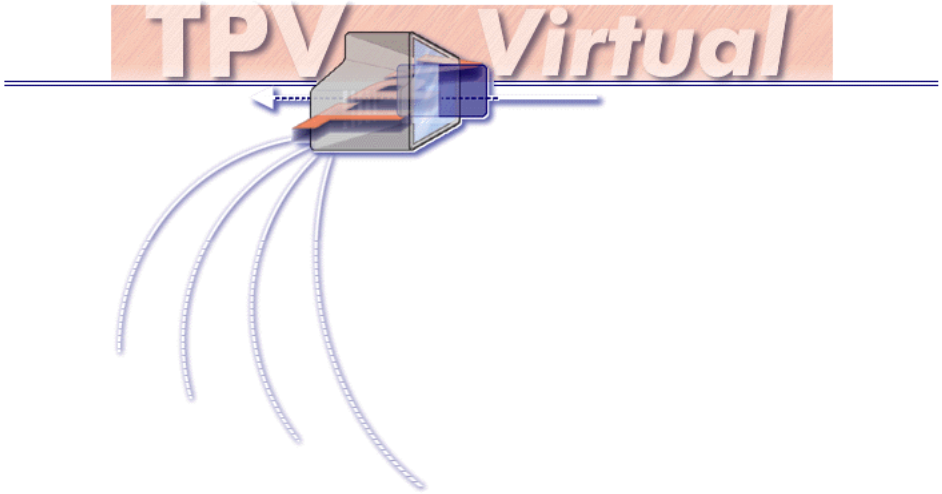
cecabank

SERVICIOS FINANCIEROS

TPV VIRTUAL 8.12
MANUAL DE IMPLEMENTACION PARA COMERCIOS



Cecabank.
Email:tpv@cecabank.es

CONTENIDO

CONTENIDO 2
1.- INTRODUCCIÓN: 2
1.1-Características más importantes: 3
2.- POR DÓNDE EMPEZAR: 4
3.- TIPOS DE COMERCIOS: 5
3.1- Estándar/Seguro: 5
3.2- Inseguro: 6
3.3- Mixto: 6
4.- MODULOS DE PAGO PARA SOLUCIONES DE COMERCIO ELECTRÓNICO DE TERCEROS 6
5.- CÓMO REALIZAR UN PAGO 7
5.1 Ejemplos de formularios 10
(a) Ejemplo de llamada en la que los datos de tarjeta son solicitados por el TPV 10
(b) Ejemplo de llamada en la que los datos de tarjeta son solicitados por el comercio 11
6.- CÁLCULO DE LA FIRMA 12
Opción cifrado=SHA2 13
Opción cifrado=SHA21 13
7.- COMUNICACIÓN ON-LINE 14
7.1- Comunicación online con respuesta requerida 16
8.- COMUNICACIÓN BATCH DE LAS OPERACIONES REALIZADAS 20
9.- CONSULTA/ANULACION DE OPERACIONES REALIZADAS: 21
10.- ANULACIÓN ON-LINE DE OPERACIONES 21
11.- OPERATORIA MULTIMONEDA 21
12.- GESTOR DE OPERACIONES 21
13.- TOKENIZACIÓN 22
14- OPERATORIA AMEX (AMERICAN EXPRESS) 22
15.- TARJETAS DE PRUEBAS 22
16.- OTRAS FORMAS DE PAGO. 24
17.- SDK PARA INVOCAR AL TPV-VIRTUAL DESDE UNA APP 25
18.- PREAUTORIZACIONES 25
19.- ERRORES MÁS FRECUENTES 25
20.- TRATAMIENTO DE ERRORES. 27
21.- CONSOLA DE ADMINISTRACIÓN TPV VIRTUAL PARA COMERCIOS 30
21.1.- Acceso 30
22.- DIRECCIONES DE SOPORTE TPV 32
23.- PARÁMETROS ACS 2.x 33
24.- USO DE EXENCIONES Y OPERACIONES FUERA DE AMBITO 33
OPERACIONES FUERA DE AMBITO: 33
EXENCIONES: 34
25.- PREGUNTAS FRECUENTES. 36
26.- RECOMENDACIONES. 38
CONTROL DE VERSIONES: 39

1.- INTRODUCCIÓN:

En este documento se describen las características del TPV virtual ofrecido por Cecabank. 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 Cecabank, 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.

1.1-Características más importantes:

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

- **Uso protocolo https.-** El *CLIENTE* sólo necesita disponer de un navegador WEB que soporte TLSv1.0, TLSv1.1 y TLSv1.2 (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 Cecabank.

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 por https.

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.

- **<u>Pago 3D-Secure (Verified by Visa / Mastercard SecureCode.-</u>** 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 Cecabank 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 por https
- ***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.*** <u>En general</u> 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 CECABANK"

Desde Cecabank 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 Cecabank 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 Cecabank.

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. 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.

3.1- Estándar/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.

3.2- 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.

3.3- 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.- MODULOS DE PAGO PARA SOLUCIONES DE COMERCIO ELECTRÓNICO DE TERCEROS

Actualmente en el mercado existen soluciones de comercio electrónico de terceros para los cuales se dispone de módulos de pago para que puedan ser instalados y resolver de una forma sencilla la implementación del TPV-Virtual.

Actualmente los módulos de pago que se disponen son para

- Woocommerce.
- Prestashop

- Oscommerce
- Magento

Si el comercio está interesado en el uso de estos módulos de pago, debe enviar un correo a tpv@cecabank.es solicitando que se le envíe la documentación relativa a su descarga e implementación.

ⓘ	Si es usuario de uno de estos módulos, de este documento los apartados que le pueden interesar son los que se encuentran a partir del 14- OPERATORI A AMEX.

5.- 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 Cecabank 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.

ⓘ	En Preguntas frecuentes 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 Cecabank, 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 Entidad en el proceso de alta
AcquirerBIN	Requerido	10	Identifica la Entidad. Facilitado por la Entidad en el proceso de alta.
TerminalID	Requerido	8	Identifica al terminal. Facilitado por la Entidad 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	12	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	Requerid	1	Actualmente siempre será 2

	o		
URL_OK	Requerido	500	URL completa (http://…). Es la URL determinada por el comercio a la que Cecabank 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 Cecabank 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 utlizando un SHA2.
Cifrado	Requerido	4	Actualmente este campo puede tomar 2 valores: • SHA2 → Utilizado por la mayoría de los comercios. El campo descripción no va incluido en la firma • SHA21 → Utilizado por los comercios que necesitan comprobar la integridad del campo descripción. Es decir, introducen en el campo descripción datos que en el caso de que se modifique por un tercero produciría un descuadre en su operativa
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 con información adicional útil para uso interno del comercio.
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 Entidad 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 Entidad 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 Entidad 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.
Sesion	Opcional		Si incluimos el parámetro Sesion en el formulario, por

			ejemplo ***Sesion=true***, permitimos la entrada de datos de la tarjeta por un espacio máximo de tiempo de 1500 segundos
Exencion_SCA	Opcional		Tipo de Exención a aplicar. En caso de que no se envíe se aplicará la configuración de las exenciones configuradas por la entidad en la consola del tpv-virtual (LOW, MIT, TRA,NONE
datos_acs_20	Opcional		En este campo se incluirá un JSON con una serie de datos que serán tratados por el TPV-Virtual para la nueva versión de 3dsecure 2.0 (Comercio seguro 2.0). El detalle de este campo así como su uso son tratados en el apartado "23 Parámetros ACS 2.0". **Este campo se tiene que enviar en Base64.**
firma_acs_20	Opcional		Firma en sha2 del campo datos_acs_20 anteponiendo por delante la clave de cifrado del comercio SHA2(Clavecifrado+ datos_acs_20)
inicioBizum	Opcional	1	0/1. Indica si se va directamente a Bizum sin pasar por la pantalla de petición de selección de forma de pago. Si este campo no viaja o su valor es 0 se montrará la pantalla mencionada anteriormente.
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 comunicación 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
14.- Ruso 15.- Noruego

El campo ACTION del formulario apuntará a una URL de un Servidor WEB de Cecabank 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 Cecabank consta de dos entornos en funcionamiento, Uno para pruebas y otro para producción. A continuación mostramos sus direcciones:

https://tpv.ceca.es/tpvweb/tpv/compra.action ENTORNO DE DESARROLLO

https://pgw.ceca.es/tpvweb/tpv/compra.action ENTORNO DE PRODUCCIÓN

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

5.1 Ejemplos de formularios

(a) 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 Entidad, 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/tpvweb/tpv/compra.action" 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=“SHA2”>
<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”>
<INPUT NAME="datos_acs_20” TYPE=hidden VALUE=”## datos_acs_20 ##”>
<INPUT NAME="firma_acs_20” TYPE=hidden VALUE=”## firma_acs_20##”>
<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.

(b) 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 Entidad para que le sea autorizada. Si el comercio utiliza esta opción y no la tiene permitida por su entidad le aparecerá un error 031 “Operación no permitida”

```
<HTML>
<HEAD>
<TITLE>P&aacute;gina de pago</TITLE>
</HEAD>
<BODY>
<FORM ACTION=" https://pgw.ceca.es/tpvweb/tpv/compra.action" 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=“SHA2”>
<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">
<INPUT NAME="datos_acs_20" TYPE=hidden VALUE="## datos_acs_20 ##">
<INPUT NAME="firma_acs_20" TYPE=hidden VALUE="## firma_acs_20##">
<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

6.- 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: **SHA-256.** El resultado se debe codificar en HEXADECIMAL con letras minúsculas.La mayoria de los lenguajes de programación tienen una función propia que calcula este valor.

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

Cadena:
SHA256("1143904411195002800005540520000000322 1__0.6753030012614888330000
0000000197821200353047091222143401060070 00")

```
Resultado:
bbe1a297df02b07d1eebf72627eb7ac4038e9fb11c1a867ca13536888f46b7ca
```

Algunos ejemplos de cadenas cifradas son:

```
SHA256("El coche amarillo")  =
91a736731a4281666fa562ed7eb5e7dbe451f92c7d973c307bc060959d6b1012
```

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 SHA-256.

ⓘ	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 SHA-256 pasamos a explicar la forma de calcular la firma para su implementación en el comercio.

Opción cifrado=SHA2

(Utilizado por la mayoría de los comercios)

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

Ejemplo:
Clave encriptacion: 99888888 (no viaja en el formulario)
MerchantID: 111950028
AcquirerBIN: 0000554052
TerminalID: 00000003
Num_operacion: 123
Importe: 500
TipoMoneda: 978
Exponente: 2
Cifrado: SHA2
Exencion_SCA

URL_OK: http://www.ceca.es
URL_NOK: http://www.ceca.es
La Cadena_sha2 a firmar será la siguiente:
9988888811195002800005540520000000312350097 82SHA2http://www.ceca.eshttp://www.ceca.es

La firma_calculada será:
2b7f686593f1a424c510321e4bc354d21924e02e980a90f4d46c41f92a06f5a9

Opción cifrado=SHA21

Utilizado por los comercios que necesitan comprobar la integridad del campo descripción. Es decir, introducen en el campo descripción datos que en el caso de que se modifique por un tercero produciría un descuadre en su operativa

La cadena a firmar se va a componer con la concatenación de los siguientes campos:
Clave_encriptacion+MerchantID+AcquirerBIN+TerminalID+Num_operacion+Importe+TipoMoneda+Exponente+Cifrado+URL_OK+URL_NOK + Descripcion + Exencion_SCA

Ejemplo:
Clave encriptacion: 99888888 (no viaja en el formulario)
MerchantID: 111950028
AcquirerBIN: 0000554052
TerminalID: 00000003
Num_operacion: 123
Importe: 500
TipoMoneda: 978
Exponente: 2
Cifrado: SHA2
URL_OK: http://www.ceca.es
URL_NOK: http://www.ceca.es
Descripcion:Esta es la descripcion
Exencion_SCA
La Cadena_sha2 a firmar será la siguiente:
9988888811195002800005540520000000312350097 82SHA2http://www.ceca.eshttp://www.ceca.esEsta es la descripcion

La firma_calculada será:
e87e737f9287984bfdc213ee27b3f5366692d661998109bf096e77e97ea49fa2

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+"SHA2"
.

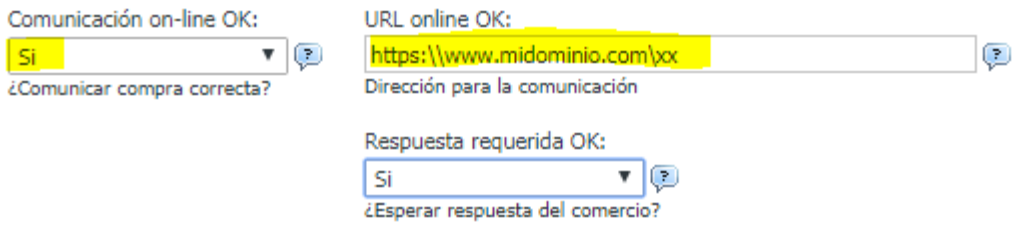
7.- COMUNICACIÓN ON-LINE

La comunicación on-line es utilizada por el comercio que necesita que las operaciones de *COMPRA* realizadas por sus clientes le sean comunicadas en el momento de producirse. Consiste en la creación de una url 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 Cecabank. Si el usuario no pulsa el botón ACEPTAR o decide cerrar la pantalla al mostrarle la página de confirmación de compra del TPV de Cecabank, 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 Cecabank 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 configurarla desde el apartado de configuración en la consola de administración del TPV-Virtual.



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 Entidad en el proceso de alta
AcquirerBIN	10	Identifica la Entidad. Facilitado por la Entidad 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	12	Importe de la operación sin formatear. Siempre será un número entero donde los dos últimos dígitos serán los céntimos de Euro. Si se desea validar la firma recibida en el comercio, este campo siempre tiene longitud fija de 12 dígitos, relleno con ceros a la izquierda.
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 Cecabank siguiendo las indicaciones explicadas a continuación y firmada por SHA-256.
Codigo_pedido	50	Actualmente sin valor, en desuso.
Codigo_cliente	50	Actualmente sin valor, en desuso.
Codigo_comercio	50	Actualmente sin valor, en desuso.
Num_aut	6	Valor asignado por la entidad emisora a la hora de autorizar una operación. Este valor contiene dígitos alfanuméricos.
BIN	6	BIN de la tarjeta, los primeros 6 dígitos de su numeración.
FinalPAN	4	Los 4 últimos dígitos de la tarjeta
Cambio_moneda	8	Tipo de cambio aplicado en el importe de la operación. Contendrá 1 en todos los pagos que sean en Euros.
Idioma	2	Idioma de la operación
Pais	3	Código ISO del país de la tarjeta que ha realizado la operación
Tipo_tarjeta	1	Valores "CRE" credito y "DEB" débito
Tipo_operacion	3	Indica el tipo de operación. Puede tomar uno de los siguientes valores A → Compra AMEX C → Compra normal (Valor más normal) E → Compra Bizum G → Autorización no contable o preautorización H → Cobro de autorización o presentación
Descripcion	200	Los 200 primeros caracteres de la descripción

La cadena a firmar la va a componer Cecabank con la concatenación de los siguientes campos:

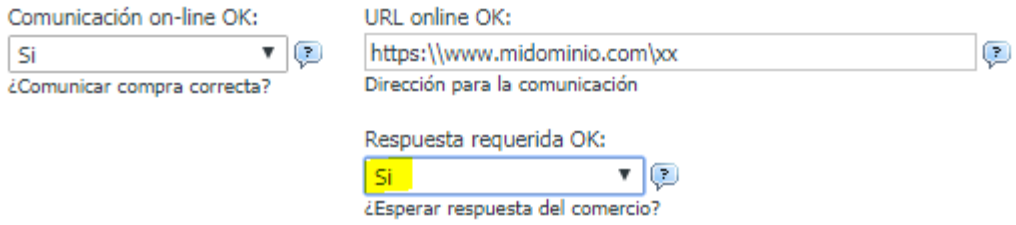
Clave_encriptacion+MerchantID+AcquirerBIN+TerminalID+Num_operacion+Importe+Tipo Moneda+Exponente+Referencia

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.….

7.1- 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:

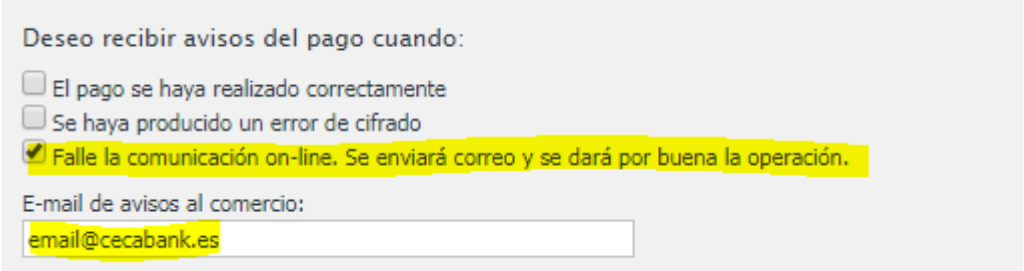


- **Comunicación ON-LINE sin respuesta requerida** . En este caso, una vez realizado el pago, el TPV virtual de Cecabank intentará comunicar la operación al comercio, pero dará por realizada correctamente la operación aunque dicha comunicación no sea posible. Es más, ni siquiera esperará recibir una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

- **Comunicación ON-LINE con respuesta requerida**. En este caso, una vez realizado el pago, el TPV virtual de Cecabank intentará comunicar la operación al comercio y este debe de responder con los siguientes patrones:
  - $*$OKY$*$ → Operación correcta y actualizada la BBDD
  - $*$NOK$*$ → Operación incorrecta y se debe de anular la operación. (Un ejemplo sería rotura de stock)

Para la comunicación de esta operatoria existe un time-out de 30 segundos. Si en ese tiempo el comercio no ha respondido o devuelve algún valor fuera de los 2 mencionados anteriormente, por defecto la operación será anulada. Este funcionamiento puede provocar descuadres en el comercio, sobre todo en el caso de que el comercio responda con $*$OKY$*$ y se pierda la comunicación, se tarde más de 30 segundos o haya un fallo a la hora de presentar la respuesta, ya que el comercio la habrá dado por buena, pero el tpv-virtual la habrá anulado. Para evitar este descuadre existe la comunicación online por email, que es un mecanismo de backup, el cual será llamada SÓLO en el caso de que el comercio tenga activada la respuesta requerida y no responda o no devuelva ninguno de los valores antes mecionados. En este caso si el comercio tiene habilitada esta opción se procederá a enviar un email y se dará la operación por buena. El comercio, al recibir este email deberá de hacer 2 cosas.

1.- Marcar la operación como pagada
2.- Revisar el motivo por el que la comunicación online ha fallado, ya sea por tiempo excesivo, Servidor no responde, o error en la respuesta.



Un ejemplo de la respuesta OK del comercio podría ser

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

Un ejemplo de la respuesta NOK del comercio podría ser

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

Un ejemplo del email que recibirá el comercio será el siguiente

Aviso TPV virtual. Operación realizada. Error de comunicación on-line
noreply para: email@dominio.com
07/10/2019 09:07
Mostrar detalles

```
AVISO POR EMAIL. OPERACIÓN REALIZADA. ERROR DE COMUNICACION ONLINE
FECHA: 07/10/2019 09:07:51

Se ha producido un error de comunicación online en la operación de comercio electrónico con estos datos. Aunque tiene
configurada la opción de respuesta requerida, no se procede a anular esta operación debido a que la comunicamos por e-mail.
Por favor, revise el estado de la operación en su aplicación.

- Entorno: Producción
- Nombre de Comercio:  Mi comercio
- Código de comercio:  999999999
- Terminal: 00000003
- Número de operación: 1234567890
- Importe: 0.05
- Moneda: 978
- Descripción: -TPV04-S-
- Error: Respuesta incorrecta
- Mas información: https://comercios.ceca.es
Este correo se ha enviado de forma automática. Por favor, no responda a este correo. Para cualquier duda o aclaración
contacte con tpv@cecabank.es
```

8.- 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*, Cecabank 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

Más 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:

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

β) **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 tpv@cecabank.es indicando su código de comercio y forma de envío, así como los datos necesarios especificados anteriormente

9.- CONSULTA/ANULACION DE OPERACIONES REALIZADAS:

Con el fin de que los Comercios puedan consultar y/o anular las operaciones efectuadas por sus clientes, Cecabank 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.

10.- 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.
.

11.- OPERATORIA MULTIMONEDA

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

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.- 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 Entidad.

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.- TOKENIZACIÓN

El servicio de tokenización consiste en generar un código a una tarjeta de un cliente que pueda ser utilizado por el comercio para poder lanzar operaciones posteriores sin tener que pedir de nuevo la tarjeta en el proceso de pago.

Para que un comercio pueda operar con el sistema de Tokenización debe estar configurado para ello solicitándolo al soporte del TPV virtual (tpv@cecabank.es) y debe utilizar la Comunicación on line para poder recoger el código token asignado.
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.

14- 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 Entidad. Seguramente suponga un nuevo contrato entre la Entidad – 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.

15.- 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 Cecabank

ⓘ	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 Cecabank 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 Entidad 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.

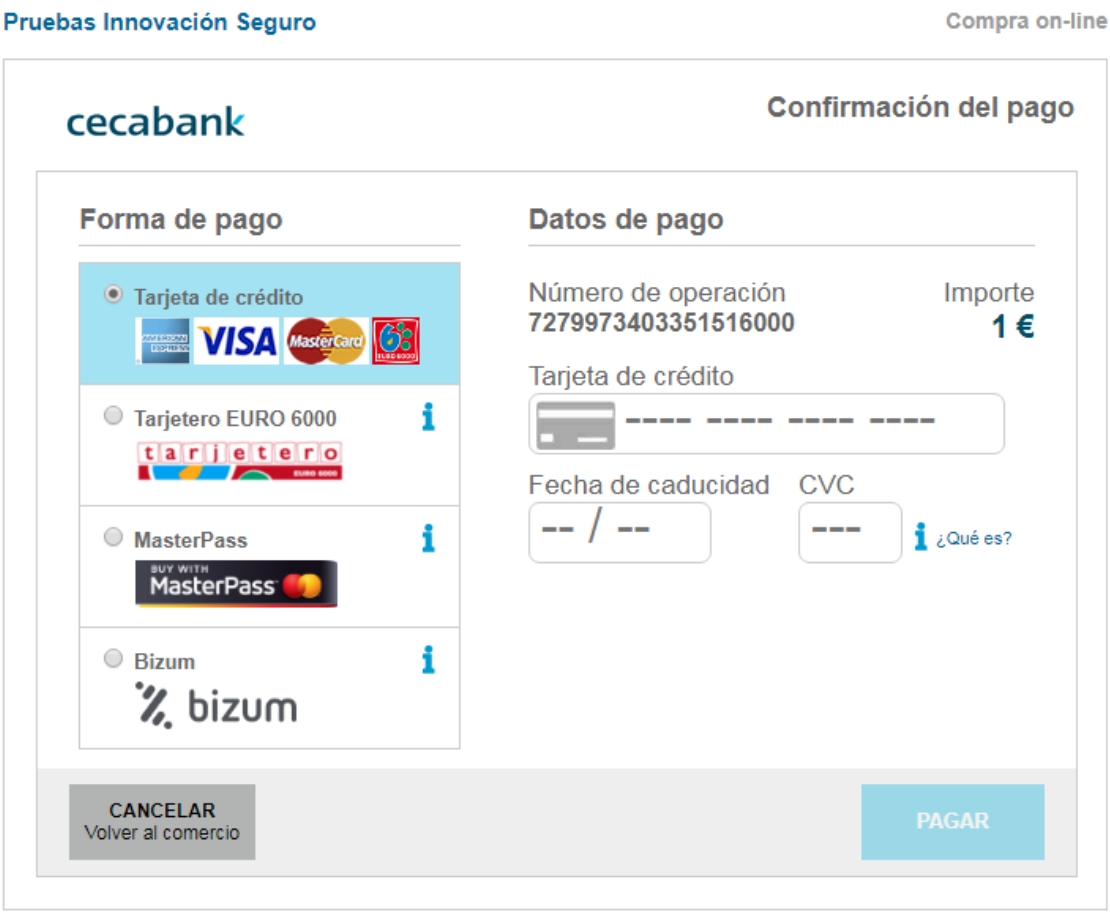
16.- OTRAS FORMAS DE PAGO.

Además del pago con tarjeta, el TPV-Virtual soporte otras formas de pago alternativas de las cuales puede beneficiarse de ellas y para la cual no requiere de ningún desarrollo adicional por parte del comercio.

Es posible que en alguna de ellas requiera la firma de un acuerdo con la empresa que da soporte a esa forma de Pago. En el caso de que el comercio quiera hacer uso de alguna de ellas y no le aparezca en la página de pago de petición de datos bancarios (ver imagen adjunta), debe de ponerse en contacto con el soporte técnico del tpv-virtual (tpv@cecabank.es) en donde le podrán dar información detallada.

Las formas de pago alternativas al pago con tarjetas que están disponible en el TPV-Virtual son

- Masterpass (Solución de Pago de Mastercard)
- Tarjetero E6000 (solución de pago de Euro 6000)
- Bizum



17.- SDK PARA INVOCAR AL TPV-VIRTUAL DESDE UNA APP

Aunque el TPV-Virtual se puede invocar desde una APP con lo descrito anteriormente abriendo un navegador desde la propia APP, se dispone de un SDK para este tipo de desarrollos. Este desarrollo está disponible para Android y para IOS.

Si el comercio está interesado en el uso de este SDK, debe enviar un correo a tpv@cecabank.es solicitando este tipo de implementación para que se le envíe la documentación correspondiente.

18.- PREAUTORIZACIONES

Una preautorización o autorización no contable es una operación en la cual se hace un primer paso que se llama "solicitud de autorización" en la cual se hace una retención en la cuenta del cliente sin que éste lo vea en su extracto, pero esa cantidad se queda bloqueada durante unos días.

Posteriormente, cuando el comercio lo desea, hace un segundo paso que se llama "cobro de autorización" que es el cargo en firme de una cantidad igual o inferior (nunca superior) al importe del primer paso. Es en este momento cuando esa operación no contable se ve reflejada en el extracto del cliente y abonada en la cuenta del comercio.

Existe otra posibilidad que consiste en anular la “solicitud de autorización” que se ha hecho anteriormente de manera que la retención que se ha aplicado en la cuenta del cliente quede liberada.

Si el comercio está interesado en utilizar esta opción debe de ponerse en contacto con su entidad para que se lo autorice y enviar un correo a tpv@cecabank.es para que le haga llegar el manual de implantación de las preautorizaciones.

19.- 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 Cecabank 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.

20.- 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
19	ERROR. Datos no numéricos
20	ERROR. Datos no alfa-numéricos
21	ERROR en el cálculo del MAC
22	ERROR en el cálculo 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 válida 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.
48	ERROR. Error en el proceso de Autentificación. No retroceda en el navegador. Debe volver al comercio y reintentar el pago.
50	ERROR. Se recibe una respuesta negativa en la consulta del estado de la autenticación.
51	ERROR. Se recibe una respuesta negativa en la consulta del estado de la autenticación.
53	ERROR. Se recibe una respuesta negativa en la consulta del estado del enrolamiento. Tarjeta no enrolada.
54	ERROR. Se recibe una respuesta negativa en la consulta del estado del enrolamiento y el importe supera el máximo permitido Tarjeta no enrolada.
55	ERROR. Indisposición temporal remota en la consulta del estado del enrolamiento en comercio.
56	ERROR. Indisposición temporal remota en la consulta del estado del enrolamiento en comercio y el importe supera el máximo permitido.
57	ERROR. Indisposición temporal remota en la consulta del estado del enrolamiento en comercio, y el importe supera el máximo permitido
58	ERROR. Sistema remoto no responde en la consulta de estado del enrolamiento
62	ERROR. El comercio tiene un filtro que no permite esta operación.(Filtro2:%d)
63	ERROR. El comercio ultraseguro no acepta pagos Visa no autentificados. Póngase en contacto con su entidad.
64	ERROR. El comercio ultraseguro no acepta pagos MasterCard no autentificado. Póngase en contacto con su entidad.
65	ERROR. El comercio ultraseguro no acepta pagos no autentificados. Póngase en contacto con su entidad.
66	ERROR. Error de proceso ultraseguro. El comercio no acepta pagos no autentificados. Póngase en contacto con su entidad.
67	ERROR. Superado límite en comercio mixto.
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 Entidad.
70	El comercio tiene un filtro que no permite esta operación.[Bines por países].
71	Este comercio solo admite el pago con tarjetas EURO 6000.
72	El comercio tiene un filtro que no permite esta operación.[Gestor de Bines].

73	El comercio tiene un filtro que no permite esta operación.[Operaciones por día e IP].
74	El comercio tiene un filtro que no permite esta operación.[Operaciones por día y tarjeta].
78	Token inválido.
80	ERROR. Faltan campos obligatorios. [MerchantID]
81	ERROR. Faltan campos obligatorios. [AcquirerBIN]
82	ERROR. Faltan campos obligatorios. [TerminalID]
83	ERROR. Faltan campos obligatorios. [NumOperacion]
84	ERROR. Faltan campos obligatorios. [Importe]
85	ERROR. Faltan campos obligatorios. [TipoMoneda]
86	ERROR. Faltan campos obligatorios. [Exponente]
87	ERROR. Faltan campos obligatorios. [UrlOK]
88	ERROR. Faltan campos obligatorios. [UrlNOK]
89	ERROR. Faltan campos obligatorios. [Firma]
93	Tiempo máximo permitido para hacer la operación expirado
100	Tarjeta no válida (en negativos)
101	Tarjeta caducada
102	Operación no realizada
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
721	Recibido mensaje de respuesta incorrecto
801	Preautorización no permitida
802	Caracteres no permitidos
803	Error al intentar un pago aplazado con esta tarjeta
808	Existen errores en anulaciones anteriores, por el momento no permitimos volver a realizar la anulación
888	Error de comunicaciones. Esta operación se encuentra bloqueada hasta que se revise su situación. Por favor vuelva a consultar su estado a partir de las 10 horas de día siguiente. Perdone las molestias.
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 (Entidad 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

21.- CONSOLA DE ADMINISTRACIÓN TPV VIRTUAL PARA COMERCIOS

El comercio dispone de una consola de Administración del TPV de Cecabank 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 o por SMS (Pago fácil)
- 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 un manual en PDF con este contenido.

21.1.- Acceso

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

https://comercios.ceca.es

El usuario de acceso será proporcionado en el correo de bienvenida recibido por el comercio y un enlace para poder definir su clave de acceso. En caso de olvido de la clave, 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 Entidad ha dado de alta.

La política de segurdad aplicada en el acceso a la consola del tpv-virtual es la siguiente:

1.- Las claves de deben tener 8 caracteres como mínimo y estar compuesta por cifras y letras.

2.- Se dispone de un máximo de 3 intentos antes de proceder a bloquear un usuario.

3.- El tiempo de bloqueo será durante 30 minutos.

4.- La clave se debe de cambiar cada 90 días. A partir de esa fecha el cambio de clave será obligatoria para poder operar en la consola del TPV-Virtual.

5.- La nueva clave definida no se debe haber sido utilizada previamente.

El umbral de tiempo de inactividad, tras el cual se exige al usuario volver a autenticarse para continuar la sesión será de 15 minutos de inactividad.

22.- DIRECCIONES DE SOPORTE TPV

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

Para cualquier problema relacionado con la implementación del TPV virtual en su comercio, pueden ponerse en contacto con la dirección de correo electrónico tpv@cecabank.es o puedes contactar online con un técnico a través del chat que se encuentra disponible en la consola del tpv-virtual

Nuestro horario de atención es de Lunes a Jueves de 08:30 a 15:00 y de 16:30 a 18:00 horas. Viernes y meses de Julio y Agosto de 08:00 a 15:00 horas

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

23.- PARÁMETROS ACS 2.2

El 3DS es un protocolo de compra segura que en el primer cuatrimestre del 2019 ha migrado a su versión 2.0.

El 3DS 2.0 aparece como una evolución del protocolo 3DS1.0 para adaptarse a los nuevos procedimientos de pago existentes en la actualidad. Básicamente los objetivos que se marca el nuevo protocolo son:

- ✓ Reducir tasas de abandono.
- ✓ Minimizar las tasas de fraude
- ✓ Optimizar la experiencia de usuario
- ✓ Mejorar la interoperabilidad global, introducir actores no contemplados en la versión anterior (pago por móvil)
- ✓ Aumentar y mejorar el intercambio de información en todo el proceso de pago

La versión 2.0 presenta mejoras en tres frentes, que se describen en la siguiente tabla, catalogadas por temas:

- ✓ Experiencia de usuario
- ✓ Información para autenticación y seguridad
- ✓ Flexibilidad en dispositivos y canales

Para conseguir estas mejoras es necesario que al TPV-Virtual se le pasa cierta información que será tratada por su entidad y por el emisor de la tarjeta. Estos nuevos campos serán enviados al TPV-virtual mediante un JSON. El detalle de este campo se encuentra en un manual aparte “Parámetros 3DSecure 2.x”. En caso de no tenerlo debe de solicitarlo en el email tpv@cecabank.es

Actualmente este campo se encuentra en fase de integración por lo que no es obligatorio su uso.

24.- USO DE EXENCIONES Y OPERACIONES FUERA DE AMBITO

La nueva directiva PSD2 permite aplicar una serie de exenciones y operaciones fuera de ámbito a la operativa del TPV-Virtual de manera que una operación realizada no requiera de autenticación por parte del cliente.

OPERACIONES FUERA DE AMBITO:

MOTO

Se considera una operativa MOTO aquella que es realizada por parte del comercio con su cliente a través de email o teléfono, por lo tanto no existe posibilidad de que el cliente se pueda autenticar. Estas operaciones no tienen garantía de pago por parte del comercio y éste debe de tener una prueba fehaciente de que la operación se ha hecho por alguno de estos canales, email o teléfono.

Para lanzar una operatoria de este tipo, el comercio debe de solicitar a su entidad un tpv-virtual de este tipo (Terminal 2000002) y lanzar una operación normal y corriente. Por el mero hecho de utilizar este terminal específico, la operación irá marcada como MOTO.

MIT

Se considera una operación MIT, aquella que es iniciada por el comercio sin estar presente el cliente. Claros ejemplos de esta operatoria son las suscripciones, los pagos aplazados, tokenización, etc.

Estas operaciones al no estar el cliente presente no requieren autenticación, pero se da la peculiaridad de que la primera operación de cada una de ellas tiene que ser autenticada, ya que en ese momento en el que el cliente acepta una suscripción, realizar un pago aplazado, etc, sí que está el cliente presente. Por ejemplo, un cliente que quiera realizar una suscripción mensual a un producto, la primera operación debe ser autenticada y venir marcada con esta característica (Suscripción), y las siguientes, en las cuales ya no está presente, serán lanzadas sin autenticación. Para operar con este tipo de excepciones se debe de usar alguna de las siguientes funcionalidades del TPV-Virtual:

- Gestor de operaciones
- Tokenización
- Envío de datos de tarjeta. (Uso poco común y destinado a comercios que almacenan los datos de la tarjeta de acuerdo a la normativa PCI-DSS. Estos requieren una certificación al respecto y están obligados a pasar auditorías de seguridad para comprobar su correcto cumplimiento)

Existe un manual específico para este tipo de operatoria. En el caso de necesitarlo debe de solicitarlo al email tpv@cecabank.es.

EXENCIONES:

LOW

Es una operación por debajo de 30 euros y en la que el comercio solicita una exención de autenticación al emisor de la tarjeta por entender que es de bajo riesgo.

El emisor es el que valorará si admite esta exención y la da como autenticada, o por el contrario no admite la exención y exige una autenticación, por lo tanto el comercio debe de estar preparado para ello y no hacer una llamada de servidor a servidor para lanzar este tipo de transacciones. Si el emisor no la acepta se desencadenará una autenticación para lo cual es necesario el flujo a través del navegador del cliente. El comercio debe de tener en cuenta que si solicita una exención de este tipo, y es aceptada por el emisor de la tarjeta, el comercio es responsable en caso de repudio de esta operación por el cliente.

TRA

Es una operación por debajo de un importe determinado y en la que el comercio solicita una exención de autenticación al emisor de la tarjeta por entender que es de bajo riesgo. Esta operación antes de enviarse a procesar pasa por un monitor de fraude propio de la entidad del comercio y que permite comprobar si la operación está o no exenta de riesgo. En el caso de que este monitor de fraude detecte algún tipo de riesgo en esta operación, se descartará esta posibilidad de exención y se enviará a procesar como una operación normal y corriente requiriendo una autenticación por parte del emisor.

El importe máximo para este tipo de operaciones depende de la entidad del comercio y puede ser menor de 100, 250 o 500 euros. Este importe será actualizado cada 3 meses por normativa del Banco de España según la casuística de la entidad del comercio.

El emisor es el que valorará si admite esta exención y la da como autenticada, o por el contrario no admite la exención y exige una autenticación, por lo tanto el comercio debe de estar preparado para ello y no hacer una llamada de servidor a servidor para lanzar este tipo de transacciones. Si el emisor no la acepta se desencadenará una autenticación para lo cual es necesario el flujo a través del navegador del cliente. El comercio debe de tener en cuenta que si solicita una exención de este tipo, y es aceptada por el emisor de la tarjeta, el comercio es responsable en caso de repudio de esta operación por el cliente.

Las casuísticas TRA y LOW se han automatizado a través de la consola del TPV_Virtual, de manera que el comercio no tenga que realizar ningún desarrollo para poder aplicarlas en su operativa. Por el mero hecho de solicitarlas a su entidad, y que ésta lo active en la consola, el comercio empezará a hacer uso de ella en toda su operatoria. Solo en el caso de que el comercio quiera elegir en qué operaciones puede hacer uso de esta casuística y en cuáles no, es cuando tiene que hacer uso del nuevo parámetro. Para ello se ha definido un parámetro (Exencion_SCA) que será enviado desde el comercio al TPV-Virtual para indicar si se puede aplicar alguna de estas exenciones o excepciones. Este campo es opcional y en el caso de que no se envíe se aplicará la configuración que la entidad haya aplicado en la consola del TPV-Virtual para el comercio.

ⓘ	Es importante indicar que para aplicar cualquiera de estas opciones es necesario que la entidad adquirente del comercio se lo haya autorizado, de tal manera que si un comercio utiliza alguna de estas opciones y el comercio no está autorizado a ello se mostrará un error de “operación no permitida”

ⓘ	Destacar que para que estas exenciones tengan éxito es recomendable que se envíen los parámetros documentados en el punto anterior “Parámetros ACS 2.x” de manera que se tenga la mayor información posible de la operación de cara a su análisis por el monitor de fraude.

Si el comercio decide no aplicar una exención a una operación determinada deberá de enviar el parámetro Exencion_SCA=NONE. Si por el contrario quiere aplicar una exención deberá de enviar el parámetro Exencion_SCA=LOW o Exencion_SCA=TRA, o bien, no enviarlo, ya que si no viaja se aplicará la configuración especificada por defecto en la Consola del TPV-Virtual

25.- COMERCIOS NO SEGURO Y PSD2

Con la nueva normativa PSD2, los comercios no seguros deben de migrar a seguros, salvo excepciones muy puntuales, por lo que los comercios que en la actualidad estén operando en la modalidad no segura, deberán analizar su casuística y en caso de ser necesario, hacer las adaptaciones necesarias de manera que empiecen a operar en modalidad segura.

En la mayoría de los casos este cambio será transparente para los comercios y no requerirá de adaptación alguna, salvo que quiera enviar los nuevos parámetros comentados en el punto anterior “PARÁMETROS ACS 2.2”, pero hay comercios que hacen la llamada de servidor a servidor sin pasar por el navegador del cliente y enviando directamente los datos de la tarjeta, en cuyo caso sí que requiere de cierta adaptación. En este caso, los comercios tienen que tener en cuenta que es posible que el emisor requiera autenticar al cliente y por lo tanto la operación no sea autorizada directamente. En este caso hay 2 posibles soluciones.

1. Que la llamada al TPV_Virtual se haga a través del navegador del cliente, de manera que si hay que autenticar al titular de la tarjeta, se pueda cargar la url del banco emisor.
2. Que siga haciendo la llamada de servidor a servidor con un “directo a autorizar” pero debe de controlar que la respuesta puede ser una denegación porque se requiere una autenticación. En este caso, el comercio debe de realizar una nueva llamada, pero esta vez a través del navegador del cliente, para poder autenticar al cliente.

En ambos cosos el comercio podrá hacer uso de las exenciones disponibles y explicadas en el punto anterior “USO DE EXENCIONES Y OPERACIONES FUERA DE AMBITO”

Para más información al respecto puede contactar con el correo tpv@cecebank.es

26.- PREGUNTAS FRECUENTES.

Al intentar operar me aparece un error:
Al realizar una operación se pueden producir diversos errores que se quedarán reflejados en el listado de operaciones. En el capítulo Tratamiento de errores aparece un listado con los códigos de error más frecuentes. Le rogamos consulte dicho apartado antes de ponerse en contacto con el soporte TPV de Cecabank, ya que están recogidos la mayoría de los mismos indicando el motivo.

¿Cómo puedo saber desde mi aplicación si la operación realizada ha sido correcta?
Para ello existe la comunicación online. Consulte el apartado de 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.

En pagos directos o pagos por email me da un error de comunicación on-line:
Cuando generamos una operación manual puede que el número de operación que estemos poniendo no lo tenga registrado en la base de datos de pedidos del comercio, en este caso poner la opción de Comunicación on-line en No a la hora de rellenar los datos de la operación en la consola.

¿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
https://tpv.ceca.es/tpvweb/tpv/compra.action
con la clave_encriptacion = 1111111 (La que aparezca en la consola de pruebas)

a entorno
https://pgw.ceca.es/tpvweb/tpv/compra.action
con la clave_encriptacion = 2222222 (La que aparezca en la consola de producción)

El entorno de pruebas sigue activo aunque el comercio pase a real.
El paso a real puedes hacerlo cuando quieras, aunque conviene avisar a tu Entidad 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.

Error 190 Operación no realizable, resto de casos.
Este error es el más frecuente a la hora de realizar una compara en un TPV. Si el comercio no ha operado nunca y le aparece este error, debe de ponerse en contacto con el soporte del TPV ya que es posible que el TPV esté mal dado de alta.
Si el comercio ya ha operado en otras ocasiones de forma correcta y aparece una operación con este error, quiere decir que el emisor de la tarjeta ha denegado el pago, por lo tanto el cliente debe operar con otra tarjeta, o bien dirigirse a su entidad para ver el motivo del error.

Comunicación on line incorrecta
Este error es debido a que el comercio ha definido una url de comunicación online con respuesta requerida y ésta no está respondiendo el patrón esperado $*$OKY$*$, o bien responde pasados 30 segundos. En este caso se debe revisar si la URL dada de alta en el apartado de configuración es correcta, y en caso de serlo, revisar en su servidor la respuesta que está dando tras la llamada del TPV. Para más información, consulte el apartado de “comunicación on-line” en la ayuda de la consola del TPV.

En el listado de operaciones veo que las operaciones se han realizado de forma correcta, pero no aparece marcada la operación como pagada en la aplicación del comercio.
Este error se puede producir por dos motivos:
1.- El comercio tiene activada la comunicación online sin respuesta requerida. En este caso se debe revisar si la URL dada de alta en el apartado de configuración es correcta, y en caso de serlo, revisar en su servidor la respuesta que está dando tras la llamada del

TPV. Para más información, consulte el apartado de Comunicación on-line en la ayuda de la consola del TPV.
2.- El comercio no tiene activada la comunicación online con respuesta requerida. En este caso, el comercio está actualizando su pedido a través de la URL-OK pasada como parámetro en la llamada al TPV. Nosotros no recomendamos que se actualice el pedido con la URL ok, ya que depende de la navegación del cliente, puede pasar que el cliente no pulse el botón, aunque se le indiques, o que haya un error de comunicación, de tal manera que se tengas la confirmación del pago. Para evitar este error es aconsejable que active la comunicación online siguiendo las instrucciones que aparecen en el apartado correspondiente.

Tengo un pedido pendiente en mi tienda pero no localizo el intento de pago
Cuando un cliente cierra la ventana y no continúa con el proceso de pago no registramos la operación como ok y tampoco con un código de error.

Necesito anular una operación
Consulte el apartado Anulación de una operación que aparece dentro de Consola de administración TPV Virtual para comercios.

Necesito anular una parte de la operación
Consulte el apartado Anulación parcial de una operación que aparece dentro de Consola de administración TPV Virtual para comercios.

Al anular una operación pero me da un error de operación inexistente
Para realizar una operación por el total de la operación, el comercio dispone de 15 días desde su ejecución. En caso de pasar más de ese tiempo, debe realizar una anulación parcial por el total del importe de la compra, si su entidad se lo permite, o bien dirigirse a su entidad para que se lo hagan desde un terminal financiero. En este caso, deberá llevar la información correspondiente a la operación que desea anular.

¿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 Cecabank. Consulte el apartado de ayuda denominado Consola de administración TPV Virtual para Comercios para obtener más información.

27.- 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

27/05/2010 Versión 5.0
- Inclusión de la nueva consola del TPV

01/09/2010 Versión 6.0
- Revisión completa del manual

01/09/2010 Versión 6.2
- Incluir Tokenización

01/01/2017 Versión 7.0
- Incluir cifrado SHA2

01/04/2017 Versión 7.0
- Incluir en el manual tiempo de inactividad tras el cual se vuelve a pedir identificación.

15/02/2018 Versión 7.4
- Incluir en manual aclaración campo **Importe** y **Num_aut** enviado en la comunicación online.

14/06/2018 Versión 7.5
- Se incluye campo **Sesion** en el formulario de envió de una operación.

24/01/2019 Versión 7.7
- Se incluye el apartado otras formas de pago

04/02/2019 Versión 7.8
- Se actualizan código de errores

01/02/2019 Versión 8.0
- Se incluye parámetros opcionales para el ACS 2.0

06/05/2019 Versión 8.1
- Se incluye posibles valores parámetros opcionales para el ACS 2.0

23/05/2019 Versión 8.2
- Se incluye preautorizaciones
- Se eliminar los parámetros del ACS 2.0 para incluirlo en otro manual

14/10/2019 Versión 8.3
- Se incluye información relativa a nuevos módulos de pagos.

21/11/2019 Versión 8.4
- Se incluyen códigos de errores 078 y 803 en el apartado 20.- TRATAMIENTO DE ERRORES.

27/11/2019 Versión 8.5

- Modificaciones en 7.- COMUNICACIÓN ONLINE
- Modificación en organización de apartados para que aparezca como apartado 4 el de MODULOS DE PAGO PARA SOLUCIONES DE COMERCIO ELECTRÓNICO DE TERCEROS

17/01/2020 Versión 8.6

- Modificación en organización de apartados para que aparezca como apartado 4 el de MODULOS DE PAGO PARA SOLUCIONES DE COMERCIO ELECTRÓNICO DE TERCEROS

24/03/2020 Versión 8.7

- Se incluye el cifrado SHA21 para incluir el campo descripción en la firma.
- Se incluyen las posibles exenciones y excepciones disponibles en la PSD2 así como su forma de implantación
- Se explica mejor el funcionamiento de la comunicación online por email

28/04/2020 Versión 8.8

- Se actualizan los códigos de errores devueltos por el ACS.
- Se incluye información sobre exenciones.

09/06/2020 Versión 8.9

- Se incluye el parámetro Tipo_operacion en la comunicación online.

02/07/2020 Versión 8.10

- Se incluye el parámetro inicioBizum para ir directamente a Bizum sin pasar por la pantalla de selección de forma de pago.

16/09/2020 Versión 8.11

- Se añade el punto “COMERCIOS NO SEGURO Y PSD2”

02/12/2020 Versión 8.13

- Se cambia para que el campo datos_acs se envíe en Base64