

# **TPV VIRTUAL**

## **Manual desarrollador Adaptación a EMV3DS - Redirección**

## CONTROL DE VERSIÓN

VERSIÓN	FECHA	AFECTA	BREVE DESCRIPCIÓN DEL CAMBIO
1.0	11-04-2019	Todo	Versión inicial

## ÍNDICE DE CONTENIDO

<b>1. INTRODUCCIÓN .....</b>	<b>4</b>
<b>2. ENTORNO DE PRUEBAS .....</b>	<b>5</b>
<b>3. MONTAR CADENA DE DATOS - Ds_MerchantParameters .....</b>	<b>7</b>
<b>4. FORMULARIO DATOS PETICIÓN OPERACIÓN.....</b>	<b>8</b>
4.1. Excepciones a SCA .....	8
4.2. Transacciones iniciadas por el comercio (MIT) .....	9
Transacciones MIT y uso de tokenización (pago por referencia) .....	10
<b>5. EJEMPLO EMV 3DS.....</b>	<b>10</b>

## 1. INTRODUCCIÓN

Con la entrada en vigor de la nueva Regulación de Pagos PSD2 el próximo 14 de Septiembre de 2019, se introduce la obligatoriedad de que las compras realizadas por TPV virtual sean Autenticadas con doble factor si la tarjeta es emitida en un país del Espacio Económico Europeo, salvo que se pueda y quiera aplicar alguna de las excepciones recogidas en dicha regulación. Esto se conoce como Autenticación Reforzada o Strong Customer Authentication (SCA).

Con esta guía se facilita la información técnica necesaria para que el comercio, o su servicio de informática, realicen de forma satisfactoria la adaptación del TPV Virtual BBVA a la nueva funcionalidad de EMV3DS (también llamada 3DS 2.0) lo que permitirá al comercio beneficiarse de un sistema de Autenticación con menos fricción, y también le ofrece la posibilidad de solicitar excepciones a la Autenticación de doble factor derivada de la nueva regulación de PSD2.

Para más información acerca de PSD2 y EMV3DS tienen a su disposición la presentación que BBVA ha creado con el fin de aclarar las novedades que comporta.

En este documento se especifica las adaptaciones que han de realizar los comercios que acceden al TPV Virtual mediante conexión por Redirección, entrada RealizarPago, en la que se redirige al pagador hacia la web del TPV Virtual de BBVA donde se introducen los datos de la tarjeta y se completa el pago.

Es importante notar que en este tipo de integración no es imprescindible realizar ningún cambio ni adaptación para poder procesar transacciones en EMV3DS, aunque es recomendable proporcionar el máximo de información complementaria (lo que requiere el envío de nuevos parámetros por parte del comercio y por tanto un desarrollo informático) a fin de que la pasarela y el Banco Emisor sean capaces de realizar una análisis de Riesgo de la transacción más eficiente.

## 2. ENTORNO DE PRUEBAS

Para poder realizar las pruebas de instalación, durante el proceso de alta de su TPV Virtual BBVA, la entidad le facilitará los parámetros de acceso a un entorno de TPV TEST donde, en un entorno aislado, idéntico al entorno de producción, podrá realizar operaciones de prueba. Estas ventas serán ficticias, por lo que no tendrán validez contable.

Para acceder a este entorno es preciso tener habilitado el acceso a los puertos 25443 y 26443.

Las características del entorno de pruebas se detallan a continuación:

URL's pago:

**Entrada 'REALIZAR PAGO':** <https://sis-t.redsys.es:25443/sis/realizarPago>

Número de comercio (Ds\_Merchant\_MerchantCode): **XXXXXXXX**

Clave secreta (Ds\_Merchant\_MerchantSignature)

SHA-1: **qwertyasdf0123456789**

SHA-256: **sq7HjrUOBfKmC576ILgskD5srU870gJ7**

Otros parámetros

Número de terminal (Ds\_Merchant\_Terminal = **001**)

Código divisa operación (Ds\_MerchantCurrency = **978**)

Tarjeta de pruebas

Ponemos a su disposición una serie de tarjetas habilitadas para funcionar exclusivamente en el entorno de pruebas:

### **Tarjetas Autorizadas:**

Tarjeta Autorizada 1

Tarjeta: **4548 8120 4940 0004**

Caducidad: **12/20**

Código de seguridad: (CVV2) **123**

Atención: Esta tarjeta está configurada simulando que el titular necesita autenticarse con su banco. Para ello se debe introducir el Código de Identificación 123456.

Tarjeta Autorizada 2 (Flujo Autenticación EMV3DS Sin solicitud de autenticación del titular):

Tarjeta: **4548 8144 7972 7229**

Caducidad: **12/20**

Código de seguridad: (CVV2) **123**

Atención:

- Esta tarjeta está configurada simulando que el titular necesita autenticarse con su banco. Para ello se debe introducir el Código de Identificación 123456.
- Esta tarjeta irá por el flujo EMV3DS, se podrán mandar datos adicionales en el parámetro DS\_MERCHANT\_EMV3DS

Tarjeta Autorizada 3 (Flujo Autenticación EMV3DS Con solicitud de autenticación del titular):

Tarjeta: **4548 8172 1249 3017**

Caducidad: **12/20**

Código de seguridad: (CVV2) **123**

Atención:

- Esta tarjeta está configurada simulando que el titular necesita autenticarse con su banco. Para ello se debe introducir el Código de Identificación 123456.
- Esta tarjeta irá por el flujo EMV3DS, se podrán mandar datos adicionales en el parámetro DS\_MERCHANT\_EMV3DS.

### **Tarjetas Denegadas (Código de respuesta 190):**

Tarjeta Denegada 1:

Tarjeta: **5576 4400 2278 8500**

Caducidad: **12/20**

Código de seguridad: (CVV2) **123**

Atención: Esta tarjeta está configurada simulando que el titular necesita autenticarse con su banco. Para ello se debe introducir el Código de Identificación 123456.

Tarjeta Denegada 2 (Flujo Autenticación EMV3DS Sin solicitud de autenticación del titular):

Tarjeta: **4907 2777 7520 5123**

Caducidad: **12/20**

Código de seguridad: (CVV2) **123**

Atención:

- Esta tarjeta está configurada simulando que el titular necesita autenticarse con su banco. Para ello se debe introducir el Código de Identificación 123456.

- Esta tarjeta irá por el flujo EMV3DS, se podrán mandar datos adicionales en el parámetro DS\_MERCHANT\_EMV3DS.

Tarjeta Denegada 3 (Flujo Autenticación EMV3DS Con solicitud de autenticación del titular):

Tarjeta: **4907 2711 4115 1707**

Caducidad: **12/20**

Código de seguridad: (CVV2) **123**

Atención:

- Esta tarjeta está configurada simulando que el titular necesita autenticarse con su banco. Para ello se debe introducir el Código de Identificación 123456.
- Esta tarjeta irá por el flujo EMV3DS, se podrán mandar datos adicionales en el parámetro DS\_MERCHANT\_EMV3DS.

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

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

### 3. MONTAR CADENA DE DATOS - Ds\_MerchantParameters

Se debe montar una cadena con todos los datos de la petición en formato JSON. JSON es un formato abierto de intercambio de datos basado en texto. Al igual que el XML está diseñado para ser legible e independiente de la plataforma tecnológica. La codificación de datos en JSON es muy ligera por lo que es ideal para intercambio de datos en aplicaciones Web.

El nombre de cada parámetro debe indicarse en mayúsculas o con estructura “CamelCase” (Por ejemplo: DS\_MERCHANT\_AMOUNT o Ds\_Merchant\_Amount).

La cadena resultante de la codificación en BASE64 será el valor del parámetro Ds\_MerchantParameters (en el libro Excel adjunto al presente documento se incluye la lista de parámetros que se pueden enviar en una solicitud de pago).

## 4. FORMULARIO DATOS PETICIÓN OPERACIÓN

Los datos a enviar al TPV Virtual están recogidos en el libro Excel Anexo. Revisar la hoja “Parámetros de Entrada” donde se recogen todos los campos obligatorios y Opcionales. Estos parámetros no son obligatorios pero permitirán al Banco Emisor a analizar de forma más eficiente el riesgo de la transacción y autorizar o aplicar, si lo considera pertinente, la excepción por TRANSACTION RISK ANALISYS (TRA).

La integración de EMV3DS incorpora el campo DS\_MERCHANT\_EMV3DS, un objeto Variable de tipo JSON descrito en la hoja “DS\_MERCHANT\_EMV3DS”.

Este campo, a su vez incorpora campos fijos y otros campos variables de estructura JSON, descritos en sus correspondientes hojas.

### 4.1. Excepciones a SCA

Por otro lado se incorpora el campo **DS\_MERCHANT\_EXCEP\_SCA** en el que el comercio puede solicitar la excepción de Autenticación a BBVA y el Banco Emisor de la tarjeta, es decir que la transacción de procese de forma No Segura, siendo consciente de que en caso de que dicha excepción se aplicase, el comercio asume la responsabilidad financiera de la transacción en caso de Fraude. La disponibilidad de esta operativa requiere activación por parte de BBVA.

DATO	NOMBRE DEL DATO	Long. / Tipo	COMENTARIOS
Indicador de solicitud de excepción.	DS_MERCHANT_EXCEP_SCA	3/A-N	Opcional. Valores posibles: MIT , LWV, TRA , COR

- 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 del adquirente/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

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).

## 4.2. Transacciones iniciadas por el comercio (MIT)

Son 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.

Sin embargo 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. En tal caso según PSD2, y mientras no se aplique otra exención, se requiere el uso de autenticación reforzada (SCA).

No obstante, con PSD2 estando en vigor, toda operativa de pago iniciada por el comercio (MIT) requiere inicialmente una operación autenticada con SCA que es aquella en la que el cliente 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 también marcarse debidamente siguiendo la especificación Card-on-file (COF) para indicar que los datos de tarjeta se están almacenando para pagos posteriores.

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

## 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 solicita 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 SIS 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").

## 5. EJEMPLO EMV 3DS

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_MERCHANTURL": "http://www.prueba.com/UrlNotificacion.php",
  "DS_MERCHANT_URLOK": "http://www.prueba.com/UrlOK.php",
  "DS_MERCHANT_URLKO": "http://www.prueba.com/UrlKO.php",
  "DS_MERCHANT_EMV3DS": {
    "shipAddrCountry": "840",
    "shipAddrCity": "Ship City Name",
    "shipAddrState": "CO",
    "shipAddrLine3": "Ship Address Line 3",
    "shipAddrLine2": "Ship Address Line 2",
    "shipAddrLine1": "Ship Address Line 1",
    "shipAddrPostCode": "Ship Post Code",
    "cardholderName": "Cardholder Name",
    "email": "example@example.com",
    "mobilePhone": {"cc": "123", "subscriber": "123456789"}
  }
}
```