Comercia Global Payments

Manual Migración
TPV Virtual
REDIRECCIÓN

Contenido

CONTROL DE VERSIONES

Versión	Fecha	Cambios
1.0	09/04/19	Documento inicial
1.1	06/06/19	Añadida información sobre excenciones, servicio S.R.O. y M.I.T.

En la presente guía encontrará ejemplos de envíos, respuestas y código fuente con el siguiente formato:

En cuadros azul claro se muestran ejemplos de peticiones a generar por la plataforma del comercio.

En cuadros verdes se muestran ejemplos de respuestas y notificaciones recibidas.

En cuadros amarillos se incluyen ejemplos de código como ayuda a la integración.

En negrita y color azul se remarcan los campos adicionales o modificaciones respecto a la integración actual.

¿CÓMO FUNCIONA LA INTEGRACIÓN POR REDIRECCIÓN?

Actualmente las integraciones del TPV virtual por Redirección siguen el siguiente esquema descrito:

Generación de la petición

1. La plataforma del comercio genera un JSON con los datos de la operación:

```
{
    "DS_MERCHANT_MERCHANTCODE": "XXXXXXXXX",
    "DS_MERCHANT_TERMINAL": "1",
    "DS_MERCHANT_TRANSACTIONTYPE": "0",
    "DS_MERCHANT_AMOUNT": "100",
    "DS_MERCHANT_CURRENCY": "978",
    "DS_MERCHANT_ORDER": "66590706"
}
```

2. Se codifica la petición generada en BASE64, se genera la firma de la petición y se forman los campos que componen el formulario que se enviará a Redsys:

```
“Ds_SignatureVersion” = “HMAC_SHA256_V1”
“Ds_MerchantParameters” =
“ewogICAgIkRTX01FUkNIQU5UX01FUkNIQU5UQ09ERSI6ICJYWFhYWFhYWFgiLAogICAgIkRTX01FUkNIQU5UX1RFUk1JTkFMIjogIjEiLAogICAgIkRTX01FUkNIQU5UX1RSQU5TQUNUSU9OVFlQRSI6ICIwIiwKICAgICJEU19NRVJDSEFOVF9BTU9VTlQiOiAiMTAwIiwKICAgICJEU19NRVJDSEFOVF9DVVJSRU5DWSI6ICI5NzgiLAogICAgIkRTX01FUkNIQU5UX09SREVSIjogIjY2NTkwNzA2Igp9”
“Ds_Signature” = “y/Jebi+eShELTff4Y8FcYPNVPjrhPBLB0y/SD4uEB6s=”
```

Conexión con el procesador de pagos

3. Se establece una conexión POST con los servidores de Redsys mediante una redirección a través del navegador del cliente a una de las siguientes URLs, dependiendo de si el entorno al que se envía es para pruebas o producción:

   Pruebas: https://sis-t.redsys.es:25443/sis/realizarPago
   Producción: https://sis.redsys.es/sis/realizarPago

4. Redsys recibe la petición, y realiza las siguientes validaciones:
   - Verifica si el JSON tiene el formato correcto.
   - Genera la firma de la petición y la compara recibida con la petición.
   - Verifica que los datos recibidos en la petición tengan el formato correcto.
   - Si no se han recibido datos de tarjeta ni token o referencia a partir del cual recuperar datos de tarjeta, mostrará la pasarela de pago al cliente para que introduzca los datos de la tarjeta.
5. Si todo es correcto, Redsys contacta con el emisor de la tarjeta y consulta la configuración de seguridad soportada por la tarjeta del titular:
   - Si el terminal opera por comercio seguro y la tarjeta es compatible con pago seguro, se requerirá al titular la autenticación de la operación mediante el método que tenga habilitado la entidad emisora (mensaje SMS, contraseña, tarjetas de coordenadas, biometría, etc.).
   - Si el terminal opera por comercio seguro y la tarjeta no es compatible con pago seguro, la operación será denegada con motivo “9104”.
   - Si el terminal opera por comercio no seguro se procederá a la solicitud de autorización de la operación al banco emisor, sin necesidad de autenticación por parte del titular.
6. Redsys muestra al cliente el resultado de la operación (autorizada o denegada).
7. Redsys devuelve a la plataforma del comercio el resultado de la operación (autorizada o denegada) indicado en el valor DS_Response, a través de la notificación por POST o GET enviada a la URL indicada en el parámetro <DS_MERCHANT_MERCHANTURL> de la petición:

```
{
    "Ds_Date":"24%2F04%2F2019",
    "Ds_Hour":"10%3A19",
    "Ds_SecurePayment":"1",
    "Ds_Card_Number":"454881******0004",
    "Ds_Card_Country":"724",
    "Ds_Amount":"100",
    "Ds_Currency":"978",
    "Ds_Order":"66590706",
    "Ds_MerchantCode":"XXXXXXXXX",
    "Ds_Terminal":"1",
    "Ds_Response":"0000",
    "Ds_MerchantData":"",
    "Ds_TransactionType":"0",
    "Ds_ConsumerLanguage":"1",
    "Ds_AuthorisationCode":"110296",
    "Ds_Card_Brand":"1"
}
```

¿CÓMO SERÁ LA OPERATIVA POR REDIRECCIÓN CON LA NUEVA NORMATIVA PSD2?

Con la nueva normativa, **el comercio electrónico no seguro no estará permitido para tarjetas emitidas dentro del Espacio Económico Europeo (EEE)**. Además, establece que será la entidad emisora de la tarjeta quien decida en última instancia cómo serán procesadas las operaciones en base al riesgo calculado de la mismas.

Esta nueva normativa establece **dos flujos en el procesamiento de operaciones**, en base a la **existencia o ausencia** de requerimiento por parte de la entidad emisora, **de autenticación del titular** de la tarjeta mediante el método que tenga habilitado para tal fin (mensaje SMS, contraseña, tarjetas de coordenadas, biometría, etc.) como requisito para autorizar la operación.

- Operación **Challenge**: operación **con requerimiento de autenticación** por el titular de la tarjeta.
- Operación **Frictionless**: operación **sin requerimiento de autenticación** por el titular de la tarjeta.

El **nuevo estándar 3DSecure v.2** incorpora una serie de **nuevos campos** a las peticiones, las cuales servirán a las entidades emisoras **para evaluar el riesgo de las operaciones** con el fin de dictaminar si las operaciones serán gestionadas **mediante Challenge o Frictionless**.

Los terminales virtuales que actualmente estén operando por comercio no seguro **deberán adaptarse al nuevo protocolo** si no quieren que su operativa pase a requerir autenticación del titular de la tarjeta para cada operación.

La normativa **no aplicará a entidades bancarias no europeas**, por lo que las tarjetas emitidas por dichas entidades quedan excluidas y podrán seguir operando mediante comercio no seguro.

Mi terminal opera con comercio no seguro, ¿puedo operar por frictionless?

El nuevo **protocolo 3DSecure v.2** establece una serie de **campos adicionales** que, al incluirlos en las peticiones de pago, permiten a las entidades **evaluar el riesgo** de las operaciones y aumentar las posibilidades de **obtener operaciones frictionless**, es decir, que no requieran autenticación del titular de la tarjeta.

Además, Caixabank dispone de un nuevo **servicio S.R.O. (Scoring de Riesgo Online)** mediante el cual podrá **maximizar** el n.º de operaciones gestionadas por operativa **Frictionless minimizando** el n.º de operaciones **fraudulentas**.

Para hacer uso de dicho servicio, será necesaria la **solicitud de activación** del servicio S.R.O. en su oficina o a su gestor habitual de Caixabank, y la **actualización de su plataforma de comercio electrónico al nuevo protocolo 3DSecure v.2** como requisito para el correcto funcionamiento del servicio.

Mi terminal opera con comercio seguro, ¿puedo obtener operaciones por frictionless?

Sí, lo indicado en el punto anterior para terminales con operativa no segura también es aplicable a terminales con operativa segura.

La actualización de su plataforma de comercio electrónico al nuevo protocolo 3DSecure v.2 **mejorará la experiencia del cliente** en su comercio electrónico, al agilizar el proceso de pago, **aumentando el ratio de operaciones autorizadas** y **reduciendo** el n.º de operaciones **sin finalizar** con estado "9999" (pendiente de autenticación del titular) y el n.º de operaciones **denegadas** con código "184" (autenticación errónea del titular).

¿CÓMO ACTUALIZO MI PLATAFORMA DE COMERCIO ELECTRÓNICO AL NUEVO PROTOCOLO 3DSECURE V.2?

Plataformas modulares (Prestashop, WooCommerce, Magento, etc.)

Para actualizar su plataforma modular al protocolo 3DSecure v.2 necesitará **cambiar el módulo de pago instalado** que conecta con el procesador de pagos por un módulo **compatible con el nuevo protocolo**. El método para realizar el cambio de dicho módulo será el habitual propio de su plataforma.

- Si su módulo es el oficial ofrecido de forma gratuita por Redsys, le informamos que dispone de los siguientes módulos actualizados en la url https://pagosonline.redsys.es/descargas.html:

PLATAFORMA	FECHA ESTIMADA DE DISPONIBILIDAD
PrestaShop	1 de Julio de 2019
WOO COMMERCE	1 de Julio de 2019
Magento Open Source eCommerce	1 de Julio de 2019

- En caso de que su plataforma no sea compatible con los módulos oficiales de Redsys, le informamos que en Internet es posible encontrar **módulos desarrollados por terceras empresas.**
- Si su módulo **no es el oficial de Redsys**, sino que ha sido desarrollado por una empresa externa, le recomendamos que **contacte con la empresa desarrolladora** para consultar la disponibilidad de una actualización del mismo.
- En caso de que su plataforma no sea compatible con ningún módulo disponible en el mercado, y **como último recurso**, puede contactar con una **empresa integradora** para que le realicen un **desarrollo a medida o adaptación de su plataforma**, utilizando como guía la documentación del punto **"Desarrollos a medida y plataformas sin módulo actualizado disponible"**.

Plataforma de tipo e-Pages (1&1, Arsys, Palbin, Comandia, etc.)

Al ser su tienda online un desarrollo de una **empresa de hosting, depende de ellos** el desarrollo y puesta en producción de la actualización al nuevo protocolo 3DSecure v.2.

Le recomendamos que **contacte con su proveedor de hosting** para consultar disponibilidad, fecha y procedimiento necesario para realizar la actualización.

Desarrollos a medida y plataformas sin módulo actualizado disponible

Para desarrollos a medida y plataformas modulares para las cuales no existan módulos actualizados al protocolo 3DSecure v.2, a continuación les facilitamos una guía de integración, así como los nuevos campos que incorpora el nuevo protocolo.

ATENCIÓN: ACTUALMENTE EL API DE REDSYS NO SOPORTA LA GENERACIÓN DE FIRMAS PARA PETICIONES CON DATOS 3DSecure v.2

AL FINAL DE ESTE DOCUMENTO FACILITAMOS EJEMPLOS DE CÓDIGO FUENTE EN PHP, ENTRE LOS CUALES DISPONE DEL CÓDIGO NECESARIO PARA REALIZAR LA FIRMA DE OPERACIONES CON 3DSecure v.2 SIN NECESIDAD DE DICHA API.

Cambios en la integración

La integración por redirección se mantendrá igual salvo la **inclusión del campo "DS_MERCHANT_EMV3DS"**, el cual contendrá un **JSON** con todos los **campos del protocolo 3DSecure v.2**

A continuación incluimos la lista de los campos definidos en el protocolo 3DSecure v.2 para conexiones por redirección.

Campos incluidos en el protocolo 3DSecure v.2

- **CardholderName**, con el nombre del titular de la tarjeta. Máximo 45 caracteres.

- **email**, con la dirección de correo electrónico del cliente. Máximo 254 caracteres.
- **homePhone**, con el teléfono del domicilio del cliente dentro de un JSON, formado por las siguientes claves y sus respectivos valores:
  - cc, con el prefijo del teléfono. Máximo 3 dígitos
  - Subscriber, con el número de teléfono. Máximo 15 dígitos.
- **mobilePhone**, con el teléfono móvil del cliente dentro de un JSON, formado por las siguientes claves y sus respectivos valores:
  - cc, con el prefijo del teléfono. Máximo 3 dígitos
  - Subscriber, con el número de teléfono. Máximo 15 dígitos.
- **workPhone**, con el teléfono del trabajo del cliente dentro de un JSON, formado por las siguientes claves y sus respectivos valores:
  - cc, con el prefijo del teléfono. Máximo 3 dígitos
  - Subscriber, con el número de teléfono. Máximo 15 dígitos.
- **shipAddrLine1**, con la primera línea de la dirección de envío solicitada por el cliente. Máximo 50 caracteres.
- **shipAddrLine2**, con la segunda línea de la dirección de envío solicitada por el cliente. Máximo 50 caracteres.
- **shipAddrLine3**, con la tercera línea de la dirección de envío solicitada por el cliente. Máximo 50 caracteres.
- **shipAddrCity**, con la ciudad de la dirección de envío solicitada por el cliente. Máximo 50 caracteres.
- **shipAddrPostCode**, con el código postal de la dirección de envío solicitada por el cliente. Máximo 16 caracteres.
- **shipAddrState**, con el código del estado o provincia, correspondiente al código de subdivisión ISO 3166-2, de la dirección de envío solicitada por el cliente. Máximo 3 caracteres.
- **shipAddrCountry**, con el código del país, correspondiente al código de al código numérico ISO 3166-1, de la dirección de envío solicitada por el cliente. Máximo 3 caracteres.
- **billAddrLine1**, con la primera línea de la dirección de facturación solicitada por el cliente. Máximo 50 caracteres.
- **billAddrLine2**, con la segunda línea de la dirección de facturación solicitada por el cliente. Máximo 50 caracteres.
- **billAddrLine3**, con la tercera línea de la dirección de facturación solicitada por el cliente. Máximo 50 caracteres.
- **billAddrCity**, con la ciudad de la dirección de facturación solicitada por el cliente. Máximo 50 caracteres.
- **billAddrPostCode**, con el código postal de la dirección de facturación solicitada por el cliente. Máximo 16 caracteres.
- **billAddrState**, con el código del estado o provincia, correspondiente al código de subdivisión ISO 3166-2, de la dirección de facturación solicitada por el cliente. Máximo 3 caracteres.
- **billAddrCountry**, con el código del país, correspondiente al código de al código numérico ISO 3166-1, de la dirección de facturación solicitada por el cliente. Máximo 3 caracteres.
- **addrMatch**, indicando si la dirección de envío es la misma que la dirección de facturación. Los valores aceptados son:
  - Y = Las direcciones de envío y facturación son iguales.
  - N = Las direcciones de envío y facturación son diferentes.
- **challengeWindowSize**, con el tamaño para la ventana de "Challenge" que el banco emisor presentará al cliente en caso de requerir la autenticación al titular de la tarjeta. Los valores en píxeles aceptados son:
  - 01 = 250 x 400
  - 02 = 390 x 400
  - 03 = 500 x 600
  - 04 = 600 x 400
  - 05 = Pantalla completa (valor por defecto)
- **acctID**, Información adicional sobre la cuenta del cliente. Máximo 64 caracteres.
- **threeDSRequestorAuthenticationInfo**, con información adicional sobre como el cliente se autenticó en el inicio de sesión en la cuenta del comercio, contenida en un JSON formado por las siguientes claves y sus respectivos valores:
  - threeDSReqAuthData, con datos que documentan y soportan un proceso de autenticación específico. No está especificado el contenido en la versión actual del protocolo.
  - threeDSReqAuthMethod, informando del mecanismo utilizado por el cliente para autenticarse en el comercio. Los valores aceptados son:
    - 01 = No se produjo la autenticación del cliente (acceso como invitado).
    - 02 = Acceso a la cuenta del cliente en la plataforma del comercio usando credenciales propias de dicha plataforma.
    - 03 = Acceso a la cuenta del cliente en la plataforma del comercio usando un ID federado.
    - 04 = Acceso a la cuenta del cliente en la plataforma del comercio usando las credenciales del emisor.
    - 05 = Acceso a la cuenta del cliente en la plataforma del comercio usando autenticación de terceros.
    - 06 = Acceso a la cuenta del cliente en la plataforma del comercio usando Autenticador FIDO.

- threeDSReqAuthTimestamp, con la fecha y hora UTC de la autenticación del cliente en el comercio. Formato aceptado: YYYYMMDDHHMM

- **acctInfo, altamente recomendado su envío con el fin de aumentar las autorizaciones "Frictionless"**. Información adicional de la cuenta de cliente en el comercio, contenida en un JSON formado por las siguientes claves y sus respectivos valores:
  - chAccAgeInd, con el periodo de tiempo que el cliente ha tenido cuenta en el comercio. Los valores aceptados son:
    - 01 = Sin cuenta (invitado)
    - 02 = Recién creada
    - 03 = Menos de 30 días
    - 04 = Entre 30 y 60 días
    - 05 = Más de 60 días
  - chAccDate, con la fecha en que el titular de la tarjeta abrió la cuenta en el comercio. Formato aceptado: YYYYMMDD
  - chAccChange, con la fecha en que se modificó por última vez la cuenta del cliente en el comercio, incluida la dirección de facturación o envío, la cuenta de pago o nuevos usuarios agregados. Formato aceptado: YYYYMMDD
  - chAccChangeInd, con el tiempo transcurrido desde que se modificó por última vez la información de la cuenta del cliente en el comercio, incluidas las direcciones de facturación o envío, la cuenta de pago o los nuevos usuarios agregados. Valores aceptados:
    - 01 = Modificado en esta sesión
    - 02 = Menos de 30 días
    - 03 = Entre 30 y 60 días
    - 04 = Más de 60 días
  - chAccPwChange, con la fecha en que el cliente tuvo un cambio de contraseña o un restablecimiento en la cuenta del comercio. Formato aceptado: YYYYMMDD
  - chAccPwChangeInd, con el tiempo transcurrido desde que el cliente tuvo un cambio de contraseña o un restablecimiento en la cuenta del comercio. Valores aceptados:
    - 01 = Sin cambio
    - 02 = Modificado en esta sesión
    - 03 = Menos de 30 días
    - 04 = Entre 30 y 60 días
    - 05 = Más de 60 días
  - nbPurchaseAccount, con el n.º de compras de la cuenta durante los últimos 6 meses.
  - provisionAttemptsDay, con el n.º de intentos de agregar tarjeta en las últimas 24 horas.
  - txnActivityDay,con el n.º de transacciones (exitosas y abandonadas) para esta cuenta del cliente en el comercio en todas las cuentas de pago en las últimas 24 horas.
  - txnActivityYear, con el n.º de transacciones (exitosas y abandonadas) para esta cuenta del cliente en el comercio en todas las cuentas de pago en el último año.
  - paymentAccAge, con la fecha en que la cuenta de pago se inscribió en la cuenta del cliente del comercio. Formato aceptado: YYYYMMDD
  - paymentAccInd, con el período de tiempo que la cuenta de pago se inscribió en la cuenta del cliente en el comercio. Valores aceptados:
    - 01 = Sin cuenta (invitado)
    - 02 = Modificado en esta sesión
    - 03 = Menos de 30 días
    - 04 = Entre 30 y 60 días
    - 05 = Más de 60 días
  - shipAddressUsage, con la fecha en que la dirección de envío utilizada para esta transacción se utilizó por primera vez con el comercio. Formato aceptado: YYYYMMDD
  - shipAddressUsageInd, indicando cuándo la dirección de envío utilizada para esta transacción se utilizó por primera vez con el comercio. Valores aceptados:
    - 01 = Por primera vez
    - 02 = Menos de 30 días
    - 03 = Entre 30 y 60 días
    - 04 = Más de 60 días

- shipNameIndicator, indicando si el nombre del cliente en la cuenta es idéntico al nombre de envío utilizado en esta transacción. Valores aceptados:
  - 01 = Nombre del cliente y nombre del envío idénticos
  - 02 = Nombre del cliente y nombre del envío diferentes
- suspiciousAccActivity, indicando si el comercio ha experimentado actividad sospechosa (incluido fraude anterior) en la cuenta del cliente. Valores aceptados:
  - 01 = Sin actividad sospechosa detectada.
  - 02 = Actividad sospechosa detectada.

- **MerchantRiskIndicator, altamente recomendado su envío con el fin de aumentar las autorizaciones "Frictionless"**. Información adicional del comercio que representa la evaluación del nivel de riesgo de fraude para la autenticación, contenida en un JSON formado por las siguientes claves y sus respectivos valores:
  - deliveryEmailAddress, con la dirección de correo electrónico a la que se entregarán los productos en el caso de entregas electrónicas.
  - deliveryTimeframe, indicando el plazo de entrega de la mercancía. Valores aceptados:
    - 01 = Entrega electrónica.
    - 02 = Envío en el mismo día.
    - 03 = Envío al siguiente día.
    - 04 = Dos o más días.
  - giftCardAmount, con el importe total de la compra en unidades principales (por ejemplo, EUR 123.45 sería 123). para compras de tarjetas prepago o tarjetas regalo.
  - giftCardCount, con el recuento total de tarjetas prepago o tarjetas/códigos regalo comprados.
  - giftCardCurr, con el código ISO-4217 de la divisa para compras de tarjetas prepago o tarjetas regalo.
  - preOrderDate, con la fecha prevista de disponibilidad de la mercancía en compras con reserva. Formato aceptado: YYYYMMDD
  - preOrderPurchaseInd, indicando si el cliente realiza un pedido con disponibilidad o fecha de reserva. Valores aceptados:
    - 01 = Mercancía disponible.
    - 02 = Mercancía disponible próximamente.
  - reorderItemsInd, indicando si el cliente había comprado la mercancía previamente. Valores aceptados:
    - 01 = Primera vez que compra la mercancía.
    - 02 = Recompra de mercancía.
  - shipIndicator, indicando el método de envío elegido para la transacción, eligiendo el que describa con mayor precisión esta transacción, no la actividad comercial en general. Si se incluyen uno o más artículos en la venta, utilice el código del Indicador de envío para los bienes físicos, o si todos los productos son digitales, utilice el código del Indicador de envío que describe el artículo más caro. Valores aceptados:
    - 01 = Envío a la dirección principal de la cuenta del cliente.
    - 02 = Envío a otra dirección almacenada en la cuenta del cliente.
    - 03 = Envío a una dirección diferente a la almacenada en la cuenta del cliente.
    - 04 = Entrega en comercio / Envío a punto de recogida
    - 05 = Mercancía digital (incluye servicios electrónicos, tarjetas/códigos regalo, etc.)
    - 06 = Entradas a eventos o billetes de viaje electrónicos.
    - 07 = Otros (por ejemplo, videojuegos, suscripciones electrónicas, etc.)

Ejemplo de una petición de autorización con datos del protocolo 3DSecure v.2 incluidos:


```
{
    "DS_MERCHANT_MERCHANTCODE": "XXXXXXXXX",
    "DS_MERCHANT_TERMINAL": "1",
    "DS_MERCHANT_TRANSACTIONTYPE": "0",
    "DS_MERCHANT_AMOUNT": "100",
    "DS_MERCHANT_CURRENCY": "978",
    "DS_MERCHANT_ORDER": "66590706",
    "DS_MERCHANT_EMV3DS": {
        "cardholderName": "Titular pruebas",
        "Email": "test@test.com",
        "HomePhone": {
            "cc": "34",
            "Subscriber": "900000000"
        },
        "MobilePhone": {
            "cc": "34",
            "Subscriber": "600000000"
        },
        "WorkPhone": {
            "cc": "34",
            "Subscriber": "900000000"
        },
        "shipAddrLine1": "Linea direccion 1",
        "shipAddrLine2": "Linea direccion 2",
        "shipAddrLine3": "Linea direccion 3",
        "shipAddrCity": "Barcelona",
        "shipAddrPostCode": "08001",
        "shipAddrState": "B",
        "shipAddrCountry": "724",
        "addrMatch": "Y",
        "billAddrLine1": "Linea direccion 1",
        "billAddrLine2": "Linea direccion 2",
        "billAddrLine3": "Linea direccion 3",
        "billAddrCity": "Barcelona",
        "billAddrPostCode": "08001",
        "billAddrState": "B",
        "billAddrCountry": "724",
        "acctInfo": {
            "chAccAgeInd": "05",
            "chAccChange": "20190101",
            "chAccChangeInd": "04",
            "chAccDate": "20190101",
            "chAccPwChange": "20190101",
            "chAccPwChangeInd": "01",
            "nbPurchaseAccount": "10",
            "provisionAttemptsDay": "0",
            "txnActivityDay": "0",
            "txnActivityYear": "10",
            "paymentAccAge": "20190101",
            "paymentAccInd": "05",
            "shipAddressUsage": "20190101",
            "shipAddressUsageInd": "04",
            "shipNameIndicator": "01",
            "suspiciousAccActivity": "01"
        },
        "merchantRiskIndicator": {
            "deliveryEmailAddress": "test@test.com",
            "deliveryTimeframe": "01",
            "giftCardAmount": "100",
            "giftCardCount": "1",
            "giftCardCurr": "978",
            "preOrderDate": "20191014",
            "preOrderPurchaseInd": "01",
            "reorderItemsInd": "01",
            "shipIndicator": "01"
        }
    }
}
```

Ejemplo de una petición de autorización con todos los datos del protocolo 3DSecure v.2 incluidos, codificada en BASE64 y con los campos que componen el formulario que se enviará a Redsys:

"**Ds_SignatureVersion**" = "HMAC_SHA256_V1"
"**Ds_MerchantParameters**" =
"ewogICAgIkRTX01FUkNIQU5UX01FUkNIQU5UQ09ERSI6ICJYWFhYWFhYWFgiLAogICAgIkRTX01FUkNIQU5UX1RFUk1JTkFMIjog
IjEiLAogICAgIkRTX01FUkNIQU5UX1RSQU5TQUNUSU9OVFlQRSI6ICIwIiwKICAgICJEU19NRVJDSEFOVF9BTU9VTlQiOiAiMTAwIiwK
ICAgICJEU19NRVJDSEFOVF9DVVJSRU5DWSI6ICI5NzgiLAogICAgIkRTX01FUkNIQU5UX09SREVSSIjogIjY2NTkwNzA2IiwKICAgICJEU
19NRVJDSEFOVF9FTVYzRFMiOiB7CiAgICAgICAgImNhcmRob2xkZXJOYW1lIjogIlRpdHVsYXIgcHJ1ZWJhcyIsCiAgICAgICAgIkVtYW
lsIjogInRlc3RAdGVzdC5jb20iLAogICAgICAgICJIb21lUGhvbmUiOiB7CiAgICAgICAgICAgICJjYyI6ICIzNCIsCiAgICAgICAgICAg
JzY3JpYmVyIjogIjkwMDAwMDAwMCIKICAgICAgICB9LAogICAgICAgICJNb2JpbGVQaG9uZSI6IHsKICAgICAgICAgICAgImNjIjogIj
M0IiwKICAgICAgICAgICAgIlN1YnNjcmliZXIiOiAiNjAwMDAwMDAwIgogICAgICAgIH0sCiAgICAgICAgImJpbGxBZGRyZXNzMSI6ICJa
W5lIiwKICAgICAgICAgICAgImNpdHkiOiAiQmFyY2Vsb25hIiwKICAgICAgICAgICAgInBvc3RhbENvZGUiOiAiMDgwMDEiLAogICAg
ICAgICAgICAgInN0YXRlIjogIkIiLAogICAgICAgICAgICAiY291bnRyeSI6ICI3MjQiLAogICAgICAgICAgICAiYWRkcmVzc01hdGNo
IjogIlkiLAogICAgICAgICAgICAiYmlsbEFkZHJMaW5lMSI6ICJMaW5lYSBkaXJlY2Npb24gMSIsCiAgICAgICAgICAgImJpbGxBZGRyZTliOiAiTGluZWEgZGlyZWNjaW9uIDIiLAogICAgICAgICAgICAiYmlsbEFkZHJDaXR5IjogIkJhcmNlbG9uYSIsCiAgICAgICAgICAgICJiaWxsQWRkcmVzczJvgIkxpbmVhIGRpcmVjY2lvbiAzIiwKICAgICAgICAgICAiYmlsbEFkZHJDaXR5IjogIkJhcmNlbG9uYSIsCiAgICAgICAgICAgImJpbGxBZGRyUG9zdENvZGUiOiAiMDgwMDEiLAogICAgICAgICAgICAiYmlsbEFkZHJTdGF0ZSI6ICJCIiwKICAgICAgICAgICAgImJpbGxBZGRyQ291bnRyeSI6ICI3MjQiCiAgICAgICAgfQogICAgfQp9"
"**Ds_Signature**" = "x1eDN28FPnImTQMTPmSwvY+92P+xzjBjVC1ILbotZmg="

Ejemplo de una petición de autorización con **exención LWV por bajo importe incluida**. La exención a aplicar se indica en el campo "DS_MERCHANT_EXCEP_SCA" **fuera** del campo "DS_MERCHANT_EMV3DS":

```
{
    "DS_MERCHANT_MERCHANTCODE": "XXXXXXXXX",
    "DS_MERCHANT_TERMINAL": "1",
    "DS_MERCHANT_TRANSACTIONTYPE": "0",
    "DS_MERCHANT_AMOUNT": "100",
    "DS_MERCHANT_CURRENCY": "978",
    "DS_MERCHANT_ORDER": "66590706",
    "DS_MERCHANT_EXCEP_SCA": "LWV",
    "DS_MERCHANT_EMV3DS":
    {
        "cardholderName": "Titular pruebas",
        "Email": "test@test.com",
        "HomePhone": { "cc": "34", "Subscriber": "900000000" },
        "MobilePhone": { "cc": "34", "Subscriber": "600000000" },
        "shipAddrLine1": "Linea direccion 1",
        "shipAddrLine2": "Linea direccion 2",
        "shipAddrLine3": "Linea direccion 3",
        "shipAddrCity": "Barcelona",
        "shipAddrPostCode": "08001",
        "shipAddrState": "B",
        "shipAddrCountry": "724",
        "addrMatch": "Y",
        "billAddrLine1": "Linea direccion 1",
        "billAddrLine2": "Linea direccion 2",
        "billAddrLine3": "Linea direccion 3",
        "billAddrCity": "Barcelona",
        "billAddrPostCode": "08001",
        "billAddrState": "B",
        "billAddrCountry": "724"
    }
}
```

TARJETAS PARA ENTORNO DE PRUEBAS

En el entorno de pruebas únicamente se pueden utilizar las siguientes tarjetas para realizar operaciones ficticias:

Resultado	PAN	3DSecure v.2.1	3DSMethod	Tipo de autorización
Autorización	4548812049400004	✗	✗	CIP
Autorización	4918019160034602	✓	✓	Frictionless
Autorización	4548814479727229	✓	✗	Frictionless
Autorización	4918019199883839	✓	✓	Challenge
Autorización	4548817212493017	✓	✗	Challenge
Denegación 190	5576440022788500	✗	✗	CIP
Denegación 190	4907277775205123	✓	✓	Frictionless
Denegación 190	4907271141151707	✓	✓	Challenge
Denegación 9598	5410082854557833	✓	✗	
Denegación 9598	5410088208000685	✓	✗	

Los datos para todas ellas, son los siguientes:

Fecha de caducidad	Cualquier fecha de caducidad válida.
CVV	123
CIP (Código de Identificación Personal)	123456

EXENCIONES DE LA NORMATIVA PSD2 Y SERVICIO S.R.O.

¿En qué tipos de operaciones se puede prescindir de la autenticación del titular?

La normativa PSD2 contempla los siguientes casos, en los cuales las operaciones quedan **fuera de la norma**, o bien pueden ser **exencionables de la autenticación** con 3DSecure mediante un **análisis de riesgo** que la entidad pone a su disposición (Scoring de Riesgo Online):

	Nombre	Escenario
Operaciones exencionables mediante S.R.O. (Scoring de Riesgo Online)	LWV (LoW Value)	**Operaciones de bajo importe** (hasta 30€ por operación, con un máximo de 5 operaciones consecutivas o 100€ acumulados sin autenticación).
	T.R.A (Transaction Risk Analysis)	**Operaciones analizadas por la entidad y evaluadas como bajo riesgo** hasta un importe máximo definido por la entidad (250€ actualmente)
	C.O.R. (Secure Corporate Payments)	**Pagos corporativos entre empresas** con métodos de pago no accesibles fuera del entorno empresarial ni para consumidores finales.
Operaciones no afectadas por la nueva normativa	Tarjetas emitidas fuera de la U.E.	Las tarjetas de **emisores no comunitarios**, como no están afectadas por la nueva normativa, por lo que podrán seguir operando por comercio no seguro.
	M.I.T. (Merchant Initiated Transaction)	**Operaciones enviadas por el comercio**, sin intervención del titular de la tarjeta, mediante el envío de datos de tarjeta o token generado previamente.
	M.O./T.O (Mail Order / Telephone Order)	Operaciones enviadas por un terminal con **operativa MO/TO** con introducción manual de datos de tarjeta del titular, facilitados mediante teléfono o correo electrónico.
	T.N.A. (Terminales No Atendidos)	**Terminales no atendidos** instalados en comercios con sectores de actividad de transportes o parkings.

¿En qué consiste el servicio Scoring de Riesgo Online (S.R.O.)?

La entidad pone a su disposición **S.R.O. (Scoring de Riesgo Online)**, un servicio mediante el cual se **analiza el riesgo de fraude** de las operaciones con el fin de obtener un **alto porcentaje de conversión** de operaciones por operativa **Frictionless (sin necesidad de autenticación del titular)**.

- Para que el servicio S.R.O. opere correctamente es necesario que **su plataforma esté adaptada** al nuevo protocolo de seguridad **3DSecure v.2**, ya que parte del análisis se basa en los nuevos campos informativos incluidos en dicho protocolo.
- Para indicar que se desea **aplicar una exención**, la plataforma del comercio debe **incluir el campo "Ds_Merchant_Excep_SCA" con el valor correspondiente de la exención que se debe aplicar a la operación, fuera del JSON** con los campos del 3DSecure v.2.
- La activación del servicio S.R.O. le permitirá hacer uso de las siguientes exenciones contempladas en la norma:
  - **L.W.V. (LoW Value – Bajo importe):** permite procesar operaciones de bajo importe sin necesidad de la autenticación del titular de la tarjeta.
    - Con la petición de pago enviada para la autorización de la operación, se deberá incluir el campo **"Ds_Merchant_Excep_SCA"** con valor **"LWV"**.
    - El **importe máximo** por operación es de **30€**
    - El **emisor de la tarjeta llevará un contador** de las operaciones autorizadas **sin autenticación**, que podrá ser tanto por n.º de operaciones como por importe acumulado:
      - El **n.º máximo de operaciones** seguidas sin autenticar es de **5**. En la 6ª operación consecutiva de menos de 30€ se solicitará S.C.A. del titular de la tarjeta, reiniciando el contador a 0 en caso de autenticación correcta.
      - El **importe acumulado máximo** es de **100€**. Si con la operación, el importe acumulado de operaciones sin autenticación supera el importe indicado, se solicitará S.C.A. (Strong Customer Authentication) del titular de la tarjeta, reiniciando el contador a 0 en caso de autenticación correcta.
  - **T.R.A. (Transaction Risk Analysis – Análisis del riesgo de la operación):** permite procesar operaciones de importe medio y bajo que, tras aplicar el **análisis de riesgo** de la operación, hayan obtenido un nivel de **riesgo bajo**, y se solicita la autorización de la operación por la operativa **Frictionless**, es decir, sin autenticación del titular.
    - Con la petición de pago enviada para la autorización de la operación, se deberá incluir el parámetro **"Ds_Merchant_Excep_SCA"** con valor **"TRA"**.
    - El **importe máximo** para la clasificación de operaciones de bajo riesgo puede ser **definido por el comercio** a través de su agente de Caixabank **hasta un máximo** definido por la entidad (**250€ actualmente**).

        - El importe máximo no es fijo, ya que depende de numerosos factores analizados por la entidad, y podría ser modificado en el futuro.
        - La exención **no aplicará** a operaciones con un **importe superior al máximo actual** y será decisión del banco emisor el requerir autenticación del titular.
        - El **importe máximo no aplicará a terminales de tipo T.N.A.** de comercios que operen en los sectores de **actividad de transportes o parkings**.
    - **C.O.R. (Secure Corporate Payments – Pagos seguros corporativos):** permite procesar pagos corporativos entre empresas con métodos de pago no accesibles fuera del entorno empresarial ni para consumidores finales.
        - Con la petición de pago enviada para la autorización de la operación, se deberá incluir el parámetro **"Ds_Merchant_Excep_SCA"** con valor **"COR"**.
- Se debe tener en cuenta que, independientemente de la exención enviada con la operación, **en última instancia la decisión** de tramitar la operación por Frictionless o Challenge siempre **dependerá del banco emisor**, el cual **puede rechazar la exención** recibida y requerir S.C.A. del titular.
- El servicio podría conllevar costes asociados por operación analizada, independientemente de su exención o no.
- Podrá **solicitar la activación** del servicio en su **oficina** o a su **gestor** de **Caixabank**.

Mi comercio opera total o parcialmente con comercio no seguro, ¿debo contratar el servicio S.R.O.?

En caso de que su comercio actual se base en **operativa no segura con tarjetas emitidas dentro de la Unión Europea**, tanto por redirección como por WebService, el **no contar con los servicios S.R.O.** de la entidad ocasionará el **rechazo** de la entidad emisora al procesado de la operación por **frictionless**. Es decir, quedaría a decisión de la entidad emisora de la tarjeta el **requerir la autenticación del titular** como paso indispensable para autorizar las operaciones, lo cual podría **afectar a la operativa actual** de su comercio.

No es posible determinar **el % de operaciones** que serán procesadas mediante operativa **Frictionless / Challenge**, ya que **dependerá de múltiples factores** como la información del cliente enviada desde su plataforma, el importe de la operación, el porcentaje de fraude de su comercio, el tipo de cliente, los varemos de riesgo establecidos por la entidad emisora, etc.

No obstante, y tras estudios de la entidad, **se ha estimado** que la media de operaciones que podrán ser gestionadas mediante operativa **frictionless** en caso de **disponer del servicio S.R.O.** es de aproximadamente **el 75%**. No obstante, dicho porcentaje variará dependiendo de los datos facilitados por el comercio y las características de la operativa del comercio, tales como importes, ratio de fraude sufrido, características del titular de la tarjeta, etc.

El servicio S.R.O. ofrece además una **ventaja adicional frente a las reglas anti-fraude actuales:**

- **Actualmente, los filtros anti-fraude** configuradas en el terminal **pueden bloquear la operativa de un cliente o terminal durante 24 horas** por la actividad del titular (operaciones acumuladas por tarjeta en 24 horas, operaciones acumuladas por IP en 24 horas, etc.) o la procedencia de la conexión del cliente (el país de la IP del cliente no coincide con el país del emisor de la tarjeta, el país de la IP del cliente es de un país no aceptado, etc.).
- **Con el nuevo servicio S.R.O., las operaciones** que actualmente son bloqueadas por los filtros anti-fraude **podrían ser convertidas en** operaciones **autorizadas**, previa autenticación de la operación por el titular de la tarjeta.

El servicio podría conllevar costes asociados por operación analizada, independientemente de su exención o no.

Podrá **solicitar la activación** del servicio en su **oficina** o a su **gestor** de **Caixabank**.

Mi comercio opera con comercio seguro, ¿podría interesarme el servicio S.R.O.?

El nuevo servicio S.R.O. también está **disponible para comercios con operativa segura**, contribuyendo a **mejorar los ratios de conversión** de operaciones **y la experiencia final del cliente,** al **procesar** operaciones con **bajo riesgo** de fraude por operativa **frictionless**, lo cual **disminuirá** el % de **operaciones sin finalizar y denegadas** por error de autenticación del titular.

El servicio S.R.O. ofrece además una **ventaja adicional frente a las reglas anti-fraude actuales:**

- **Actualmente, los filtros anti-fraude** configuradas en el terminal **pueden bloquear la operativa de un cliente o terminal durante 24 horas** por la actividad del titular (operaciones acumuladas por tarjeta en 24 horas, operaciones acumuladas por IP en 24 horas, etc.) o la procedencia de la conexión del cliente (el país de la IP del cliente no coincide con el país del emisor de la tarjeta, el país de la IP del cliente es de un país no aceptado, etc.).
- **Con el nuevo servicio S.R.O., las operaciones** que actualmente son bloqueadas por los filtros anti-fraude **podrían ser convertidas en** operaciones **autorizadas**, previa autenticación de la operación por el titular de la tarjeta.

El servicio podría conllevar costes asociados por operación exencionada, pero no por las operaciones analizadas.

Podrá **solicitar la activación** del servicio en su **oficina** o a su **gestor** de **Caixabank**.

Actualmente mi operativa incluye pago por referencia / pago no seguro, ¿podré seguir operando?

Las operaciones enviadas por el comercio sin que hayan sido iniciadas por el titular de la tarjeta, ya sea mediante el envío de datos de tarjeta almacenados o el envío de un token o referencia, se denominan **M.I.T. (Merchant Initiated Transaction)** y **no se encuentran afectadas por la normativa**. Es el caso de domiciliaciones, suscripciones, pagos periódicos, etc.

Para poder enviar operaciones M.I.T. deberá tener en cuenta los siguientes puntos:

- Es necesario **tener activado el servicio S.R.O. con operativa M.I.T habilitada**.
- Para el envío de operaciones M.I.T. sobre una tarjeta, token o referencia, el titular deberá haber autenticado una **operación inicial mediante S.C.A. (Strong Customer Authentication), o** bien disponer el comercio de un **contrato físico o acuerdo legal, aceptado por el titular de la tarjeta**, en el cual se especifiquen los objetos, importes y periodicidad de los cargos a su tarjeta.
- Las operaciones **deben ser lanzadas** desde el comercio mediante una **programación automática**, e incluyendo el campo **"Ds_Merchant_Excep_SCA"** con valor **"MIT"**.
  - Los **pagos iniciados por** una acción del **titular de la tarjeta**, como por ejemplo un pago mediante 1-click, **no podrán ser clasificadas como operaciones M.I.T.**, y su envío como tal podría ser causa de sanciones.
- Las marcas de tarjetas monitorizarán el correcto uso de las operaciones M.I.T., pudiendo solicitar el bloqueo e inicio de acciones legales contra los comercios que no cumplan los requisitos arriba indicados.

Podrá **solicitar la activación** del servicio en su **oficina** o a su **gestor** de **Caixabank**.

Actualmente dispongo de referencias o tokens de clientes, ¿serán válidos con la nueva normativa?

Sí, los tokens generados antes de la entrada en vigor de la normativa **seguirán siendo válidos** a partir del 14/09/19. No será necesario por lo tanto la generación por el comercio de nuevas referencias.

CÓDIGOS DE ERROR Y DENEGACIONES EMV3DS V.2.1

A continuación dispone del listado con los códigos de error y de denegación incorporados por la actualización a la nueva normativa:

Denegación	Error SIS0XXX	Motivo
9569	SIS0569	Operación de Inicia Petición rechazada, no se ha informado la tarjeta
9570	SIS0570	Operación de Inicia Petición rechazada, se ha enviado tarjeta y referencia
9581	SIS0581	Operación de autenticación EMV3DS rechazada, datos DS_MERCHANT_EMV3DS no está indicado o es demasiado grande y no se puede convertir en JSON
9585	SIS0585	Operación de autenticación EMV3DS rechazada
9592	SIS0592	Error en la operación de autenticación EMV3DS
9593	SIS0593	Error en la operación de autenticación EMV3DS
9595	SIS0595	El comercio indicado no tiene métodos de pago seguros permitidos en EMV3DS V2
9598	SIS0598	Error en la operación de autenticación EMV3DS
9599	SIS0599	Error en la operación de autenticación EMV3DS
9600	SIS0600	Error en la operación de autenticación EMV3DS (Areq N)
9601	SIS0601	Error en la operación de autenticación EMV3DS (Areq R)
9602	SIS0602	Error en la operación de autenticación EMV3DS(Areq U). No método de pago válido
9616	SIS0616	Error del parámetro DS_MERCHANT_EXCEP_SCA tiene un valor erróneo
9617	SIS0617	Error en el proceso de autenticación EMV3DS V2 -(Areq A). No método de pago válido
9617	SIS0617	Error del parámetro DS_MERCHANT_EXCEP_SCA es de tipo MIT y no vienen datos de COF o de pago por referencia
9618	SIS0618	Ya existe una anulación asociada al pago

CÓDIGO PHP DE EJEMPLO

Generación de la petición para REST / Redirección

```php
<?php

$datos_peticion = new \stdClass();

// Declaración de la versión de firma
$version_firma="HMAC_SHA256_V1";


// Recolección de las claves y valores del JSON

// Datos obligatorios

// FUC del comercio
$datos_peticion->DS_MERCHANT_MERCHANTCODE = $_POST['Numero_Comercio'];

// Nº de terminal al que se envía la operación
$datos_peticion->DS_MERCHANT_TERMINAL = $_POST['Terminal'];

// Tipo de operación (autorización, pre-autorización, devolución, etc.)
$datos_peticion->DS_MERCHANT_TRANSACTIONTYPE = $_POST['Tipo_Transaccion'];

// Importe de la operación
$datos_peticion->DS_MERCHANT_AMOUNT = $_POST['Importe'];

// Divisa de la operación (euros, dólares, libras, etc.)
$datos_peticion->DS_MERCHANT_CURRENCY = $_POST['Divisa'];

// Número de pedido
$datos_peticion->DS_MERCHANT_ORDER = $_POST['Numero_Pedido'];


// Datos opcionales

// URL en la que queremos recibir la notificación con el resultado de la operación
if (isset($_POST["Enviar_URL_Notificacion"])){
        $datos_peticion->DS_MERCHANT_MERCHANTURL = $_POST['URL_Notificacion'];}

// Descripción del producto a mostrar en la pasarela de pago
if (isset($_POST["Enviar_Producto"])){
        $datos_peticion->DS_MERCHANT_PRODUCTDESCRIPTION = $_POST['Producto'];}

// Nombre del titular de la tarjeta
if (isset($_POST["Enviar_Titular_Tarjeta"])){
                $datos_peticion->DS_MERCHANT_TITULAR = $_POST['Titular_Tarjeta'];}

// URL a la que se debe redirigir al cliente cuando la operación sea autorizada
if (isset($_POST["Enviar_URLOK"])){
        $datos_peticion->DS_MERCHANT_URLOK = $_POST['URLOK'];}

// URL a la que se debe redirigir al cliente cuando la operación sea denegada
if (isset($_POST["Enviar_URLKO"])){
        $datos_peticion->DS_MERCHANT_URLKO = $_POST['URLKO'];}

// Nombre del comercio a mostrar en la pasarela
if (isset($_POST["Enviar_Nombre_Comercio"])){
        $datos_peticion->DS_MERCHANT_MERCHANTNAME = $_POST['Nombre_Comercio'];}

if (isset($_POST["Enviar_Descriptor_Flexible"])){
        $datos_peticion->DS_MERCHANT_MERCHANTDESCRIPTOR = $_POST['Descriptor_Flexible'];}

// Código del idioma en el que se debe mostrar la pasarela de pago al cliente
if (isset($_POST["Enviar_Idioma"])){
        $datos_peticion->DS_MERCHANT_CONSUMERLANGUAGE = $_POST['Idioma'];}
```

```
// Mostrar al cliente únicamente los métodos de pago indicados
if (isset($_POST["Enviar_Metodos_Pago"])){
        $datos_peticion->DS_MERCHANT_PAYMETHODS = $_POST['Metodos_Pago'];}

if (isset($_POST["Enviar_Tipo_Fraccionamiento"])){
                $datos_peticion->DS_MERCHANT_PARTIALPAYMENTTYPE = $_POST['Tipo_Fraccionamiento'];}

if (isset($_POST["Enviar_Fraccionamiento"])){
        $datos_peticion->DS_MERCHANT_PARTIALPAYMENT = $_POST['Fraccionamiento'];}

// Información del módulo usado (nombre, versión, etc.)
if (isset($_POST["Enviar_Informacion_Modulo"])){
        $datos_peticion->DS_MERCHANT_MODULE = $_POST['Informacion_Modulo'];}

// Mostrar al cliente la pasarela con el código de personalización enviado
if (isset($_POST["Enviar_Personalizacion"])){
        $datos_peticion->DS_MERCHANT_PERSOCODE = $_POST['Personalizacion'];}

// Referencia del recibo para el pago de tributos
if (isset($_POST["Enviar_Codigo_Tributo"])){
        $datos_peticion->DS_MERCHANT_TAX_REFERENCE = $_POST['Codigo_Tributo'];}

// Datos adicionales que serán devueltos en la notificación
if (isset($_POST["Enviar_Datos_Comercio"])){
        $datos_peticion->DS_MERCHANT_MERCHANTDATA = $_POST['Datos_Comercio'];}


// Datos de tarjeta (Operativa XML-Entidad)

// PAN de la tarjeta
if(isset($_POST["Enviar_PAN"])){
        $datos_peticion->DS_MERCHANT_PAN = $_POST['Pan'];}

// Fecha de caducidad de la tarjeta
if(isset($_POST["Enviar_Fecha_Caducidad_Tarjeta"])){
        $datos_peticion->DS_MERCHANT_EXPIRYDATE = $_POST['Fecha_Caducidad_Tarjeta'];}

// CVV2 de la tarjeta
if(isset($_POST["Enviar_CVV2"])){
        $datos_peticion->DS_MERCHANT_CVV2 = $_POST['CVV2'];}


// Pago por referencia

// Solicitar generar referencia
if(isset($_POST["Solicitar_Referencia"])){
        $datos_peticion->DS_MERCHANT_IDENTIFIER = "REQUIRED";}
// Enviar referencia
if(isset($_POST["Enviar_Referencia"])){
        $datos_peticion->DS_MERCHANT_IDENTIFIER = $_POST['Referencia'];}

if (isset($_POST["Enviar_Grupo_Referencia"])){
        $datos_peticion->DS_MERCHANT_GROUP = $_POST['Grupo_Referencia'];}

if(isset($_POST["Enviar_Pago_Directo"])){
        $datos_peticion->DS_MERCHANT_DIRECTPAYMENT = $_POST['Pago_Directo'];}


// Datos para 3DSecure v.2

//Inclusión del código facilitado en el siguiente apartado “Generación del JSON EMV3DS” que recoge los datos para 3DSecure v.2 y genera la variable $json_datos_3DSecure_v2
include_once ('peticion_3dsecure_v2.php');

// Inclusión en la petición del JSON EMV3DS generado en el apartado “Generación del JSON EMV3DS”.
$datos_peticion->DS_MERCHANT_EMV3DS = $datos_3DSecure_v2;


// Generación del JSON con los datos de la petición.
```

```
$json_datos_peticion = json_encode($datos_peticion);


// Codificación en Base64 del JSON con los datos de la petición.
$json_peticion_codificado = base64_encode($json_datos_peticion);


//Generación del firma SHA256 mediante el código facilitado en el apartado “Generación de la firma SHA256 sin API”
include_once ('firma_SHA256.php');

?>
```

Generación del JSON EMV3DS (peticion_3dsecure_v2.php)

```
<?php

// Inicialización de las variables
$datos_3DSecure_v2 = new \stdClass();
$telefono_domicilio = new \stdClass();
$telefono_movil = new \stdClass();
$telefono_trabajo = new \stdClass();
$informacion_inicio_sesion = new \stdClass();
$informacion_cuenta_titular = new \stdClass();
$indicador_riesgo_comercio = new \stdClass();


// Datos para 3DSecure v.2.1

if(isset($_POST["Enviar_Nombre_Titular"])){
        $datos_3DSecure_v2->cardholderName = $_POST['Nombre_Titular'];}
if(isset($_POST["Enviar_Tamano_Ventana_Challenge"])){
        $datos_3DSecure_v2->challengeWindowSize = $_POST['Tamano_Ventana_Challenge'];}
if(isset($_POST["Enviar_Email"])){
        $datos_3DSecure_v2->Email = $_POST['Email'];}

// Teléfono del domicilio del cliente.
if(isset($_POST["Enviar_Telefono_Domicilio"])){
        $telefono_domicilio->cc = $_POST['Prefijo_Telefono_Domicilio'];
        $telefono_domicilio->Subscriber = $_POST['Numero_Telefono_Domicilio'];
        // Añadimos los datos del teléfono del domicilio del cliente a la subclave HomePhone que depende de la clave
datos_3DSecure_v2
        $datos_3DSecure_v2->HomePhone = $telefono_domicilio;}

// Teléfono móvil del cliente.
if(isset($_POST["Enviar_Telefono_Movil"])){
        $telefono_movil->cc = $_POST['Prefijo_Telefono_Movil'];
        $telefono_movil->Subscriber = $_POST['Numero_Telefono_Movil'];
        // Añadimos los datos del teléfono móvil del cliente a la subclave MobilePhone que depende de la clave
datos_3DSecure_v2
        $datos_3DSecure_v2->MobilePhone = $telefono_movil;}

// Teléfono del trabajo del cliente.
if(isset($_POST["Enviar_Telefono_Trabajo"])){
        $telefono_trabajo->cc = $_POST['Prefijo_Telefono_Trabajo'];
        $telefono_trabajo->Subscriber = $_POST['Numero_Telefono_Trabajo'];
        // Añadimos los datos del teléfono de trabajo del cliente a la subclave WorkPhone que depende de la clave
datos_3DSecure_v2
        $datos_3DSecure_v2->WorkPhone = $telefono_trabajo;}

// Dirección de envío.
if(isset($_POST["Enviar_Direccion_Envio_1"])){
        $datos_3DSecure_v2->shipAddrLine1 = $_POST['Direccion_Envio_1'];}
if(isset($_POST["Enviar_Direccion_Envio_2"])){
        $datos_3DSecure_v2->shipAddrLine2 = $_POST['Direccion_Envio_2'];}
if(isset($_POST["Enviar_Direccion_Envio_3"])){
        $datos_3DSecure_v2->shipAddrLine3 = $_POST['Direccion_Envio_3'];}
if(isset($_POST["Enviar_Ciudad_Direccion_Envio"])){
        $datos_3DSecure_v2->shipAddrCity = $_POST['Ciudad_Direccion_Envio'];}
if(isset($_POST["Enviar_CP_Envio"])){
        $datos_3DSecure_v2->shipAddrPostCode = $_POST['CP_Envio'];}
if(isset($_POST["Enviar_Provincia_Envio"])){
        $datos_3DSecure_v2->shipAddrState = $_POST['Provincia_Envio'];}
if(isset($_POST["Enviar_Pais_Direccion_Envio"])){
        $datos_3DSecure_v2->shipAddrCountry = $_POST['Pais_Direccion_Envio'];}

// Coincidencia de las direcciones de envío y facturación.
if(isset($_POST["Enviar_Indicador_Coincidencia_Direccion"])){
        $datos_3DSecure_v2->addrMatch = $_POST['Indicador_Coincidencia_Direccion'];}
```

```
// Dirección de facturación.
if(isset($_POST["Enviar_Direccion_Facturacion_1"])){
	$datos_3DSecure_v2->billAddrLine1 = $_POST['Direccion_Facturacion_1'];}
if(isset($_POST["Enviar_Direccion_Facturacion_2"])){
	$datos_3DSecure_v2->billAddrLine2 = $_POST['Direccion_Facturacion_2'];}
if(isset($_POST["Enviar_Direccion_Facturacion_3"])){
	$datos_3DSecure_v2->billAddrLine3 = $_POST['Direccion_Facturacion_3'];}
if(isset($_POST["Enviar_Ciudad_Direccion_Facturacion"])){
	$datos_3DSecure_v2->billAddrCity = $_POST['Ciudad_Direccion_Facturacion'];}
if(isset($_POST["Enviar_CP_Facturacion"])){
	$datos_3DSecure_v2->billAddrPostCode = $_POST['CP_Facturacion'];}
if(isset($_POST["Enviar_Provincia_Facturacion"])){
	$datos_3DSecure_v2->billAddrState = $_POST['Provincia_Facturacion'];}
if(isset($_POST["Enviar_Pais_Direccion_Facturacion"])){
	$datos_3DSecure_v2->billAddrCountry = $_POST['Pais_Direccion_Facturacion'];}

// Información del inicio de sesión del cliente en la plataforma del comercio.
if(isset($_POST["Enviar_Informacion_Inicio_Sesion"])){
	if(isset($_POST["Enviar_Datos_Inicio_Sesion"])){
		$informacion_inicio_sesion->threeDSReqAuthData = $_POST['Datos_Inicio_Sesion'];}
	if(isset($_POST["Enviar_Metodo_Autenticacion_Inicio_Sesion"])){
		$informacion_inicio_sesion->threeDSReqAuthMethod =
$_POST['Metodo_Autenticacion_Inicio_Sesion'];}
	if(isset($_POST["Enviar_Fecha_Hora_Inicio_Sesion"])){
		$informacion_inicio_sesion->threeDSReqAuthTimestamp = $_POST['Fecha_Hora_Inicio_Sesion'];}
	// Añadimos los datos de la sesión del cliente en su cuenta del comercio a la subclave
threeDSRequestorAuthenticationInfo que depende de la clave datos_3DSecure_v2
	$datos_3DSecure_v2->threeDSRequestorAuthenticationInfo = $informacion_inicio_sesion;}

// Información sobre la actividad en la cuenta del cliente en la plataforma del comercio.
if(isset($_POST["Enviar_Informacion_Cuenta_Titular"])){
	if(isset($_POST["Enviar_Indicador_Permanencia_Cuenta"])){
		$informacion_cuenta_titular->chAccAgeInd = $_POST['Indicador_Permanencia_Cuenta'];}
	if(isset($_POST["Enviar_Fecha_Modificacion_Cuenta"])){
		$informacion_cuenta_titular->chAccChange = $_POST['Fecha_Modificacion_Cuenta'];}
	if(isset($_POST["Enviar_Indicador_Modificacion_Cuenta"])){
		$informacion_cuenta_titular->chAccChangeInd = $_POST['Indicador_Modificacion_Cuenta'];}
	if(isset($_POST["Enviar_Fecha_Alta_Cuenta"])){
		$informacion_cuenta_titular->chAccDate = $_POST['Fecha_Alta_Cuenta'];}
	if(isset($_POST["Enviar_Fecha_Cambio_Contrasena"])){
		$informacion_cuenta_titular->chAccPwChange = $_POST['Fecha_Cambio_Contrasena'];}
	if(isset($_POST["Enviar_Indicador_Cambio_Contrasena"])){
		$informacion_cuenta_titular->chAccPwChangeInd = $_POST['Indicador_Cambio_Contrasena'];}
	if(isset($_POST["Enviar_Numero_Compras_6_Meses"])){
		$informacion_cuenta_titular->nbPurchaseAccount = $_POST['Numero_Compras_6_Meses'];}
	if(isset($_POST["Enviar_Numero_Intentos_Agregar_Tarjeta_24h"])){
		$informacion_cuenta_titular->provisionAttemptsDay =
$_POST['Numero_Intentos_Agregar_Tarjeta_24h'];}
	if(isset($_POST["Enviar_Numero_Transacciones_24h"])){
		$informacion_cuenta_titular->txnActivityDay = $_POST['Numero_Transacciones_24h'];}
	if(isset($_POST["Enviar_Numero_Transacciones_Anyo"])){
		$informacion_cuenta_titular->txnActivityYear = $_POST['Numero_Transacciones_Anyo'];}
	if(isset($_POST["Enviar_Alta_Cuenta_Pago"])){
		$informacion_cuenta_titular->paymentAccAge = $_POST['Alta_Cuenta_Pago'];}
	if(isset($_POST["Enviar_Indicador_Creacion_Cuenta_Pago"])){
		$informacion_cuenta_titular->paymentAccInd = $_POST['Indicador_Creacion_Cuenta_Pago'];}
	if(isset($_POST["Enviar_Fecha_Direccion_Envio"])){
		$informacion_cuenta_titular->shipAddressUsage = $_POST['Fecha_Direccion_Envio'];}
	if(isset($_POST["Enviar_Indicador_Direccion_Envio"])){
		$informacion_cuenta_titular->shipAddressUsageInd = $_POST['Indicador_Direccion_Envio'];}
	if(isset($_POST["Enviar_Indicador_Nombre_Titular"])){
		$informacion_cuenta_titular->shipNameIndicator = $_POST['Indicador_Nombre_Titular'];}
	if(isset($_POST["Enviar_Indicador_Actividad_Sospechosa"])){
		$informacion_cuenta_titular->suspiciousAccActivity = $_POST['Indicador_Actividad_Sospechosa'];}
	// Añadimos los datos de la actividad de la cuenta a la subclave acctInfo que depende de la clave
datos_3DSecure_v2
	$datos_3DSecure_v2->acctInfo = $informacion_cuenta_titular;}

if(isset($_POST["Enviar_Informacion_Adicional_Cuenta_Cliente"])){
	$datos_3DSecure_v2->acctID = $_POST['Informacion_Adicional_Cuenta_Cliente'];}
```

```
if(isset($_POST["Enviar_Datos_Pago_Aplazado"])){
        $datos_3DSecure_v2->purchaseInstalData = $_POST['Datos_Pago_Aplazado'];}
if(isset($_POST["Enviar_Finalizacion_Pago_Recurrente"])){
        $datos_3DSecure_v2->recurringExpiry = $_POST['Finalizacion_Pago_Recurrente'];}
if(isset($_POST["Enviar_Frecuencia_Pagos_Recurrentes"])){
        $datos_3DSecure_v2->recurringFrequency = $_POST['Frecuencia_Pagos_Recurrentes'];}

// Información sobre el riesgo del cliente.
if(isset($_POST["Enviar_Indicador_Riesgo_Comerciante"])){
        if(isset($_POST["Enviar_Direccion_Entrega_Electronica"])){
                $indicador_riesgo_comercio->deliveryEmailAddress = $_POST['Direccion_Entrega_Electronica'];}
        if(isset($_POST["Enviar_Plazo_Entrega"])){
                $indicador_riesgo_comercio->deliveryTimeframe = $_POST['Plazo_Entrega'];}
        if(isset($_POST["Enviar_Importe_Tarjeta_Regalo"])){
                $indicador_riesgo_comercio->giftCardAmount = $_POST['Importe_Tarjeta_Regalo'];}
        if(isset($_POST["Enviar_Recuento_Tarjeta_Regalo"])){
                $indicador_riesgo_comercio->giftCardCount = $_POST['Recuento_Tarjeta_Regalo'];}
        if(isset($_POST["Enviar_Divisa_Tarjeta_Regalo"])){
                $indicador_riesgo_comercio->giftCardCurr = $_POST['Divisa_Tarjeta_Regalo'];}
        if(isset($_POST["Enviar_Fecha_Compra_Reserva"])){
                $indicador_riesgo_comercio->preOrderDate = $_POST['Fecha_Compra_Reserva'];}
        if(isset($_POST["Enviar_Indicador_Disponibilidad_Pedido"])){
                $indicador_riesgo_comercio->preOrderPurchaseInd = $_POST['Indicador_Disponibilidad_Pedido'];}
        if(isset($_POST["Enviar_Indicador_Recompra"])){
                $indicador_riesgo_comercio->reorderItemsInd = $_POST['Indicador_Recompra'];}
        if(isset($_POST["Enviar_Metodo_Envio"])){
                $indicador_riesgo_comercio->shipIndicator = $_POST['Metodo_Envio'];}
        // Añadimos los datos del riesgo a la subclave merchantRiskIndicator que depende de la clave
datos_3DSecure_v2
        $datos_3DSecure_v2->merchantRiskIndicator = $indicador_riesgo_comercio;}


// Generación del JSON con los datos de 3DSecure v.2.1
$json_datos_3DSecure_v2 = json_encode($datos_3DSecure_v2);

?>
```

Generación de la firma SHA-256 sin API (firma_SHA256.php)

```
<?php

// Generación de la firma SHA256

// Decodificación en Base64 del la clave SHA256
$clave_decodificada = base64_decode($_POST['Clave_SHA256']);

// Código para PHP5
if($_POST["Version_PHP"] == "PHP5"){
		// Se establece un IV por defecto
		$bytes = array(0,0,0,0,0,0,0,0);
		$iv = implode(array_map("chr", $bytes));
		// Se cifra
		$clave_cifrado = mcrypt_encrypt(MCRYPT_3DES, $clave_decodificada, $_POST['Numero_Pedido'],
MCRYPT_MODE_CBC, $iv);
};

// Código para PHP7
if($_POST["Version_PHP"] == "PHP7"){
		// Se diversifica la clave con el Número de Pedido y se genera la clave de cifrado.
		$l = ceil(strlen($_POST['Numero_Pedido']) / 8) * 8;
		// Se cifra
		$clave_cifrado = substr(openssl_encrypt($_POST['Numero_Pedido'] . str_repeat("\0", $l -
strlen($_POST['Numero_Pedido'])), 'des-ede3-cbc', $clave_decodificada, OPENSSL_RAW_DATA, "\0\0\0\0\0\0\0\0"), 0,
$l);}

// MAC256 del JSON codificado y la clave de cifrado generada.
$firma = hash_hmac('sha256', $datos_peticion, $clave_cifrado, true);

// Codificación en Base64 de la firma.
$firma_codificada = base64_encode($firma);

?>
```

Comercia Global Payments

Para cualquier consulta no dude en contactarnos:

soporte.migraciones@comerciaglobalpay.com

www.comerciaglobalpayments.com