BBVA

Creando Oportunidades

TPV VIRTUAL

Manual desarrollador

Adaptación a EMV3DS 2.2
Entrada Redirección

Versión 1.1

CONTROL DE VERSIÓN

VERSIÓN	FECHA	AFECTA	BREVE DESCRIPCIÓN DELCAMBIO
1.0	09-01-2020	Todo	Versión inicial
1.1	20-07-2020	Introducción	Fecha aplicación SCA para entidades españolas

BBVA
Creando Oportunidades

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN

Con la entrada en vigor de la nueva Regulación de Pagos PSD2 el pasado 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 Autenthication (SCA). **Sin embargo la obligación de aplicar SCA se ha retrasado hasta el próximo 14 de noviembre de 2020 para las entidades españolas.**

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 (en su versión 3DS 2.2) 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 y previsiblemente el número de operaciones autorizadas sea mayor.

Asimismo en el presente manual os indicamos que los cambios se limitan a la introducción de dos nuevos campos:

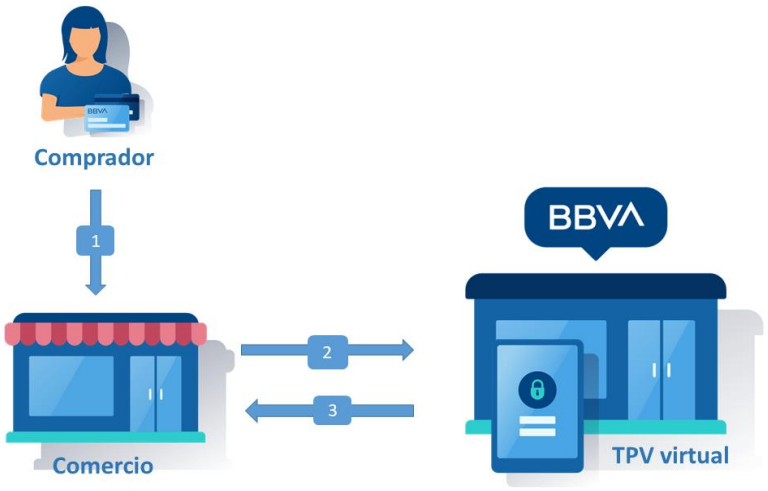
DS_MERCHANT_EMV3DS: campo opcional con estructura JSON que incluye multiples subcampos donde se incluirán los datos adicionales para la evaluación del riesgo por parte del Banco Emisor.

DS_MERCHANT_EXCEP_SCA: campo opcional donde el comercio puede solicitar que se aplique una excepción a SCA de las previstas en la regulación. Es necesario que el banco adquirente autorice expresamente al comercio al uso de estas excepciones. De igual modo el

banco emisor puede decidir no autorizar dicha petición de excepción y “obligar” a que el cliente realice la autenticación (Challenge required) para que esta sea autorizada.

1.1. Descripción del flujo de una operación

En el siguiente esquema se presenta el flujo de una transacción por Redirección



1. El titular selecciona los productos que desea comprar en el comercio, cesta de la compra.

2. El comercio redirige la sesion del navegador del cliente a la URL del TPV virtual. En esta URL el cliente introduce los datos de tarjeta.

3. El TPV virtual informa al comercio del resultado de la operación y devuelve la sesion del navegador del cliente al comercio para que continue navegando en su tienda web.

En este modelo los datos de la tarjeta se informan en el TPV Virtual de BBVA, con lo que el comercio no tiene contacto con estos datos y de esta forma evita tener cumplir con los requisitos del programa PCI-DSS de seguridad en el tratamiento de datos de tarjeta.

2. TRANSACCIÓN EN EL TPV VIRTUAL

2.1. Envío de petición al TPV Virtual

El comercio debe enviar al TPV Virtual los datos de la petición de pago codificados en UTF8 a través del navegador del titular. Para ello deberá preparar un formulario con 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 petición codificada en Base 64 y sin retornos de carro (En el Excel adjunto 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.

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

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

2.2. Recepción del resultado (Notificación Online)

Una vez gestionada la transacción, el TPV Virtual puede informar al servidor del comercio el resultado de la misma mediante una conexión directa al servidor del comercio (paso 3 del flujo descrito). Esta notificación es opcional.

La notificación on-line consiste en un POST HTTP (Notificación Síncrona y Asíncrona) con la información del resultado codificada en UTF-8.

En el POST 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 (En el Anexo 12.2 se incluye la lista de parámetros que se pueden incluir en la notificación on-line).

• 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.

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

Alternativamente se puede enviar la respuesta mediante un email a la dirección de correo electrónico informada en la configuración del Terminal.

2.3. Retorno del control de la navegación del Comprador

En el paso 3 del flujo el TPV Virtual, se mostrará al cliente un recibo con el resultado de la operación, siempre y cuando la configuración del comercio así lo especifique.

Además, en caso de que la operación se deniegue, el cliente tendrá la opción de reintentar el pago con otra tarjeta u otro método de pago, siempre y cuando la configuración del comercio lo permita.

Se puede obviar la pantalla de recibo pero en ese caso es el comercio quién está obligado a mostrar al comprador el resultado del intento de pago.

Por último, en este paso se devuelve al comercio el control de la navegación del titular. De esta forma el comercio puede completar el flujo del pago manteniendo una secuencia de navegación natural para el cliente/comprador.

Opcionalmente el TPV Virtual puede incluir los mismos campos de la notificación on-line.

3. 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 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 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

4. FORMULARIO DE ENVÍO DE PETICIÓN

4.1. Ejemplos de formularios

El comercio deberá montar un formulario con los parámetros de la petición de pago que debe hacer llegar al TPV Virtual a través del navegador del cliente.

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).

También disponéis de más información técnica y ejemplos en la siguiente URL para desarrolladores:

https://pagosonline.redsys.es/modelos-de-integracion.html#flujo-redireccion

Os adjuntamos diversos ejemplos de formulario de pagos a continuación:

Ejemplo de formulario de pago **sin envío de datos de tarjeta**:

El campo Merchant Parameters sería el siguiente:

{"DS_MERCHANT_AMOUNT":"145","DS_MERCHANT_ORDER":"1446117555","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_URLOK":"http:\/\/www.prueba.com\/urlOK.php","DS_MERCHANT_URLKO":"http:\/\/www.prueba.com\/urlKO.php"}

Que habría que posteriormente codificar en BASE64 sin retornos de carro para asegurarnos de que se mantiene constante y no es alterada en su paso por el navegador del cliente/comprador.

```
<form name="from" action="https://sis-t.redsys.es:25443/sis/realizarPago" method="POST">
<input type="hidden" name="Ds_SignatureVersion" value="HMAC_SHA256_V1"/>
<input type="hidden" name="Ds_MerchantParameters" value="
        eyJEU19NRVJDSEFOVF9BTU9VTlQiOiIxNDUiLCJEU19NRVJDSEFOVF9PUkRFUiI6IjE0NDYxMTc1
        NTUiLCJEU19NRVJDSEFOVF9NRVJDSEFOVENPREUiOiI5OTkwMDg4ODEiLCJEU19NRVJDSEFO
        VF9DVVJSRU5DWSI6Ijk3OCIsIkRTX01FUkNIQU5UX1RSQU5TQUNUU9OVFlQRSI6IjAiLCJEU19N
        RVJDSEFOVF9URVJNSU5BTCI6IjEiLCJEU19NRVJDSEFOVF9NRVJDSEFOVFVSTCI6Imh0dHA6X
        C9cL3d3dy5wcnVlYmEuY29tXC91cmxOb3RpZmljYWNpb24ucGhwIiwiRFNfTUVSQ0hBTlRfVVJMT0si
```

OiJodHRwOlwvXC93d3cucHJ1ZWJhLmNvbVwvdXJsT0sucGhwIiwiRFNfTUVSQ0hBTlRfVVJMS08iOiJodHRwOlwvXC93d3cucHVlYmEuY29tXC91cmxLTy5waHAifQ==">
<input type="hidden" name="Ds_Signature"
value="PqV2+SF6asdasMjXasKJRTh3UIYya1hmU/igHkzhC+R="/>
</form>

Ejemplo de formulario de pago **con envío de datos de tarjeta**:

Ds_Merchant_Parameters:

{"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_URLOK":"http:\/\/www.prueba.com\/urlOK.php","DS_MERCHANT_URLKO":"http:\/\/www.prueba.com\/urlKO.php","DS_MERCHANT_PAN":"454881********04","DS_MERCHANT_EXPIRYDATE":"1512","DS_MERCHANT_CVV2":"123"}

Pasado a BASE64:

<form name="from" action="https://sis-t.redsys.es:25443/sis/realizarPago" method="POST">
<input type="hidden" name="Ds_SignatureVersion" value="HMAC_SHA256_V1"/>
<input type="hidden" name="Ds_MerchantParameters" value="
eyJEU19NRVJDSEFOVF9BTU9VTlQiOiIxNDUiLCJEU19NRVJDSEFOVF9PUkRFUiI6IjE0NDYwNjg1ODEiLCJEU19NRVJDSEFOVF9NRVJDSEFOVENPREUiOiI5OTkwMDg4ODEiLCJEU19NRVJDSEFOVF9DVVJSRU5DWSI6Ijk3OCIsIkRTX01FUkNIQU5UX1RSQU5TQUNUSU9OVFlQRSI6IjAiLCJEU19NRVJDSEFOVF9URVJNSU5BTCI6IjEiLCJEU19NRVJDSEFOVF9NRVJDSEFOVFVSTCI6Imh0dHA6XC9cL3d3dy5wcnVlYmEuY29tXC91cmxOb3RpZmljYWNpb24ucGhwIiwiRFNfTUVSQ0hBTlRfVVJMT0siOiJodHRwOlwvXC93d3cucHVlYmEuY29tXC91cmxPSy5waHAiLCJEU19NRVJDSEFOVF9VUkxLTyI6Imh0dHA6XC9cL3d3dy5wcnVlYmEuY29tXC91cmxLTy5waHAifQ==
<input type="hidden" name="Ds_Signature"
value="PqV2+SF6asdasMjXasKJRTh3UIYya1hmU/igHkzhC+R="/>
</form>

4.2. Utilización de librerías de ayuda

Los comercios disponen de unas librerías que les pueden facilitar la integración del TPV virtual si así lo consideran. Estas librerías están disponibles para JAVA, PHP y .NET y se pueden utilizar tanto para el envío de peticiones como para la recepción de la Notificación online (respuesta).

5. Adaptación a PSD2 – EMV3DS (o 3DSECURE v2.2)

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.

En la nueva versión del protocolo de seguridad 3DSECURE v2.2 se contempla el envío de datos adicionales al Banco Emisor. 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.

5.1. 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.

No obstante la aceptación final de dicha solicitud de “no autenticar” al titular de una tarjeta depende en última instancia de la entidad emisora de la tarjeta. Por ello se denomina “solicitud” de exención. El marcaje de solicitud de exención en una transacción no garantiza la aceptación de la misma por parte del banco emisor de la tarjeta. En caso de no aceptación se va requerir que se proceda a autenticar la transacción.

Por esta razón, el tpv virtual acogiéndose a las best practices del sector y para asegurar la mejor experiencia de pago al usuario priorizará siempre iniciar el flujo de autenticación con el emisor (vía EMV3DS, si el emisor lo soporta) indicando al emisor en dicha solicitud la preferencia del comercio de no autenticar en base a la exención solicitada. De esta forma se mejora la usabilidad, y en caso de que el emisor no acepte la exención, se autentica en el mismo momento al usuario. Si el emisor accede a aplicar la exención solicitada, se cierra el flujo de autenticación sin requerir ni mostrar ninguna pantalla o acción al titular, siendo un proceso transparente para el usuario.

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: Las exenciones no tienen aplicación (se ignoran) para tarjetas emitidas por entidades adquirentes que están fuera del Espacio Económico Europeo (EEA)

5.2. 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 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 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”).

6. EJEMPLO EMV 3DS

A continuación, se muestra un ejemplo del parámetro Ds_Merchant_Parameters en el que se incluyen algunos de los datos adicionales que se pueden enviar opcionalmente, 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"}
}
}
```