Santander Elavon

SANTANDER ELAVON MERCHANT SERVICES

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

Versión: 1.2

Índice

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 de los mensajes XML del servicio 3D Secure como parte del servicio 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 Remote de 3D Secure y lo están implementando.

1.3 Requisitos previos

Para utilizar esta guía, debes tener experiencia y conocimiento en los siguientes conceptos:

- El uso correcto del servicio de autorización de TPV Virtual de Santander Elavon, tal y como se expone en la guía *TPV Virtual Santander Elavon: Guía de desarrollador-Remote*.
- *TPV Virtual Santander Elavon: Guía de integración-Definiciones XML.*

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-Remote*.

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

Si deseas utilizar 3D Secure debes integrarte en TPV Virtual de Santander Elavon. La Guía del desarrollador del servicio de autorización de TPV Virtual de Santander Elavon proporciona información detallada sobre cómo llevar a cabo la integración, así como ejemplos con código de muestra. El resto del documento tratará el formato de los mensajes XML de 3D Secure necesarios y la forma correcta de utilizarlos.

2.1 Integración de la aplicación

Ponte en contacto con los desarrolladores web o de aplicaciones para modificar tu sitio de Internet con el fin de que este se conecte correctamente con TPV Virtual de Santander Elavon.

2.2 Detalles del comercio de Verified by Visa/SecureCode

TPV Virtual de Santander Elavon tendrán que configurar tu cuenta como de comercio en los directorios de Visa y MasterCard. Para obtener más información sobre este proceso, ponte en contacto con TPV Virtual de Santander Elavon.

3 3D Secure

3D Secure es el nombre genérico con el que se denomina al proceso de autentificación del titular de una tarjeta desarrollado por los diferentes 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 autentificación. 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 autentificaba 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, chargeback 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 autentificación 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 autentificarse 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 3D Secure 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 Procesos y escenarios

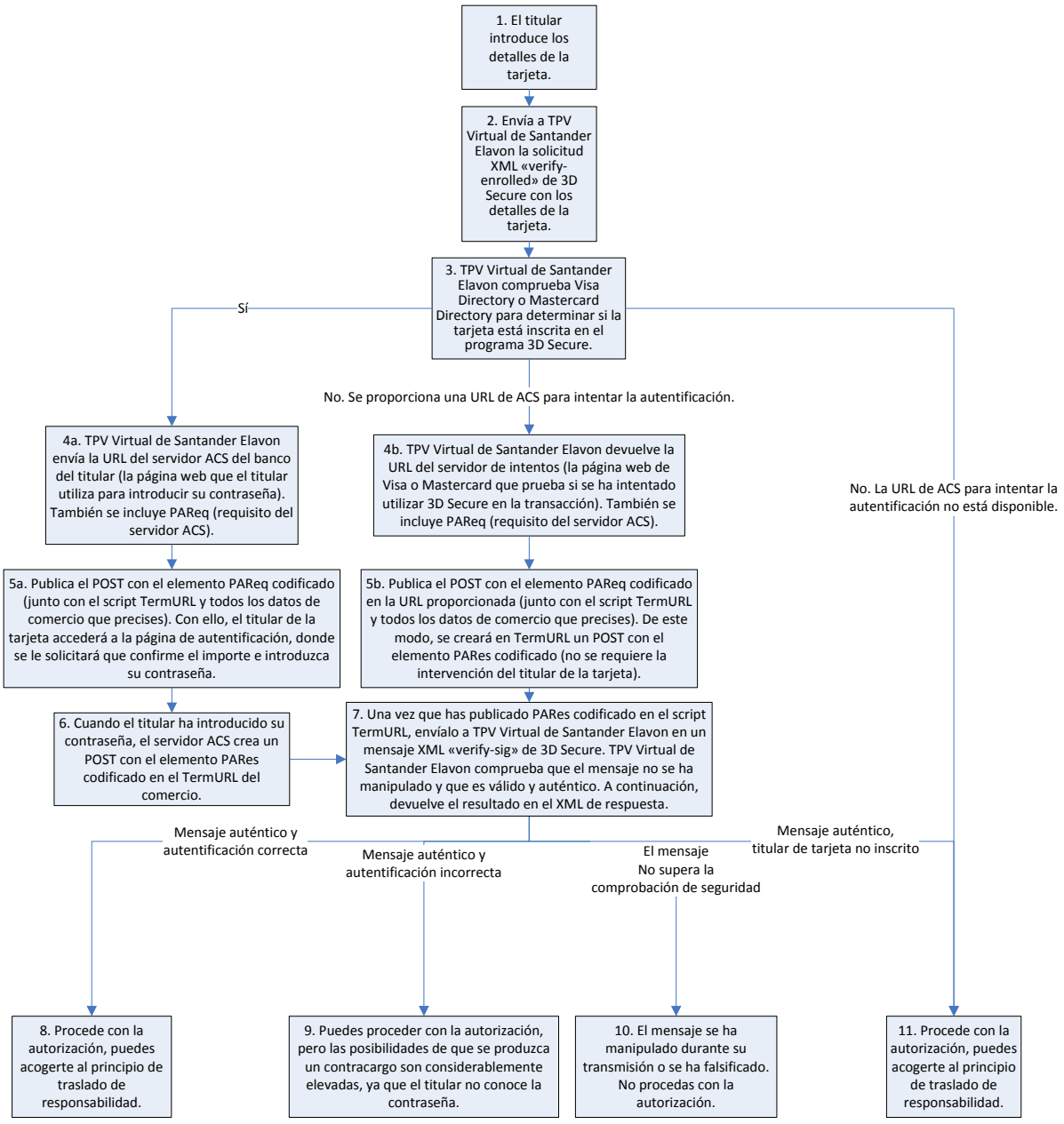
4.1 Escenarios

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 autentificación del titular de la tarjeta, antes de que se produzca la autorización. Tú decides en qué escenarios continuar con la autorización.

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.

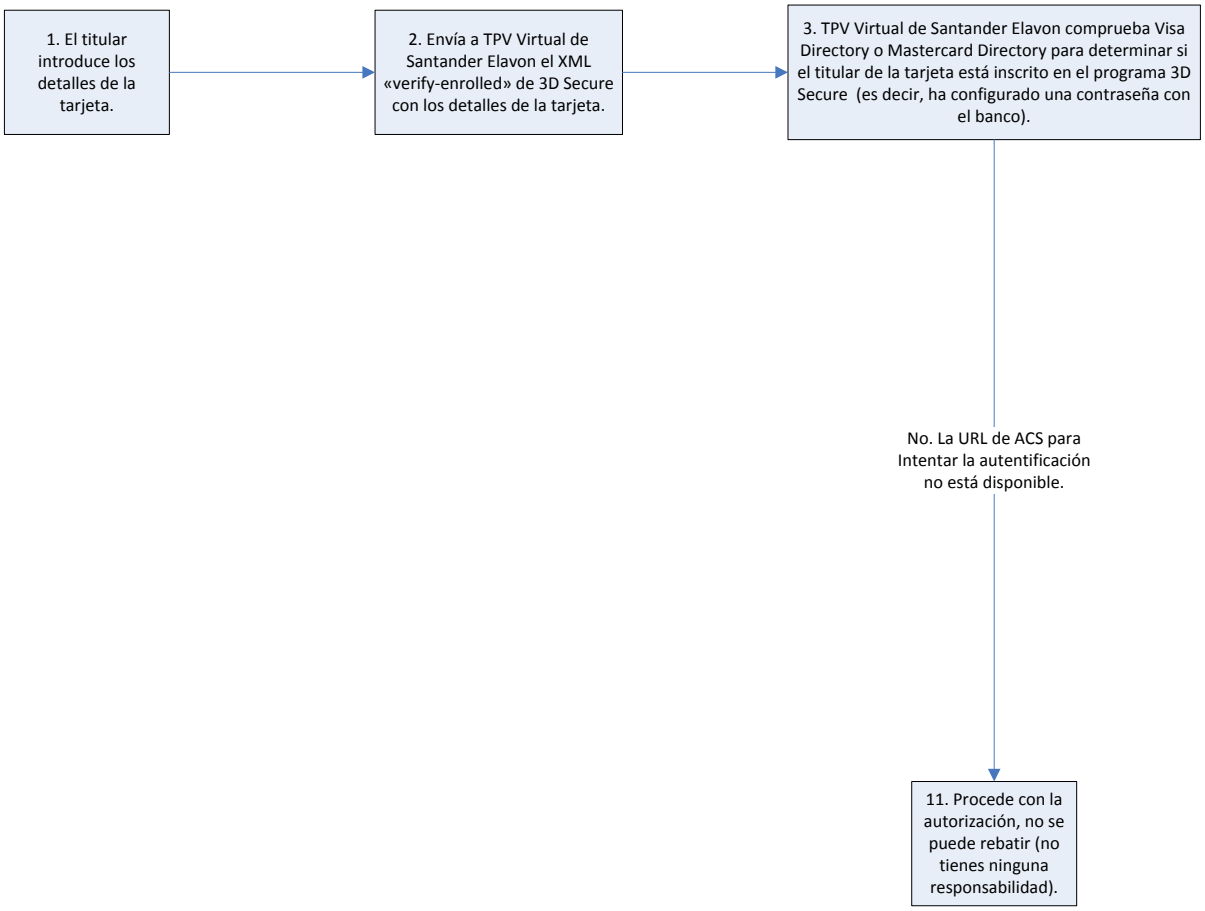
Escenario	Nombre	Descripción	Acción
5	Autentificación correcta.	El titular de la tarjeta está inscrito y ha introducido su contraseña correctamente.	Se puede aplicar el principio de traslado de responsabilidad.
6	Intento de autentificación confirmado	El titular de la tarjeta está inscrito, pero el banco no tiene forma de comprobar la contraseña y, por lo tanto, confirma el intento de autentificación.	Se puede aplicar el principio de traslado de responsabilidad.
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 autentificado.	No se puede aplicar el principio de traslado de responsabilidad.
8	Autentificación 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 autentificación.	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 autentificación.	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.

El siguiente diagrama muestra las combinaciones posibles que pueden surgir durante una transacción de 3D Secure. En las secciones siguientes, se seleccionarán algunos de los escenarios más habituales y se explicarán en detalle.



5 Escenarios

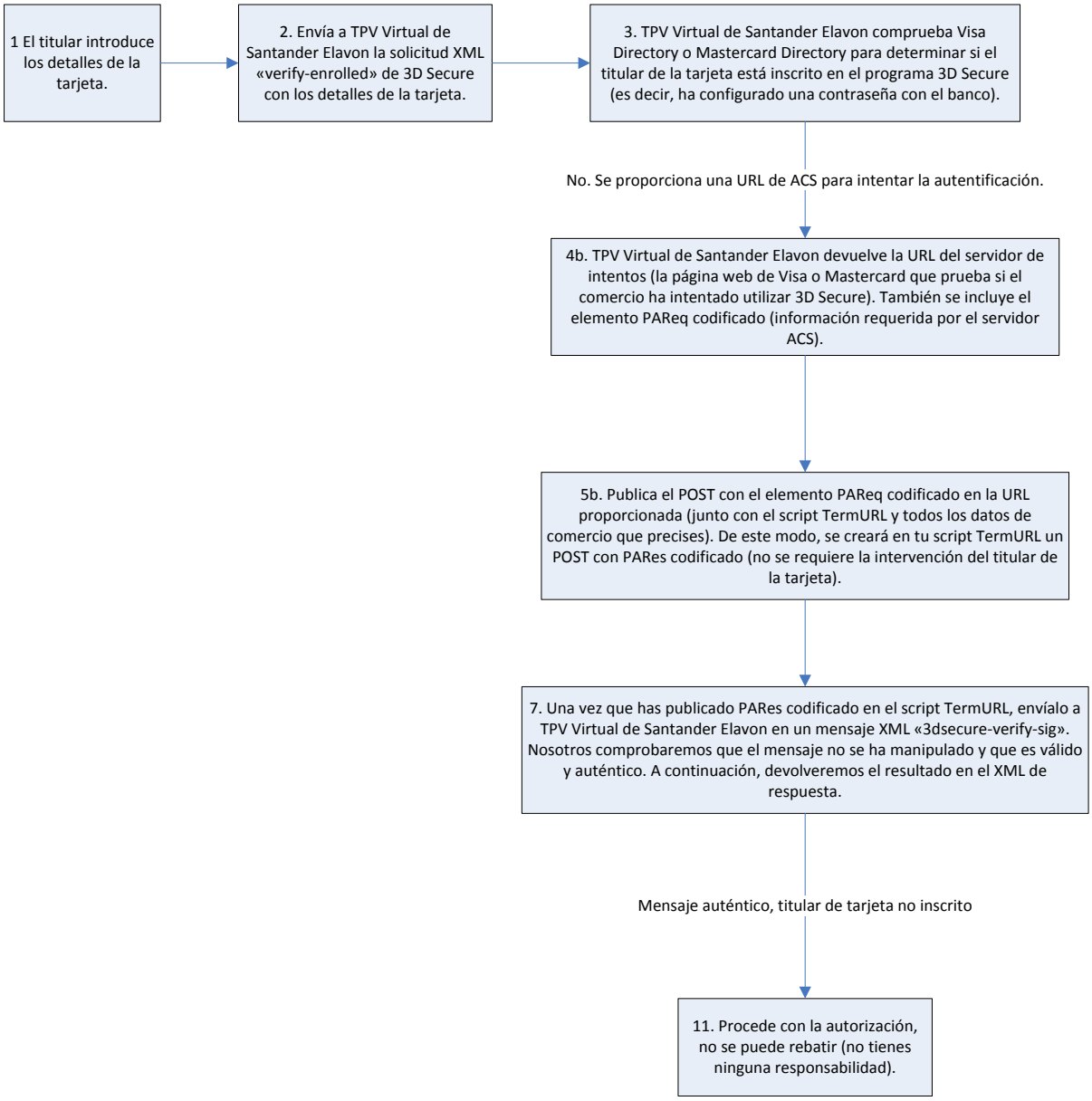
5.1 Escenario 1: Titular de la tarjeta no inscrito



Este es el escenario en el que el banco emisor del titular de la tarjeta no la ha inscrito en 3D Secure. En este escenario, el comercio puede continuar directamente con la autorización una vez que haya recibido la respuesta de inscripción comprobada como *«N».* Debe definirse el valor ECI apropiado en la solicitud de autorización final para valerse del principio de traslado de la responsabilidad (ver a continuación).

Nota: Algunos tipos de tarjetas no están cubiertos por el principio de traslado de responsabilidad en caso de recibir una respuesta de tipo *«No inscrito».* Entre estas se incluyen las tarjetas comerciales y las tarjetas de prepago anónimas. Pregunta a tu banco adquirente para confirmar las normas que se aplican en tu situación.

5.2 Escenario 2: Intento de autentificación confirmado

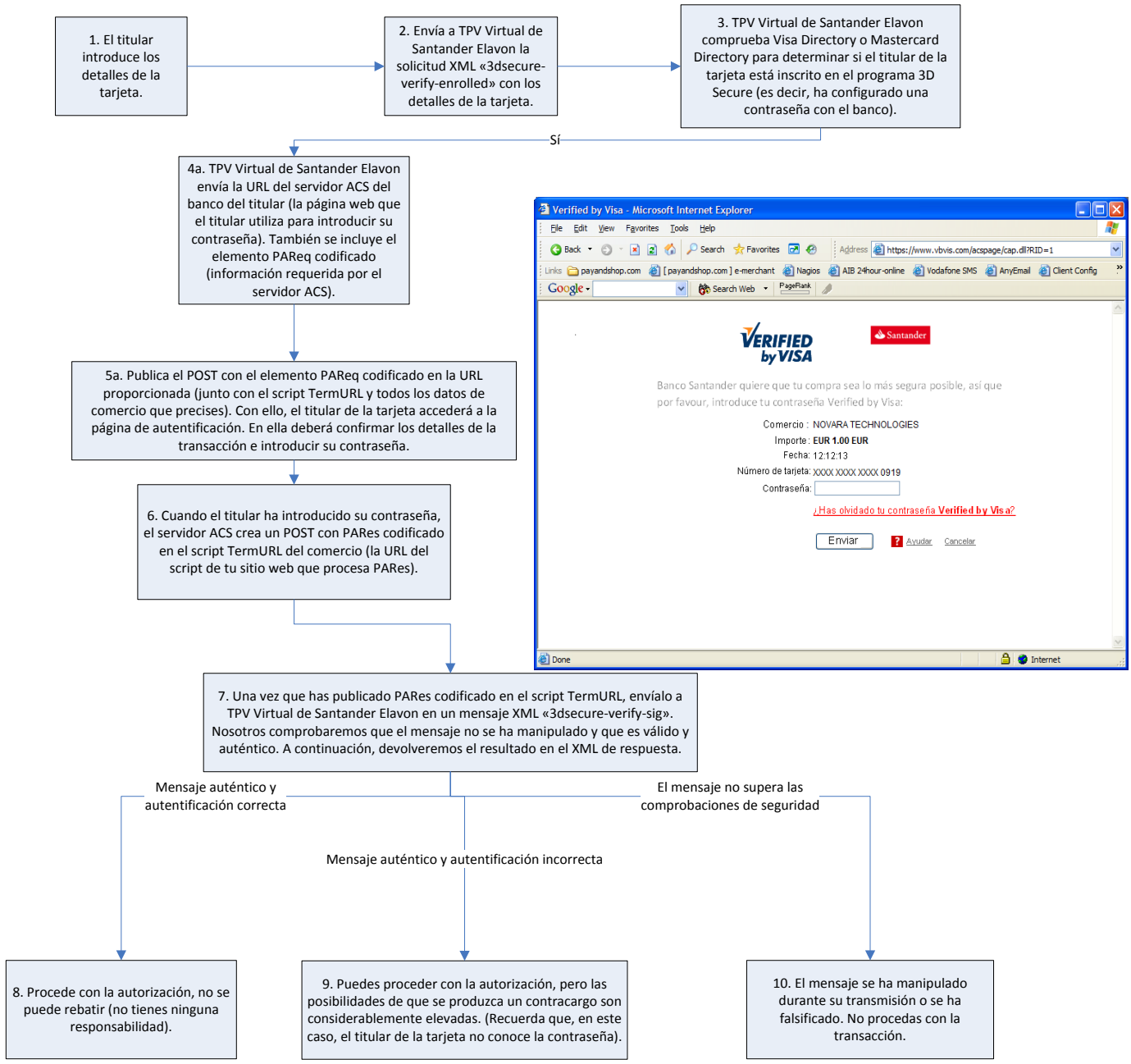


Visa y MasterCard han proporcionado un servidor ACS predeterminado de intentos de autentificación, por el cual, si el banco no participa todavía en el programa 3D Secure, este proporcionará un servidor con dichas características para su uso por parte del comercio. Este servidor genera un valor CAVV/UCAF que el comercio empleará para demostrar el intento de uso del sistema 3D Secure.

En este escenario, se envían automáticamente varios formularios con campos ocultos mediante JavaScript (para ello, puedes utilizar *«document.form.submit();»*) y se genera el

valor CAVV/UCAF que debe enviarse a TPV Virtual de Santander Elavon en el mensaje XML *3ds-verifysig*.

5.3 Escenario 3: Titular de la tarjeta inscrito



En este escenario, el titular de la tarjeta se ha inscrito con el banco emisor. La respuesta al mensaje *3ds-verifyenrolled* contendrá la URL del ACS del banco emisor. Se trata de una

página webcon la marca del banco emisor en la que se pide al titular de la tarjeta que verifique que los detalles de la transacción mostrados son correctos y que introduzca su contraseña. Más arriba se muestra un ejemplo. Una vez que el titular de la tarjeta ha verificado la transacción, se devuelve un formulario oculto al sitio web del comercio con valores **PARes** codificados que, a su vez, deberá enviarse a TPV Virtual de Santander Elavon en el mensaje XML de tipo *3ds-verifysig*.

6 Integración de 3D Secure

La secuencia de sucesos que se debe seguir es la siguiente:

1. El titular introduce los detalles de su tarjeta.
2. Según cuál sea el tipo de tarjeta:
    a. Visa/MasterCard. Continúa en el paso **3**.
3. Envía una solicitud *3ds-verifyenrolled* a TPV Virtual de Santander Elavon.
4. En función de cuál sea la respuesta, lleva a cabo una de las acciones siguientes:
    a. Si el código de respuesta es *«00»* y la etiqueta de inscripción es *«Y»*, quiere decir que también se devolverá una URL. Redirige al titular de la tarjeta a esta URL mediante el formulario oculto.
    b. Si el código de respuesta es *«110»* y la etiqueta de inscripción es *«N»*, quiere decir que el titular de la tarjeta no está inscrito. Continúa en el paso **8a**.
    c. Si la etiqueta de inscripción es *«U»*, quiere decir que el estado de inscripción no se pudo verificar. Continúa en el paso **8c**.
    d. Si el código de respuesta es *«220»*, quiere decir que puede que el servidor del directorio de esquemas de tarjetas no esté disponible. Puedes continuar con la autorización, pero no podrás valerte del principio de traslado de responsabilidad. Continúa en el paso **8c**.
5. El titular de la tarjeta introducirá su contraseña en el sitio web del banco y se le redirigirá de nuevo al sitio web del comercio mediante un formulario oculto que transmita los valores.
6. Toma estos valores devueltos del emisor y crea una solicitud *3ds-verifysig*. Envíala a TPV Virtual de Santander Elavon.
7. En función de cuál sea el resultado, lleva a cabo una de las acciones siguientes:
    a. Si el resultado es *«00»*, quiere decir que el mensaje no se ha manipulado. Continúa:
        i. Si el estado es *«Y»*, quiere decir que el titular de la tarjeta ha introducido su contraseña correctamente. Se trata de una transacción **completa** de 3D Secure. Continúa en el paso **8b**.

ii. Si el estado es *«N»*, quiere decir que el titular de la tarjeta ha introducido una contraseña equivocada. **No puedes valerte del principio** de traslado de responsabilidad, por lo que es preferible que no continúes con la autorización.

iii. Si el estado es *«U»*, puede que el banco emisor haya tenido problemas con sus sistemas en ese momento y no haya podido comprobar la contraseña. Puedes continuar con la transacción (continúa en el paso **8c**), pero **no puedes valerte del principio** de traslado de responsabilidad.

iv. Si el estado es *«A»*, el banco emisor confirma el intento de autentificación llevado a cabo por el comercio y acepta el principio de traslado de responsabilidad. Continúa en el paso **8a**.

b. Si el resultado es *«110»*, quiere decir que las firmas digitales no coinciden con el mensaje y es probable que el mensaje se haya manipulado. **No puedes valerte del principio** de traslado de responsabilidad, por lo que es preferible que no continúes con la autorización.

8. En este momento, puedes enviar el mensaje de autorización de la tarjeta de crédito real a TPV Virtual de Santander Elavon. En función de los resultados anteriores, lleva a cabo una de estas acciones:

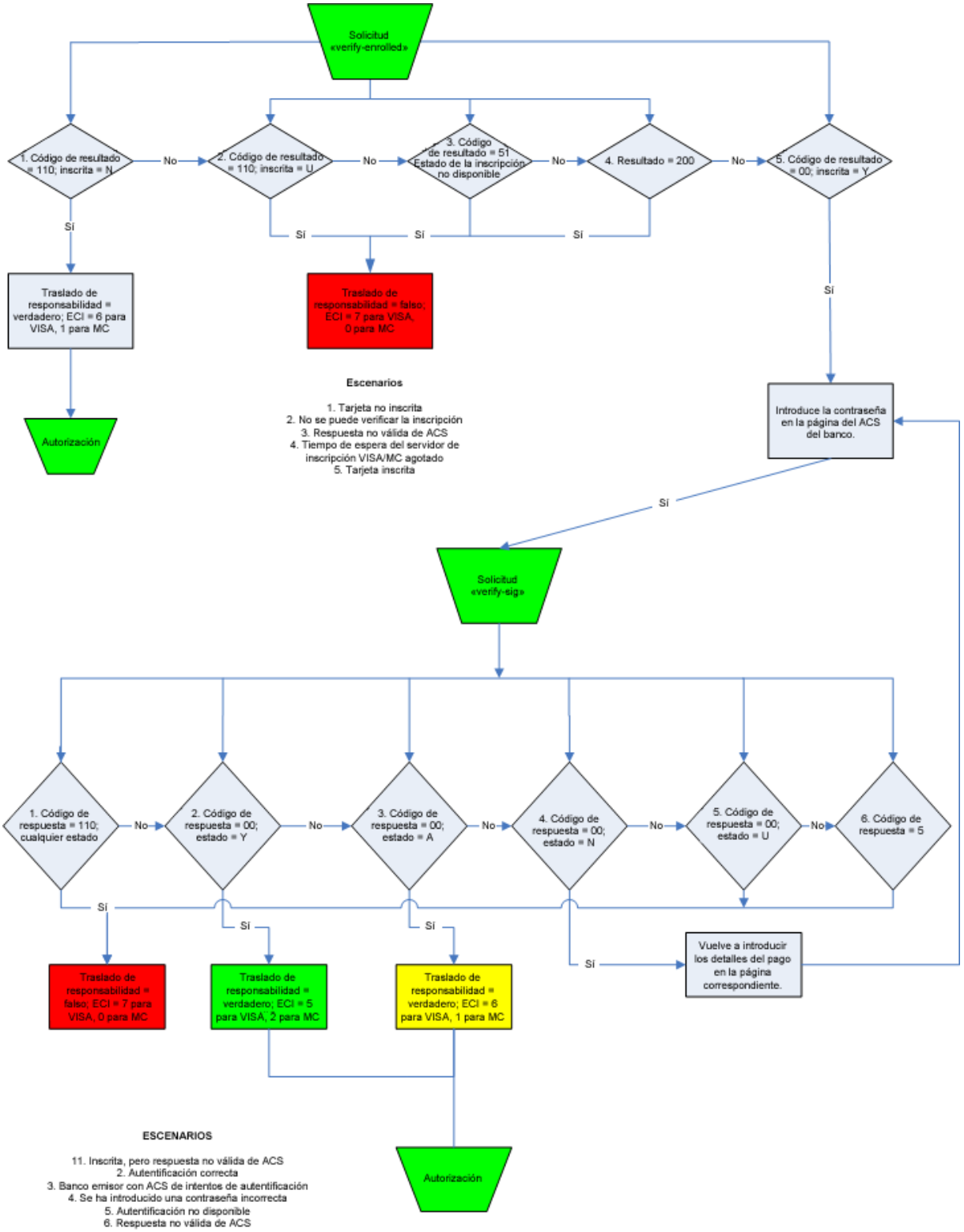
a. Envía un mensaje de autorización normal de TPV Virtual de Santander Elavon (define el campo ECI en 6 o 1). El comercio **no es** responsable de las devoluciones por contracargo.

b. Envía un mensaje de autorización normal de TPV Virtual de Santander Elavon (define el campo ECI en 5 o 2). El comercio **no es** responsable de las devoluciones por contracargo.

c. Envía un mensaje de autorización normal de TPV Virtual de Santander Elavon (define el campo ECI en 7 o 0). El comercio *será* responsable de las devoluciones por contracargo.

La siguiente tabla muestra los escenarios correspondientes a los códigos de resultado y respuesta del diagrama.

Código de resultado 1	Tarjeta no inscrita
Código de resultado 2	No se puede comprobar la inscripción
Código de resultado 3	Respuesta no válida del servidor ACS
Código de resultado 4	Se ha agotado el tiempo de espera del servidor de inscripción de Visa/MC
Código de resultado 5	Tarjeta inscrita
Código de respuesta 1	Inscrito pero respuesta no válida de ACS
Código de respuesta 2	Autentificación correcta
Código de respuesta 3	Banco emisor con ACS de intentos de autentificación
Código de respuesta 4	Contraseña incorrecta
Código de respuesta 5	Autentificación no disponible
Código de respuesta 6	Respuesta no válida del servidor ACS



Escenarios de códigos de respuesta

7 Envío de solicitudes XML

Las solicitudes XML de 3D Secure deben enviarse a la siguiente URL:
https://api.prueba.santanderelavontpvvirtual.es/3dsecure

Las solicitudes XML de autorización normales deben enviarse a la siguiente URL:
https://api.prueba.santanderelavontpvvirtual.es/remote

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.

7.1 Verificación de inscripción: Solicitud 3ds-verifyenrolled

La solicitud *3ds-verifyenrolled* es muy similar a la solicitud estándar *auth*. Una vez que el titular ha introducido la información de su tarjeta en el sitio web del comercio, solo hay que enviar el siguiente fragmento de XML a TPV Virtual de Santander Elavon.

Las siguientes secciones proporcionan la información necesaria para la solicitud 3ds-verifyenrolled:

- Ejemplo
- Sintaxis XML
- Sintaxis de valor hash

```
<request  timestamp="20100625172305" type="3ds-verifyenrolled">
    <merchantid>tuiddecliente</merchantid>
    <account/>
    <orderid>idpedido</orderid>
    <amount currency="EUR">2499</amount>
    <card>
        <number>4012001037141112</number>
        <expdate>0415</expdate>
        <type>visa</type>
        <chname>Juan Pérez Gómez </chname>
    </card>
    <sha1hash>c914a520f88743e40d0620e1b5328c4eebb33725</sha1hash>
</request>
```

Nota: Debe utilizarse el mismo ID de pedido para las solicitudes *3ds-verifyenrolled, 3ds-verifysig* y *auth*.

7.2 Sintaxis XML

La siguiente tabla ofrece la información indicada a continuación para cada campo o elemento XML:

- La sintaxis para el elemento o campo
- Una indicación sobre si el elemento o campo es obligatorio (M), opcional (O) o condicional (C) en función de otro campo
- Una descripción

Elemento/Campo	M/O/C	Descripción
<request timestamp="**20100625172305**" type="**3ds-verifyenrolled**">	**M**	
<merchantid>**tuiddecliente**</merchantid>	**M**	El ID de cliente que asignó TPV Virtual de Santander Elavon.
<account/>	**M**	La cuenta que se va a utilizar. Si aparece en blanco, se programa con la cuenta predeterminada.
<orderid>**idpedido**</orderid>	**M**	Un ID único para identificar esta transacción.
<amount currency="**EUR**">**2499**</amount>	**M**	El importe y la divisa de la transacción.
<card>	**M**	Los detalles de la tarjeta.
<number>**4012001037141112**</number>	**M**	El número de la tarjeta.
<expdate>**0415**</expdate>	**M**	La fecha de caducidad.
<type>**visa**</type>	**M**	El tipo de tarjeta.
<chname>**Juan Pérez Gómez**</chname>	**M**	El nombre del titular de la tarjeta.
</card>		
<sha1hash>**c914a520….328c4eebb33725**</sha1hash>	**M**	Hash SHA1 de los elementos en el XML como se indica en la *TPV*

		Virtual Santander Elavon: Guía de desarrollador-Remote.
</request>	**M**	

7.3 Sintaxis de valor hash

La siguiente tabla muestra la sintaxis de valor hash para la solicitud 3ds-verifyenrolled:

Nota: Consulta la *TPV Virtual Santander Elavon: Guía de desarrollador-Remote* para obtener detalles sobre cómo crear el hash.

Formato	timestamp.merchantid.orderid.amount.currency.cardnumber
Ejemplo	20100625172305.tuiddecliente.idpedido.2499.EUR.4012001037141112

7.4 Respuesta a la verificación de inscripción

Las siguientes secciones proporcionan información sobre la respuesta a la verificación de inscripción:

- Respuesta
- Sintaxis XML
- Sintaxis de valor hash

```
<response timestamp="20030625171810">
   <merchantid>tuiddecliente</merchantid>
   <account>cuenta</account>
   <orderid>idpedido</orderid>
   <authcode></authcode>
   <result>00</result>
   <message>Inscrito</message>
   <pasref></pasref>
   <timetaken>3</timetaken>
   <authtimetaken>0</authtimetaken>
   <pareq>eJxVUttygkAM/ZUdnitZFlBw4na02tE6bR0vD+0bLlHpFFDASv++u6i1
      zVNycju54H2dfrIvKsokz3qWY3OLUabyOMm2PWu1fGwF1r3E5a4gGi5lH
      QuS+ExlGW2JJXHPCjcuVyLYbIRQnrf2o3VMEY+57q05oIsibP+nA4SL02k
      7mELhKupqxVqF2WVxEgdBpMX6dwE4YJhSsVkKB3RH9ypGFyvNXpkrLW
      982HcancQzn7MopSkO2RnqmxJZYXQgKjyY1YV39Lt6O5XA4/Fp9xV1b4L
```

```
        cDqdbDcum8xKJ9oqTxFMAMKN5OxotFIXrJNY1otpMH0qYQwP43w08Pn0
        /W1Ql6+nj+cegonAOKpICs5d3hY+czpdJ+g6HKHBUoNEyk8OwzZaDXXE
        58R3JtG/as7DBH+IqhZFvpS3zLsBHqeq4VU7/OMTA7Cr45wo/0wNptWlV
        4Xb8Thftv3A30xs+7GYaokej3c415TxhgIJhUu54TLF2jt33f8ADVyvnA=</pareq>
    <url>http://www.acs.com</url>
    <enrolled>Y</enrolled>
    <xid>7ba3b1e6e6b542489b73243aac050777</xid>
    <sha1hash>9eda1f99191d4e994627ddf38550b9f47981f614</sha1hash>
</response>
```

7.5 Sintaxis XML

La siguiente tabla ofrece la información indicada a continuación para cada campo o elemento XML:

- La sintaxis para el elemento o campo
- Una indicación sobre si el elemento o campo es obligatorio (M), opcional (O) o
- condicional (C) en función de otro campo
- Una descripción

Nota: El elemento <*pareq*> contiene el mensaje PAReq que requiere el servidor ACS. Se ha preformateado y codificado, y está listo para su envío al servidor ACS como campo oculto en un formulario.

Elemento/Campo	M/O/C	Descripción
<result>**00**</result>	**M**	El resultado de la transacción. Consulta a continuación más valores posibles.
<message>**Inscrito**</message>	**M**	Texto de respuesta legible.
<pareq>**eJxVUttygkAM/…TLF2jt33f8ADVyvnA=** </pareq>	**M**	El elemento PAReq precodificado que debes enviar a la URL de ACS del banco emisor. Para hacerlo, consulta a continuación el código de muestra.
<url>**http://www.acs.com**</url>	**M**	La URL de ACS del banco emisor.
<enrolled>**Y**</enrolled>	**M**	Respuesta de inscripción no válida de ACS.

<xid>**7ba3b1e6e6b542489b73243aac0 50777**</xid>	**M**	XID de ACS.

La siguiente tabla muestra la sintaxis de valor hash para la solicitud 3ds-verifyenrolled:

Nota: Consulta la guía *TPV Virtual Santander Elavon: Guía de desarrollador-Remote* para obtener detalles sobre cómo crear el hash.

Formato	timestamp.merchantid.orderid.result.message.pasref.authcode
Ejemplo	20030625171810.tuiddecliente.idpedido.00.Inscrito

7.6 Respuesta a la verificación de inscripción: Respuesta para No inscrito

Las siguientes secciones proporcionan información sobre la respuesta a la verificación de inscripción:

- Respuesta
- Sintaxis XML
- Sintaxis de valor hash

```
<response timestamp="20030625171810">
   <merchantid>tuiddecliente</merchantid>
   <account>cuenta</account>
   <orderid>idpedido</orderid>
   <authcode></authcode>
   <result>110</result>
   <message>No inscrito</message>
   <pasref></pasref>
   <timetaken>3</timetaken>
   <authtimetaken>0</authtimetaken>
   <pareq>eJxVUttygkAM/ZUdnitZFlBw4na02tE6bR0vD+0bLlHpFFDASv++u6i1
         zVNycju54H2dfrIvKsokz3qWY3OLUabyOMm2PWu1fGwF1r3E5a4gGi5lH
      QuS+ExlGW2JJXHPCjcuVyLYbIRQnrf2o3VMEY+57q05oIsibP+nA4SL02k
      7mELhKupqxVqF2WVxEgdBpMX6dwE4YJhSsVkKB3RH9ypGFyvNXpkrLW
      982HcancQzn7MopSkO2RnqmxJZYXQgKjyY1YV39Lt6O5XA4/Fp9xV1b4L
      cDqdbDcum8xKJ9oqTxFMAMKN5OxotFlXrJNY1otpMH0qYQwP43w08Pn0
      /W1Ql6+nj+cegonAOKpICs5d3hY+czpdJ+g6HKHBUoNEyk8OwzZaDXXE
      58R3JtG/as7DBH+IqhZFvpS3zLsBHqeq4VU7/OMTA7Cr45wo/0wNptWlV</pareq>
```

```
        4Xb8Thftv3A30xs+7GYaokej3c415TxhgIJhUu54TLF2jt33f8ADVyvnA=</pareq>
    <url></url>
    <enrolled>N</enrolled>
    <xid>e9dafe706f7142469c45d4877aaf5984</xid>
    <sha1hash>9eda1f99191d4e994627ddf38550b9f47981f614</sha1hash>
</response>
```

7.7 Sintaxis XML

La siguiente tabla ofrece la información indicada a continuación para cada campo o elemento XML:

- La sintaxis para el elemento o campo
- Una indicación sobre si el elemento o campo es obligatorio (M), opcional (O) o condicional (C) en función de otro campo
- Una descripción

Elemento/Campo	M/O/C	Descripción
<result>**110**</result>	M	El resultado de la transacción. Consulta a continuación más valores posibles.
<message>**No inscrito**</message>	M	Texto de respuesta legible.
<pareq>**eJxVUttygkAM/…TLF2jt33f8ADVyvnA=** </pareq>	M	El elemento PAReq precodificado que debes enviar a la URL de ACS del banco emisor. Para hacerlo, consulta a continuación el código de muestra.
<url></url>	M	La URL de ACS del banco emisor.
<enrolled>**N**</enrolled>	M	Respuesta de inscripción no válida de ACS.
<xid>**e9dafe706f7142469c45d4877aaf5 984**</xid>	M	XID de ACS.

7.8 Sintaxis de valor hash

La siguiente tabla muestra la sintaxis de valor hash para la solicitud 3ds-verifyenrolled:

Formato	timestamp.merchantid.orderid.result.message.pasref.authcode

Ejemplo	20030625171810.tuiddecliente.idpedido.00.Inscrito.

7.9 Códigos de respuesta para 3ds-verifyenrolled

Los códigos de respuesta siguientes deben devolverse en respuesta a una solicitud *3ds-verifyenrolled*:

00	Inscrito	El titular de la tarjeta está inscrito.
110	No inscrito	El titular de la tarjeta no está inscrito, sin embargo, debe enviar el elemento PAReq codificado al servidor ACS de intentos de autentificación (si estuviera disponible).
220	Tiempo de espera del mensaje agotado	Puede que el servidor del directorio de esquemas de tarjetas no esté disponible. Si se procesa la autorización, no podrá valerse del principio de traslado de responsabilidad.
5xx		Error en sintaxis o formato XML. Corrige el error e inténtalo de nuevo.
521	Solicitud de inscripción enviada para una tarjeta Solo.	El número de tarjeta no es de una tarjeta Switch. Las transacciones de 3D Secure no son compatibles con tarjetas Solo.

Si el código de respuesta a la solicitud 3ds-verifyenrolled es *«110»* y el resultado de inscripción es *«N»*, y no se ha proporcionado una URL para intentar la autentificación, puedes continuar con la autorización añadiendo los siguientes campos adicionales a la solicitud. TPV Virtual de Santander Elavon no ha devuelto ECI ni CAVV en este escenario. El ECI es el único campo de 3D Secure que debe incluirse en la solicitud de autorización.

<eci>**6**</eci> para una transacción de Visa.

<eci>**1**</eci> para una transacción de MasterCard.

7.10 Apertura de la URL de ACS

Hasta hace poco, se proponía que la URL de ACS se abriese en una ventana emergente, pero con la creciente presencia de aplicaciones de eliminación de ventanas emergentes (como la de la barra de herramientas de Google), se ha decidido que la URL simplemente se

abra en la ventana principal. El elemento PAReq especificado en la respuesta debe enviarse a la URL de ACS. A continuación, se ofrece el código de ejemplo correspondiente.

```
<HTML>
<HEAD>
<TITLE>Página de 3D Secure de muestra</TITLE>
<SCRIPT LANGUAGE="Javascript" >
<!--
function OnLoadEvent()  {
document.form.submit();
}
//-->
</SCRIPT>
</HEAD>
<BODY onLoad="OnLoadEvent()">
<FORM NAME="form" ACTION="https://www.acs.com/" METHOD="POST">
<INPUT TYPE="hidden" NAME="PaReq"
VALUE="c7fb83b8ag.....73t4a827t4af8738a">
<INPUT TYPE="hidden" NAME="TermUrl"
VALUE="https://www.mywebsite.com/process.cgi">
<INPUT TYPE="hidden" NAME="MD"
VALUE="fsjdh43493aewrtfdssaSKJ.....sdfk">
<NOSCRIPT><INPUT TYPE="submit"></NOSCRIPT>
</FORM>
</BODY>
</HTML>
```

Este código HTML debe crearse sobre la marcha al recibir la respuesta. Los campos del formulario que deben rellenarse son los siguientes:

PAReq	El elemento PAReq codificado que recibas de TPV Virtual de Santander Elavon.
TermUrl	La URL a la que debe responder el servidor ACS. Esta debe encontrarse en tu sitio web y ser una dirección HTTPS.
MD	Datos del comercio. Cualquier dato que quieras que el servidor ACS te devuelva. Algunos datos útiles son el ID de pedido y los detalles de la tarjeta (así, al recibir una autentificación correcta, puedes enviar el mensaje de autorización). Cualquier información de este campo debe estar cifrada, comprimida y con codificación base64.

7.11 Comprobación de la firma en PARes: Solicitud 3ds-verifysig

Las siguientes secciones proporcionan información sobre la solicitud 3ds-verifysig:

- Ejemplo
- Sintaxis XML
- Sintaxis de valor hash

```
<request timestamp="20100625172325" type="3ds-verifysig">
   <merchantid>tuiddecliente</merchantid>
   <account/>
   <orderid>idpedido</orderid>
   <amount currency="EUR">2499</amount>
   <card>
      <number>4012001037141112</number>
      <expdate>0415</expdate>
      <type>visa</type>
      <chname>Juan Pérez Gómez</chname>
   </card>
   <pares>eJztWFmT4jgS/.....  a/A2OMEv4=</pares>
   <sha1hash>e0817f5ffeca1241c23a52b0eafa5c578ef68356</sha1hash>
</request>
```

7.12 Sintaxis XML

La siguiente tabla ofrece la información indicada a continuación para cada campo o elemento XML:

- La sintaxis para el elemento o campo
- Una indicación sobre si el elemento o campo es obligatorio (M), opcional (O) o condicional (C) en función de otro campo
- Una descripción

La tabla a continuación ofrece una explicación de los campos de 3D Secure.

Elemento/Campo	**M/O/C**	**Descripción**
<pares>**eJztWFmT4jgS/..... a/A2OMEv4=**</pares>	M	El elemento PARes codificado de ACS.

<sha1hash>**e0817f5f…afa5c578ef68356**</sha1hash>	M	Hash SHA1 de los elementos en el XML como se indica en la *TPV Virtual Santander Elavon: Guía de desarrollador-Remote*.

7.13 Sintaxis de valor hash

La siguiente tabla muestra la sintaxis de valor hash para la solicitud 3ds-verifyenrolled:

Formato	timestamp.merchantid.orderid.amount.currency.cardnumber
Ejemplo	20030625172325.tuiddecliente.idpedido.2499.EUR.4012001037141112

7.14 Respuesta a la solicitud 3ds-verifysig

Las siguientes secciones proporcionan información sobre la solicitud 3ds-verifysig:

- Respuesta
- Sintaxis XML
- Sintaxis de valor hash
- Códigos de resultado posibles
- Códigos de estado posibles de 3D Secure

Respuesta

```
<response timestamp="20100625171823">
   <merchantid>tuiddecliente</merchantid>
   <account/>
   <orderid>idpedido</orderid>
   <result>00</result>
   <message>Autentificación correcta</message>
   <threedsecure>
      <status>N</status>
      <eci/>
      <xid/>
      <cavv/>
      <algorithm/>
   </threedsecure>
   <sha1hash>e5a7745da5dc32d234c3f52860132c482107e9ac</sha1hash>
```

```
</response>
```

7.15 Sintaxis XML

La siguiente tabla ofrece la información indicada a continuación para cada campo o elemento XML:

- La sintaxis para el elemento o campo
- Una indicación sobre si el elemento o campo es obligatorio (M), opcional (O) o condicional (C) en función de otro campo
- Una descripción

Elemento/Campo	M/O/C	Descripción
<threedsecure>	M	Los elementos de 3D Secure.
<status>**Y**</status>	M	El resultado de la autentificación necesario para la solicitud de autorización (ver la tabla a continuación).
<eci>**5** </eci>	O	El indicador de comercio electrónico necesario para la solicitud de autorización.
<xid>**crqAeMwkEL9r4POdxpByWJ1/wYg=** </xid>	O	El campo XID necesario para la solicitud de autorización.
<cavv>**AAABASY3QHgwUVdEBTdAAAAAAAA=**</cavv>	O	El valor CAVV o UCAF necesario para la solicitud de autorización.
<algorithm>**1** </algorithm>	O	El algoritmo utilizado.
</threedsecure>	R	

7.16 Sintaxis de valor hash

La siguiente tabla muestra la sintaxis de valor hash para la solicitud 3ds-verifysig:

Formato	timestamp.merchantid.orderid.result.message.pasref.authcode
Ejemplo	20030625171823.tuiddecliente.idpedido.00.Autentificación correcta.

Los códigos de resultado posibles de TPV Virtual de Santander Elavon son los siguientes:

00	La firma se ha validado correctamente en PARes
110	La firma en PARes no se ha validado. Considera esta acción como una autentificación fraudulenta.

Los códigos de estado posibles de 3D Secure son los siguientes:

Y	El titular de la tarjeta se ha autentificado correctamente. Puedes continuar con la autorización y valerte del principio de traslado de responsabilidad.
N	El titular de la tarjeta no se ha autentificado correctamente. Si autorizas esta transacción **serás** responsable de los contracargos.
A	El titular de la tarjeta está inscrito y el banco confirma el intento de autentificación.
U	La autentificación del titular de la tarjeta no está disponible temporalmente. **No** hay principio de traslado de responsabilidad disponible.

Precaución: Los campos ECI, XID y CAVV son necesarios en la solicitud de autorización que se envía a TPV Virtual de Santander Elavon. Estos deben coincidir con el contenido que se devuelva en la respuesta de *verifysig*, ya que, de lo contrario, la autorización fallará.

7.17 Cambios en el mensaje de solicitud de autorización.

En el caso de una tarjeta no inscrita (la solicitud 3ds-verifyenrolled obtiene la respuesta *«110»* y el resultado de inscripción *«N»*), la etiqueta ECI debe definirse manualmente en 1 (MC o 6 (Visa). Para este escenario, el ECI es el único campo de 3D Secure que debe incluirse en la solicitud de autorización.

En el caso de una tarjeta registrada, los campos CAVV, XID y ECI deben ser idénticos en la solicitud de autorización a los que se devuelven en la respuesta verifysig. Si alguno de estos valores no coincide con los valores devueltos en la respuesta verifysig, la transacción fallará y aparecerá el mensaje de error que se muestra a continuación.

Mensaje de error

```
<response timestamp="20100322231944">
<result>508</ result>
< message>Los datos de transacción de 3D Secure no coinciden con los datos en la base de datos</
message>
</response>
```

Precaución: Debes asegurarte de que se cumplen los cambios indicados en esta sección para poder valerte del principio de traslado de responsabilidad.

Las siguientes secciones proporcionan información sobre el mensaje de solicitud de autorización y un ejemplo en el que la tarjeta está totalmente inscrita:

- Mensaje de error
- Ejemplo
- Sintaxis XML
- Sintaxis de valor hash
- Indicadores de comercio electrónico
- Códigos de respuesta para las autorizaciones de 3D Secure

A continuación, se muestra el aspecto que debe tener el XML de la solicitud de autorización.

Ejemplo:

```
<request timestamp="20100625172325" type="auth">
    <merchantid>tuiddecliente</merchantid>
    <account/>
    <orderid>idpedido</orderid>
    <amount currency="EUR">2499</amount>
    <card>
        <number>4012001037141112</number>
        <expdate>0415</expdate>
        <type>visa</type>
        <chname>Juan Pérez Gómez </chname>
        <cvn>
        <number>453</number>
        <presind>1</presind>
        </cvn>
    </card>
    <autosettle flag="1" />
    <mpi>
        <cavv>AAACAWQWaRKIFwQlVBZpAAAAAAA=</cavv>
```

```
        <xid>I2ncCuvKNtCtRY3OoC/ztHS8ZvI=</xid>
        <eci>5</eci>
    </mpi>

    <sha1hash>e0817f5ffeca1241c23a52b0eafa5c578ef68356</sha1hash>
    <comments>
        <commentid="1" />
        <commentid="2" />
    </comments>
    <autosettle flag="1"/>
</request>
```

7.18 Sintaxis XML

La siguiente tabla ofrece la información indicada a continuación para cada campo o elemento XML:

- La sintaxis para el elemento o campo
- Una descripción

Elemento/Campo	Descripción
<mpi>	El elemento que contiene la información de 3D Secure.
<cavv>**AAACAWQWaRKIFwQlVBZpAAAAAAA=**</cavv>	El valor CAVV/UCAF, si lo hubiera.
<xid>**I2ncCuvKNtCtRY3OoC/ztHS8ZvI=**</xid>	El valor XID, si lo hubiera.
<eci>**5**</eci>	El indicador de comercio electrónico. Ver a continuación.
</mpi>	

7.19 Sintaxis de valor hash

La siguiente tabla muestra la sintaxis de valor hash para la solicitud de autorización:

Formato	timestamp.merchantid.orderid.amount.currency.cardnumber

Ejemplo	20030625172325.tuiddecliente.idpedido.2499.EUR.4012001037141112

Visa	MC	Indicador de comercio electrónico (ECI)
5	2	3D Secure completo: Titular de la tarjeta inscrito.
6	1	3D Secure de comercio: Titular de la tarjeta no inscrito o se utilizó el servidor ACS de intentos de autentificación.
7	0	Transacción no perteneciente a 3D Secure. Por ejemplo, un reembolso o una transacción de 3D Secure que se denegó en mitad del proceso. El comercio debe decidir si continuar con ella o no. Deja de aplicarse el principio de traslado de responsabilidad. Sería mejor ofrecer al cliente la posibilidad de intentarlo de nuevo ahora o más tarde.

7.20 Códigos de respuesta para las autorizaciones de 3D Secure

Los siguientes códigos de respuesta pueden devolverse como respuesta a una solicitud de autorización de 3D Secure, junto con los códigos de respuesta indicados en la guía *TPV Virtual Santander Elavon: Guía de desarrollador-Remote*.

508	El comercio tiene el servicio 3D Secure activado, pero está desactivado para este tipo de tarjeta.	Este mensaje de error aparecerá si se envían los datos de 3D Secure (ECI = 5, 6, 1 o 2) en el mensaje de autorización, pero el tipo de tarjeta se ha desactivado para 3D Secure en la cuenta de TPV Virtual de Santander Elavon del comercio.

7.21 XML de respuesta de autorización

A continuación, se muestra el XML de respuesta para 3D Secure:

```
<response timestamp="20100323112029">
 <merchantid>tuiddecliente</merchantid>
 <account>NOMBRECUENTA</account>
 <orderid>idpedido</orderid>
 <authcode>601146</authcode>
 <result>00</result>
 <cvnresult>I</cvnresult>
 <avspostcoderesponse>U</avspostcoderesponse>
 <avsaddressresponse>U</avsaddressresponse>
 <batchid>157994</batchid>
 <message>CÓDIGO AUTORIZACIÓN 601546</message>
 <pasref>11431128282456</pasref>
 <timetaken>1</timetaken>
 <authtimetaken>1</authtimetaken>
<cardissuer>
 <bank>SANTANDERbank>
 <country>España</country>
 <countrycode>ES</countrycode>
 <region>EUR</region>
 </cardissuer>
 <sha1hash>e3ee934ee44dc356726544d1ea9acc2329945346</sha1hash>
 </response>
```

7.22 Sintaxis de valor hash

La siguiente tabla muestra la sintaxis de valor hash para la solicitud de autorización:

Formato	timestamp.merchantid.orderid.result.message.pasref.authcode
Ejemplo	20100323112029.tuiddecliente.idpedido-de-solicitud.00.CÓDIGO DE AUTORIZACIÓN 601546.11431128282456.601146

8 Anexo A: Código de muestra

8.1 Perl

Este código permite codificar el campo MD.

```
use Compress::Zlib;
use MIME::Base64;
use Crypt::CBC;
my $cipher = Crypt::CBC->new({'key' => 'my secret key',
'cipher' => 'Blowfish'});
$data= "ORDERID=$orderid&CARDNUMBER=4242424242424242&CARDNAME=Jo
hn%20Doe";
my $ciphertext = $cipher->encrypt($data);
my $deflated = compress($ciphertext);
my $MD = encode_base64($deflated);
$MD =~ s/\s*$//s;
$MD =~ s/[\s\n]//g;

print "<input type="hidden" name="MD" value="$MD">\n";
```

Este código permite descodificar el campo MD en la respuesta de ACS.

```
use Compress::Zlib;
use MIME::Base64;
use Crypt::CBC;
# Obtener datos de formulario de la forma habitual
my $MD = $formdata{MD};
my $cipher = Crypt::CBC->new({'key' => 'my secret key',
'cipher' => 'Blowfish'});
$MD = decode_base64($MD)
$MD = uncompress($MD)
$MD = $cipher->decrypt($MD)
my @mdlist = split(/&/,  $MD);
my %MerchantData;
foreach my $item (@mdlist) {
```

```
my ($field, $value) = split(/=/, $item);
$MerchantData{$field} = $value;
$MerchantData{$field} =~ s/\+/ /g;
$MerchantData{$field} =~ s/%([0-9A-F][0-9A-F])/
sprintf("%c",hex($1))/eg;
}

$cardnumber = $MerchantData{CARDNUMBER};
```

8.2 Java

El código de muestra siguiente puede utilizarse para codificar y descodificar datos.

```
import javax.crypto.*;
import javax.crypto.spec.*;
import java.security.*;
import java.util.zip.*;
public class testblowfish  {
public static void main(String[] args) {
testblowfish obj = new testblowfish();
obj.cipher();
System.exit(0);
}
void cipher() {
// Crear el vector de inicialización: utilizado para el cifrado
byte[] bIV = { (byte)0x94, (byte)0x4b, (byte)0x4a, (byte)0x68,
(byte)0x23, (byte)0x28, (byte)0x79, (byte)0x71 };
// Configurar la clave para cifrado...  Esta es una clave de 448 bits que
// es el máximo permitido por Blowfish.
byte[] bKey = { (byte)0xb9, (byte)0x1c, (byte)0xb8, (byte)0x24,
(byte)0xf7, (byte)0x3b, (byte)0x9b, (byte)0x33, (byte)0x28,
(byte)0xf4, (byte)0x79, (byte)0xe7, (byte)0xf1, (byte)0x64,
(byte)0x27, (byte)0xb0, (byte)0xbd, (byte)0xc0, (byte)0x40,
(byte)0x8b, (byte)0x9b, (byte)0x37, (byte)0xa0, (byte)0x3a,
(byte)0xc6, (byte)0x08, (byte)0x78, (byte)0x66, (byte)0x68,
(byte)0xda, (byte)0x21, (byte)0xec, (byte)0xc1, (byte)0xde,
(byte)0x73, (byte)0x2b, (byte)0x68, (byte)0xb8, (byte)0x91,
(byte)0x91, (byte)0xbe, (byte)0xbe, (byte)0x8c, (byte)0x38,
(byte)0x41, (byte)0xb1, (byte)0x48, (byte)0xca, (byte)0xe9,
```

```
(byte)0xef, (byte)0x2f, (byte)0x92, (byte)0x3d, (byte)0x8d,
(byte)0xc5, (byte)0xda };


int i;
 String s;
byte[] bx;
byte[] dx;
java.security.Key k;
java.security.Provider p;
javax.crypto.spec.IvParameterSpec iv;
```

Guía del desarrollador de Remote de 3D Secure

Información privada y confidencial de TPV Virtual de Santander Elavon 40

```
 Cipher c;
 String strHexCipherText = "";
 SecretKeySpec sks;
 SecretKey sk;
 // Serializar la información que quieres pasar a través del servidor ACS
de algún modo.
 String toEncrypt =
 "ORDERID=834823883&CARDNUMBER=4242424242424242&CARDNAME=John Doe";
try {
 // Blowfish/CBC
iv = new  javax.crypto.spec.IvParameterSpec(bIV);
sks = new SecretKeySpec(bKey, "Blowfish");
 //sk =
 (SecretKeyFactory.getInstance("Blowfish")).generateSecret(sks);
 // Cifrar la información serializada.  Es el campo MD.
 c = Cipher.getInstance("Blowfish/CBC/PKCS5Padding");
c.init(Cipher.ENCRYPT_MODE, sks, iv);
bx = c.doFinal(toEncrypt.getBytes());
 // Imprimir la versión codificada con Base64 de la cadena cifrada.
   String base64Encoded = new sun.misc.BASE64Encoder().encode(bx);
System.out.println(base64Encoded);
 //  ----------------------------------------------------------------
 // Recuperar la información serializada del campo MD cuando el servidor ACS
```

te devuelva una respuesta.

```
c = Cipher.getInstance("Blowfish/CBC/PKCS5Padding");
c.init(Cipher.DECRYPT_MODE, sks, iv);
dx =
c.doFinal(newsun.misc.BASE64Decoder().decodeBuffer(base64Encoded));
 // Imprimir la cadena descifrada de texto sin formato.
System.out.println(new String(dx));
 } catch(Exception e) {
e.printStackTrace();
 }
 }
}
```

SANTANDER ELAVON MERCHANT SERVICES

Santander Elavon Merchant Services
Avda. de Bruselas 36, Planta 3º
28108 Alcobendas | Madrid