

Webpay

ELO-322 Redes de Computadores I

Yeraldy Cabrera Troncoso

Aldo Passi Rojas

Primer semestre 2015

Resumen

Si de avances tecnológicos hablamos, el que llegó para cambiar al mundo fue el internet. Dentro de la variada gama de usos que se le da existe el compra/venta de bienes y servicios, y para nuestro beneficio, esto dejó de ser inseguro gracias a servicios dedicados al rubro antes nombrado como lo es Webpay.

El sistema de pago webpay consiste en un servicio digital que te permite realizar compras por internet. Este servicio pertenece al banco Transbank el cual vende a las empresas un KCC (kit conexión al comercio) que le permite al cliente poder comprar en tal sitio web o casa de comercio.

Usamos este sistema pero nadie se cuestiona si su seguridad es efectiva. Quizá una persona normal no consiga información pero otro bien informado del tema pueda incluso robar el número de cuenta y la contraseña, por eso ¿Qué tan seguro es? Lo suficiente, usa un protocolo de encriptación llamado TLSv1.2, este se encarga de que cada paquete entregado por ambos lados, dícese del cliente al servidor o servidores, quede totalmente cifrado y para descifrarlo te tomaría años y años. Tampoco olvidemos que nunca llega tu información a la tienda en específico producto de cuando realizas la compra te conectas automáticamente con el servidor de webpay y posteriormente con el de tu banco para autenticarte y luego este pueda autorizarte para que al final se concrete la compra.

Introducción

Analizaremos a fondo el servicio Webpay, para eso responderemos a las preguntas de rigor ¿Qué es el sistema Webpay?, ¿Cómo funciona?, ¿Qué tanta seguridad ofrece a sus clientes?

Webpay

A base del internet como medio, Webpay es un servicio digital que ofrece el banco Transbank para comprar/vender productos en línea por medio de tarjeta de crédito o débito.

El servicio se sustenta por medio de un software, que el banco te vende, llamado KCC (kit de conexión al comercio) que crea dos componentes independientes que interactúan entre sí. Uno se encuentra físicamente en el servidor de la tienda de comercio, donde pueda existir alguna compra/venta y la otra en el denominado Servidor de Pago de Transbank a través del cual se realiza la transacción.

Secuencia Webpay

Este proceso aparece descrito en el manual de integración [1] como:¹

1. Esta comienza cuando el potencial cliente de una tienda virtual presiona el botón pagar.
2. En ese instante la tienda se comunica con Transbank, por medio del KCC, para solicitar autorización para transar la compra.
3. En este punto, la aplicación ubicada en el Servidor de Pago toma el control de la transacción comunicándose directamente con el cliente, solicitando los datos de su tarjeta.
4. Una vez realizado el envío de dicha información directamente a Transbank, se verifica la disponibilidad de cursar la transacción.
5. En caso de que la tienda opere con Webpay Plus, se solicita la autenticación del tarjetahabiente en su emisor.
6. El emisor despliega página de autenticación para el tarjetahabiente.
7. El tarjetahabiente ingresa los datos solicitados para autenticación, estos dependen de cada emisor.
8. El emisor envía a Transbank el resultado de la autenticación, si esta es positiva continua con los pasos siguientes, en caso contrario, Webpay rechaza la transacción.

¹ Véase anexo, figura 2 para secuencia de Webpay gráfica.

9. Webpay solicita la autorización de la transacción al autorizador del emisor de la tarjeta de crédito.

10. Autorizador responde (aprobado, rechazado) a Transbank.

11. Transbank responde a Webpay el resultado de la autorización de la transacción.

12. Luego se le envía una respuesta positiva o negativa a la tienda virtual, así esta puede cerrar la transacción ya sea en forma exitosa o no.

KCC (Kit de conexión al comercio)

El KCC es el software que se instala en el servidor de comercio que establece la conexión entre la tienda virtual con el servidor de pago transbank.

Para que el KCC se conecte y sea funcional debe ser instalado y configurado por parte del comercio afiliado al servicio Webpay de Transbank. Dentro de esta configuración podemos establecer la moneda, el puerto (80 en caso de servidor web), la ip de host (privada), entre varios otros.

Atributos de Webpay

Para tener un buen funcionamiento se es necesario buenas características, entre esas:

- a) Protocolos SSL/TLS: Se encargan de la seguridad a la hora de enviar paquetes. Se usa el método de two-key cryptography.
- b) Encriptación de mensajería y firma digital.
- c) Todo intercambio de información es, en todos los casos, entre el cliente y transbank.

Medios de conexión

El medio de conexión indica a KCC la forma en la que se comunicara con TBK. Esto se define a través del parámetro MEDCOM² que se encuentra ubicado en el archivo tbk_config.dat.

El valor de este término es 1 para que exista un canal SSL entre el comercio y transbank para que el intercambio de paquetes sea encriptado y en segundo plano un token identificador es enviado al cliente para re direccionarlo al formulario de pago Webpay.

Toda conexión con transbank debe ser por el puerto 443 y las ip son en total 6.

² Véase anexo, figura 1 para líneas de código del TBK.

Arquitectura del KCC

El KCC es una aplicación que básicamente está compuesta por:

- Subprogramas
- Archivos de configuración
- Archivos de registro
- Páginas web
- Llave publica de transbank

Estos subprogramas son los encargados de comunicarse con el servidor de transbank (tbk_bp_pago), recibir la respuesta de transbank (tbk_bp_resultado) y validar la firma digital para saber que la respuesta viene de transbank (tbk_bp_mac).

También existe un flujo entre el servidor comercial y el servidor de transbank que no profundizare porque no viene al caso.³

Condiciones de Excepción

Condiciones mínimas para que en ciertas instancias la transacción sea reversada, estas son:⁴

- Timeout: Este se produce cuando el tiempo de espera, por parte de transbank, de la comprobación (ACK), de que fue realizado el cierre de la compra es elevado. Se asume que la compra no fue realizada (Tiempo límite 30 segundos).
- Error en cierre de la compra: Ocurre cuando el string de confirmación del cierre de la compra es distinto de "ACEPTADO".

³ Véase anexo, figura 3 para secuencia grafica enfocada.

⁴ Véase anexo, figura 4 para diagrama de flujo.

Conclusión

Podemos hacer varias observaciones, webpay al ser un servicio otorgado por internet, nos hace por obligación buscar la forma de aumentar su seguridad, este medio, al igual que un camión que traslada dinero a los cajeros, es propenso a ataques que pueden resultar en hurto de nuestra información, cambio en los datos para que esta no se concrete, entre varias cosas.

Depende mucho de la congestión de la red ya que se realizan varias comunicaciones entre cliente/transbank, cliente/banco, servidor comercial/transbank o servidor comercial/cliente, por lo tanto, una red con congestión provocaría la pérdida del servicio, varias veces hemos desistido de su uso por que se nos hacía imposible, un caso cotidiano, intentar comprar algo en un día de oferta organizado.

Referencia

- [1] Transbank S.A
Manual de integración – Kit de conexión al comercio (KCC) Version 6.0

Anexos

```

IDCOMERCIO = 597026007976
MEDCOM = 1
PARAMVERIFCOM = 1
TBK_KEY_ID = 100
URLCGICOM = http://misitio.com/cgi-bin/tbk_bp_resultado.cgi
SERVERCOM = 173.236.32.11
PORTCOM = 80
WHITELISTCOM = ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz 0123456789./:=&?
-
HOST = 173.236.32.11
WPORT = 80
URLCGITRA = /filtroUnificado/bp_revision.cgi
URLCGIMEDTRA = /filtroUnificado/bp_validacion.cgi
SERVERTRA = https://certificacion.webpay.cl
PORTTRA = 6443
PREFIJO_CONF_TR = HTML_
HTML_TR_NORMAL = http://misitio.com/?q=webpay/close/CLP
    
```

Figura 1: Líneas de comando que encontraremos dentro del archivo TBK

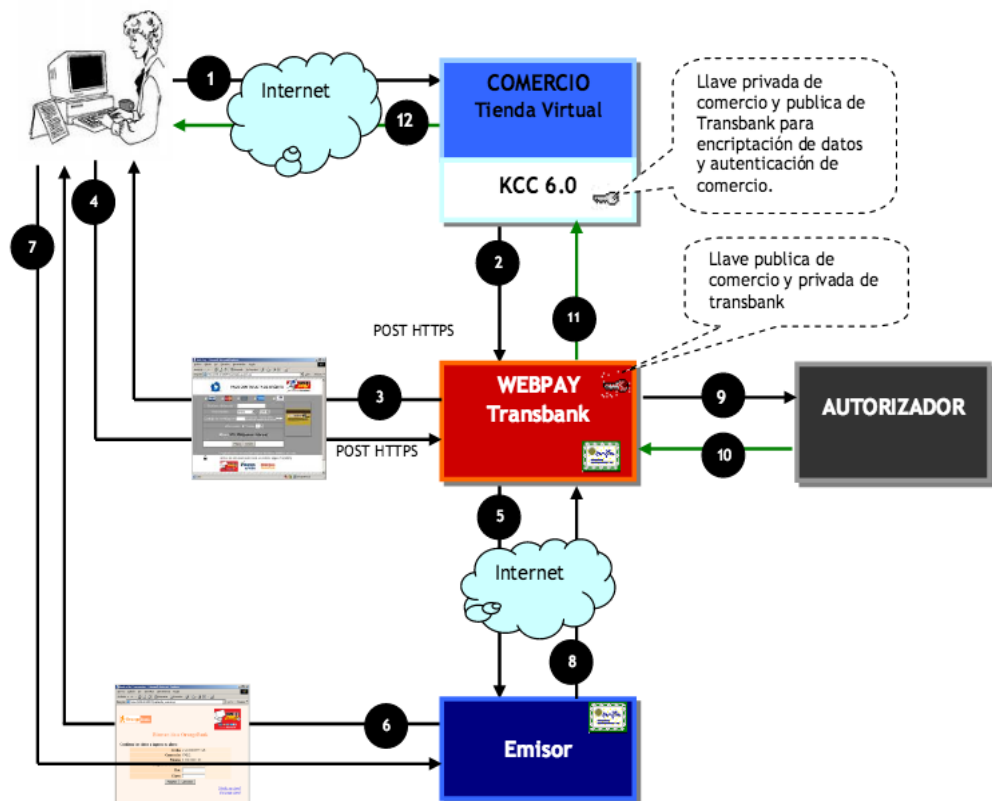


Figura 2: Secuencia que usa Webpay para las transacciones de dinero

Anexos



Figura 3: Secuencia que usa el servidor de comercio con el servidor transbank

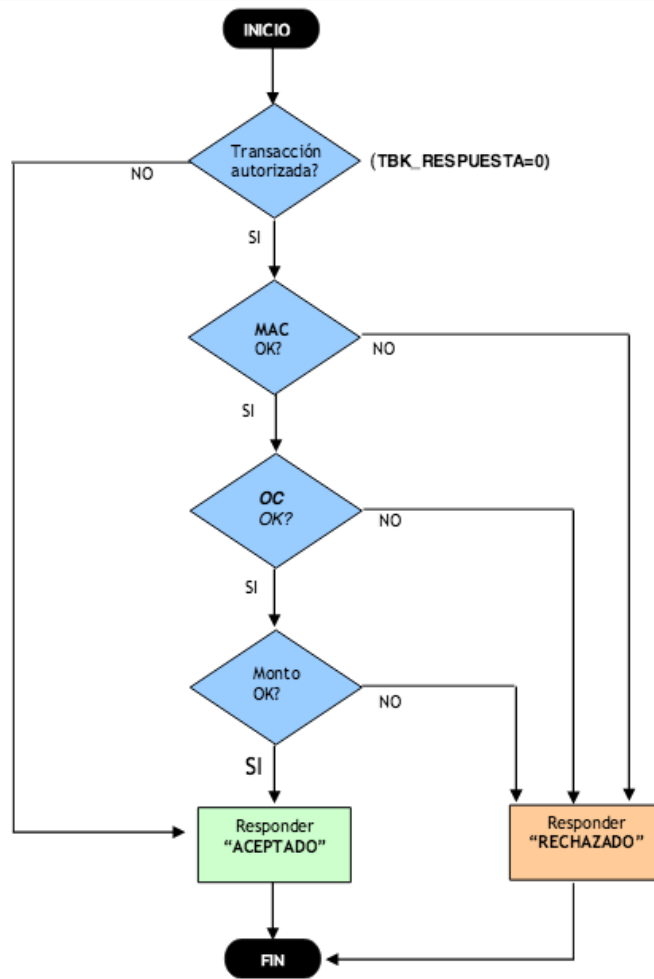


Figura 4: Diagrama de flujo para autorizar una transacción