DirectLink con 3-D Secure

Tabla de contenidos

1. 3-D Secure v1.0

1.1 Introducción

El protocolo 3-D permite la identificación del titular de la tarjeta durante el proceso de compra. El titular de la tarjeta debe estar conectado a Internet durante el proceso de identificación. Por tanto, 3-D Secure no funciona para centros de llamadas o pagos periódicos.

Visa ha implementado el protocolo 3-D Secure con el nombre Verified By Visa, MasterCard con el nombre SecureCode, JCB con el nombre J-Secure y American Express con el nombre SafeKey.

El principio de la integración de DirectLink con 3-D Secure es iniciar un pago en modo DirectLink y finalizarlo en modo e-Commerce si se solicita la autenticación del titular.

Este documento describe la integración del protocolo 3-D Secure en DirectLink. Para obtener más información sobre DirectLink o e-Commerce, consulte la documentación de DirectLink o e-Commerce.

1.2 Flujo de transacciones 3-D a través de DirectLink

El flujo de transacciones implica los siguientes pasos:

1. Envíenos una solicitud de DirectLink para la transacción con el número de parámetros adicionales (véase Parámetros de solicitud extra).
2. Nuestro sistema recibe el número de tarjeta en su solicitud y comprueba en línea si la tarjeta está registrada en el directorio VISA/MasterCard/JCB/AmEx (registrada significa que la identificación es posible para el número de tarjeta; por ejemplo, es una tarjeta 3-D Secure).
3. Si el titular de la tarjeta está registrado, la respuesta a la solicitud de DirectLink contendrá un estado de pago específico y código html que se devolverá al cliente para iniciar el proceso de identificación (véase Campos devueltos adicionales). El bloque de código html iniciará automáticamente el proceso de identificación entre el titular de la tarjeta (cliente) y su banco emisor.
4. El titular de la tarjeta se identifica a sí mismo en la página del banco emisor.
5. Nuestro sistema recibe la respuesta de identificación del emisor.
6. Si la identificación ha sido correcta, nuestro sistema enviará la transacción financiera real a la entidad adquirente.
7. Recibirá el resultado de la identificación global y el proceso de autorización en línea a través de los canales de respuesta del modo e-Commerce.

Comentarios:

- La aplicación de la transferencia de responsabilidad dependerá del contrato de su entidad adquirente. Por tanto, le recomendamos consultar los términos y condiciones con su entidad adquirente.
- Si el titular de la tarjeta no está registrado (en el paso 3), recibirá la respuesta XML de DirectLink estándar que contiene el resultado del proceso de autorización en línea.
- Para recibir los códigos de estado/error de pago exactos (en el paso 7), deberá implementar la respuesta posventa en línea o sin conexión, tal como se describe en la documentación de e-Commerce.

1.2.1 Parámetros de solicitud extra

Aparte de los parámetros de DirectLink estándar, también es posible que tenga que enviar la siguiente información:

Campo	Descripción
FLAG3D	Valor fijo: 'Y' Indica a nuestro sistema que lleve a cabo una identificación 3-D Secure si es necesario.

Si desea más información, vaya a Respuesta de transacción.

1.2.2 Campos devueltos adicionales

Si el titular no está registrado, se devolverá la respuesta de DirectLink normal. Si el titular está registrado, se devolverán los siguientes campos (adicionales):

Campo	Descripción
STATUS	Nuevo valor: “46” (esperando identificación)
HTML_ANSWER	Se puede añadir código HTML codificado con BASE64 en la página HTML devuelta al cliente. Esta etiqueta se añade como elemento secundario de la etiqueta global XML <ncresponse>. El campo HTML_Answer contiene código HTML que añadirse a la página HTML devuelta al navegador del cliente. Este código cargará automáticamente la página de identificación del banco emisor en una ventana emergente en la ventana principal, dependiendo del valor del parámetro WIN3DS. Para evitar cualquier interferencia entre las etiquetas HTML incluidas en el contenido de la etiqueta HTML_ANSWER XML con el resto del XML devuelto como respuesta a la solicitud de DirectLink, el contenido de HTML_ANSWER es codificado mediante BASE64 por nuestro sistema antes de enviar la respuesta. En consecuencia, se debe descodificar mediante BASE64 antes de incluirlo en la página HTML enviada al titular de la tarjeta.

1.2.3 Comentarios

Tarjetas de prueba

Puede usar las siguientes tarjetas de prueba para simular una tarjeta registrada 3-D Secure en nuestro entorno de prueba:

Marca	Número de tarjeta	Fecha de caducidad	Contraseña
VISA	4000000000000002	Cualquier fecha del futuro	11111
MasterCard	5300000000000006	Cualquier fecha del futuro	11111
American Express	371449635311004	Cualquier fecha del futuro	11111

Identificación incorrecta

Si una transacción está bloqueada debido a una identificación incorrecta, el resultado de la transacción será:

STATUS = 0

NCSTATUS = 5

NCERROR = 40001134

2. 3-D Secure v2.1 (Disponible en TEST)

2.1 Introducción

En 2013, la Comisión Europea publicó una propuesta para elaborar una versión revisada de la Directiva sobre servicios de pago, conocida como PSD2, para simplificar el procesamiento de pagos y crear reglas y reglamentos para los servicios de pago en la UE, lo que desencadenó la necesidad de desarrollar una versión nueva de 3-D Secure, denominada v2.1.

El cambio más importante es que se le solicita que, en calidad de comerciante, comparta más datos: los emisores tienen un gran interés en que los puntos de datos mejoren la precisión en las decisiones, lo que en última instancia conducirá a un escenario libre de problemas, pero son ustedes, los comerciantes, los que están en primera línea en lo que se refiere a la captura de datos. El enfoque de 3DS v2 sobre la evaluación de riesgos es más efectivo, pero le obliga a cambiar todo el ecosistema para que pueda hacer llegar los datos al emisor.

Los principales esquemas de las tarjetas de pago han actualizado sus logotipos 3DS con la introducción de esta nueva guía.
Asegúrese de implementar estos nuevos logotipos en la creación de su página de pago (Visa / Mastercard / JCB /…).

2.2 Flujo de transacciones 3-D a través de DirectLink

El flujo de la transacción implica los pasos siguientes:

1. Nos envía una solicitud de DirectLink para la transacción que contiene una serie de parámetros adicionales.

Estos parámetros se pueden agrupar en tres conjuntos:

a. Los parámetros obligatorios que deben capturarse en la página de pago donde el titular de la tarjeta está ingresando los detalles de la tarjeta.

Parámetros	Descripción	Formato	Obligatorio
browserAcceptHeader	Contenido exacto de los encabezados HTTP Accept, tal como se envían al comerciante desde el navegador del titular de la tarjeta. *	Tipo de datos: cadena Longitud: variable, máx. 2.048 caracteres Valor aceptado: Si la longitud total del encabezado Accept enviado por el navegador supera los 2.048 caracteres, el servidor 3DS truncará el excedente.	Sí
browserColorDepth	Valor que representa la profundidad de bits de la paleta de colores para visualizar imágenes, en bits por píxel. La proporciona el navegador del titular de la tarjeta mediante la propiedad de profundidad de color de pantalla.	Tipo de datos: cadena Valores aceptados: 1 = 1 bit 4 = 4 bits 8 = 8 bits 15 = 15 bits 16 = 16 bits 24 = 24 bits 32 = 32 bits	Sí

Parámetros	Descripción	Formato	Obligatorio
		48 = 48 bits	
browserJavaEnabled	Valor booleano que representa la capacidad del navegador del titular de la tarjeta para ejecutar Java. El valor es devuelto por la propiedad de Java Enabled del navegador.	Tipo de datos: booleano Valores aceptados: true false	Sí
browserLanguage	Valor que representa el idioma del navegador, tal como se define en IETF BCP47. Lo devuelve la propiedad Language del navegador.	Tipo de datos: cadena Longitud: variable, 1-8 caracteres	Sí
browserScreenHeight	Altura total de la pantalla del titular de la tarjeta, en píxeles. El valor es devuelto por la propiedad Screen Height.	Tipo de datos: Int entre 0 y 999999	Sí
browserScreenWidth	Anchura total de la pantalla del titular de la tarjeta, en píxeles. El valor es devuelto por la propiedad Screen Width.	Tipo de datos: Int entre 0 y 999999	Sí
browserTimeZone	Diferencia horaria entre la hora UTC y la hora local del navegador del titular de la tarjeta, en minutos.	Tipo de datos: Int entre -720 y 840	Sí
browserUserAgent	Contenido exacto del encabezado HTTP User-Agent. *	Tipo de datos: cadena Longitud: variable, máx. 2.048 caracteres Nota: si la longitud total del encabezado User-Agent enviado por el navegador supera los 2.048 caracteres, el servidor 3DS truncará el excedente.	Sí

*No tiene que enviar HTTP_ACCEPT y HTTP_USER_AGENT con browserAcceptHeader y browserUserAgent; los rellenaremos con los parámetros del navegador.

Nota: No olvide calcular los parámetros en su firma SHA.

A continuación encontrará un ejemplo de código Javascript para capturar estos parámetros.

```
<script type="text/javascript" language="javascript">

function createHiddenInput(form, name, value)
{
var input = document.createElement("input");
input.setAttribute("type", "hidden");
input.setAttribute("name", name);
input.setAttribute("value", value);
form.appendChild(input);
}
```

```
var myCCForms = document.getElementsByName("MyForm");
if (myCCForms != null && myCCForms.length > 0)
{
var myCCForm = myCCForms[0];
createHiddenInput(myCCForm, "browserColorDepth", screen.colorDepth);
createHiddenInput(myCCForm, "browserJavaEnabled", navigator.javaEnabled());
createHiddenInput(myCCForm, "browserLanguage", navigator.language);
createHiddenInput(myCCForm, "browserScreenHeight", screen.height);
createHiddenInput(myCCForm, "browserScreenWidth", screen.width);
createHiddenInput(myCCForm, "browserTimeZone", new Date().getTimezoneOffset());
}
</script>
```

b. Parámetros adicionales obligatorios (véase Parámetros de solicitud extra)

c. Parámetros recomendados (lista de parámetros) que, si se envían, tendrán un efecto positivo en la tasa de conversión de las transacciones. De acuerdo con la información que contienen estos parámetros, puede producirse un flujo de autenticación sin problemas, en el que ya no se tenga que autenticar al titular de la tarjeta, por lo que se prevé que la transacción se complete de forma más rápida. Por el contrario, si no se proporciona ninguno de estos parámetros, se llevará a cabo el redireccionamiento relacionado con la autenticación normal.

Nuestro sistema recibe el número de tarjeta en su solicitud y comprueba en línea si la tarjeta está registrada en el directorio VISA/MasterCard/JCB/AmEx (registrada significa que la identificación es posible para el número de tarjeta; por ejemplo, es una tarjeta 3-D Secure).

2. De acuerdo con la respuesta del directorio de los sistemas, si el titular de la tarjeta está registrado para 3-D Secure, se prevén dos posibles flujos, en función de si se han proporcionado los parámetros adicionales indicados en el apartado **1.c** (Parámetros recomendados-lista de parámetros) anterior:

2.1. **Un flujo sin problemas**: El titular de la tarjeta no necesita físicamente autenticarse porque la autenticación se realizó en segundo plano sin su aportación. En este caso, el cambio de responsabilidad es del banco emisor.>

2.2. **Un flujo con comprobación:** Se debe realizar una identificación adicional del titular de la tarjeta.

i. La respuesta a la solicitud de **DirectLink** contiene un estado de pago específico y un código html que se debe devolver al cliente para iniciar el proceso de identificación (véase Campos de devolución adicionales). El bloque de código html iniciará automáticamente el proceso de identificación entre el (cliente) titular de la tarjeta y el banco emisor.

ii. El titular de la tarjeta se identifica a sí mismo en la página del banco emisor.

iii. Nuestro sistema recibe la respuesta de identificación del emisor.

iv. Si la identificación ha sido correcta, nuestro sistema enviará la transacción financiera real a la entidad adquirente.

3. Recibirá el resultado de la identificación global y el proceso de autorización en línea a través de los canales de respuesta del modo e-Commerce.

2.2.1 Parámetros de solicitud extra

Aparte de los parámetros de DirectLink estándar, también es posible que tenga que enviar la siguiente información:

Campo	Descripción
FLAG3D	Valor fijo: 'Y' Indica a nuestro sistema que lleve a cabo una identificación 3-D Secure si es necesario.
HTTP_ACCEPT	El campo Aceptar de la cabecera de la solicitud en el navegador del titular de la tarjeta se utiliza para especificar determinados tipos de medios aceptables para la respuesta. El emisor utiliza este valor para comprobar si el navegador del titular de la tarjeta es compatible con el sistema de identificación del emisor. * Por ejemplo: Aceptar: */*
HTTP_USER_AGENT	El campo Agente del usuario de la cabecera de la solicitud en el navegador del titular de la tarjeta contiene información sobre el agente del usuario que originó la solicitud. El emisor utiliza este valor para comprobar si el navegador del titular de la tarjeta es compatible con el sistema de identificación del emisor. * Por ejemplo: Agente del usuario: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
WIN3DS	Forma de mostrar la página de identificación al cliente. Valores posibles: • MAINW: muestra la página de identificación en la ventana principal (valor predeterminado). • POPUP: muestra la página de identificación en una ventana emergente y vuelve a la ventana principal al final. • POPIX: muestra la página de identificación en una ventana emergente y permanece en la ventana emergente.
ACCEPTURL	URL de la página web para mostrar al cliente cuando se autoriza el pago. (o se espera que se autorice).
DECLINEURL	URL al que se redirecciona al cliente si se ha alcanzado el máximo número de intentos de autorización fallidos (10 de forma predeterminada, pero que puede cambiar en la página Información técnica, pestaña "Parámetros de transacción globales", sección "Reintento de pago").
EXCEPTIONURL	URL de la página web para mostrar al cliente cuando el resultado del pago es dudoso.
PARAMPLUS	Campo para enviar parámetros varios y los valores que desea que se devuelvan en la solicitud de posventa o en el redireccionamiento final.
COMPLUS	Campo para enviar un valor que desea que se devuelva en la solicitud de postventa o en la respuesta.
LANGUAGE	Idioma del cliente, por ejemplo: "en_US"
Opcional	
TP	Para cambiar el diseño de la página "order_A3DS", puede enviar un nombre/url de plantilla con este parámetro. (vaya a e-Commerce: Plantilla dinámica).

*No será necesario enviar HTTP_ACCEPT y HTTP_USER_AGENT si se envían browserAcceptHeader y browserUserAgent.

Si desea más información, vaya a Respuesta de transacción.

2.2.2 Campos devueltos adicionales

Si el titular no está registrado, se devolverá la respuesta de DirectLink normal. Si el titular está registrado, se devolverán los siguientes campos (adicionales):

Campo	Descripción
STATUS	Nuevo valor: “46” (esperando identificación)
HTML_ANSWER	Se puede añadir código HTML codificado con BASE64 en la página HTML devuelta al cliente. Esta etiqueta se añade como elemento secundario de la etiqueta global XML <ncresponse>. El campo HTML_Answer contiene código HTML que añadirse a la página HTML devuelta al navegador del cliente. Este código cargará automáticamente la página de identificación del banco emisor en una ventana emergente en la ventana principal, dependiendo del valor del parámetro WIN3DS. Para evitar cualquier interferencia entre las etiquetas HTML incluidas en el contenido de la etiqueta HTML_ANSWER XML con el resto del XML devuelto como respuesta a la solicitud de DirectLink, el contenido de HTML_ANSWER es codificado mediante BASE64 por nuestro sistema antes de enviar la respuesta. En consecuencia, se debe descodificar mediante BASE64 antes de incluirlo en la página HTML enviada al titular de la tarjeta.

2.2.3 Comentarios

Tarjetas de prueba

Puede usar las siguientes tarjetas de prueba para simular una tarjeta registrada 3-D Secure en nuestro entorno de prueba:

Flujo sin problemas Marca	Número de tarjeta	Fecha de caducidad
VISA	4186455175836497	Cualquier fecha del futuro
Mastercard	5137009801943438	Cualquier fecha del futuro
American Express	375418081197346	Cualquier fecha del futuro

Nota: Puede descargar más número de tarjetas de prueba aquí.

Flujo con comprobación Marca	Número de tarjeta	Fecha de caducidad
VISA	4874970686672022	Cualquier fecha del futuro
Mastercard	5130257474533310	Cualquier fecha del futuro
American Express	379764422997381	Cualquier fecha del futuro

Nota: Puede descargar más número de tarjetas de prueba aquí.

Identificación incorrecta

Si una transacción está bloqueada debido a una identificación incorrecta, el resultado de la transacción será:

STATUS = 0

NCSTATUS = 5

NCERROR = 40001134

2.3 Exclusiones y exenciones para 3DsV2

2.3.1 3DSv2 y exclusiones

Con la introducción de 3DSv2, por normal general la autenticación del titular de la tarjeta será obligatoria según lo define la Segunda Directiva de Servicios de Pago (2015/2366 PSD2) de la UE. Sin embargo, algunas transacciones se excluyen de esta regla si se aplica uno de los siguientes escenarios:

- Pedidos por correo/pedidos por teléfono
- Viaje de ida: El PSP del beneficiario (también conocido como adquirente del comerciante) o el PSP del pagador (también conocido como emisor del método de pago del comprador) se encuentra fuera de la zona del EEE.
- Tarjetas prepago anónimas de hasta 150 € (artículo 63)
- MIT - transacciones iniciadas por el comerciante

2.3.2 Flujo SCA y 3DS sin fricción/con comprobación

Parte de esta nueva normativa es la Autenticación sólida de clientes (SCA). Esto implica la posibilidad de que el emisor (el banco del titular de la tarjeta) solicite información adicional al titular de la tarjeta. En tal escenario, el proceso de autenticación dará como resultado un flujo con comprobación (que requiere que el titular de la tarjeta se autentique de forma activa) en lugar de un flujo sin fricción (que no requiere autenticación por parte del titular de la tarjeta).
Sin embargo, ofrecemos a nuestros comerciantes la posibilidad de indicar su flujo preferido. Esto se puede lograr enviando parámetros adicionales que serán utilizados por el emisor para la evaluación de riesgos. En función de la decisión del emisor, podría tener lugar un flujo sin fricción. En algunos escenarios, 3DS podría incluso omitirse por completo si se aplican exenciones específicas.

2.3.3 Indicación del flujo preferido

Para indicar la preferencia por un flujo sin fricción durante la solicitud de autenticación, el comerciante puede enviar el parámetro adicional Mpi.threeDSRequestorChallengeIndicator. Dependiendo de la evaluación del riesgo de fraude del comerciante, se pueden enviar valores específicos (por ejemplo, para una evaluación de bajo riesgo: 02, para un mayor riesgo de fraude: 03).

Parámetro	Valores	Obligatorio/Opcional
Mpi.threeDSRequestorChallengeIndicator	01 = Sin preferencia 02 = Ninguna comprobación solicitada 03 = Comprobación solicitada: preferencia del comerciante 04 = Comprobación solicitada: orden	Obligatorio (en caso de una preferencia para un flujo específico)

El comerciante puede aumentar aún más la posibilidad de un flujo/tasa de conversión sin fricción enviando más campos opcionales.

2.3.4 Exenciones de 3DS

Para algunas transacciones, el comerciante puede omitir 3DS (lo que se traduce en un flujo sin fricción) e ir directamente a la autorización. Este proceso está limitado a transacciones que están excluidas de SCA (como se describe anteriormente) o que pueden beneficiarse de exenciones específicas. Estas exenciones deben ser parte de un acuerdo entre el comerciante y su adquirente. En un escenario como este,

el comerciante indicará omitir el proceso de autenticación enviando estos parámetros adicionales:

Parámetro	Valores	Obligatorio/Opcional
FLAG3DS	N = Saltar el proceso de autenticación 3DS	Obligatorio (en caso de que deba omitirse 3DS)
3DS_EXEMPTION_INDICATOR	Justificación para omitir 3DS. Los valores numéricos pueden ser los siguientes dependiendo de la transacción 03 = TRA* de emisor 04 = Exención baja 05 = TRA* de comerciante/adquiriente 06 = Lista blanca 07 = Corporativo 08 = Envío con retraso 09 = Autenticación delegada (cartera certificada)	Obligatorio (en caso de que deba omitirse 3DS)

* Análisis del riesgo de la transacción (Transaction Risk Analysis)

Sin embargo, sigue siendo decisión del emisor llevarse a cabo o no un proceso de autenticación. Si el emisor insiste en usar 3DS, la transacción será rechazada.