

Api MPI Plugin Verified By Visa

Visa Argentina

OnLine - Desarrollo de sistemas

Visa Argentina

versión 1.0.17, 2007-02-13

Resumen

Especificación para la utilización del VisaArgentina MPI para el Sistema de Autenticación Verified By Visa

1. Objetivos

- Ofrecer una API para que los sitios web de los establecimientos adheridos al Programa Verified by Visa puedan comunicarse con el "Visa MPI" sobre el protocolo 3DSecure y de este modo utilizar esta operatoria de transacciones de eCommerce seguras.
- Sencillez de utilización y adaptabilidad a diferentes plataformas.
- Fácil implementación sobre los sistemas de los establecimientos.

2. Descripción General

Actualmente cualquier sitio de eCommerce, obtiene los datos de la tarjeta, y con dicha información realiza una transacción de compra online o autorización, sobre ISO 8583, a través de su sistema propio. Para reforzar la seguridad en este esquema Visa impulsa el programa de autenticación Verified by Visa basado en el protocolo 3DSecure. Este programa permite, previamente a la realización de la transacción de autorización, una autenticación en línea del tarjetahabiente. Esta autenticación genera un código interno de validación que garantiza en un alto grado la identidad del mismo, a través de una clave personal segura. Para incorporarse en Verified by Visa, el site de eCommerce deberá implementar el protocolo ApiMPI, realizando una modificación sobre su sistema transaccional y autorizador para permitir la comunicación con los componentes de Verified By Visa. Estas modificaciones permitirán al sitio de comercio electrónico realizar una validación de autenticación en línea sobre un tarjetahabiente que quiera realizar una compra online y que este enrolado dentro

del programa Verified by Visa. (Nota: Tener en cuenta que la transacción de VbV solo resuelve la autenticación del tarjetahabiente, la gestión de la autorización sufre una pequeña modificación dentro de la variabilidad estándar.)

3. Implementación

La implementación se realiza mediante llamadas XML por POST HTTP sobre SSL bajo el estándar XML-RPC [www.xmlrpc.com] De esta forma todos los sitios implementados en PHP, JSP, ASP o cualquier otra plataforma podrán conectarse a VbV.

Existen 4 puntos a modificar en el site:

1. Al momento que el usuario completa los datos de su tarjeta y presiona el botón pagar, el site debe realizar una llamada XML-RPC a una dirección de Visa Argentina de la cual obtendrá un parámetro identificador de la autenticación a realizar.
2. Redireccionar al Browser del tarjetahabiente a una URL preestablecida por Visa, donde iniciará el circuito de autenticación de VbV.
3. Implementar un servicio XML-RPC el cual atenderá el mensaje XML-RPC de respuesta que enviará Visa al site (similar al punto 1 pero con los roles cliente servidor intercambiados)
4. Implementar una página de respuesta donde Visa redireccionará al Browser para continuar con la transacción de compra normalmente.

Los puntos 1 y 3 son conexiones IP/TCP/HTTPS/XML-RPC. Los puntos 2 y 4 son implementados a través de Redirecciones HTTPS (a través del Browser)

4. Especificación

4.1. Llamadas XML-RPC

4.1.1. Registración de la Compra

RegistrarCompra() A realizar cuando el usuario aprueba dentro del carrito de compras del establecimiento el pago mediante 3-D Secure. Función implementada por el MPI de Visa. Registra los datos de una compra dentro del sistema.

Parámetros

UsuarioCSP (String):

Identificador asignado al Establecimiento por Visa.

ClaveCSP (String):

Clave asociada al identificador asignada al Establecimiento por Visa.

Merchant_acqBIN (String):

Código del Banco Pagador del Comercio

Merchant_merID (String):

Identificador interno asignado por Visa para el Comercio

CodigoMoneda (String):

Codigo ISO para la moneda. Idem al usado en la mensajería (32 Peso Arg)

Importe (String):

Importe en pesos de la transacción a realizar, expresado en centavos.

pan (String):

Código de la Tarjeta

VtoTarj (String):

Vencimiento de la Tarjeta AAMM

Parámetros de retorno Identificador de Compra (String) 0 si se produce un error.

Dependiendo del tipo de error, el sistema puede devolver un código de error negativo según la tabla de Errores en el Apéndice A de este documento.

Detalle Esta llamada RPC generará un registro en el componente MPI de Visa que identificará la transacción de autenticación y los datos de la compra para la cual se realiza la transacción de autenticación. Si hay errores en la registración de la compra el sistema retorna un Identificador de Compra = '0' (Parámetros inválidos, violaciones de seguridad, no disponibilidad del servicio) En caso de haber problemas de comunicaciones inherente a la conexión, es responsabilidad del establecimiento manejar el tratamiento de los errores. Si la registración es exitosa la llamada al método retorna un identificador de compra válido (mayor a 0)

4.1.2. Registración de Información de Autenticación

ResultadoAutenticacion() Función implementada por el Sitio del Establecimiento. Procesa los datos salientes de 3-D Secure y los registra dentro del sistema del establecimiento. Esta llamada se realiza solo si el proceso de autenticación se completa (autenticando o no al usuario correctamente)

Los campos Descripción, TX.time, TX.status, TX.cavv y TX.eci pueden venir vacíos, dependiendo del valor del Resultado o de TX.status.

Parámetros

`idCompra` (String): El identificador de compra obtenido con `'RegistrarCompra()'`

`Resultado` (String): Código de Resultado de la Autenticación

`Descripción` (String): Descripción del resultado.

`TX.time` (String): Fecha en que el PARES fue signado por el ACS. El valor es expresado en GMT con el formato AAAAMMDD HH:MM:SS

`TX.status` (String): Indica el Estado de la transacción: Y, N, U, A, P.

`TX.cavv` (String): Contiene el CAVV.

`TX.eci` (String): Contiene el ECI.

La codificación del parámetro Resultado

0: Transacción Completada.

1: Error en el Sistema (el resto de los campos contiene una cadena de longitud 0)

Parámetros de Retorno

`Retorno` (String): Cadena de texto `'ok'` si todo resulta bien y el sitio del Establecimiento está listo para recibir al usuario via un Redirect sobre el Browser cualquier otro valor si el sitio desea registrar la autenticacion como cancelada (el usuario de todas formas será reenviado al sitio del comercio para continuar la operación.

4.2. Páginas Web de Interacción entre Sites

4.2.1. Página de Pago con Tarjeta en Site eCommerce

Procesa el pago con Tarjeta, realiza una llamada a `'RegistrarCompra()'` y redirecciona al Browser del usuario a la UVR por POST con el parámetro `'idCompra'`
UVR: URL_VISA_REGISTRARCOMPRA

4.2.2. Página Autenticación VbV

Autentica al tarjetahabiente, realiza una llamada a `'ResultadoAutenticacion()'` y redirecciona al Browser del usuario a la UER por POST con el parámetro `'idCompra'` (case-sensitive)

UER:URL_ESTABLECIMIENTO_RESULTADOAUTENTICACION

4.3. Secuencia de Eventos

1. El Usuario, una vez terminada su compra en el carrito de compras del sitio del establecimiento, hace click en el botón comprar y autentica por 3-D Secure.
2. Se procesa la página y se invoca 'RegistrarCompra()' implementado en el MPI de Visa.
3. La llamada XML-RPC retorna un identificador de compra válido, '0' o un código de error negativo si se produjo algún error.
 - a) Si se recibe un valor '0' o se produce un error en la llamada (ej. un error de comunicación) se debe proceder enviando un mensaje ISO estándar.
4. La página web del establecimiento redirecciona el cliente a una URL provista por Visa mandando como campo 'idCompra' el identificador de compra mediante Post.
5. De aquí en adelante nuestra implementación de 3-D Secure se hace cargo de la validación de la transacción.
6. Si la autenticación se completa satisfactoriamente y el MPI recupera el resultado de la autenticación, llama al método 'ResultadoAutenticacion()' implementado en el sitio del establecimiento informando el resultado y los datos de la misma
7. La implementación del sitio registra el resultado de la autenticación de la transacción dentro de los sistemas del establecimiento y retorna el resultado de la llamada.
 - a) Si la llamada no es satisfactoria (El comercio responde con un valor diferente de .°k") se le informa al usuario de que se presentó un problema en el proceso de autenticación.
8. El MPI deriva al usuario a la página indicada por el Establecimiento durante el Proceso de Inscripción de Establecimientos con el campo idCompra con el valor del identificador de la compra mediante HTTPS POST.
9. De completarse satisfactoriamente todo el circuito, el eCommerce realizará la transacción ISO 8583 adjuntando los valores recibidos TX.eci y TX.cavv, siguiendo el siguiente pseudocódigo:
 - a) Si el argumento *ResultadoAutenticacion().Resultado="0"*:
 - 1) Si TX.status=Y ó TX.status=P ó TX.status=A genera un mensaje (completando TX.eci y TX.cavv). Transacción Ok con garantía de pago para el comercio.
 - 2) Si TX.status=U genera un mensaje completando los valores recibidos en TX.eci y TX.cavv. Transacción sin garantía de pago al Comercio.

- 3) Si TX.status=N el CSP tiene que delegar la decisión de enviar una autorización con riesgo al comercio o no enviar ninguna autorización. Se debe implementar un esquema configurable de negocio por comercio en el cual dependiendo de las características de la venta a realizar se decida o no el envío de la autorización. De enviarse la autorización, esta será una autorización con los valores recibidos de TX.eci y TX.cavv. Esta autorización no tiene garantía de pago para el comercio.
- b) Si el argumento *ResultadoAutenticacion().Resultado="1"*
 - 1) Tiene que generar un mensaje estándar no VbV.

El análisis de los casos de contingencias puede encontrarse en [OELOC].

4.3.1. Ejemplos

Envío y Recepción de Mensaje XML-RPC:

```
<?xml version="1.0" ?>
<methodCall>
  <methodName>registrarCompra</methodName>
  <params>
    <param><value>dec1</value></param>
    <param><value>dec1pass</value></param>
    <param><value>450799</value></param>
    <param><value>1313</value></param>
    <param><value>32</value></param>
    <param><value>1421</value></param>
    <param><value>450799000000010</value></param>
    <param><value>512</value></param>
  </params>
</methodCall>

<?xml version="1.0" ?>
<methodResponse>
  <params>
    <param><value>11254</value></param>
  </params>
</methodResponse>
```

El Reenvío del usuario se hace a través de: <https://tds-test.visa.com.ar/mpi/3dsecure/mpi-compra> (Metodo HTTP POST enviando idCompra=XXXXX)

La llamada y respuesta del mensaje de resultado autenticación:

```
<?xml version="1.0"?>
<methodCall>
  <methodName>ResultadoAutenticacion</methodName>
  <params>
```

```

    <param>
      <value>11254</value>
    </param>
    <param>
      <value>0</value>
    </param>
    <param>
      <value>ok</value>
    </param>
    <param>
      <value>20050914 17:14:54</value>
    </param>
    <param>
      <value>Y</value>
    </param>
    <param>
      <value>MTExMTExMTExMTExMTExMTExMTE=</value>
    </param>
    <param>
      <value>05</value>
    </param>
  </params>
</methodCall>

```

y la respuesta

```

<?xml version="1.0" ?>
<methodResponse>
  <params>
    <param><value>ok</value></param>
  </params>
</methodResponse>

```

Finalmente el sistema reenvia el browser del usuario a la URL `URL_ESTABLECIMIENTO_MPI` adjuntando via POST el parametro `idCompra`.

4.4. Enrolamiento de Comercios

Aquellos comercios que participan del plan deberán proveer de una dirección de IP fija la cual Visa utilizará para validar el acceso. Adicionalmente Visa les proveera la información concerniente a:

UsuarioCSP (String) Identificador asignado al Establecimiento por Visa.

ClaveCSP (String) Clave asociada al identificador asignada al Establecimiento por Visa.

Merchant_acqBIN (String) Código del Banco Pagador del Comercio

Merchant_merID (String) Identificador interno asignado por Visa para el Comercio. Debe coincidir con el número de comercio utilizado en la mensajería ISO.

URLs de acceso de producción y de test.

4.5. Proceso Homologación

1. Enviar a `seginf@visa.com.ar`
 - a) Dos números de establecimientos a utilizar tanto como para la mensajería ISO como para el proceso de autenticación de VbV.
 - b) Certificado digital SSL Server que estarán utilizando para el ambiente de testing para el servidor SSL Server.
 - c) Las dos URLS a utilizar para el ambiente de prueba (ver Resumen de URLS)
2. Visa Argentina entonces le brindará al comercio
 - a) UsuarioCSP y password para el ambiente de pruebas.
 - b) Tarjetahabiente con el password para poder realizar las pruebas.

4.5.1. Pruebas a realizar

- CASO-1: Chequeo conectividad SSL del Servicio XML-RPC en Visa.
- CASO-2: Chequeo conectividad SSL del Servicio XML-RPC en el Comercio.
- CASO-3: Transaccion STATUS 'P'
- CASO-4: Transaccion STATUS 'Y'

4.6. Mensajería ISO 8583

Desde el punto de vista de un sitio de eCommerce, el resultado de una transaccion de VbV son los valores recibidos de la marca ECI y el CAVV. Estos valores deben propagarse en la mensajería ISO 8583 para gestionar la autorización de la compra (en el caso que se envíe PreAutorización y CompraOffline, estos campos se adicionan en ambos mensajes). El detalle de los mensajes puede encontrarse en el documento [DCAVV].

Los Pasos a seguir son los siguientes:

1. . Se recibe el CAVV de 28 bytes codificados en base 64.
2. . Se decodifica, obteniendo un array de 20 bytes.
3. . Ese array de 20 bytes esta codificado en BCD por lo que hay que convertirlo en una cadena de 40 digitos ASCII.
4. . Con esos 40 digitos ASCII mas el valor de la marca ECI obtenida de la transaccion se completa un campo (59) del mensaje de autorización.

Ejemplo:

1. . Al finalizar la transacción de VbV se recibe de la llamada xml-rpc el CAVV:AAABARkBAAAAA.
2. . Se recibe de VbV en la misma llamada el valor para la marca ECI:05
3. . Decodificados de base64 a BCD 0 0 1 1 25 1 0 0 0 0 0 0 5 1 0 0 0 0 0 0
4. . Decodificación de BCD a ASCII:00 00 01 01 19 01 00 00 00 00 00 05 01
00 00 00 00 00 00
5. . El CAVV a enviar queda entonces como: 00000101190100000000000050100000000000
6. . Con estos dos datos se compone el mensaje completando el campo 59 según la especificación de mensajería en [DCAAV]

4.7. Requerimientos de SSL

Visa exige que para el acceso tanto por Browser como las llamadas por XML-RPC sean sobre SSL, con un certificado emitido por una entidad certificante válida.

4.8. Resumen de URLS

URL_VISA_MPI:

URL de Visa donde redireccionar al Browser del usuario para iniciar la autenticación.

En test es <https://tds-test.visa.com.ar/mpi/3dsecure/mpi-compra>

URL_VISA_REGISTRARCOMPRA:

URL del servicio XML-RPC en Visa que atiende la llamada de 'RegistrarCompra()'.

En test es <https://tds-test.visa.com.ar/mpi/3dsecure/mpi-establecimiento>

URL_ESTABLECIMIENTO_MPI:

URL del establecimiento donde redireccionar al Browser del usuario una vez finalizada la autenticación VbV.

URL_ESTABLECIMIENTO_RESULTADOAUTENTICACION:

URL del servicio XML_RPC en el establecimiento que atiende la llamada 'ResultadoAutenticacion()'

5. Apéndice A

Tablas de código de error que puede devolver el MPI en las llamadas.

- 0001: El importe es menor o igual a 0.
- 0002: El importe tiene más de 12 cifras.
- 0003: La tarjeta está vencida.
- 0004: La fecha de vencimiento no es válida.
- 0005: La fecha de vencimiento no se ha ingresado.
- 0006: Usuario/Clave incorrecto.
- 0007: Acceso al servicio denegado.
- 0008: Error de conectividad en el sistema.
- 0009: El Usuario CSP no coincide con el comercio ingresado.
- 0010: La asociacion UsuarioCSP / Establecimiento / CodBancoAdquirente es inválida.

6. Glosario y Diccionario de Acrónimos

3DSECURE:

3 Domain Secure - (Seguridad en 3 dominios), Protocolo desarrollado por Visa International para realizar transacciones de autenticación.

ACS:

Access Control Server - Componente de 3DSecure del lado emisor que se encarga de realizar la validación para un tarjetahabiente que administre.

CAVV:

Cardholder Authentication Verification Value: Este valor lo genera el emisor de una transaccion para marcar que una transaccion ha sido verificado por el protocolo 3DSecure.

Comercio:

Site de eCommerce que se adhiere al protocolo de autenticación 3DSecure.

ECI:

Electronic Commerce Indicator. Identifica el nivel de seguridad establecido para una transacción en base a si el canal es seguro y si el comercio y el usuario están autenticados.

Establecimiento:

(ver comercio)

MPI:

Merchant Plug In - Componente de 3DSecure que inicia las transacciones de autenticación contra los ACS de emisores de otras implementaciones regionales.

RPC:

Remote Procedure Call - Protocolo estándar que especifica la llamada a un procedimiento ubicado en otro equipo, simulando el comportamiento como si se encontrara dentro del mismo sistema.

XML-RPC:

Estándar de comunicación interproceso para implementar una llamada RPC utilizando XML.

PAN:

Personal Account Number. Es el Número de tarjeta.

7. Referencias

OELOC - *Operatoria Ecommerce Locales Comercios090905.xls*

DCAVV - *Definiciones para el envío del Cardholder Authentication Verification Value* emitido por la Gerencia de Tecnología y Riesgo de Visa Argentina.

- XML <http://www.w3c.org/>
- XML-RPC <http://www.xmlrpc.com/spec>