Manual de Producto

Servicio de POS Virtual

Página dejada en blanco intencionalmente

Tabla de Contenido

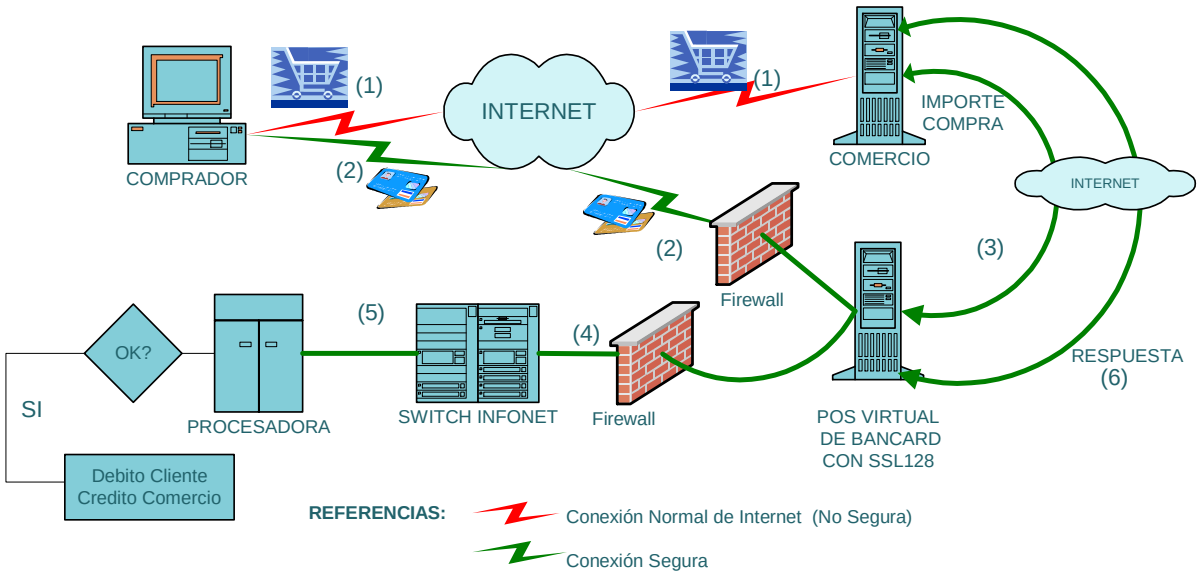
Página dejada en blanco intencionalmente

Detalle del Servicio de POS Virtual

Breve Descripción

Este servicio consiste en la autorización y captura en línea de transacciones de ventas vía internet, para comercios localizados en el país.

El esquema general del mismo es el siguiente:



El servicio está compuesto de una conexión del comercio con Bancard y un integrador del servicio WEB con el esquema actual de procesamiento de transacciones.

Los comercios o CSP's (proveedores de servicios de internet para comercios) deberán integrar a su sitio Web la conexión que permitirá, una vez que el usuario selecciona los productos que desea comprar, y desea pagar con tarjeta de crédito, establecer una conexión HTTP con el servidor WEB seguro de Bancard, (que utiliza el protocolo SSL de RSA con una clave de 128 bits y protegido por firewall), pasándole los parámetros necesarios (importe, código de operación, etc.). Este servidor se encargará de desplegar el formulario personalizado de acuerdo al comercio (POS Virtual), que solicitará al usuario ingresar la información de su tarjeta de crédito dentro de una conexión encriptada entre dicho usuario y el servidor WEB de Bancard exclusivamente (los datos de la tarjeta no quedan expuestos al comercio o CSP en ningún momento).

Nombre, Logo y colores Personalizados

Sello de Certificación SSL de 128 Bits al oprimirlo, aparece la información que se muestra abajo.

VeriSign™
The Sign of Trust on the Net

WWW.BANCARD.COM.PY es un Sitio Seguro CertiSur

CertiSur

La **Seguridad** sigue siendo una de los principales preocupaciones para los consumidores on-line. El **Programa de Sitio Seguro de CertiSur** le permite a Ud. obtener más información sobre los sitios seguros que visita antes de enviarles información que considere confidencial. Por favor, verifique que la información que aparece en esta página coincide con la información del sitio que Ud. está visitando.

Nombre	WWW.BANCARD.COM.PY
Estado	**Valido**
Período de Validez	03-NOV-03 - 30-NOV-04
Información de la Empresa	Country = PY State = Central Locality = Asuncion Organization = Bancard SA Organizational Unit = Infonet Common Name = www.bancard.com.py

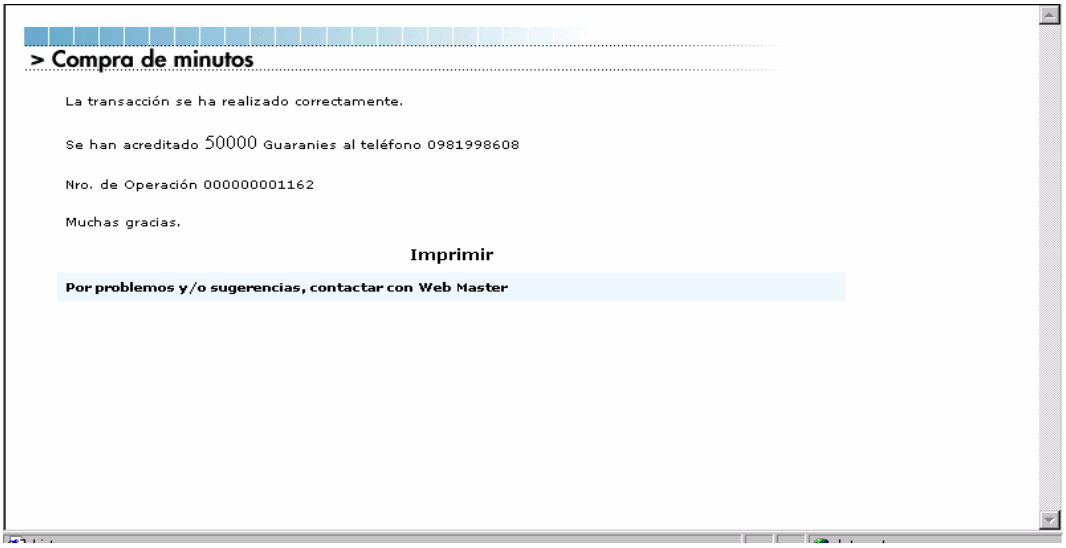
Si la información es correcta, Ud puede enviar información sensible, (ej. número de tarjeta de crédito) con la seguridad que:

- Este sitio tiene un Server ID emitido por CertiSur S.A.
- CertiSur S.A. ha verificado el nombre de la Organización y que BANCARD SA ha entregado documentación que demuestra el derecho a su uso.
- El sitio legítimamente opera bajo el auspicio de BANCARD SA.
- Toda la información enviada a este sitio, si se encuentra bajo una conexión SSL, será encriptada, protegiendo su divulgación hacia terceras partes.

Para asegurar que este es un **Sitio Seguro CertiSur** legítimo, debe verificar:

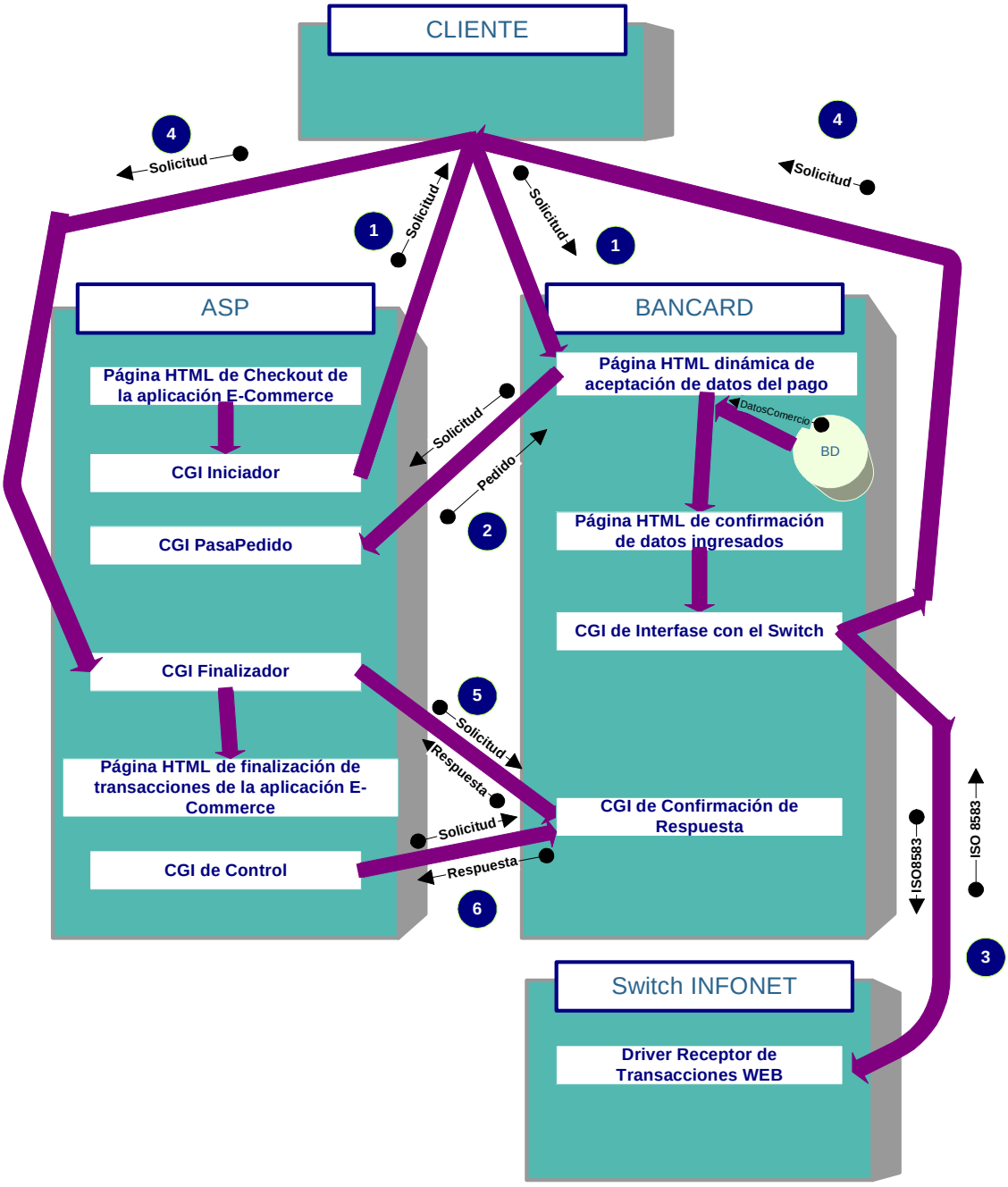
1. El URL del sitio que Ud está visitando viene de WWW.BANCARD.COM.PY.
2. El URL de esta página es **https://digitalid.certisur.com/**.
3. El Estado del Server ID es **Válido**.

El servidor corre una aplicación que extrae los datos del entorno WEB (CGI) y encapsula estos datos en el formato ISO 8583 (algoritmo estándar adaptado por Bancard) para enviarlos, al Switch Infonet, el cual procesa la transacción. La respuesta proveniente del Switch es enviada al comercio a través de una llamada (RELOCATE) a un CGI (a ser desarrollado por el comercio para permitirle la integración transparente con su aplicación de e-commerce) pasándole unos parámetros que identifican la transacción, este CGI se encarga de obtener en forma segura (utilizando protocolo HTTPS), el código de respuesta (aprobación, negación), además de otros datos que le permitirán conocer mas detalles de la transacción, con los cuales se encargará de finalizar la transacción con el cliente informándole en esa última pantalla de la transacción, por ejemplo: el número de operación que se le asignó, o indicando si se le enviará un mail para confirmar, o cualquier otra modalidad de finalización que el Comercio desee implementar, o si ocurrió un rechazo, dándole la oportunidad de reintentarlo. Solo a modo de ejemplo se muestra a continuación la forma como lo finaliza uno de los comercios que ya certificó para operar con este servicio:



Todo este proceso se puede resumir en forma muy general en el siguiente diagrama de flujos:

Esquema de Conexión



Donde:

Elemento	Descripción
Solicitud	Solicitud enviada por el Comercio. (Ver detalle mas abajo)
Pedido	Detalle del Pedido enviado por el Comercio. (Ver detalle mas abajo)
Datos Comercio	Datos registrados por Bancard para los comercios que operan en e-commerce.
ISO 8583	Mensajería para transacciones financieras standard.
Respuesta	Respuesta devuelta al Comercio (Ver detalle mas abajo)

SOLICITUD - Detalle de parámetros

Nombre	Descripción	Tipo	Obligatorio
clavecomercio_input	Código de Comercio especialmente asignado por Bancard para operar en e-commerce	N(7)	SI
nro_pedido_input	Número único por pedido de autorización generado por la aplicación de e-commerce del comercio	N(12)	SI

PEDIDO - Detalle de parámetros

Nombre	Descripción	Tipo	Obligatorio
isp_input	Código de ISP asignado por Bancard	N(7)	SI
monto_input	Importe en guaraníes de la operación	N(10)	SI
mto_orig_input	Importe en la moneda original de la operación (los dos últimos dígitos son los decimales). Si la moneda original es guaraníes debe traer el mismo valor que monto_input.	N(12)	SI
mone_orig_input	Código de la moneda original de la operación, sus valores posibles son: 600 – Guaraníes 840 – Dólares	N(3)	SI
oper_input	Tipo de operación o de pedido que se está realizando, sus valores posibles son: 0 – Autorización 1 – Reversa	N(1)	SI
servicio_input	Campo de servicio de uso reservado para casos especiales	A(80)	NO

RESPUESTA - Detalle de parámetros

Nombre	Descripción	Tipo	Obligatorio
respuesta_output	Código de Respuesta a la solicitud	A(2)	SI
msg_output	Descripción del mensaje correspondiente al código de respuesta a la solicitud. **ATENCIÓN:** Los espacios entre palabras van remplazados con sub-guión, por razones de sintaxis (Ej: Monto_Inválido), por lo que se deberá sustituir los sub_guiones por espacios antes de desplegar el mensaje.	A(40)	SI
nro_autori_output	Número de autorización asignado a la operación. Solo es asignado cuando el codigo de respuesta es 00, o sea Aprobado (sino viene 0).	A(6)	NO
monto_input	Importe en guaraníes de la operación que fue aprobado	N(10)	SI
nombre_output	Nombre del tarjetahabiente cuya tarjeta fue utilizada para la autorización	A(40)	SI
servicio_output	Campo de servicio de uso reservado para casos especiales	A(80)	NO

Como llamar a la Página de Pagos

El procedimiento a utilizar para solicitar y obtener una autorización a través del servicio de POS Virtual de Bancard, puede resumirse en los siguientes pasos:

1. Una vez terminada la compra; desde la página de Checkout se deberá llamar al CGI Iniciador del aplicativo de e-commerce el cual deberá realizar dos funciones específicas para la conexión con el POS Virtual (esto independientemente a otras funciones que pudiera realizar, y que tengan relación solo con el aplicativo de e-commerce), en primer lugar se deberá generar una página estática o dinámica (Ver mas detalle en el punto "Página de Pedido"), cuyo contenido sean los parámetros del "Pedido", separados por ":". Por jemplo:

   0000901:0000008400:000000000200:840:0:Campo_de Servicio_opcional:

   Luego deberá realizar la siguiente re-dirección (LOCATION), pasando solo los parámetros de la "Solicitud" (punto 1 del esquema):

   `https://www.bancard.com.py/cgi-bin/pagina_pagos?clavecomercio_input=nnn&nro_pedido_input=nnn`

2. Una vez que Bancard reciba la "Solicitud" procederá a leer los parámetros del pedido, mediante un URL que tendrá almacenado y un indicador de si es una página dinámica o estática, obrando en concecuencia (Punto 2 del esquema).
3. Con la "Solicitud" y el "Pedido", Bancard presentará al cliente las páginas de ingreso y de confirmación de datos, dentro de su ambiente seguro.
4. Después de obtener los datos del cliente, Bancard procesará la solicitu de autorización correspondiente (Punto 3 del esquema).
5. Una vez obtenido una respuesta a la solicitud, Bancard volverá a re-direccionar (LOCATION), al cliente hacia el aplicativo del Comercio. (Punto 4 del esquema), pasandole de nuevo solo los datos de la "Solicitud" recibida. Ejemplo:

   `http://URLdeRespuestaDelComercio?clavecomercio_input=nnn&nro_pedido_input=nnn`

6. El CGI finalizador del comercio recibirá la solicitud, y antes de presentar la página de finalización deberá leer los parámetros de la "Respuesta" (Punto 5 del esquema), del servidor seguro de Bancard, obrando en consecuencia a dicha respuesta (Ver ejemplos de cómo hacer esta lectura en el punto "Ejemplo de Lectura de Respuesta"). Ejemplos:

   De la llamada:

   `https://www.bancard.com.py/webbancard/?MIval=/ECOM/pasa_respuesta.html&clavecomercio_input=nnn&nro_pedido_input=nnn`

   De los datos recibidos:

   `00:Transacción aceptada_____:058058:0000035000: Prueba_____ _____::`

Los comercios que tengan habilitado por Bancard la posibilidad de realizar extornos deberán considerar en forma adicional lo siguiente:

1. El proceso de extorno debe realizarse ya sin la participación del cliente como “puente” o medio por el cual se canaliza la transacción, como sucede con las solicitudes de autorización.
2. La comunicación será de server a server, pero siguiendo la misma metodología de lectura de páginas tanto para el “Pedido” como para la “Respuesta”.

Página de Pedido

La aplicación de e-commerce utilizada por el comercio puede dejar disponible los parámetros del “Pedido” a través de una página estática, o una página dinámica, debiendo considerar para cada uno de los casos lo siguiente:

Dinámica

1. El comercio deberá indicarle a Bancard que la página es del tipo dinámico, y proporciarle a este último el URL desde donde podrá acceder al mismo.
2. La página deberá generar un texto del tipo “Plain Text”, sin ningún agregado de comandos HTML, cuyo contenido sean los parámetros del “Pedido”, separados por “:”. Por jemplo:

   0000901:0000008400:000000000200:840:0:Campo_de Servicio_opcional:
3. Los nombres de los parámetros que recibirá la página dinámica deberán ser los mismos que los definidos por Bancard para la “Solicitud”.
4. A continuación se muestra un ejemplo completo de todo esto:

   Ejemplo:

   http://URLdelaPaginadePedido?clavecomercio_input=nnn&nro_pedido_input=nnn

Estática

1. El comercio deberá indicarle a Bancard que la página es del tipo estático, y proporciarle a este último el URL desde donde podrá acceder al mismo.
2. El nombre de la página estática puede contener un prefijo, si se utiliza este prefijo este debe estar incluido en el URL mencionado en el punto anterior. Seguido por la clave del comercio y el número de pedido de autorización.

   Ejemplo:

Prefijo	= Pedido_Aut_
Clave Comercio	= 1234567
Nro. Pedido Autorización	= 000000001234
Nombre de la Página	= Pedido_Aut_1234567000000001234

3. La página deberá ser un texto del tipo “Plain Text”, sin ningún agregado de comandos HTML, cuyo contenido sean los parámetros del “Pedido”, separados por “:”. Por jemplo:

   0000901:0000008400:000000000200:840:0::

4. A continuación se muestra un ejemplo completo de todo esto:

   Ejemplo:

   http://URLdelaPagina/Pedido_Aut_12345670000000001234

5. La página estática deberá ser generada por cada pedido en el CGI Iniciador y eliminado en el CGI Finalizador.

Ejemplo de Lectura de Respuesta

La aplicación de e-commerce utilizada por el comercio puede usar cualquier método que le permita la plataforma/lenguaje utilizado para el desarrollo del mismo, que permita leer una página de un servidor web por medio del protocolo HTTPS, o llamar a una subrutina que realice esta función.

Bancard deja a elección de los desarrolladores de aplicaciones de e-commerce la forma de realizar esta función, pero a modo de ejemplo solamente proporciona el código necesario en dos lenguajes multiplataformas, muy conocidos y de amplia divulgación, como son el PERL y el JAVA.

Ejemplo en código PERL

```
#!/usr/bin/perl -w

use LWP::UserAgent;

sub msj
{
 my $m = shift @_;
 print "$m\n";
}

sub salir
{
 my $m = shift @_;
 msj("$m");
 exit;
}

#Cambie por su valor de codigo de comercio
$cc = "9999";
#Cambie por su valor de numero de transaccion
$nt = "123";
```

```
$url =
"https://www.bancard.com.py/webbancard/?MIval=/ECOM/pasa_respuesta.html&clavecomercio_inpu
t=$cc&nro_pedido_input=$nt";

$ua = new LWP::UserAgent;
my $req = new HTTP::Request GET => $url;
my $res = $ua->request($req);
if ($res->is_success)
{
 @valores = split(/:/,$res->content);
 $cuantos = @valores;
 salir("Cantidad erronea de parametros") if ($cuantos != 5);
 $w1 = $valores[0];
 $w2 = $valores[1];
 $w3 = $valores[2];
 $w4 = $valores[3];
 $w5 = $valores[4];
}
else
{

  salir("Error al acceder informacion web");
}

salir("Valores:\n$w1\n$w2\n$w3\n$w4\n$w5");
```

Requerimientos para PERL

Se requiere tener instalado el PERL en el servidor web del comercio, con los módulos Bundle::LWP y Crypt::SSLeary.

Ejemplo en código JAVA

```
import java.net.*;
import java.io.*;
import java.util.StringTokenizer;

public class clientejava {
public static void main(String[] args) throws Exception {

      URL respuesta = new
URL("https://www.bancard.com.py/webbancard/?MIval=/ECOM/pasa_respuesta.html&clavecomercio
_input=9999&nro_pedido_input=123");
     BufferedReader in = new BufferedReader(
                        new InputStreamReader(
                        respuesta.openStream()));

     String inputLine;

     inputLine = in.readLine();

     StringTokenizer myTokenizer = new
     StringTokenizer(inputLine,":");
     String w1 = myTokenizer.nextToken( );
     System.out.println(w1);
     String w2 = myTokenizer.nextToken( );
     System.out.println(w2);
     String w3 = myTokenizer.nextToken( );
     System.out.println(w3);
     String w4 = myTokenizer.nextToken( );
     System.out.println(w4);
     String w5 = myTokenizer.nextToken( );
     System.out.println(w5);
     in.close();
  }
}
```

Requerimientos para JAVA

Se requiere tener instalada la máquina virtual de SUN con el JDK2 o superior en el servidor web del comercio, con la extensión de máquina virtual JSSE.

Procedimiento de Control de Integridad

Con el objeto de preservar la integridad de todas las transacciones, se sugiere, por ahora con carácter opcional, que los aplicativos de e-commerce certificados para operar con el servicio de POS Virtual de Bancard, implementen un procedimiento (CGI de Control) de verificación de integridad de las transacciones que el comercio tiene como pendiente de respuesta, para confirmar que las mismas sean transacciones "*abandonadas*" por el comprador antes de la aprobación por parte de Bancard, y no despues de haber sido aprobadas.

La forma de implementar el procedimiento queda a exclusivo criterio del desarrollador del aplicativo de e-commerce, pero deberan considerarse las siguientes mínimas pautas generales:

1. Deberá ser un procedimiento que se ejecute en forma automática cada "X" determinado tiempo; establecido por el comercio de acuerdo a sus requerimientos. (Por ejemplo un comercio de entrega inmediata puede necesitar hacerlo cada 10 minutos, sin embargo uno que vende heladeras puede necesitar hacerlo cada 1 o 2 horas a lo sumo).
2. El CGI de control deberá leer los parámetros de la "Respuesta" (Punto 6 del esquema), del servidor seguro de Bancard, obrando en consecuencia a dicha respuesta (Ver ejemplos de cómo hacer esta lectura en el punto "Ejemplo de Lectura de Respuesta"). Ejemplos:

   De la llamada:

   `https://www.bancard.com.py/webbancard/?MIval=/ECOM/pasa_respuesta.html&clavecomercio_input=nnn&nro_pedido_input=nnn`

   De los datos recibidos:

   `00:Transacción aceptada_____:058058:0000035000: Prueba_____ _____::`
3. Solo se deben verificar las transacciones que no todavía no tienen respuesta, las mismas deberán tener los indicadores correspondientes de tal forma que solo sean verificadas una sola vez (una vez obtenida la respuesta ya no se debe volver a verificar).

Consideraciones de Seguridad o Check List de Certificación

La aplicación de e-commerce utilizada por el comercio deberá tener en cuenta las siguientes consideraciones de seguridad:

1. El aplicativo de e-commerce no podrá llamar a la página del POS Virtual dentro de un frame (Siempre debe ser llamado con el parámetro TOP).
2. La aplicación podrá registrar todos datos que requiera el comercio del cliente, salvo todos aquellos que se relacionen a sus tarjetas de crédito (Número de tarjeta, código de seguridad, vencimiento, etc.)
3. Todos los CGI del comercio (Iniciador, Pasa Pedido y Finalizador) deberán ser programas debidamente protegidos dentro del servidor WEB del comercio.
4. En la página HTML del checkout presentado al cliente no deben poder verse y mucho menos poder modificarse las variables pre-establecidas enviadas a Bancard, en especial el monto de la transacción a aprobar.
5. El CGI iniciador deberá generar un número secuencial único por cada pedido de autorización realizado, es decir si una misma compra requiere de más de una autorización (porque la tarjeta seleccionada en el primer intento no tenía fondos suficientes por ejemplo), cada uno de esos pedidos debe llegar a Bancard con diferentes números únicos generados por y para el comercio.
6. El CGI finalizador deberá realizar una verificación de consistencia del monto solicitado y el efectivamente autorizado que recibe como una de las variables de la respuesta. Esta verificación deberá realizarse antes de presentar la página HTML final al comprador. El comercio debe visualizar en su página de respuesta, todos los datos de la transacción: fecha, número de pedido, monto enviado, monto recibido, número de autorización si fuese aprobada. En el caso de que se registre una diferencia entre el monto enviado y recibido, debe solicitarle al cliente que se comunique con el comercio. Si existe esta diferencia el comercio no puede rechazar la transacción, esto lo define únicamente Bancard, por tanto se debe mostrar la respuesta que se obtuvo.
7. El CGI finalizador deberá realizar una verificación de consistencia para asegurarse de que la respuesta recibida de Bancard haya sido generada por el CGI iniciador de la aplicación del comercio, y que no existan respuestas “duplicadas” (un número de pedido de autorización solo debe procesarse una sola vez). Si el CGI finalizador recibe una respuesta cuyo pedido no fue generado en el sitio, debe solicitar al cliente que se comunique con el comercio. En su página de respuesta se debe visualizar todos los datos de la transacción: fecha, número de pedido, monto enviado, monto recibido, número de autorización si fuese aprobada. El comercio no puede rechazar una transacción, esto lo define únicamente Bancard.
8. Generar un LOG de las inconsistencias encontradas, incluyendo la dirección IP origen para poder rastrear al que intenta realizar alguna violación de la seguridad.
9. Definir una política de seguridad que incluya el análisis periódico de los LOGS generados en busca de elementos extraños.