
  "DS_MERCHANT_AMOUNT":"1000"}

* DS_MERCHANT_TRANSACTIONTYPE":"2" para CONFIRMACIÓN
* DS_MERCHANT_TRANSACTIONTYPE":"3" para DEVOLUCIÓN
* DS_MERCHANT_TRANSACTIONTYPE":"9" para ANULACIÓN
```

Petición de Tokenización (Pago por Referencia - Pago 1-Clic)

A continuación, se muestra un ejemplo del parámetro Ds_Merchant_Parameters, previo a ser codificado en Base 64:

```
{ "DS_MERCHANT_ORDER":"1552565870",
```

"DS_MERCHANT_MERCHANTCODE":"999008881",
"DS_MERCHANT_TERMINAL":"999",
"DS_MERCHANT_CURRENCY":"978",
"DS_MERCHANT_TRANSACTIONTYPE":"0",
"DS_MERCHANT_AMOUNT":"1000",
"DS_MERCHANT_PAN":"XXXXXXXXXXXXX",
"DS_MERCHANT_EXPIRYDATE":"XXXX",
"DS_MERCHANT_CVV2":"XXX"
" DS_MERCHANT_IDENTIFIER ":" REQUIRED "}

Petición de pago con Tokenización (Pago por Referencia - Pago 1-Clic)

A continuación, se muestra un ejemplo del parámetro Ds_Merchant_Parameters, previo a ser codificado en Base 64:

{ “DS_MERCHANT_ORDER":"1552565870",
"DS_MERCHANT_MERCHANTCODE":"999008881",
"DS_MERCHANT_TERMINAL":"999",
"DS_MERCHANT_CURRENCY":"978",
"DS_MERCHANT_TRANSACTIONTYPE":"0",
"DS_MERCHANT_AMOUNT":"1000",
" DS_MERCHANT_IDENTIFIER ":"XXXXXXXXXXXXXXXXXXXXXXX"}

12.2. Parámetros de la respuesta

Las peticiones REST generan una respuesta síncrona a la petición enviada por el comercio, en la cual se informará el resultado de la operación.

El resultado de la operación se informará mediante el parámetro Ds_Response o “Código de respuesta”. Además, se informará dicho código de respuesta en la consulta de operaciones, siempre y cuando la operación no está autorizada, tal y como se muestra en la siguiente imagen:

Fecha	Tipo operación	Número de pedido	Resultado operación y código	Importe
29/06/2018 10:01:44	Autorización	290618100053	Autorizada 101311	1,00 EUR
29/06/2018 10:46:55	Autorización	5674	Sin Finalizar 9998	1,45 EUR
29/06/2018 10:54:06	Autorización	7907vPBMh	Sin Finalizar 9998	1,45 EUR

Un ejemplo de respuesta de una operación de pago autorizada sería la siguiente:

{
"Ds_Amount":"1000",
"Ds_Currency":"978",
"Ds_Order":"1552568529",
"Ds_MerchantCode":"999008881",

"Ds_Terminal":"2",

"Ds_Response":"0000",

"Ds_AuthorisationCode":"842841",

"Ds_TransactionType":"0",

"Ds_SecurePayment":"0",

"Ds_Language":"1",

"Ds_CardNumber":"XXXXXXXXXXXXXXXX",

"Ds_Card_Type":"C",

"Ds_MerchantData":"",

"Ds_Card_Country":"724",

"Ds_Card_Brand":"1"

}

NOTA2: El listado completo de todos los parámetros de salida del TPV Virtual se presenta en la hoja de cálculo "TPV-Virtual Parámetros Entrada-Salida.xlsx".

13. Códigos de error

En este apartado se muestra la manera de informar los posibles errores que se pueden producir en el proceso de integración.

El error que se ha producido se informará en el parámetro *errorCode*, tal y como se muestra a continuación:

{"errorCode":"SIS0042"}

NOTA: El listado completo de todos los códigos de error del TPV Virtual se presenta en la hoja de cálculo "TPV-Virtual Parámetros Entrada-Salida.xlsx".

14. 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.

14.1. Qué hacer en caso de timeout del TPV Virtual

Para las peticiones de un pago o una preautorización se deberá mandar una anulación, si la petición es de una confirmación se deberá mandar una devolución.

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

15. Errores frecuentes

Error de firma

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 del TPV Virtal de BBVA.

Tengo en mi comercio denegaciones por número de repetido, 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 BBVA.

16. Preguntas Frecuentes

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

Para ver la clave del TPV Virtual hay que seguir los siguientes pasos:

Acceda a su módulo de administración de su TPV virtual. Seleccione la opción "comercio" y pulse “ver clave”

Introduzca su contraseña de su usuario del TPV virtual y pulse aceptar. -Tendrá acceso a ver la clave del comercio durante 10 segundos.

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.