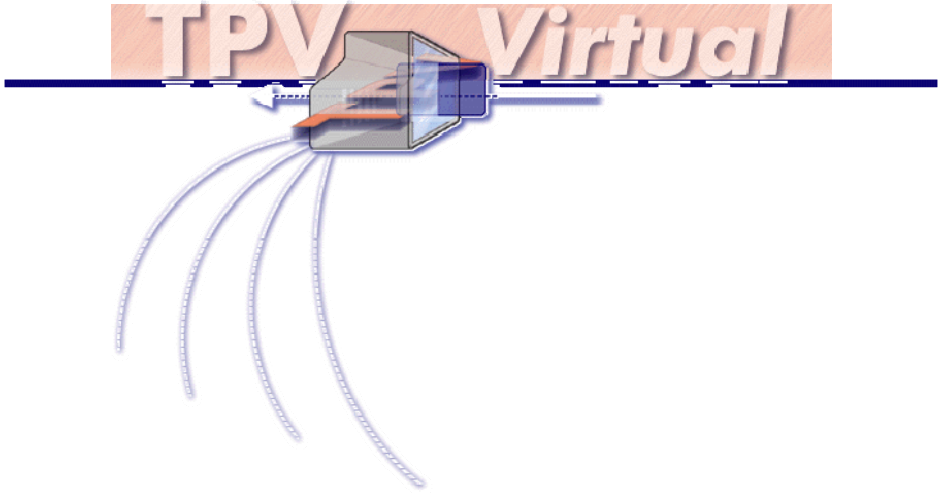
CONFEDERACION ESPAÑOLA DE CAJAS DE AHORROS

TPV VIRTUAL 6.0
MANUAL DE IMPLEMENTACION PARA COMERCIOS



Confederación Española de Cajas de Ahorros.
Avda. de Bruselas, 37 – 28028 Madrid – Tel.: 91 596 53 28
Email: soporte.tpv@ceca.es

CONTENIDO

1.- INTRODUCCIÓN:

En este documento se describen las características del TPV virtual ofrecido por CECA. Un TPV es un software que se implementa en los SERVIDORES WEB DEL COMERCIO y que permite realizar pagos mediante una tarjeta de crédito/débito en internet.

Esta nueva versión es totalmente compatible con las versiones anteriores, por lo que aquellos *COMERCIOS* que ya estén utilizando el TPV virtual de CECA, podrán continuar haciéndolo sin necesidad de realizar ningún cambio en su programación, a no ser obviamente, que quieran incorporar alguna de las nuevas características.

	La implementación de un TPV requiere unos conocimientos mínimos de programación, por parte del cliente.

Características más importantes:

Las características más importantes, la versión 5.0 del TPV virtual permite:

- **Uso protocolo SSL.-** El *CLIENTE* sólo necesita disponer de un navegador WEB que soporte SSL 3.0 con claves de cifrado de 128 bits (prácticamente todas las versiones actuales de navegadores existentes en el mercado cumplen este requisito) y el *COMERCIO* sólo requiere estar creado y autorizado en las tablas del TPV virtual de CECA.

  Esta característica ya estaba presente en la versión anterior del TPV virtual.

  Esta solución garantiza:

  - ***Secreto*** en la comunicación entre el CLIENTE/COMERCIO y el TPV virtual, puesto que todo el diálogo es SSL 3.0 con claves de cifrado de 128 bits (la versión SSL 2.0 no será soportada).

    Además, desde la versión 2.0, se añadió la funcionalidad de que los datos de la tarjeta de crédito/débito (PAN y Caducidad) puedan ser requeridos opcionalmente desde una página HTML presentada directamente por el TPV virtual, en lugar de por el *COMERCIO*, con lo que se le garantiza al *CLIENTE* por un lado que estos datos viajan siempre adecuadamente cifrados por la RED y por otro que nunca se le facilitan al *COMERCIO*.

  - ***Autentificación*** del *COMERCIO* e ***Integridad*** de los datos enviados entre el *CLIENTE/COMERCIO* y el TPV virtual.

- **Comunicaciones Firmadas** Todas las comunicaciones hacia el TPV virtual van protegidas por una firma electrónica que es calculada e insertada por el *COMERCIO* en base a sus propios datos (MerchantID, AcquirerBIN y TerminalID) y a los datos de la operación (Número de operación, Importe, Tipo de Moneda, Exponente). La firma electrónica es recalculada por el TPV virtual y comparada con la firma electrónica recibida antes de proceder a aceptar cualquier pago. De esta forma se evita que un tercero pueda manipular cualquier dato entre el envío de los datos desde el comercio hasta el TPV virtual.

  El mismo mecanismo se sigue en la comunicación desde el TPV Virtual hacia el *COMERCIO*, en caso de que la haya.

- **Pago 3D-Secure (Verified by Visa / Mastercard SecureCode.-** Una **Compra securizada en Internet** consiste básicamente en la Autentificación del titular de la tarjeta. El CLIENTE, para ser autenticado por su entidad emisora debe tener acceso a alguna herramienta de identificación. El *COMERCIO* sólo requiere estar creado y autorizado en las tablas del TPV virtual de CECA y haber sido declarado como Securizado o Mixto. La transacción se procesará independientemente de si el CLIENTE dispone o no de una herramienta de autenticación.

  Esta solución garantiza:
  - ***Secreto*** en la comunicación entre el CLIENTE/COMERCIO y el TPV virtual, puesto que todo el diálogo es SSL 3.0 con claves de cifrado de 128 bits.
  - ***Securización*** del *COMERCIO* e ***Integridad*** de los datos enviados entre el *CLIENTE/COMERCIO* y el TPV virtual.
  - ***Autenticación*** del Cliente. Las operaciones realizadas por este método tratan de garantizar el pago al comercio en las operaciones en que los titulares niegan su participación en las mismas (repudio). . El emisor de la tarjeta trata de autentificar al titular.
  - ***Garantía de pago.*** En general para este tipo de operaciones, el COMERCIO tendrá garantía de pago ante posibles repudios del titular. . Para mas detalle sobre la garantía de pago, revisar la versión actualizada del "REGLAMENTO DEL TERMINAL PUNTO DE VENTA VIRTUAL DE CONFEDERACIÓN ESPAÑOLA DE CAJAS DE AHORROS"

  Desde CECA (Confederación Española de Cajas de Ahorro) impulsamos el estándar internacional de Comercio Electrónico Seguro desarrollado por Visa y MasterCard, basado en la securización de la identidad del comercio y autenticación del titular de la tarjeta.. El mecanismo de autenticación lo marcarán los distintos emisores pudiendo ser totalmente diferentes en función de la entidad. Cuando el cliente aprueba la operación a través de una identificación positiva el comercio recibe entonces confirmación del pago. Es en ese momento cuando la compra está efectuada y pagada con seguridad para el comercio y para el titular. Una compra efectuada a través de este sistema tendrá en general garantía de pago para el comercio ante posibles repudios del titular. De está forma se trata de eliminar uno de los mayores problemas de las operaciones actuales en Internet que denominaríamos como compras estándar, donde al no estar identificado el cliente, este puede a posteriori anular la operación alegando desconocimiento o participación en la operación.

	En ciertos casos puntuales, y ante la certeza de que un comercio escudado en la garantía de pago ha iniciado una actividad fraudulenta (o ha relajado sus mecanismos de control del fraude permitiendo a un tercero una actividad fraudulenta en el mismo), los sistemas internacionales o nacionales pueden acordar su pérdida de la garantía de pago durante un periodo determinado de tiempo, así como imponerle otras penalizaciones.

2.- POR DÓNDE EMPEZAR:

A continuación se muestran una serie de pasos a realizar para implementar un TPV en la WEB del comercio. Estos pasos son orientativos, y cada comercio puede adaptarlos según su forma de trabajar.

1. Cómo se decía en el punto primero de este manual, la persona que vaya a implementar el TPV deberá tener los conocimientos de programación necesarios.

2. El comercio deberá tener un espacio web donde albergar la tienda, ya sea a través de sus propios recursos o contratando un hosting con alguna empresa que permita la instalación de TPVs.

3. Tener instalada alguna aplicación de comercio electrónico (página web de la tienda) que permita al cliente poder seleccionar los productos que desea comprar

4. Una vez que el cliente ha seleccionado los productos y va a proceder al pago, se debe calcular una firma a partir de una serie de campos. Para calcular dicha firma el comercio debe utilizar la clave de cifrado recibida. Una vez calculada la firma desde el comercio ésta será enviada a CECA junto con el resto de campos necesarios, bien al entorno de pruebas bien al entorno de producción (Ver Apartado Cómo realizar un pago). En el caso de que se produzca algún error le rogamos que consulte el apartado de errores frecuentes dentro del capítulo cómo realizar un pago antes de ponerse en contacto con el soporte TPV de CECA.

5. En esta nueva versión ya no es necesario personalizar las páginas de pago como en versiones anteriores, ya que el propio TPV las incorpora de serie cumpliendo con una serie de requisitos explicados en el apartado 7 del manual.

6. Por último y si de desea tener confirmación en la WEB del comercio de las operaciones realizadas se procederá a configurar la comunicación on-line. Para ello el comercio tendrá que realizar el desarrollo de un proceso con esa función y configurarla en la consola de administración.. (Ver apartado Comunicación on-line)

3.- TIPOS DE COMERCIOS:

Existen varios tipos de comercios definidos dentro de la solución TPV de las Cajas de Ahorros. El desarrollo WEB para un comercio es el mismo para todos los casos, sólo depende del acuerdo que se tenga con la entidad. El cambio de un tipo a otro es transparente para el comercio, pero antes se debe tener claro lo que significa cada tipo.

Estándar/Inseguro:

No se pide ninguna autentificación del cliente, solo se comprueba que la tarjeta tenga saldo y en algunos casos el CVV2/CVC2. Es importante destacar que ***No existe garantía de pago para el comercio***, es decir, un cliente puede ir a su oficina varios meses después de realizar una operación y reclamar el importe alegando que desconoce el motivo del cargo. El banco retrocederá la operación y después debe ser el comercio quien inicie las acciones legales que considere oportunas contra el cliente para demostrar que el cargo es válido, pero por defecto, la entidad retrocede las operaciones. Sin duda alguna este tipo de comercio es el que más operaciones puede procesar, sin embargo debido al alto número de incidencias tiende a desaparecer salvo en sectores que tienen un fraude bajo, como venta de entradas, donde posteriormente se exige la presentación de la tarjeta. La mayoría de entidades no concede altas para este tipo de comercios.

Seguro:

Solo se admiten operaciones donde el cliente se ha autenticado correctamente contra su entidad o bien la entidad se hace responsable del posible uso fraudulento de sus tarjetas en caso de no autenticar al titular y autorizar la operación. En principio, todas ***las operaciones que se admiten con este sistema tienen garantía de pago.*** Por tanto la ventaja es clara, sin embargo actualmente no todas las tarjetas están activas para funcionar en este sistema y son muchos los clientes que por desconocimiento o simplemente porque no quieren introducir sus datos de Banca Electrónica, no se autentican y por tanto la operación no finaliza correctamente.

	En ciertos casos puntuales, y ante la certeza de que un comercio escudado en la garantía de pago ha iniciado una actividad fraudulenta (o ha relajado sus mecanismos de control del fraude permitiendo a un tercero una actividad fraudulenta en el mismo), los sistemas internacionales o nacionales pueden acordar su pérdida de la garantía de pago durante un periodo determinado de tiempo, así como imponerle otras penalizaciones.

Mixto:

Es una mezcla de lo anterior. En primer lugar las operaciones se intentan hacer como seguras. Si la operación no puede ser lanzada por este modo, se lanza como una operación normal, siempre y cuando el importe sea menor al definido por el comercio (Limite a securizar), que puede consultar y modificar desde la administración del comercio. En este caso ***en las operaciones seguras el comercio tiene garantía de pago y en las no seguras el responsable es el propio comercio.***

	Que el comercio sea mixto no quiere decir que las operaciones con importes inferiores a importe indicado se procesen de modo inseguro. El limite securizado no funciona de ese modo. Si una tarjeta admite autenticación, el proceso de autenticación se inicia independientemente del importe de la operación. El TPV interroga a Visa/MasterCard para saber si una tarjeta admite autenticación. Si la tarjeta admite auntenticación en todos los casos (no importa el importe) se presenta la pagina de autenticación de la entidad que corresponda. Una vez se presenta la pagina del banco para iniciar el proceso de autenticación hay dos opciones. -. El banco que corresponda no permite continuar sin autentificarte -. El banco que corresponda permite continuar temporalmente sin autentificarte o te pide el CVC2 o un dato de seguridad inferior para que temporalmente puedas comprar en comercio seguro El TPV no influye para nada en este proceso, es decisión única del banco emisor que permita a sus clientes continuar o no continuar, es decir, comprar o no comprar en comercio seguro sin autenticarse.

4.- CÓMO REALIZAR UN PAGO

Realizar un pago es tan sencillo como, una vez que el cliente ha elegido los productos y decide realizar el pago, mostrar un formulario con una serie de campos y enviarlos al TPV de CECA para que se encargue de procesarlo. Una vez terminado el pago, se devolverá el controla a la URL_OK o URL_NOK, dependiendo de su resultado.

Al final de este capítulo se muestran los errores más frecuentes que se pueden producir a la hora de realizar un pago. Le rogamos que antes de ponerse en contacto con el soporte TPV de CECA, consulte este apartado.

Los campos a enviar en el formulario son los siguientes:

Nombre	**Requerido/ Opcional**	**Long.**	**Descripción**
MerchantID	Requerido	9	Identifica al comercio. Facilitado por la caja en el proceso de alta
AcquirerBIN	Requerido	10	Identifica la caja. Facilitado por la caja en el proceso de alta.
TerminalID	Requerido	8	Identifica al terminal. Facilitado por la caja en el proceso de alta.
Num_operacion	Requerido	50	Identifica para el comercio la operación, nº de pedido, factura, albaran, etc.… Puede ser alfanumérico pero están prohibidos los caracteres extraños típicos como ¿,?,%,&,*,etc. Ver nota al final de la tabla
Importe	Requerido	10	Importe de la operación sin formatear. Siempre será un número entero donde los dos últimos dígitos serán los céntimos de Euro.
TipoMoneda	Requerido	3	Es el *código ISO-4217* correspondiente a la moneda en la que se efectúa el pago. Contendrá el valor *978* para Euros. *** Ver apéndice para códigos otras moneda**
Exponente	Requerido	1	Actualmente siempre será 2
URL_OK	Requerido	500	URL completa (http://…). Es la URL determinada por el comercio a la que CECA devolverá el control en el caso de que la operación finalice correctamente. **Esta URL no deberá utilizarse para actualizar la operación como pagada en el servidor del comercio. Ver más información al final de la tabla.**
URL_NOK	Requerido	500	URL completa (http://…) Es la URL determinada por el comercio a la que CECA devolverá el control en el caso de que la operación no pueda realizarse por algún motivo.
Firma	Requerido	256	Es una *cadena de caracteres* calculada por el comercio siguiendo las indicaciones explicadas en el punto Cálculo de la firma. .
Cifrado	Requerido	4	Valor fijo SHA1.
Idioma	Opcional	1	Código de idioma. Ver más información al final de la tabla.
Pago_soportado	Requerido	3	Valor fijo SSL.
Descripcion	Opcional	1000	Campo reservado para mostrar información extra en la página de pago.
Pago_elegido	Opcional		Dependiendo de quien solicite los datos de la tarjeta. Si los solicita el comercio será SSL. Si los solicita el TPV será vacío o no viajará.
PAN	Opcional	19	Nº de tarjeta del cliente.. Este campo tendrá contenido sólo en el caso de que la caja haya autorizado al comercio a solicitar este tipo de datos. En caso contrario dejarlo sin contenido.
Caducidad	Opcional	6	Fecha de Caducidad. Formato AAAAMM.. Este campo tendrá contenido sólo en el caso de que la caja haya autorizado al comercio a solicitar este tipo de datos. En caso contrario dejarlo sin contenido.
CVV2	Opcional		CVC2 de la tarjeta. Este campo tendrá contenido sólo en el caso de que la caja haya autorizado al comercio a solicitar este tipo de datos. En caso contrario dejarlo sin contenido.
Referencia	Opcional	30	Si el comercio está realizando el pago de una compra el campo viajará sin contenido. Si el comercio está realizando la anulación de una operación, se informará con el valor correspondiente.

Cualquier otro parámetro enviado al TPV virtual no será tenido en cuenta y se perderá en el proceso.

	El campo **número de operación** no debe volverse a repetir hasta transcurridos 24 horas, independientemente de si la operación ha sido o no procesada con éxito. En el caso de repetirse aparecerá un error de "operación incorrecta"

	La URL_OK no debe utilizarse para actualizar la operación como pagada en el servidor del comercio, ya que antes de llamar a esta URL al cliente se le presenta una pantalla de confirmación de la compra proporcionada por el TPV en la que se indica que la operación se ha realizado correctamente con un botón ACEPTAR. Al pulsar el botón ACEPTAR es cuando se realiza la llamada a esta URL, por lo que es posible que el cliente no pulse sobre el botón ACEPTAR o cierra la pantalla, quedándose el comercio sin marcar la operación como pagada. En el caso de que el comercio quiera este tipo de confirmación se deberá utilizar la comunición on-line, la cual se explica en el apartado correspondiente de este manual.

Los códigos de idioma a utilizar son los siguientes:

1.- Español	**2.-** Catalán	**3.-** Euskera	**4.-** Gallego	**5.**- Valenciano
6.- Inglés	**7.**- Francés	**8.**- Alemán	**9.**- Portugués	**10.**- Italiano

El campo ACTION del formulario apuntará a una URL de un Servidor WEB de CECA correspondiente al CGI que tratará tanto los datos de la operación rellenos por el Servidor WEB del Comercio como los posibles datos de la tarjeta rellenos por el cliente.

El TPV de CECA consta de dos entornos en funcionamiento, Uno para pruebas y otro para producción. A continuación mostramos sus direcciones:

https://pgw.ceca.es/cgi-bin/tpv ENTORNO DE PRODUCCION

http://tpv.ceca.es:8000/cgi-bin/tpv ENTORNO DE DESARROLLO

Estos serán los únicos valores válidos en el campo ACTION de los formularios descritos anteriormente.

4.1 Ejemplos de formularios

Ejemplo de llamada en la que los datos de tarjeta son solicitados por el TPV

	**Importante:** Esta opción es la que utiliza la mayoría de los comercios. Por defecto los comercios no están autorizados a solicitar los datos de la tarjeta, pasando esta labor al TPV. En el caso de que el comercio quiera solicitar los datos y éste no esté autorizado por su caja, se le mostrará el mensaje "error en la operatoria del comercio".

```
<HTML>
<HEAD>
<TITLE>P&aacute;gina de pago</TITLE>
</HEAD>
<BODY>
<FORM ACTION="https://pgw.ceca.es/cgi-bin/tpv" METHOD="POST" ENCTYPE="application/x-
www-form-urlencoded">
<INPUT NAME="MerchantID" TYPE=hidden VALUE=##MerchantID##>
<INPUT NAME="AcquirerBIN" TYPE=hidden VALUE=##AcquirerBIN##>
<INPUT NAME="TerminalID" TYPE=hidden VALUE=##TerminalID##>
<INPUT NAME="URL_OK" TYPE=hidden VALUE=##URL_OK##>
<INPUT NAME="URL_NOK" TYPE=hidden VALUE=##URL_NOK##>
<INPUT NAME="Firma" TYPE=hidden VALUE=##Firma##>
<INPUT NAME="Cifrado" TYPE=hidden VALUE"SHA1">
<INPUT NAME="Num_operacion" TYPE=hidden VALUE=##Num_operacion##>
<INPUT NAME="Importe" TYPE=hidden VALUE=##Importe##>
<INPUT NAME="TipoMoneda" TYPE=hidden VALUE=978>
<INPUT NAME="Exponente" TYPE=hidden VALUE=2>
<INPUT NAME="Pago_soportado" TYPE=hidden VALUE=SSL>
<INPUT NAME="Idioma" TYPE=hidden VALUE="1">
<CENTER>
<INPUT TYPE="submit" VALUE="Comprar">
</CENTER>
</FORM>
</BODY>
</HTML>
```

	**Importante:** Si hace un copiado de este código a través de la opción copy-paste asegúrese de que el código destino es correcto. En algunos casos se ha detectado que al copiar el código las " (comillas dobles) se han sustituido por '' (2 comillas simples)

Obviamente, la aplicación deberá sustituir los literales de los campos VALUE que comienzan y terminan con ## por los valores adecuados.

Ejemplo de llamada en la que los datos de tarjeta son solicitados por el comercio

	**Importante:** Esta opción no está permitida por defecto y en caso de utilizarse aparecerá el error "Error en la operatoria del comercio". El comercio debe justificar la necesidad de esta forma de operar así como auditar los procesos de seguridad necesarios para solicitar y almacenar los datos bancarios desde su servidor. En el caso de querer utilizarla debe ponerse en contacto con su Caja para que le sea autorizada.

```
<HTML>
<HEAD>
<TITLE>P&aacute;gina de pago</TITLE>
</HEAD>
<BODY>
<FORM ACTION="https://pgw.ceca.es/cgi-bin/tpv" METHOD="POST" ENCTYPE="application/x-www-form-
urlencoded">
<INPUT NAME="MerchantID" TYPE=hidden VALUE=##MerchantID##>
<INPUT NAME="AcquirerBIN" TYPE=hidden VALUE=##AcquirerBIN##>
<INPUT NAME="TerminalID" TYPE=hidden VALUE=##TerminalID##>
<INPUT NAME="URL_OK" TYPE=hidden VALUE=##URL_OK##>
<INPUT NAME="URL_NOK" TYPE=hidden VALUE=##URL_NOK##>
<INPUT NAME="Firma" TYPE=hidden VALUE=##Firma##>
<INPUT NAME="Cifrado" TYPE=hidden VALUE"SHA1">
<INPUT NAME="Num_operacion" TYPE=hidden VALUE=##Num_operacion##>
<INPUT NAME="Importe" TYPE=hidden VALUE=##Importe##>
<INPUT NAME="TipoMoneda" TYPE=hidden VALUE=978>
<INPUT NAME="Exponente" TYPE=hidden VALUE=2>
<INPUT NAME="Pago_soportado" TYPE=hidden VALUE=SSL>
<INPUT NAME="Pago_elegido" TYPE=hidden VALUE=SSL>
Tarjeta:<INPUT NAME="PAN" TYPE=text VALUE=><br>
Caducidad:<INPUT NAME="Caducidad" TYPE=text VALUE=><br>
CVV2/CVC2:<INPUT NAME="CVV2" TYPE=text VALUE=><br>
<INPUT NAME="Idioma" TYPE=hidden VALUE="1">
<CENTER>
<INPUT TYPE="submit" VALUE="Comprar">
</CENTER>
</FORM>
</BODY>
</HTML>
```

	**Importante:** Si hace un copiado de este código a través de la opción copy-paste asegúrese de que el código destino es correcto. En algunos casos se ha detectado que al copiar el código las " (comillas dobles) se han sustituido por '' (2 comillas simples)

Obviamente, la aplicación deberá sustituir los literales de los campos VALUE que comienzan y terminan con ## por los valores adecuados.

Es decir además de los campos habituales en este caso deberá de enviar los siguientes campos:

- *PAN: Nú*mero entero sin espacios en blanco ni caracteres extraños.
- *Caducidad*: Estrictamente en el formato AAAAMM.
- *CVV2*: Tres dígitos numérico (más información en apéndice)
- *Pago_soportado*=SSL
- *Pago_elegido*=SSL

4.2 Errores más frecuentes

A continuación se muestran los errores más frecuentes producidos a la hora de realizar un pago.

Al intentar operar me aparece un error "Faltan campos obligatorios"
En el 99% de los casos esto es debido a que el campo firma no está viajando o lo está haciendo sin contenido. Asegúrese de que viaja correctamente. Si la firma viaja pero no es correcta el error es otro.

Este error también es debido por el campo Pago Soportado no viaja. Este campo actualmente es obligatorio y tiene que venir con valor SSL

En el caso de que los datos de la tarjeta sean solicitados por el comercio asegúrese de que los campos Pago_elegido=SSL, PAN, Caducidad y CVV2 son enviados. Un error frecuente es envían Pago_elegido=SSL pero no enviar los datos de la tarjeta.

Por último, si ninguna de las circunstancias anteriores se cumple, revise que todos los campos obligatorios indicados en la tabla del apartado Como hacer un pago se están enviando.

Al intentar operar me aparece una cadena parecida a una firma
En la pantalla se muestra la firma enviada, un guión y la firma esperada. Ello es debido que la firma no se ha calculado de la forma correcta. Revise el apartado Cálculo de la firma y asegúrese que la cadena a firmar incluye todos los campos y en el orden indicado.

Al intentar operar me aparece un error de operación incorrecta
Este error se produce cuando al TPV llega un número de operación que ya ha sido utilizado con anterioridad, independientemente de si la operación se ha procesado con éxito o no. Los números de operaciones no pueden repetirse en un intervalo de 24 horas.

Al intentar operar me aparece un error 190 Resto de casos
El error 190 es el más habitual en el entorno de producción. Denegación por el emisor de la tarjeta. El TPV pide la autorización a la entidad emisora y esta deniega sin especificar una causa exacta de denegación. Normalmente suele ser porque se introduce mal los datos de la tarjeta, en concreto el CVV2. Para solventar el error se deberá comprobar que los datos introducidos son correctos y en caso de persistir, probar con otra tarjeta real.

Si el fallo se produce en el entorno de pruebas probar de nuevo con otra tarjeta de las que aparece en el apartado Tarjetas de pruebas.

Existe un caso puntual en el que se produce este error y es debido a que el comercio no está dado bien de alta. Si al menos una operación se ha realizado en el comercio este error se descarta, por lo que en el caso de que el fallo se produzca con más de una tarjeta, deberá ponerse en contacto con el soporte TPV de CECA para que le revisen la configuración.

Al intentar operar me aparece un error Comunicación online incorrecta
Este error se produce porque el comercio tiene configurada la comunicación online con respuesta requerida y la URL a la que invocamos no devuelve el patrón esperado. Ver capítulo Comunicación online para más detalle.

En la consola de administración del TPV, dentro de apartado configuración se muestran los tres valores necesarios para que funcione este servicio
Comunicación on-line (SI/NO)
Respuesta requerida (SI/NO)
URL online

Si el comercio no ha solicitado este servicio o desea desactivarlo, deberá entrar en la consola y modificar el parámetro Comunicación on-line=NO
Si el comercio sí que ha solicitado este servicio, deberá entrar en la consola y comprobar que la URL online es correcta. En caso de serlo deberá comprobar que se está devolviendo en patrón **$*$OKY$*$,** ya que este error se produce porque la URL no responde, o porque ésta falla al invocarse.

Al intentar operar me aparece un error Error al obtener la clave.
Este error se produce porque los campos MerchantID, AcquirerBIN o TerminalID son erróneos. Revise que los valores introducidos son correctos.

Al intentar operar me aparece el error Error en la operatoria del comercio.
Su comercio no está configurado para que pueda solicitar los datos de la tarjeta y nos está enviando los siguientes parámetros Pago_elegido=SSL, PAN, Caducidad y CVV2. Envío el parámetro Pago_elegido sin contenido y no envío PAN, Caducidad y CVV2.

5.- CÁLCULO DE LA FIRMA

Uno de los parámetros que recibe TPV en su llamada es el parámetro firma. Dicho parámetro es utilizado para autenticar la llamada realizada y comprobar que su contenido no ha sido alterado por terceros.

El algoritmo utilizado para calcular la Firma es: **Secure Hashing Standard FIPS PUB 180-1** [http://www.itl.nist.gov/fipspubs/fip180-1.htm], comúnmente conocido como **SHA-1**. El resultado produce una salida de 160 bits (20 bytes) que se debe codificar en HEXADECIMAL con letras minúsculas. La mayoría de los algoritmos suelen devolver 5 bloques de 4 bytes cada uno, para posteriormente convertirlo en una cadena a enviar en un formulario HTML. Dicha cadena se debe convertir a hexadecimal y rellenar a ceros por la izquierda en caso necesario. La mayoria de los lenguajes de programación tienen una segunda función que realiza esta operación.

Para aclarar un poco lo explicado en el párrafo anterior vamos a utilizar el siguiente ejemplo:

Cadena:
SHA1("1143904411195002800005540520000000322 1__0.675303001261488833000000000001978212003530470912221434010600 7000")
Longitud: 106
Resultado: 62753a72 498191fd 09175074 7b8750bc 6cb06e8f

En el tercer bloque, algunos algoritmos pueden devolver 9175074 , es necesario que sean 8 caracteres, por tanto será 09175074 .

Algunos ejemplos de cadenas cifradas son:
SHA1("") = da39a3ee5e6b4b0d3255bfef95601890afd80709
SHA1("El coche amarillo") = 968be676ad7988e8d911fce686da3fececbb22eb

En la ayuda de la consola de Administración, dentro del apartado Utilidades y descargas, existe una opción para calcular la firma en la que puede introducir una cadena y como resultado le aparece la firma en SHA1.

	Es importarte asegurarse que el comercio consigue reproducir el resultado del ejemplo anterior de la misma manera que va a proceder a calcular la firma. En caso de no obtener el resultado esperado es mejor no avanzar con el siguiente paso y analizar el problema.

Una vez explicado a grandes rasgos el funcionamiento del algoritmo SHA1 pasamos a explicar la forma de calcular la firma para su implementación en el comercio.

La palabra a firmar se va a componer con la concatenación de los siguientes campos:
Clave_encriptacion+MerchantID+AcquirerBIN+TerminalID+Num_operacion+Importe+TipoMoneda+Exponente+ +Cadena SHA1+URL_OK+URL_NOK

Ejemplo:
Clave encriptacion: 99888888 (no viaja en el formulario)
MerchantID: 111950028
AcquirerBIN: 0000554052
TerminalID: 00000003
Num_operacion: 123
Importe: 500
TipoMoneda: 978
Exponente: 2
Cadena SHA1

URL_OK: http://www.ceca.es
URL_NOK: http://www.ceca.es
La Cadena_sha1 a firmar será la siguiente:
99888888111950028000055405200000003123500978 2SHA1http://www.ceca.eshttp://www.ceca.es

La firma_calculada será:
15ba153908476895d9edd75ff23b207707d2c885

Normalmente un comercio no realiza las anulaciones de las operaciones a través de su aplicación, sino que las realiza manualmente desde la Consola de administración. En el caso de que el comercio decida hacer la programación, la cadena a firma sería la siguiente:.

Clave_encriptacion+MerchantID+AcquirerBIN+TerminalID+Num_operacion+Importe+TipoMoneda+ Exponente+Referencia+ Cadena SHA1

.

6.- COMUNICACIÓN ON-LINE

La comunicación on-line es utilizada por los comercios que necesita que las operaciones de *COMPRA* realizadas por sus clientes le sean comunicadas en el momento de producirse. Consiste en la creación de un proceso por parte del comercio al cual el TPV invocará cuando se haya tenido la aceptación de la operación por parte de la entidad emisora de la tarjeta del cliente. Dicha llamada será realizada por POST y podrá ser realizada por HTTP o HTTPS.

Importante: Existen comercios que utilizan la URL_OK enviada como parámetro en el proceso de pago para realizar este tipo de chequeos, Esta forma de operar es errónea, ya que esta URL debe utilizarse única y exclusivamente para devolver el control al comercio una vez realizado el pago. La URL_OK es llamada al final de la operación **sólo si** el usuario pincha el botón de ACEPTAR en la pantalla de confirmación de compra mostrada por el TPV de CECA. Si el usuario no pulsa el botón ACEPTAR o decide cerrar la pantalla al mostrarle la página de confirmación de compra del TPV de CECA, no se realizará la llamada a la URL-OK y por lo tanto la operación estará realizada, pero al comercio le aparecerá como pendiente de pago en su aplicación.
La comunicación ON_LINE es una llamada directa entre el TPV de CECA y el comercio y será el único proceso válido para realizar este tipo de comunicaciones, ya que garantiza que la llamada se realizará siempre, independientemente de la forma de actuar del cliente.

Para activar la comunicación ON_LINE el comercio deberá darla de alta desde la consola de administración, en el apartado de configuración del comercio. La llamada será realizada a la URL dada de alta y se concatenarán los siguientes parámetros

Nombre	Longitud	Descripción
MerchantID	9	Identifica al comercio. Facilitado por la caja en el proceso de alta
AcquirerBIN	10	Identifica la caja. Facilitado por la caja en el proceso de alta.
TerminalID	8	Identificativo del Terminal. Actualmente para todos los TPV virtuales es siempre 00000003.
Num_operacion	50	Identifica para el comercio la operación, nº de pedido, factura, albarán, etc.… Puede ser alfanumérico pero están prohibidos los caracteres extraños típicos como ¿,?,%,&,*,etc.…
Importe	10	Importe de la operación sin formatear. Siempre será una número entero donde los dos últimos dígitos serán los céntimos de Euro.
TipoMoneda	3	Es el *código ISO-4217* correspondiente a la moneda en la que se efectúa el pago. Contendrá el valor *724* para Pesetas y *978* para Euros. Actualmente solo se permiten pagos en Euros, luego el valor será 978.
Exponente	1	Actualmente siempre será 2
Referencia	30	*Referencia.-* Es el único valor devuelto por la Pasarela SET/SEP. Este dato es imprescindible para realizar cualquier tipo de reclamación y/o anulación de la compra.
Firma	256	Es una *cadena de caracteres* calculada por CECA siguiendo las indicaciones explicadas a continuación y firmada por SHA1. .
Num_aut	6	Valor asignado por la entidad emisora a la hora de autorizar una operación.
Idioma	2	Idioma de la operación
Pais	3	Código ISO del país de la tarjeta que ha realizado la operación
Descripcion	200	Los 200 primeros caracteres de la descripción

La palabra a firmar la va a componer CECA con la concatenación de los siguientes campos:

Clave_encriptacion+MerchantID+AcquirerBIN+TerminalID+Num_operacion+Importe+TipoMoneda+Exponente+Referencia

La funcionalidad de este proceso será la que determine el comercio, pero principalmente consistirá en actualizar sus bases de datos internas (situación del pedido).

	La URL a la que se envían los datos puede ser cualquier lenguaje de programación que pueda capturar los datos enviados por un formulario HTML por método POST. ASP, PHP, .net, perl, etc.…..

Comunicación online con respuesta requerida:

En el caso que nos ocupa, en el que el comercio solicite una comunicación ON-LINE de las operaciones de compra realizadas por sus clientes, se contemplan además dos posibilidades:

- **Comunicación ON-LINE sin respuesta requerida** . En este caso, una vez realizado el pago, el TPV virtual de CECA intentará comunicar la operación al comercio, pero dará por realizada correctamente la operación aunque dicha comunicación no sea posible. Es más, ni siquiera esperará recibir una respuesta desde el comercio.

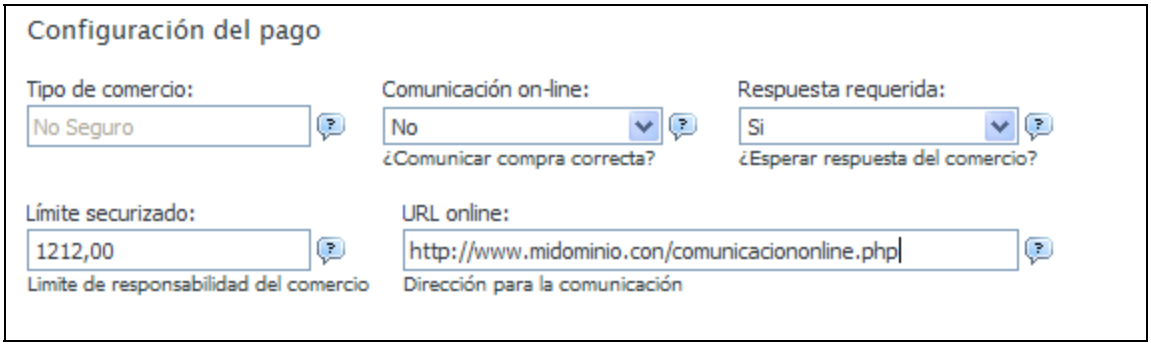
- **Comunicación ON-LINE con respuesta requerida**. En este caso, si una vez realizado el pago, el programa no consigue comunicar la operación al comercio ó detecta a partir de la respuesta recibida que algo no ha ido bien, **anulará** la operación y la dará como errónea al cliente.

Para que el programa sea capaz de discernir a partir de la respuesta recibida desde el Comercio si todo ha funcionado correctamente ó si se ha producido algún error, es necesario que en la respuesta generada por el CGI del comercio aparezca el texto **$*$OKY$*$** sólo cuando todo vaya bien, de modo similar a como figura en el siguiente ejemplo:

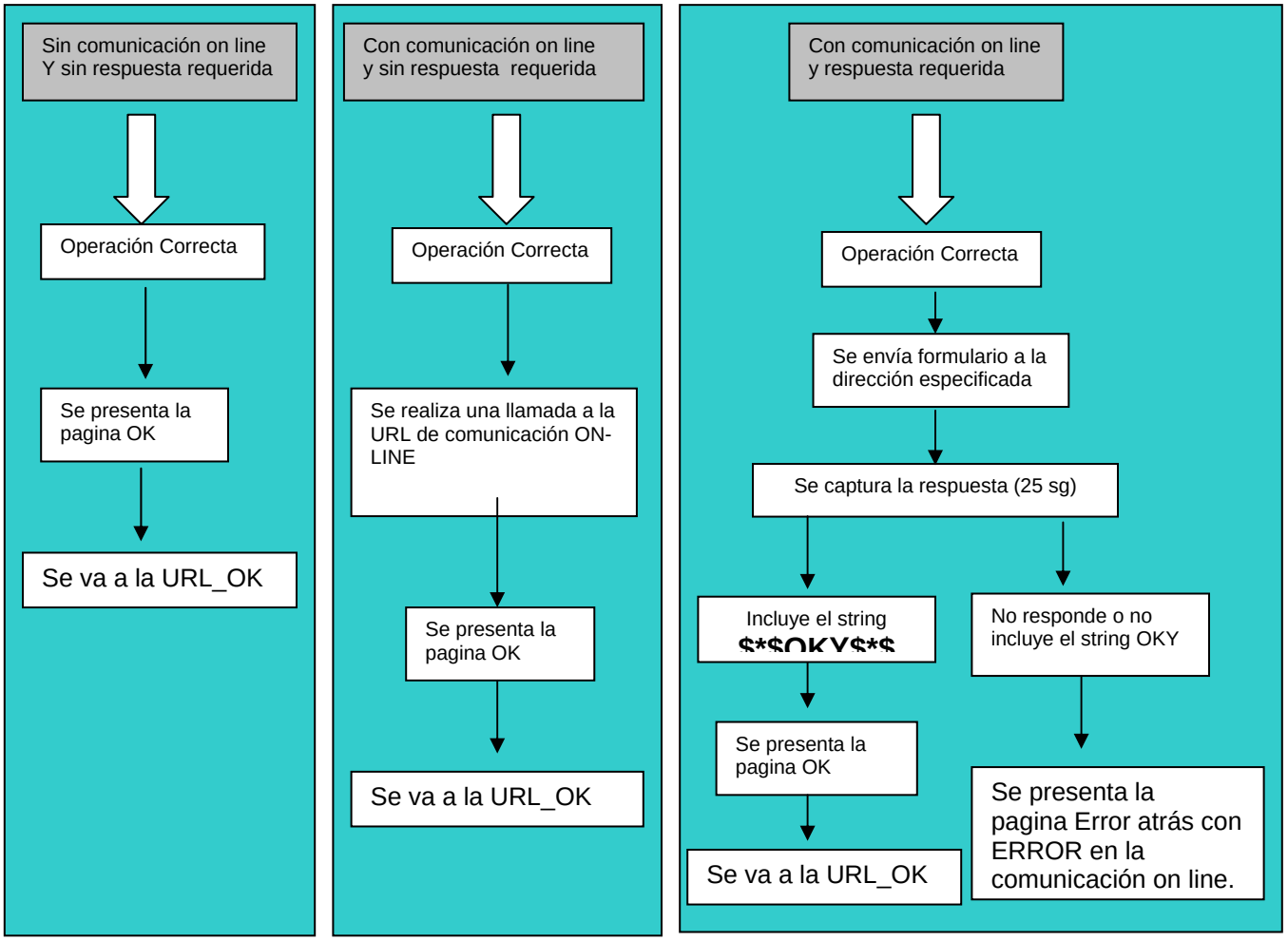
```
<HTML>
<HEAD>
   <TITLE>Respuesta correcta a la comunicación ON-LINE</TITLE>
</HEAD>
  <BODY>
     $*$OKY$*$
  </BODY>
</HTML>
```

Ver y modificar la configuración online actual de su comercio

La activación y modificación de la comunicación ON-LINE, puede ser realizada por el comercio a través de la consola de administración del TPV, dentro del apartado Configuración del comercio.



Esquema del proceso



7.- COMUNICACIÓN BATCH DE LAS OPERACIONES REALIZADAS

Tanto si el Comercio utiliza ó no la facilidad de comunicación ON-LINE de las operaciones de compra realizada por sus clientes, tal y como se describió en el apartado *compras en INTERNET*, CECA podrá generar y enviar al Comercio al final de cada día, un fichero que contendrá el listado de las operaciones efectuadas durante el mismo.

Por motivos de seguridad, este fichero irá cifrado con un algoritmo estándar tripledes (des-ede3-cbc) cuyo clave será la clave de encriptación del comercio en el entorno de producción.

Para descifrar el fichero el comercio puede utilizar el estándar OpenSSL y la instrucción en el caso de un comercio con clave de cifrado 12345678 sería

openssl des3 **-d -k** 12345678 **-in /**tmp/ficherocifrado **-out** /tmp/ficherodescifrado

Mas información en http://www.openssl.org/docs/apps/enc.html

Para el envío de este fichero, el Comercio podrá optar por uno de los siguientes sistemas:

a) **E-MAIL**.- El Comercio deberá determinar la cuenta de correo.

b) **FTP**.- En este caso el Comercio deberá especificar los siguientes datos:

- Nombre ó dirección IP en INTERNET del servidor de FTP.
- Usuario y contraseña de acceso.

El fichero se depositará siempre en el *directorio raíz* del usuario proporcionado, con el nombre *AAAAMMDD*.TPV, correspondiendo *AAAAMMDD* al año, mes y día de la fecha de transmisión respectivamente.

El formato del fichero consistirá en registros de longitud variable, separados unos de otros por los caracteres *RETORNO DE CARRO* (Valor hexadecimal 0x0d) y *SALTO DE LINEA* (Valor hexadecimal 0x0a) con el fin de que sean fácilmente editables en un PC. Dentro de cada registro, los campos irán separados unos de otros por el carácter "**,**" (coma). Cada registro constará de los siguientes campos:

1. ***Tipo de operación***. Puede tomar los valores **C** (compra) o **D** (devolución).
2. ***Fecha*.** Fecha y hora en formato DD/MM/AAAA hh:mm:ss.
3. ***Número de operación***. Número de operación asignado por el comercio.
4. ***Importe.*** Importe sin formatear.
5. ***Referencia.*** Es la referencia asignada por la Pasarela SET/SEP a la operación y que en el caso de una Compra, es necesario conocer para poder efectuar reclamaciones y/o anulaciones posteriores.
6. ***Num*_aut.** Numero de autorización de la operación proporcionada por la entidad resolutora de la operación.

	Para solicitar este envío deberá comunicarlo a través del correo soporte.tpv@ceca.es indicando su código de comercio y forma de envío, así como los datos necesarios especificados anteriormente

8.- CONSULTA/ANULACION DE OPERACIONES REALIZADAS:

Con el fin de que los Comercios puedan consultar y/o anular las operaciones efectuadas por sus clientes, CECA ha instalado en uno de sus servidores WEB seguros, una aplicación accesible desde cualquier navegador, que permite a los comercios realizar un seguimiento online de su actividad. Para mayor información sobre esta herramienta consultar el apartado "**Consola de administración del comercio**" de este manual.

9.- ANULACIÓN ON-LINE DE OPERACIONES

Con objeto de permitir a los Servidores de Comercio solicitar la anulación de operaciones de Compra ON-LINE desde el propio Servidor, es decir, sin necesidad de utilizar la **Consola de administración del comercio**, existe un CGI que permite realizar esta funcionalidad a partir de un formulario HTML generado por el Comercio.

Dentro de la consola de administración del TPV existe un apartado de ayuda donde se explica detalladamente su funcionamiento y la forma de implementarse en el comercio. En caso de que esta operatoria sea de su interés, le rogamos consulte la ayuda.

.

10.- OPERATORIA MULTIMONEDA

La mayoría de los comercios realizan sus operaciones en Euros y así está configurado por defecto. No obstante el TPV de CECA tiene la posibilidad de poder operar en otras divisas. Este tipo de servicio requiere una autorización previa por parte de su Caja.

Dentro de la consola de administración del TPV existe un apartado de ayuda donde se explica detalladamente su funcionamiento y la forma de implementarse en el comercio. En caso de que esta operatoria sea de su interés, le rogamos consulte la ayuda.

11.- GESTOR DE OPERACIONES

El gestor de operaciones o pagos aplazados es una utilidad ofrecida a los comercios a través de la cual se puede realizar una operación en pagos fraccionados. Este tipo de operaciones suele ser utilizadas para servicios de suscripción, reservas con adelanto de una cantidad, pagos aplazados,… Este tipo de servicio requiere una autorización previa por parte de su Caja.

Dentro de la consola de administración del TPV existe un apartado de ayuda donde se explica detalladamente su funcionamiento y la forma de implementarse en el comercio. En caso de que esta operatoria sea de su interés, le rogamos consulte la ayuda.

12.- OPERATORIA AMEX (AMERICAN EXPRESS)

Esta opción no está activada por defecto en ningún TPV. Si un comercio desea operar con este tipo de tarjetas debe realizar los siguientes pasos administrativos antes de realizar los cambios necesarios en la programación del TPV:

1. Contactar con su entidad para ver si es viable utilizar este tipo de tarjetas
2. Dirigirse a American Express (correo electrónico: wthspain@aexp.com) y firmar un acuerdo de adquirencia con esta Compañía
3. Contactar de nuevo con su entidad para que le habiliten este tipo de operaciones en la administración del TPV

	IMPORTANTE Cualquier tema administrativo, consulta de operaciones, reclamaciones, etc, deben ser resueltos entre American Express y el Comercio en función del contrato entre ambas partes y las leyes aplicables en cada momento, los abonos son realizados directamente por American Express al comercio sin pasar por la entidad adquirente del TPV Virtual.

El comercio por defecto no puede utilizar la operativa AMEX, debe contar con el visto bueno de su caja. Seguramente suponga un nuevo contrato entre la Caja – AMEX y el comercio, debe dirigirse a su oficina y tramitar el alta.

Dentro de la consola de administración del TPV existe un apartado de ayuda donde se explica detalladamente su funcionamiento y la forma de implementarse en el comercio. En caso de que esta operatoria sea de su interés, le rogamos consulte la ayuda.

13.- TARJETAS DE PRUEBAS

Con el fin de que los comercios puedan comprobar el correcto funcionamiento de su aplicación, ponemos a su disposición en el entorno de PRUEBAS las siguientes tarjetas:

5540500001000004	Caducidad:	AAAA12 (Diciembre del año en curso) CVV2: 989
5020470001370055	Caducidad:	AAAA12 (Diciembre del año en curso) CVV2: 989
5020080001000006	Caducidad:	AAAA12 (Diciembre del año en curso) CVV2: 989
4507670001000009	Caducidad:	AAAA12 (Diciembre del año en curso) CVV2: 989

	AAAA será sustituido por el año en curso. Las tarjetas se renuevan anualmente. Transcurrido el año en curso, simplemente aumentar un año la fecha.

No existen tarjetas para probar en el entorno de producción, por lo que el comercio deberá probar con sus propias tarjetas y posteriormente anular la operación desde la consola de administración del TPV de CECA

	**Acerca de la petición de datos** La petición de estos dos datos (fecha de caducidad y número de tarjeta), ya bien sea desde el servidor del comercio o bien desde el servidor CECA mediante las paginas a personalizar puede realizarse de distintas formas, así por ejemplo es aconsejable solicitar la fecha a través de un combo de forma que el cliente solo debe elegir una fecha y no se preocupa del formato. Es importante indicar que la fecha de caducidad a introducir en el campo “Caducidad” debe ser estrictamente en el formato AAAAMM, aunque en las páginas se solicite de otra forma, se tendrá que componer a posteriori este formato. El número de tarjeta (campo PAN) deberá ser un número entero sin caracteres extraños o espacios en blanco.

	A partir **del 1 de Abril de 2006** la nueva política de seguridad para comercio electrónico obligará a los comercios que quieran solicitar los datos de tarjeta al cliente y que no quieran delegar esta función en el TPV virtual, deban contar con una autorización expresa de la caja correspondiente y cumplir las condiciones de seguridad y tratamiento de la información impuestas por cada entidad.

	A partir **del 1 de diciembre de 2008** la nueva política de seguridad para comercio electrónico obligará a que todas las operaciones de comercio electrónico sean tramitadas con el valor del CVV2/CVC2 de la tarjeta. Más información en anexo IV Petición de CVV2/CVC2.

14.- TRATAMIENTO DE ERRORES.

En las páginas de error se puede visualizar un código de error de rechazo de la operación, ya bien sea debido a la propia aplicación o bien al rechazo por parte del emisor de la operación. Este código viene recogido en el parámetro “COD_AUT”, que para las compras correctas siempre será de valor “000” y para las anulaciones correctas “400” (“900” para anulaciones parciales). El resto de valores representa un código de error.

Cod. Autorización	Mensaje
0	Operación aprobada
1	COMUNICACION ON-LINE INCORRECTA
2	ERROR AL CALCULAR FIRMA
5	ERROR. Error en el SELECT COMERCIOS <%d>
6	ERROR. Faltan campos obligatorios
7	ERROR. MerchantID inexistente <%d>
9	ERROR. No se pudo conectar a ORACLE <%d>
10	ERROR. Tarjeta errónea
12	FIRMA: %s-%s
13	OPERACION INCORRECTA
14	ERROR. Error en el SELECT OPERACIONES <%d>
15	ERROR. Operación inexistente <%d>
16	ERROR. Operación ya anulada <%d>
17	ERROR AL OBTENER CLAVE
18	ERROR. El ETILL no acepta el pedido
20	ERROR. Tipo de moneda no valido. La operación debe realizarse en Euros
21	ERROR. El comercio tiene un filtro que no permite esta operación
22	ERROR. El comercio tiene un filtro que no permite esta operación
23	ERROR. Operación UCAF no autorizada. Importe (%d) mayor del limite establecido (%d).
19	ERROR. Datos no numéricos
20	ERROR. Datos no alfa-numéricos
21	ERROR en el calculo del MAC
22	ERROR en el calculo del MAC [%s - %s][cadena:%s]
23	ERROR. Usuario o password no valido.
24	ERROR. Tipo de moneda no valido. La operación debe realizarse en Euros.
25	ERROR. Importe no Integer.
26	ERROR. Operación no realizable 100.
27	ERROR. Formato CVV2/CVC2 no valido.
28	ERROR. Debe especificar el CVV2/CVC2 de su tarjeta.
29	ERROR. CVV2 no Integer.
30	ERROR. En estos momentos no es posible continuar sin cvc2/cvv2
31	ERROR. ERROR en la operatoria del comercio.
32	ERROR. Tipo de moneda no valido. La operación debe realizarse en Euros.
33	ERROR. El comercio solo puede realizar pagos en Euros
34	ERROR. Moneda o conversión no valida para esta tarjeta.[%d]
35	ERROR. Moneda o conversión no valida.[%d]
36	ERROR. Conversión a Euros no válida [%s][%s].
37	ERROR. El comercio no dispone de esta opción.
38	ERROR. Respuesta Errónea del Gestor de operaciones. [%d][%s].

39	ERROR. No es posible continuar con la preautorizacion.
40	ERROR. Error de comunicaciones Lu´s. No es posible finalizar la operación.
41	ERROR. TimeOut SEP. No es posible finalizar la operación.
42	ERROR. SEP devuelve un 20 ERROR. No es posible finalizar la operación.
43	ERROR. Error inesperado. No es posible finalizar la operación [%d].
44	ERROR. Respuesta Errónea de SEP. No es posible finalizar la operación.
45	ERROR. No es posible continuar con la preautorización.
46	ERROR. Error en el proceso de Autentificación. No retroceda en el navegador. Debe volver al comercio y reintentar el pago.
47	ERROR. Entidad no disponible. Inténtelo dentro de unos minutos
48	ERROR. Error en el proceso de Autentificación. Respuesta PAREQ no valida [%d]. No retroceda en el navegador. Debe volver al comercio y reintentar el pago.
49	ERROR. Error en el proceso de Autentificación. Respuesta PAREQ de su entidad no valida: %s,TXSTATUS
50	ERROR. Fallo en el proceso de Autentificación. Es necesario una identificación positiva para finalizar el proceso de compra: %s,TXSTATUS
51	ERROR. Fallo en el proceso de Autentificación. El comercio no acepta pagos no seguros: %s. Póngase en contacto con la entidad emisora de su tarjeta.,TXSTATUS
52	ERROR. En estos momentos no es posible iniciar un pago seguro
53	ERROR. Comercio seguro. Su tarjeta no admite autentificación y no puede operar en este comercio [%s]. Póngase en contacto con la entidad emisora de su tarjeta.
54	ERROR. No es posible iniciar un pago seguro y el importe supera el máximo permitido (%f <= %s). [Resultado: %s]
55	ERROR. En este momento no es posible iniciar un pago seguro. [Resultado: %s]
56	ERROR. No es posible iniciar un pago seguro y el importe supera el máximo permitido (%f <= %s). [Resultado: %s]
57	ERROR. En este momento no es posible iniciar un pago seguro y el importe supera el máximo permitido (%f <= %s). [Resultado: %s]
58	ERROR. En este momento no es posible iniciar un pago seguro. [Resultado: %s]
59	ERROR. El comercio tiene un filtro que no permite esta operación.
60	ERROR. El Comercio solo admite pago seguro. Necesita autentificarse para continuar.
61	ERROR. Operación segura no permitida. Importe (%14.2f) mayor del limite establecido (%14.2f).
62	ERROR. El comercio tiene un filtro que no permite esta operación.(Filtro2:%d)
63	ERROR. El comercio no acepta pagos Visa no autentificados. Póngase en contacto con su entidad para activar este tipo de pago.
64	ERROR. El comercio no acepta pagos MasterCard no autentificado. Póngase en contacto con su entidad para activar este tipo de pago.
65	ERROR. El comercio no acepta pagos no autentificados. Póngase en contacto con su entidad para activar este tipo de pago.
66	ERROR. Error de proceso. El comercio no acepta pagos no autentificados. Póngase en contacto con su entidad para activar este tipo de pago.
67	ERROR. Operación segura no autorizada. Importe (%14.2f) mayor del limite establecido (%14.2f).
68	ERROR. Respuesta Errónea del Gestor de operaciones. Operación anulada [%s].Gestor: [%d][%s].
69	ERROR. Operatoria UCAF no valida. Póngase en contacto con su comercio o caja.
100	Tarjeta no válida (en negativos)
101	Tarjeta caducada
104	Tarjeta no válida (electrón)
106	Tarjeta no válida (reintentos de PIN)

111	Número de tarjeta mal tecleado (check)
112	Tarjeta no válida (se exige PIN)
114	No admitida la forma de pago solicitada
116	Saldo insuficiente
118	Tarjeta no válida (no existente en ficheros)
120	Tarjeta no válida en este comercio
121	Disponible sobrepasado
123	Número máximo de operaciones superado
125	La tarjeta todavía no es operativa
180	Tarjeta no soportada por el sistema
190	Operación no realizable (resto de casos)
400	Anulación aceptada
480	Anulación por TO aceptada sin encontrar la operación original
900	Devolución aceptada
904	Operación no realizable (error de formato)
908	Tarjeta desconocida
909	Operación no realizable (error de sistema)
912	Su entidad no está disponible
913	Operación no realizable (clave duplicada)
914	No existe la operación a anular
930	Operación no realizable (caja merchant no válida)
931	Operación no realizable (comercio no dado de alta)
932	Operación no realizable (bin merchant no existe)
933	Operación no realizable (sector desconocido)
940	Ya recibida una anulación
944	Operación no realizable (sesión no válida)
948	Operación no realizable (fecha/hora inválida)
950	Devolución no aceptada
999	Operación no realizable (resto de casos)

	El error más habitual será el 190 que es la denegación por el emisor de la tarjeta. El TPV pide la autorización a la entidad emisora y esta deniega sin especificar una causa exacta de denegación. Deberá el cliente ponerse en contacto con su entidad para saber la causa exacta, es esta la única forma de conocer la causa exacta de esta denegación

15.- CONSOLA DE ADMINISTRACIÓN TPV VIRTUAL PARA COMERCIOS

El comercio dispone de una consola de Administración del TPV de CECA para realizar las siguientes operaciones:

- Comparativa de operaciones por día
- Consulta de operaciones.
- Informes diarios de operaciones
- Anulación de operaciones
- Pagos periódicos o gestor de operaciones
- Realizar un pago desde la consola
- Realizar un pago por email
- Modificar la configuración del comercio
- Dar de alta filtros para evitar determinadas operaciones
- Dar de alta nuevos usuarios para acceso a la consola.
- …

Desde la consola puede acceder a una ayuda online sobre estas funcionalidades, así como la descarga de una manual en PDF con este contenido.

15.1.- Acceso

La dirección establecida para el acceso a la consola de administración del TPV virtual es:

https://comercios.ceca.es

El usuario y password de acceso serán proporcionados en el correo de bienvenida recibido por el comercio. En caso de no conocer la clave o haberla olvidado, en la pantalla de identificación existe un enlace de recordar clave donde puede recuperarla. Para ello se le enviará un correo con las instrucciones necesarias a la dirección de email que su Caja ha dado de alta.

16.- DIRECCIONES DE SOPORTE TPV

Si necesitan resolver cualquier duda relacionada con este producto, deben inicialmente ponerse *siempre* en contacto con su **Caja de Ahorros**.

Para cualquier problema relacionado con la implementación del TPV virtual en su comercio, pueden ponerse en contacto con la dirección de correo electrónico soporte.tpv@ceca.es y teléfono 915965328.

	Le recomendamos que antes de contactar con el soporte del TPV de las Cajas de Ahorros consulte el apartado de preguntas frecuentes, ya que en la mayoría de los casos en ese apartado se encuentra la solución al problema.

PREGUNTAS FRECUENTES.

Al intentar operar me aparece un error:
Al realizar una operación se pueden producir diversos errores. En el capítulo de Cómo realizar un pago aparece un apartado con los errores más frecuentes. Le rogamos consulte dicho apartado antes de ponerse en contacto con el soporte TPV de CECA, ya que están recogidos la mayoría de los mismos indicando el motivo y la solución.

¿Cómo puedo saber desde mi aplicación si la operación realizada ha sido correcta?
Para ello existe la comunicación online. Consulte el apartado 8 Comunicación on-line de este manual. No es recomendable usar la URL_OK para esta tarea ya que entonces se depende de la navegación del usuario, es decir, de que el usuario pinche el botón ok, cosa que no siempre ocurre a veces cierran pulsando el aspa directamente.

Aparece una compra y a continuación una anulación con un intervalo de menos de un minuto:
Normalmente este tipo de error es debido a que la comunicación online que el comercio tiene activada ha fallado y el comercio tiene activada la respuesta requerida. Cuando no se recibe respuesta por parte del comercio al invocar a la url de la comunicación online se procede a la anulación de la operación. Revise que la comunicación online funciona correctamente.

La operación ha finalizado correctamente pero no se ha realizado la comunicación on-line
Si se realiza una compra en la web del comercio y en el mismo navegador web, compartiendo cookies, se encuentra la Web de administración abierta o ha estado abierta, no se produce el proceso de comunicación on-line aunque la operación se realiza de forma correcta. Debe reiniciar el navegador WEB o abrir sesiones distintas de navegación.

¿Qué tengo que hacer para pasar de pruebas a producción?
Pasar de pruebas a real es tan sencillo como cambiar el valor de la clave de cifrado y la dirección del actión a donde envías los datos, pasando de

clave_encriptacion = “clave de pruebas”
http://tpv.ceca.es:8000/cgi-bin/tpv

a

clave_encriptacion = “clave de real”
https://pgw.ceca.es/cgi-bin/tpv

Los datos de la clave de encriptación puedes consultarlo en la consola de administración del TPV. El entorno de pruebas sigue activo aunque el comercio pase a real.

En resumen, el paso a real puedes hacerlo cuando quieras, aunque conviene avisar a tu Caja de la entrada en producción para estar pendiente de posibles incidencias en medios de pago.

¿Existen tarjetas para probar en el entorno de producción?
Existen tarjetas de prueba para el entorno de desarrollo. Para el entorno de producción son necesarias tarjetas de verdad y que soporten autenticación si el comercio es seguro.

¿Cómo puedo acceder a la consola de administración del comercio?
Desde la dirección https://comercios.ceca.es puede acceder a la consola de administración del TPV de CECA. Consulte el apartado de ayuda denominado Consola de administración TPV Virtual para Comercios para obtener más información.

RECOMENDACIONES.

- Desde el TPV virtual siempre recomendamos que en los procesos de actualización de tablas, bases de datos o actualización de registros por parte del comercio con el fin de confirmar inmediatamente la terminación de una transacción se realice utilizando la llamada “Comunicación on line” que se explica en este mismo manual y nunca a través de las paginas y el proceso de navegación del cliente.
- En este proceso de Comunicación on line es conveniente
    - Verificar que el valor de referencia no está vacío.
    - Recalcular la firma para comprobar el origen y valor de la referencia.
    - Verificar que número de operación e importe se corresponden con una operación pendiente de pago.
    - Verificar dirección IP de procedencia
    - Y en los casos posibles utilizar una dirección HTTPS.
- Se recomienda la generación del número de operación de forma que estos no se repitan. En caso de ser un número cíclico que su periodo de repetición sea tan grande que sea imposible completar un ciclo.

- **Administración de password y acceso al comercio.**
    - Recomendamos enérgicamente que el password de acceso a los entornos de administración se cambie la primera vez de uso y que en este cambio se indique una password mayor de 8 dígitos, que sea alfanumérica con al menos 3 dígitos numéricos y de una complejidad relativa. También puede incorporar distinción entre mayúsculas y minúsculas.

Recomendaciones de la Agencia de Protección de Datos.

La Agencia Española de protección de datos, entidad cuya misión es velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos, edita unas interesantes recomendaciones para el sector de comercio electrónico que es conveniente conocer, estudiar y aplicar. Desde el TPV virtual aconsejamos que el comercio siga todas las recomendaciones que esta entidad dicta. Desde la WEB

https://www.agpd.es/

se puede acceder a esta y otras documentaciones. En la sección “Protegiendo sus datos” – “Recomendaciones” puede encontrar estas recomendaciones.

https://www.agpd.es/index.php?idSeccion=75

La documentación PDF puede encontrarse en*:

https://www.agpd.es/upload/recomendaciones_comercio_electronico_pdf.pdf

(* Esta dirección podría variar, se recomienda el acceso desde la pagina principal)

CONTROL DE VERSIONES:

01/12/2009 Versión 4.5

- Revisión íntegra del manual

14/01/2010 Versión 4.6

- Modificar el apartado de American Express para introducir los pasos administrativos a seguir por el comercio

17/02/2010 Versión 4.7

- Modificar el apartado de American Express para hacer referencia al documento "REQUISITOS PARA UTILIZAR EL NOMBRE Y EL LOGO DE AMERICAN EXPRESS® EN SU SITIO WEB" proporcionado por AMEX
- Inclusión de cifrado por SHA1

27/05/2010 Versión 5.0

- Inclusión de la nueva consola del TPV

01/09/2010 Versión 6.0

- Revisión completa del manual