

TPV Virtual Santander Elavon: Guía de desarrollador - 3D Secure - Redirect

Versión: 1.2

Índice

1	Acerca de esta guía	1
1.1	Objetivo.....	1
1.2	Destinatarios.....	1
1.3	Requisitos previos.....	1
1.4	Documentos relacionados.....	1
1.5	Convenciones.....	2
2	Introducción	3
3	3D Secure	4
4	Funcionamiento de Redirect de 3D Secure	7
4.1	Escenarios.....	7
4.2	Secuencia de sucesos.....	9
4.3	Mensaje de respuesta de 3D Secure para Redirect.....	11
5	Escenarios, resultados y mensajes	12

1 Acerca de esta guía

En esta sección se ofrece una descripción general de esta guía, se define cuál es su objetivo, quiénes son sus destinatarios y se hace referencia a otros documentos relacionados. Este documento es confidencial y solo pueden utilizarlo los clientes del servicio TPV Virtual de Santander Elavon. Además, ten en cuenta que se ha proporcionado bajo las condiciones particulares de tu contrato de procesamiento de pagos.

1.1 Objetivo

El objetivo de esta guía es proporcionar un resumen del servicio 3D Secure con integración Redirect que ofrece TPV Virtual de Santander Elavon.

Nota: Cuando pruebe este servicio, todo el tráfico de test debe ser enviado a la pasarela utilizando la URL de pruebas. El entorno de producción no puede ser utilizado para pruebas.

1.2 Destinatarios

Los destinatarios de esta guía son aquellos comercios y desarrolladores que se han dado de alta en el servicio 3D Secure con la opción de integración Redirect y lo están implementando.

1.3 Requisitos previos

Para utilizar esta guía, debes tener experiencia y conocimiento en el siguiente concepto:

- El uso correcto del servicio de autorización para integraciones Redirect de TPV Virtual de Santander Elavon, tal y como se expone en la guía *TPV Virtual Santander Elavon: Guía de desarrollador-3D Secure-Redirect*.

1.4 Documentos relacionados

Además de esta guía, para obtener información sobre el servicio 3D Secure, puedes consultar los siguientes documentos que forman parte de la documentación de TPV Virtual de Santander Elavon:

- *TPV Virtual Santander Elavon: Guía de desarrollador-3D Secure – Redirect*

1.5 Convenciones

En la documentación de TPV Virtual de Santander Elavon, se han aplicado las siguientes convenciones:

Nota: Señala sugerencias o consejos para el usuario.

Precaución: Señala una nota importante. Indica un posible impacto económico.

2 Introducción

Para utilizar el servicio 3D Secure para la opción de integración Redirect, debes comunicar a TPV Virtual de Santander Elavon los escenarios, expuestos en esta guía, en los cuales deseas continuar con una autorización. De forma predeterminada, TPV Virtual de Santander Elavon solo permitirá que se proceda a la fase de autorización de una transacción cuando resulte posible valerse del principio de traslado de responsabilidad en caso de fraude que proporciona el servicio 3D Secure.

3 3D Secure

3D Secure es el nombre genérico con el que se denomina al proceso de autenticación de titulares de tarjeta desarrollado por los esquemas de tarjeta. El sistema implementado por Visa se conoce como «*Verified by Visa*» (o VbyV) y el de MasterCard como «*SecureCode*». El proceso que tiene lugar en ambos casos es el mismo.

En todo pago online con tarjeta de crédito existen dos fases importantes: la autorización y la autenticación. Antes de la llegada de 3D Secure, la única fase que se desarrollaba online era la autorización, que consiste en comprobar la cuenta de la tarjeta de crédito para verificar la existencia de fondos, pero no se autenticaba el titular de esta. En las compras presenciales (es decir, no online, sino cuando el cliente en persona paga en una caja), también se requiere que el titular de la tarjeta de crédito firme un recibo o introduzca su PIN. Con este procedimiento, el comercio se protege del fraude, ya que dispone de un papel físico para demostrar que el cliente ha realizado la compra. En Internet, el comercio no posee ninguna prueba de que el titular de la tarjeta realmente haya efectuado la compra; si este último rechaza la transacción (es decir, alega que no fue él), el comercio es el único responsable y debe reembolsarle el importe. Este proceso se conoce como contracargo o «*devolución de importes cargados*».

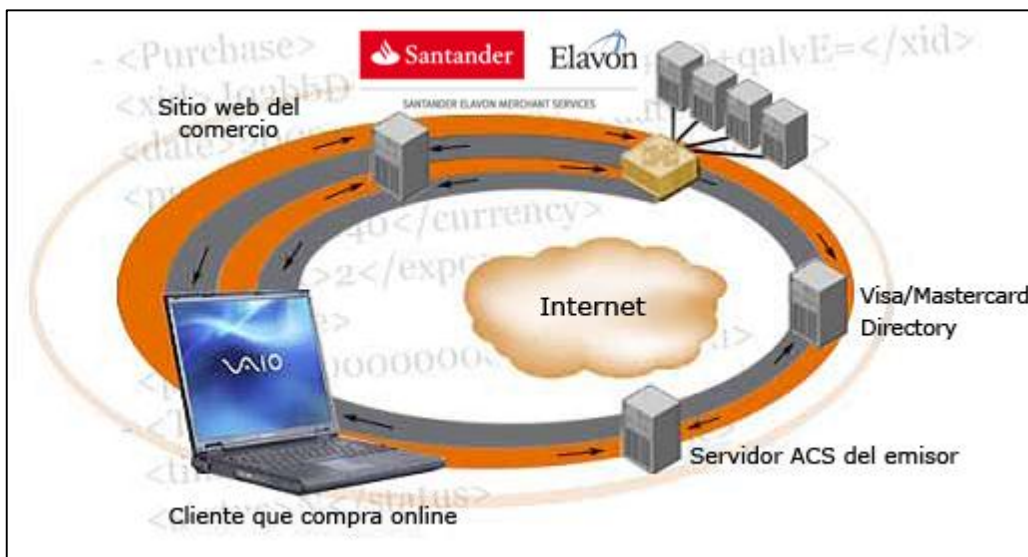
El propósito de 3D Secure consiste en acabar con el riesgo de que se produzca un contracargo. Al obligar al titular de la tarjeta a iniciar sesión en el sitio web de su propio banco (el banco emisor de la tarjeta) antes de realizar una transacción online, la responsabilidad de esta vuelve a recaer en el titular de la tarjeta. Este ya no puede alegar que no fue él quien realizó la compra porque se entiende que solo él conoce su contraseña. Este nuevo proceso de autenticación implica la implementación de varios elementos de software adicionales.

- El comercio debe disponer de MPI (*Merchant Plug-In*), complemento de software que se comunica con los demás elementos que participan en una transacción. El MPI de TPV Virtual de Santander Elavon es 3D Secure. A diferencia de la mayoría de los proveedores de MPI, TPV Virtual de Santander Elavon aloja el servicio 3D Secure, lo que supone que el comercio no tiene que instalar ningún software en su sitio web.
- Visa y MasterCard han creado sistemas nuevos llamados «*Visa Directory*» y «*MasterCard Directory*» respectivamente. Dichos sistemas contienen información sobre qué bancos han implementado el proceso 3D Secure.

- El banco del titular de la tarjeta («*banco emisor*») debe implementar un software llamado servidor de control de acceso (ACS, del inglés «*Access Control Server*») que permite al titular introducir su contraseña y autenticarse mientras realiza compras online. El banco emisor, por tanto, debe proporcionar a los titulares de las tarjetas un mecanismo para realizar dicho proceso y permitirles la configuración de sus contraseñas.
- Los titulares de las tarjetas deben configurar sus contraseñas.

Visto de este modo, puede parecer que implementar 3D Secure supone incorporar una multitud de nuevas acciones a realizar durante el proceso, pero la realidad es que su implementación se ha realizado de tal forma que no se requieren todas y cada una de estas acciones para que el comercio perciba sus ventajas. Cuando el comercio implementa un MPI y el banco adquirente puede aceptar nuevos datos en los mensajes, el comercio no es responsable de las devoluciones por contracargo. La responsabilidad recae en el banco emisor, que se ve presionado a implementar su propio ACS, de forma que la responsabilidad vuelva al titular de la tarjeta.

El siguiente diagrama muestra la sucesión de acciones que tiene lugar cuando se implementa el proceso 3D Secure:



El cliente realiza su compra online e introduce los detalles de su tarjeta. El comercio envía dichos detalles a 3D Secure, que los reenvía al sistema «*Visa/MasterCard Directory*». Dicho sistema sabe si el banco del titular de la tarjeta ha implementado el proceso 3D Secure y comprueba si el titular dispone de contraseña. Si es así, la ubicación del sitio web del ACS se envía de vuelta al

sitio web del comercio. El comercio redirige al titular de la tarjeta a dicho sitio web, donde se le presenta el inicio de sesión en su banco habitual. Cuando se ha iniciado sesión correctamente, la información se reenvía a 3D Secure a través del sitio web del comercio para su validación. Si se valida correctamente, parte de la información vuelve al comercio para que autorice la tarjeta con normalidad y con la confianza de que la transacción no se devolverá a consecuencia de un contracargo.

Si el titular de la tarjeta no dispone de contraseña, el sistema «*Visa/MasterCard Directory*» se lo comunicará a 3D Secure y el comercio procederá con la autorización, pero con la seguridad de que la transacción no se devolverá a consecuencia de un contracargo. Esta es la principal ventaja que brinda la implementación de 3D Secure.

4 Funcionamiento de 3D Secure con integración redirect

Con 3D Secure, la transacción pasa por dos fases distintas:

- Autenticación
- Autorización

3D Secure añade la primera fase (la autenticación) al proceso de transacción. Los dos procedimientos más importantes que se llevan a cabo en la fase de autenticación son los siguientes:

- Inscripción. Se comprueba si el titular de la tarjeta está inscrito en 3D Secure.
- Autenticación. Si el usuario está inscrito, se le solicita su contraseña.

Una vez realizado el proceso de autenticación, y en función de su resultado, el comercio podrá decidir si continuar con la autorización o no.

En la fase de autenticación pueden darse 10 escenarios. En algunos de ellos, el comercio puede valerse del principio de traslado de responsabilidad en caso de contracargo como consecuencia de una transacción fraudulenta. Esto significa que el banco emisor sería el responsable del contracargo.

4.1 Escenarios

La siguiente tabla de escenarios muestra las circunstancias en las que puedes valerte del principio de traslado de responsabilidad en caso de contracargo como consecuencia de una transacción fraudulenta.

Estos escenarios se presentan en la fase de autenticación del titular de la tarjeta, antes de que se produzca la autorización.

Deberás comunicar a TPV Virtual de Santander Elavon en qué escenarios continuarás con una autorización. TPV Virtual de Santander Elavon recomienda encarecidamente que solo procedas con las transacciones que te permitan valerte del traslado completo de la responsabilidad. Ponte en contacto con TPV Virtual de Santander Elavon para analizar las opciones de configuración de 3D Secure.

Escenarios, títulos, descripciones y acciones

Escenario	Nombre	Descripción	Acción
1	Titular de la tarjeta no inscrito.	El titular de la tarjeta no está inscrito en el servicio 3D Secure.	Se puede aplicar el principio de traslado de responsabilidad.
2	No se puede verificar la inscripción	El servidor de inscripción del banco está inactivo temporalmente, por lo que TPV Virtual de Santander Elavon no puede comprobar si el titular de la tarjeta está inscrito.	No se puede aplicar el principio de traslado de responsabilidad.
3	Respuesta no válida del servidor de inscripción	El servidor de inscripción del banco ha devuelto una respuesta no válida a TPV Virtual de Santander Elavon. TPV Virtual de Santander Elavon no puede comprobar si el titular de la tarjeta está inscrito.	No se puede aplicar el principio de traslado de responsabilidad.
4	El titular está inscrito, pero la respuesta de ACS no es válida	El titular de la tarjeta está inscrito, pero la respuesta del sitio web del banco se ha manipulado. Debe considerarse como una transacción fraudulenta.	No se puede aplicar el principio de traslado de responsabilidad.
5	Autenticación correcta.	El titular de la tarjeta está inscrito y ha introducido su contraseña correctamente.	Se puede aplicar el principio de traslado de responsabilidad.
6	Intento de autenticación confirmado.	El titular de la tarjeta está inscrito, pero el banco no tiene forma de comprobar la contraseña y, por lo tanto, confirma el intento de autenticación.	Se puede aplicar el principio de traslado de responsabilidad.

Escenario	Nombre	Descripción	Acción
7	Se ha introducido una contraseña incorrecta	El titular de la tarjeta está inscrito, pero ha introducido una contraseña incorrecta. El titular no se ha autenticado.	No se puede aplicar el principio de traslado de responsabilidad.
8	Autenticación no disponible	El titular de la tarjeta está inscrito, pero el sitio web del banco no está disponible temporalmente. No se puede continuar con la autenticación.	No se puede aplicar el principio de traslado de responsabilidad.
9	Respuesta no válida de ACS	El titular de la tarjeta está inscrito, pero el sitio web del banco ha devuelto una respuesta no válida a TPV Virtual de Santander Elavon. No se puede continuar con la autenticación.	No se puede aplicar el principio de traslado de responsabilidad.
10	Error irrecuperable de 3D Secure	El servicio 3D Secure está inactivo temporalmente.	No se puede aplicar el principio de traslado de responsabilidad.

4.2 Secuencia de sucesos

A continuación, se presenta la secuencia de sucesos que tienen lugar en la fase de autenticación. Además, se exponen los casos en los que se presentan los anteriores escenarios.

1. El titular de la tarjeta introduce los detalles de su tarjeta.

Si la tarjeta es Visa o MasterCard. Si es Laser, American Express, Diners o cualquier otra que no sea compatible con 3D Secure, ve al paso 4c.

Nota: Laser, American Express y Diners no son tarjetas utilizadas en España a día de hoy.

2. TPV Virtual de Santander Elavon comprueba si el titular de la tarjeta está inscrito en 3D Secure, es decir, si ha configurado una contraseña con su banco.

En función de cuál sea la respuesta, se llevará a cabo lo siguiente:

- Si el titular de la tarjeta está inscrito en 3D Secure, se le redirige al sitio web de su banco y se le solicita que introduzca su contraseña. Ve al paso 3.
 - Si el titular de la tarjeta no está inscrito en 3D Secure, ve al paso 4a. No serás responsable del contracargo. (Escenario 1)
3. El titular de la tarjeta introduce su contraseña en el sitio web del banco y se le redirige de nuevo al sitio web del comercio. En función de cuál sea el resultado de la autenticación, se darán los siguientes casos:
- Si el mensaje de 3D Secure se ha manipulado, considera la transacción como fraudulenta; continúa con el paso 4c por tu cuenta y riesgo. Si continúas, no podrás valerte del principio de traslado de responsabilidad, es decir, serás responsable del contracargo. (Escenario 4)
 - Si el titular de la tarjeta introduce su contraseña correctamente, se autentifica. No serás responsable del contracargo. Ve al paso 4b. (Escenario 5)
 - Si el titular de la tarjeta introduce la contraseña incorrectamente, no se autentifica; continúa con el paso 4c por tu cuenta y riesgo. Si continúas, no podrás valerte del principio de traslado de responsabilidad, es decir, serás responsable del contracargo. (Escenario 7)
 - El banco emisor confirma el intento del comercio y asume la responsabilidad. No serás responsable del contracargo. Continúa con el paso 4a. (Escenario 6)
 - Si el banco emisor del titular de la tarjeta no está disponible temporalmente y no puede comprobar la contraseña, el titular no se autentifica. Continúa con el paso 4c por tu cuenta y riesgo. Si continúas, no podrás valerte del principio de traslado de responsabilidad, es decir, serás responsable del contracargo. (Escenario 8)
 - Si se recibe una respuesta no válida del banco emisor del titular de la tarjeta, continúa con el paso 4c por tu cuenta y riesgo. No se puede aplicar el principio de traslado de responsabilidad, es decir, serás responsable del contracargo. (Escenario 9)
 - Si el servicio 3D Secure no está disponible temporalmente, continúa con el paso 4c por tu cuenta y riesgo. Si continúas, no podrás valerte del principio de traslado de responsabilidad, es decir, serás responsable del contracargo. (Escenario 10)
4. En función de cuáles sean los resultados anteriores, TPV Virtual de Santander Elavon procederá de la siguiente manera:

- a) El titular de la tarjeta no está inscrito o el banco confirma el intento, por lo que puedes continuar con la autorización habitual. El comercio no es responsable del contracargo.
- b) El titular de la tarjeta se ha autenticado por completo, por lo que puedes continuar con la autorización habitual. El comercio no es responsable del contracargo.
- c) El titular de la tarjeta no se ha autenticado. El comercio es responsable del contracargo.

4.3 Mensaje de respuesta de 3D Secure para Redirect

Una vez activado 3D Secure en tu cuenta, se devolverán algunos campos de 3D Secure adicionales (eci, xid y CAVV) en la respuesta de redireccionamiento. Consulta la Guía del desarrollador de Autorización de TPV Virtual de Santander Elavon para obtener información detallada sobre estos campos.

Si decides no proceder con la autorización en alguno de los escenarios anteriores, TPV Virtual de Santander Elavon devolverá una nueva respuesta «110», además de un mensaje nuevo según el escenario en el que se haya detenido la transacción.

Puedes incorporar una gestión de errores adicional a tu script de respuesta de redireccionamiento para que procese este resultado «110», si bien la mayoría de los comercios no tendrán que hacerlo porque la gestión actual normalmente cubre cualquier resultado de operación incorrecta (diferente de «00»).

Ten en cuenta que estos mensajes solo se devuelven si decides no continuar con la autorización en un escenario concreto. Si decides proceder con ella, se recibirán las respuestas de autorización habituales (consulta la *TPV Virtual Santander Elavon: Guía de desarrollador-3D Secure-Redirect*).

5 Escenarios, resultados y mensajes

Escenario	Resultado	Mensaje
1	110	Tarjeta no inscrita con 3D Secure; transacción interrumpida. Ponte en contacto con el comercio.
2	110	No se puede determinar el estado de la inscripción del titular de la tarjeta; transacción interrumpida. Ponte en contacto con el comercio.
3	110	Respuesta no válida del servidor de inscripción, transacción interrumpida. Ponte en contacto con el comercio.
4	110	Respuesta no válida de la pasarela de autenticación de TPV Virtual de Santander Elavon. Ponte en contacto con el comercio.
5	110	Transacción bloqueada por la configuración del comercio. Ponte en contacto con el comercio.
6	110	Transacción bloqueada por la configuración del comercio. Ponte en contacto con el comercio.
7	110	Transacción bloqueada por la configuración del comercio. Ponte en contacto con el comercio.
8	110	Transacción bloqueada por la configuración del comercio. Ponte en contacto con el comercio.
9	110	Transacción bloqueada por la configuración del comercio. Ponte en contacto con el comercio.
10	110	Error interno de TPV Virtual de Santander Elavon; transacción interrumpida. Ponte en contacto con el comercio.



SANTANDER ELAVON MERCHANT SERVICES

Santander Elavon Merchant Services

Avda. de Bruselas 36, Planta 3º

28108 Alcobendas | Madrid