TPV Virtual

MANUAL DEL COMERCIO

Versión 8.1
Abril 2015

CX CatalunyaCaixa

1. INTRODUCCIÓN

El TPV virtual de CatalunyaCaixa es una aplicación informática que permite a los comercios y empresas que venden sus productos y servicios a través de Internet el cobro de las transacciones pagadas con tarjetas financieras y su abono en cuenta.

Las tarjetas aceptadas son las mismas que se admiten en los comercios con TPV físico, concretamente **Visa, MasterCard y Maestro**. Se puede solicitar la posibilidad de operar con **tarjetas JCB,** así como **American Express y Diners Club**.

El TPV virtual soporta diferentes idiomas (**Castellano, Catalán, Inglés, Francés, Alemán, Holandés, Italiano, Sueco, Portugués, Valenciano, Polaco, Gallego y Euskera**) y puede operar con monedes diferentes (**Euro, Dólar, Libra Esterlina, Yen, Real Brasileño, Franco Suizo, Dólar Australiano, Dólar Canadiense, Sol Peruano, Rupia India, Peso Mejicano, Peso xileno, Lira Turca, Bolívar Venezolano, Peso Colombiano, Rand Sudafricano, Nuevo Sloty Polaco, Corona Danesa, Corona Sueca, Corona Noruega, Peso Uruguayo y Colones de Costa Rica** en el momento de creación de este manual).

El TPV virtual utiliza funciones y algoritmos estándares de Internet, razón por la cual puede ser instalado en cualquier servidor o plataforma con independencia del sistema operativo y del lenguaje de programación. Además, está diseñado para visualizarse tanto en navegadores para equipos de sobremesa (**PC estándar**) como para dispositivos "de mano" (tipo **PDA**). La comunicación con el TPV virtual se realiza siempre bajo entorno de **conexión segura SSL**.

Este sistema incorpora una herramienta, llamada **MÓDULO DE ADMINISTRACIÓN**, que permite al comercio realizar, entre otras, consultas de movimientos (seleccionándolas según diferentes parámetros), consultas de totales, anulaciones de operaciones y devoluciones parciales.

El TPV virtual de CatalunyaCaixa implementa de forma obligatoria la introducción del **CVV2** de la tarjeta (serie de tres números situados en la parte posterior de la tarjeta), ya que se ha demostrado como un método eficaz contra el fraude.

El TPV virtual de CatalunyaCaixa ha sido uno de los primeros en adaptarse a las nuevas tecnologías de autenticación de clientes y en proteger a sus comercios virtuales contra retrocesiones de operaciones adoptando entre otros el sistema **3DSECURE, que incorpora los protocolos VERIFIED by VISA y MASTERCARD SECURECODE.**

2. GARANTÍAS DE SEGURIDAD – 3DSECURE

El TPV virtual es un dispositivo preparado para trabajar en modo totalmente seguro dentro de la operativa de ventas a través de Internet, es decir:

1. Intentará contactar con el banco emisor de la tarjeta para solicitar la autenticación del titular (verificación de su identidad) antes de solicitar la correspondiente petición de autorización. De esta forma se garantiza que solo **el titular genuino,** dueño de la tarjeta, podrá operar con ella.

2. Implementa SSL en todas las comunicaciones que impiden la interceptación de la información por terceros. Por tanto, la **confidencialidad está asegurada** en todas las comunicaciones que se establezcan durante la transacción.

3. También habilita mecanismos para probar la **autenticidad del origen** de las transacciones y que **impiden, asimismo, la manipulación de datos por terceros**. De esta forma se asegura **la integridad** de los datos de la transacción.

4. Los datos de **las tarjetas no son normalmente conocidos por el comercio**, con lo que se evita que esta información pueda ser utilizada posteriormente por terceros de forma fraudulenta. Esta información es almacenada convenientemente por el TPV Virtual que a su vez la proporcionará al sistema de pagos cuando sea necesario (por ejemplo en una devolución).

Por tanto, todas las transacciones que se realicen a través del TPV Virtual contarán con todas las garantías de seguridad, confidencialidad e integridad para los agentes participantes: titulares de tarjetas y sus entidades emisoras, comercios y CatalunyaCaixa.

La operatoria se produce de la siguiente forma:

1. El comprador accede a la página web del comercio y selecciona los productos o servicios que desea adquirir.

2. Una vez el comprador ha rellenado el formulario con los datos necesarios para la entrega del pedido, la web del comercio le deberá ofrecer un botón para el pago con tarjeta (habitualmente con un logotipo de las marcas internacionales de tarjetas).

3. Cuando el comprador seleccione este botón, se establecerá el enlace con el TPV Virtual de CatalunyaCaixa. Para realizar el pago, el cliente deberá introducir su número de tarjeta, caducidad y Código de Seguridad CVV2 (número de tres posiciones situado en la parte posterior de la tarjeta).

4. Si la tarjeta dispone de un sistema de autenticación proporcionado por su banco, se abrirá una ventana en el navegador del comprador para que se identifique delante de su entidad financiera emisora de la tarjeta.

5. Una vez procesada la operación el TPV Virtual informará del resultado, tanto al comprador como al comercio.

Puede ocurrir en algún caso que el banco emisor y el titular de la tarjeta todavía no hayan pactado ningún método de autenticación, por lo que el paso 4 no siempre se

realizará, si bien desde el punto de vista del comercio la transacción seguirá siendo considerada segura, esto es: **EL TITULAR NO LA PUEDE RETROCEDER ARGUMENTANDO QUE ÉL NO LA HA REALIZADO**, aunque no se haya autenticado, ya que los organismos internacionales como VISA y MasterCard obligan al banco emisor de la tarjeta a asumir la responsabilidad en estos casos.

El TPV virtual de CatalunyaCaixa está certificado por los sistemas de tarjetas VISA, y MASTERCARD como terminal virtual seguro y, por tanto, **hay garantía de cobro por parte de los comercios de todas las operaciones excepto en los casos siguientes:**

1. El comercio no puede acreditar documentalmente que el producto o servicio ha sido entregado al titular de la tarjeta de acuerdo con los términos y condiciones de la venta.

2. En el caso de pagos recurrentes, al procesar el pago inicial la entidad emisora de la tarjeta no ha llevado a cabo el proceso de autenticación positiva del titular.

3. Operaciones realizadas con tarjetas Visa Business, Visa Corporate y Visa Purchasing.

El TPV Virtual se irá actualizando con las últimas versiones de pago seguro que vayan dictando los organismos internacionales, si bien se asegura que **el comercio NO tendrá que realizar adaptaciones,** ya que éstas se implementarán siempre de forma centralizada.

3. ASPECTOS OPERATIVOS

3.1. TIPOS DE PETICIONES DE AUTORIZACIÓN

En función de las necesidades de cada comercio el TPV Virtual ofrece una elevada variedad de peticiones de autorización, que el comercio puede combinar según sus necesidades.

Pago estándar **(Ds_Merchant_TransactionType = "0")**

Es el caso más general. En él la transacción es iniciada por el titular que está presente durante el proceso de la misma. Una vez se ha recibido la petición de compra por parte del comercio, el TPV Virtual solicita al cliente los datos para realizar la transacción de autorización.

Si el banco del titular de la tarjeta dispone de un sistema de autenticación se solicitará al titular por parte del banco emisor la correspondiente prueba de autenticación.

La solicitud de Autorización se lleva a cabo en tiempo real, produciendo un cargo inmediato en la cuenta del titular asociada a la tarjeta (crédito o débito). Hay que notar que las garantías en ambos tipos de tarjetas son idénticas.

La transacción es capturada automáticamente por el TPV Virtual y enviada diariamente al proceso batch para que se proceda al abono al comercio.

El titular de la tarjeta recibe un justificante del pago realizado.

Preautorización **(Ds_Merchant_TransactionType = "1")**

NOTA: de acuerdo a la normativa de las marcas internacionales, esta operativa está restringida a aquellos comercios cuya actividad sea una de las siguientes: hoteles, agencias de viajes y alquiler de vehículos.

Puede utilizarse cuando en el momento de la compra no se puede determinar el importe exacto de la misma o, por alguna razón, el comercio no desea que el importe sea cargado en la cuenta del cliente de forma inmediata.

La transacción es transparente para el titular que en todo momento actúa exactamente igual que en el caso anterior, es decir, facilita sus datos y se autentica si corresponde, recibiendo por parte del TPV Virtual el correspondiente justificante.

La solicitud de preautorización se lleva a cabo en tiempo real, produciendo una retención por el importe de la venta en la cuenta del titular.

La transacción no se captura y, por tanto, no produce efectos contables en la cuenta del titular ni por tanto abono al comercio (**en el caso de tarjetas de débito algunas entidades emisoras SI efectúan apuntes contables al titular que anulan automáticamente pasados unos días**).

Toda preautorización debe tener una Confirmación de Preautorización en un período máximo de 7 días naturales. En caso contrario perderá su validez como garantía de pago.

Confirmación de Preautorización (Ds_Merchant_TransactionType = "2")

Complementa de forma inseparable la operación anterior.

El titular no está presente y, por tanto, es siempre iniciada por el comercio.

Debe realizarse en los 7 días siguientes a la preautorización original y su importe debe ser MENOR o IGUAL que la de la original.

Esta transacción se trata contablemente, regularizando automáticamente el apunte en la cuenta del titular y enviándose al proceso batch para su abono al comercio.

La confirmación de preautorización tiene garantía de pago y conserva las condiciones respecto a transacción segura de su Preautorización original.

El TPV Virtual validará la existencia de la operación original y el importe que se desea confirmar, rechazando la operación en caso de existir algún error.

Anulación de Preautorización (Ds_Merchant_TransactionType = "9")

El titular no está presente y, por tanto, es siempre iniciada por el comercio. Debe realizarse en los 7 días siguientes a la preautorización original.

El TPV Virtual validará la existencia de la operación original, rechazando la operación en caso de existir algún error.

Devolución Parcial o Total (Ds_Merchant_TransactionType = "3")

Son transacciones contables iniciadas por el comercio. También podrá utilizar el módulo de administración del TPV Virtual para realizarlas manualmente.

El TPV Virtual comprueba la existencia de la autorización original que se desea devolver, así como que la suma de los importes devueltos no supere en ningún caso el importe autorizado original.

Producen efecto contable en la cuenta del titular **(algunas entidades emisoras pueden demorar unos días el abono al titular)** y, por tanto, son capturadas automáticamente y enviadas al proceso de liquidación que procederá a realizar el cargo correspondiente en la cuenta del comercio.

Transacción recurrente (Ds_Merchant_TransactionType = "5")

Permite la suscripción del titular de la tarjeta a un servicio periódico ofrecido por el comercio.

El importe total de este servicio será abonado por medio del pago de un determinado número de cuotas.

Mediante esta operación, el comercio informará la cantidad total a pagar, el número mínimo de días a partir del cual se puede hacer el pago de la siguiente cuota y la fecha límite del pago de la última cuota, que no podrá ser superior a 12 meses.

El flujo de la operación es similar a la petición de autorización normal. Además se deberá informar al cliente del importe total a pagar y cuotas que lo componen, realizándose la autenticación con estos datos.
Por el contrario, la solicitud de autorización, que tendrá carácter contable, se realizará únicamente por el importe de la primera cuota como una solicitud de autorización normal.

Posteriormente, el comercio enviará transacciones sucesivas de autorización al vencimiento de cada cuota.

Transacción Sucesiva (Ds_Merchant_TransactionType = "6")

Complementa de forma inseparable la operación anterior.

El titular no está presente y, por tanto, es siempre iniciada por el comercio.

Debe realizarse según las condiciones de la transacción recurrente original en cuanto a importe, cuotas y fecha límite. Estos extremos serán validados por el TPV Virtual, que rechazará la transacción en caso de encontrar algún error.

Esta transacción se trata contablemente, produciendo un apunte en la cuenta del titular para cada cuota y enviándose al proceso de liquidación diario para su abono al comercio.

Las transacciones sucesivas conservan las mismas condiciones de seguridad respecto a la transacción recurrente original, excepto en el caso de que la operación original haya sido considerada segura pero no haya existido autenticación positiva del cliente. En este caso las sucesivas no se consideran seguras.

Para su realización es necesario solicitar una nueva petición de autorización para cada cuota.

Autenticación (Ds_Merchant_TransactionType = "7")

Este tipo de operación puede ser utilizado por el comercio cuando el importe de la venta no puede ser determinado con exactitud en el momento de producirse la misma.

La operativa es similar a la de preautorizaciones, aunque en este caso no se produce solicitud de autorización, por lo que la transacción no es contable y no provoca retenciones en cuenta al titular. No se valida ni CVV2, ni la fecha de caducidad de la tarjeta ni si el titular tiene saldo. Sólo se valida que existe aquella numeración de tarjeta, y en el caso de que la operación se procese por 3D Secure la identidad del titular.

Posteriormente y dentro de los siguientes 45 días naturales el comercio enviará una confirmación de autenticación que completará la operación original.

Confirmación de autenticación **(Ds_Merchant_TransactionType = "8")**

Complementa de forma inseparable la operación anterior.

El titular no está presente y, por tanto, es siempre iniciada por el comercio.

Su importe puede ser diferente al de la operación original (incluso MAYOR con un máximo de un 15% respecto el importe original).

Esta transacción se trata contablemente, produciendo un apunte en la cuenta del titular y enviándose al proceso de liquidación diario para su abono al comercio.

Las confirmaciones de autenticación conservan las mismas condiciones de seguridad respecto a la autenticación original.

El TPV Virtual validará la existencia de la operación, rechazándola en caso de existir algún error.

Preautorización Diferida **(Ds_Merchant_TransactionType = "O")**

Son operaciones similares a las preautorizaciones pero están disponibles para todos los sectores de actividad. En tiempo real se obtiene una autorización por parte del banco emisor que tendrá que ser confirmada en las 72 horas siguientes si se quiere realizar la operación de forma definitiva.

Si pasadas 72 horas desde el día/hora de la preautorización no se ha enviado la confirmación, la autorización se anulará automáticamente y, por tanto, no podrá confirmarse.

A diferencia de las preautorizaciones tradicionales **el importe** de la Confirmación de la Preautorización Diferida **ha de ser exactamente igual** que el de su respectiva preautorización.

La solicitud de preautorización se lleva a cabo en tiempo real, produciendo una retención por el importe de la venta en la cuenta del titular.

La transacción no se captura y, por tanto, no produce efectos contables en la cuenta del titular ni por tanto abono al comercio (**en el caso de tarjetas de débito algunas entidades emisoras Sí efectúan apuntes contables al titular que anulan automáticamente pasados unos días**).

Para activar el servicio de Preautorización Diferida, es necesario que el comercio lo solicite explícitamente a su oficina de CatalunyaCaixa.

Confirmación de Preautorización Diferida **(Ds_Merchant_TransactionType = "P")**

Complementa de forma inseparable la operación anterior.

El titular no está presente y, por tanto, es siempre iniciada por el comercio. Debe realizarse en las siguientes 72 horas a la preautorización original y su importe debe ser EL MISMO que la de la original.

Esta transacción se trata contablemente, regularizando automáticamente el apunte en la cuenta del titular y enviándose al proceso batch para su abono al comercio. La confirmación de preautorización tiene garantía de pago y conserva las condiciones respecto a transacción segura de su Preautorización original.

El TPV Virtual validará la existencia de la operación original y el importe que se desea confirmar, rechazando la operación en caso de existir algún error.

Anulación de Preautorización Diferida (Ds_Merchant_TransactionType = "Q")

El titular no está presente y, por tanto, es siempre iniciada por el comercio. Debe realizarse en las 72 horas siguientes a la preautorización original.

El TPV Virtual validará la existencia de la operación original, rechazando la operación en caso de existir algún error.

Preautorización Diferida Recurrente (Ds_Merchant_TransactionType = "R")

Similar a la Transacción recurrente permite la suscripción del titular de la tarjeta a un servicio periódico ofrecido por el comercio. Se diferencia, no obstante, en que la primera autorización no tendrá validez contable excepto que se realice la confirmación en las 72 horas posteriores a la preautorización. A diferencia de las preautorizaciones tradicionales, **el importe** de la Confirmación de Preautorización Diferida Recurrente **ha de ser exactamente igual** que el de su respectiva preautorización.

Si pasadas 72 horas desde el día/hora de la preautorización no se ha enviado la confirmación, la autorización se anulará automáticamente y, por tanto, no podrá confirmarse.

El importe total de este servicio será abonado por medio del pago de un determinado número de cuotas. Mediante esta operación, el comercio informará la cantidad total a pagar, el número mínimo de días a partir del cual se puede hacer el pago de la siguiente cuota y la fecha límite del pago de la última cuota.

Confirmación de Preautorización Diferida Recurrente y Transacción Sucesiva (Ds_Merchant_TransactionType = "S")

El mismo tipo de transacción se utiliza tanto para la confirmación de la preautorización recurrente 72 horas (primera operación) como para los pagos sucesivos vinculados a esta primera autorización.

Complementan de forma inseparable la operación anterior. Para su realización es necesario solicitar una nueva petición de autorización para cada cuota. El titular no está presente y, por tanto, es siempre iniciada por el comercio.

Esta transacción se trata contablemente, produciendo un apunte en la cuenta del titular para cada cuota y enviándose al proceso de liquidación diario para su abono al comercio.

Las transacciones sucesivas conservan las mismas condiciones de seguridad respecto a la transacción recurrente original, excepto en el caso de que la operación original

haya sido considerada segura pero no haya existido autenticación positiva del cliente. En este caso las sucesivas no se consideran seguras.

A continuación se inserta una tabla donde se resumen las principales características de cada operación:

Tipo de Operación	Iniciada por	Contable	Operación Original Validaciones	Garantía – Operación Segura
Autorización	Titular	SI		Cuando se reúnan condiciones
Preautorización	Titular	NO		Cuando se reúnan condiciones
Confirmación de Preautorización	Comercio	SI	Preautorización: 7 días Importe < ó =	Mismas que la original
Anulación de Preautorización	Comercio	NO	Preautorización: 7 días Importe =	
Devolución automática	comercio	SI	Autorización: Suma de importes devueltos < ó =120 días	
Recurrente	Titular	SI		Cuando se reúnen condiciones
Sucesiva	Comercio	SI	Recurrente: importe, cuotas y fecha límite	Si la original ha sido autenticada
Autenticación	Titular	NO		Cuando se reúnen condiciones
Confirmación de autenticación	Comercio	SI	Autenticación: 45 días	Mismas que la original
Preautorización Diferida	Titular	NO		Cuando se reúnan condiciones
Confirmación de Preautorización Diferida	Comercio	SI	Preautorización: 72 horas máximo Importe =	Mismas que la original
Anulación de Preautorización Diferida	Comercio	NO	Preautorización: 72 horas máximo	
Preautorización recurrente Diferida	Titular	NO		Cuando se reúnan condiciones
Confirmación de preautorización recurrente Diferida	Comercio	SI	Preautorización Recurrente: 72 horas máximo Importe =	Si la original ha sido autenticada
Sucesiva de Preautorización	Comercio	SI	Preautorización Recurrente: importe, cuotas y fecha límite	Si la original ha sido autenticada

3.2. LIMITACIÓN DE OPERATORIA

Puesto que se realizan en un entorno no presencial, las operaciones de TPV Virtual son las más susceptibles de recibir pagos de tarjetas fraudulentas donde el titular no es quien realiza la compra. Para reducir el riesgo de estas operaciones, CatalunyaCaixa aplicará una serie de condiciones que limitan la operatoria de cada comercio. Estás limitaciones han de ajustarse a unos valores que no condicionen las

expectativas de venta del comercio pero que a su vez evite desviaciones exageradas de su facturación habitual (en la mayoría de los casos significan que se está recibiendo un ataque con tarjetas robadas y/o fraudulentas).

- Número máximo de operaciones por día (autorizadas y denegadas)
- Importe máximo por operación
- Importe máximo acumulado diario
- Número máximo diario de operaciones (aceptadas y denegadas) por tarjeta
- Importe máximo diario por tarjeta
- Número máximo diario de operaciones (aceptadas y denegadas) por usuario (dirección I.P.)
- Importe máximo diario por usuario (dirección I.P.)

En caso de querer modificar alguno de estos parámetros se tendrá que solicitar a su oficina de CatalunyaCaixa.

3.3. MEDIDAS DE SEGURIDAD ADICIONALES

Para proteger los intereses de su comercio y reducir al máximo el volumen de incidencias, sugerimos adoptar las siguientes medidas de seguridad adicionales a la hora de aceptar pagos con tarjetas.

SEÑALES PARA DETECTAR FRAUDE EN INTERNET

Cuando aparezca alguna de las siguientes señales en una compra por internet, el comercio debe sospechar de ella, pero cuando aparecen más de una, el comercio debe tomar medidas para evitar ser víctima de un fraude.

- Persona que compra en la tienda por primera vez
- Múltiples operaciones de una misma tarjeta en un periodo corto de tiempo
- Múltiples operaciones de una misma tarjeta (o tarjetas de numeración similar) con diferentes direcciones de entrega
- Operaciones con números de tarjetas similares
- Pedidos con la misma dirección de envío pero realizadas con múltiples tarjetas
- Múltiples tarjetas usadas desde una misma dirección IP
- Pedidos consistentes en múltiples cantidades del mismo producto
- Pedidos de importe superior al normal
- Pedidos en los que la entrega ha de ser urgente, o incluso "para el día siguiente". Los delincuentes quieren estos productos obtenidos fraudulentamente tan pronto como sea posible, para una posible reventa y no están preocupados por el sobrecoste del envío.
- Pedidos de productos de alto valor. Estos productos tienen un alto valor de reventa.
- Pedidos enviados a direcciones internacionales.

CONTROL DE OPERACIONES

1. En el MÓDULO DE ADMINISTRADOR DEL TPV VIRTUAL se informa la DIRECCIÓN I.P. del comprador y debería comprobarse que:

1.a Un mismo usuario (misma dirección IP) no ha pagado (o ha intentado pagar) con más de dos tarjetas diferentes.

1.b Un mismo usuario (I.P.) o una misma tarjeta, no han realizado múltiples operaciones en un corto periodo de tiempo.

1.c No se están realizando compras con tarjetas generadas (los primeros dígitos de los números de tarjetas son iguales pero los últimos cambian).

1.d Al realizar diferentes compras, un mismo usuario (I.P.) o una misma tarjeta no se ha registrado a la web con datos diferentes.

1.e Si el terminal ha rechazado la primera operación de la tarjeta, verificar que no se han procesado más operaciones con la misma I.P. o con la misma tarjeta por importes más bajos.

2. Mediante el mensaje de respuesta (campo "DS_Response") o el MÓDULO DE ADMINISTRACIÓN DEL TPV VIRTUAL se informa si la operación ha sido aceptada (códigos 000 a 099) o denegada (resto de códigos). Los códigos de denegación tipo 2xx, indican que la tarjeta está bloqueada por pérdida, robo, falsificación del plástico o por uso fraudulento de la numeración de la tarjeta. En estos casos el comercio tendrá que bloquear el usuario (identificable mediante dirección I.P. y datos de registro) para no permitirle la opción de intentar ningún nuevo pago.

3. También en el mensaje de respuesta hay el campo "Ds_Card_Country" que informa del código I.S.O. del país donde se ha emitido la tarjeta. Mediante la comparación con la dirección I.P. del comprador se pueden filtrar comportamientos sospechosos de ser fraudulentos (p.ex. una tarjeta emitida en un país pero que opera mediante una I.P. de otra país diferente).

4. Comprobar la validez de los datos de registro del cliente:

4.a Validar los números de teléfono usando directorios de teléfonos.

4.b Validar que el código del teléfono y/o su prefijo coincide con el área geográfica de la dirección de envío del pedido.

4.c Validar la correspondencia entre el código postal y la ciudad del envío.

4.d Validar de la dirección email enviando una orden de confirmación.

5. Establecer límites de control basados en múltiples parámetros. El comercio puede reducir considerablemente su riesgo de exposición al fraude aplicando controles de operaciones propios para identificar transacciones de alto riesgo antes de enviarlas para ser procesadas. Este tipo de controles ayudan a determinar si un titular o una operación han de ser revisada manualmente por el comercio.

5.a Aplicar límites de revisión basados en el número y/o el importe de las operaciones realizadas por un mismo usuario en periodo determinado de tiempo.

5.b Aplicar límites de revisión basados en el importe de la venta.

5.c Asegurarse que estos límites de revisión se basan en múltiples parámetros,

incluyendo dirección de entrega, número de teléfono o dirección email.

5.d Contactar con aquellos compradores que excedan estos límites para determinar si la operativa es legítima y debe ser aceptada, asumiendo siempre que esta operación haya sido aceptada por el banco emisor.

5.e No permitir a los compradores utilizar más de un usuario, o más de una tarjeta para cada compra.

Modificar los controles de operaciones y los límites de revisión en función de la propia experiencia del comercio dependiendo de cada producto, localidades de envío y patrones de compra de los clientes.

En el caso qua la operación no supere todos los controles indicados, el comercio ha de rechazar la tarjeta como medio de pago y anular, si procede, la operación del TPV.

Los responsables del comercio han de conocer estas medidas de seguridad, hacer acciones de formación a todos los empleados que gestionen los pagos con tarjeta y verificar periódicamente el cumplimiento de estas medidas de seguridad. En caso contrario, se corre el riesgo de que las operaciones fraudulentas se puedan retroceder al comercio y, si el número de operaciones retrocedidas o fraudulentas es significativo, se proceda al bloqueo del terminal y la rescisión del contrato con CatalunyaCaixa.

3.4. SOLICITUD DE DOCUMENTACION / FOTOCOPIAS

Toda persona que realice una compra (presencial o no) mediante una tarjeta financiera tiene derecho a realizar una solicitud de documentación al comercio que justifique el pago. El plazo máximo para esta solicitud es de 12 meses desde la fecha de la operación.

Esta solicitud se debe normalmente a que el propietario de la tarjeta no se acuerda de la operación, o quiere tener más datos de esta, o bien argumenta no haber realizado la operación y pretende devolverla. En algunos casos es porque no relaciona el nombre del comercio con la página web en la que realizó la operación.

Cuando la entidad emisora de la tarjeta solicite el comprobante de una operación, se enviará centralizadamente una carta al comercio indicándole:

1. Los datos de la operación de la que se solicita el comprobante.
2. El número de fax al que ha de transmitir el comprobante junto con la carta recibida.
3. La fecha tope para enviar el comprobante.
4. En el caso que el comercio no tenga fax, se le indica que lleve la carta y el comprobante a su oficina para que ésta realice la transmisión.

El comercio **está obligado** a presentarla. **El plazo de presentación es de 7 días hábiles.**

Si hay envío de mercancía, se deberá adjuntar el certificado de entrega librado por la empresa que realizó el envío. Como norma general **dicho certificado deberá estar firmado por el titular de la tarjeta**, no por una tercera persona.
Como excepción, y para aquellos casos en que no sea posible librar la mercancía al titular de tarjeta (bien por imposibilidad de estar en el lugar y en tiempo pactado para recibirlo, bien porque se trate de un regalo) se permitirá hacer el envió a una tercera persona. En este caso, debería quedar registrado este supuesto en el formulario de pedido que el cliente realizó en el comercio, con la siguiente información:

- Persona autorizada, identificada con nombre y documento de identidad (DNI, Pasaporte, etc.). El pedido se ha de entregar únicamente a esa persona y el albarán de entrega debería de incluir la firma del receptor así como la anotación conforme se ha comprobado el documento de identidad proporcionado.
- Recepción del hotel, identificado por nombre, dirección del hotel, nombre y documento del huésped que lo ha de recibir. La recepción ha de estar firmada por un empleado correctamente identificado del hotel y sellado por este. Además en el comprobante de recepción debería constar que se ha comprobado que el receptor de la mercancía está alojado en el hotel.

Es recomendable no especificar una fecha concreta de entrega de mercancía, salvo en los casos en que esto sea imprescindible, sino un intervalo de días, ya que el incumplimiento es motivo suficiente de devolución.

En el caso de tratarse de un comercio que ofrece servicios y no productos, es decir, que no hay entrega de mercancía, el comercio informará en el formulario de respuesta los siguientes datos:

- Nombre del comercio
- CIF/NIF del comercio
- Código del Comercio (FUC)
- Número de autorización
- Fecha operación
- Número de tarjeta
- Dirección de página web (URL)
- importe transacción
- Moneda
- Nombre del Comprador
- Descripción del producto comprado
- Definir la política sobre devoluciones que sigue el comercio, o bien indicar la URL donde los usuarios pueden informarse de ella

3.5. REGLAMENTACION

El TPV Virtual, por su naturaleza, está sujeto a unas reglas que se derivan de su participación en los sistemas de medios de pago internacionales así como de su gestión por parte de CatalunyaCaixa.

Esta normativa está recogida en el contrato de Establecimientos firmado entre CatalunyaCaixa y el comercio.

Algunas de las reglas más relevantes son enumeradas a continuación:

1. El comercio solo podrá procesar transacciones originadas desde la página(s) web registrada(s) en el contrato con CatalunyaCaixa.

2. El sitio web ha de cumplir, entre otros, los siguientes requisitos:

   2.1 El nombre del comercio y el de la persona propietaria, física o jurídica, de dicha web han de aparecer en la página principal y en la página de pago por tarjeta del site.
   2.2 Política de anulación de compras y devolución de productos.
   2.3 Política de envío de mercancías y plazo de entrega.
   2.4 Datos del servicio de atención al cliente y la manera de acceder al mismo.
   2.5 Política de privacidad y protección de datos personales.

3. El comercio procederá a la anulación inmediata de las operaciones de tarjeta cuando se haya producido un cargo indebido, o no se haya materializado completamente el proceso de venta y entrega de mercancía.

4. El comercio no almacenará de ninguna manera los datos de las tarjetas en su instalación, excepto que fuese necesario para su funcionamiento, en cuyo caso estará sujeto al programa de Seguridad PCI/DSS de VISA y MASTERCARD. Aún en este caso está terminantemente prohibido guardar el CVV2 bajo ninguna circunstancia.

5. El comercio solo podrá procesar bajo un mismo número de establecimiento operaciones que se engloben bajo el código de actividad con el que se ha registrado. Además, en los casos en que el comercio se dedique a actividades especiales (tabaco, medicamentos, contenidos de adultos, líneas aéreas y juegos de azar), tendrá que solicitarse expresamente autorización de forma previa a CatalunyaCaixa para que ésta transmita la propuesta a las marcas de tarjetas.

4. MÓDULO DE ADMINISTRACIÓN

4.1. ACCESO

El Módulo de Administración del TPV virtual de CatalunyaCaixa permite al comercio realizar devoluciones de operaciones así como consultar el detalle de las operaciones y los totales de facturación de tarjetas.

Para acceder al Módulo de Administración el comercio debe seleccionar la correspondiente opción en el menú del servicio de Banca Virtual de CatalunyaCaixa (https://www.catalunyacaixa.com), o bien, conectarse a la siguiente dirección de Internet:

https://canales.redsys.es/cx/

4.2. USUARIOS

CatalunyaCaixa facilitará previamente al comercio un usuario/contraseña de acceso al Módulo de Administración con perfil administrador. En la gestión de usuarios será posible dar de alta nuevos usuarios con uno de los dos siguientes perfiles de acceso:

1. Perfil informativo: sólo se permitirá la consulta de movimientos y totales.
2. Perfil administrador: además de las consultas de movimientos y totales se pueden hacer devoluciones, totales o parciales, de las operaciones de venta.

Por motivos de seguridad es recomendable cambiar las contraseñas.

Dentro del apartado "Usuarios" se incluyen los siguientes subapartados:

1. Contraseña: permite modificar la contraseña de acceso del usuario que en ese momento está conectado.
2. Usuarios: permite realizar todas las funciones de consulta, alta, baja y modificación de usuarios de comercios.
3. Generar Usuarios: permite generar de forma automática, a partir de un código de comercio y número de terminal, un usuario de acceso al módulo de administración con unas características o permisos establecidos por defecto y enviar los datos de dicho usuario al email del comercio especificado.

Los usuarios que se den de alta pueden ser de dos tipos:

1. Terminal: para gestionar las operaciones realizadas en un comercio y terminal determinado
2. Comercio: para gestionar las operaciones realizadas por todos los terminales de un comercio.

4.3. CONSULTA DE OPERACIONES

Para poder consultar las operaciones realizadas durante **los últimos 365 días naturales**, tanto de las autorizadas como de las denegadas, se deberá seleccionar el botón CONSULTAS de la página principal e introducir la fecha de inicio y la fecha de

fin correspondiente al período del cual se desea obtener la información.

No se pueden realizar consultas de más de 30 días consecutivos. En caso de necesitarse se han de realizar consultas consecutivas de periodos de 30 días.

Si se desea consultar una operación en concreto y se conoce el número de referencia de la compra, también se puede acceder directamente al detalle de esa operación.

Una vez pulsado el botón ACEPTAR aparecerá una pantalla donde se relacionarán las operaciones encontradas con los datos de búsqueda.

El resultado de la búsqueda, además de visualizarse por pantalla, se podrá IMPRIMIR o EXPORTAR a fichero de texto con campos delimitados por el separador "**;**".

Fecha ; Hora ; Autorizacion ; Pedido ; Compra (Ptas.) ; Compra (Euros) ; Devolución (Ptas.) ; Devolución (Euros)
25/04/2001;13:03:14;Autorizada 045803;125747 ;500;3,01;15;0,09
25/04/2001;13:05:23;Denegada ;130009 ;500;3,01;
25/04/2001;13:06:05;Autorizada 085903;130043 ;500;3,01;3;0,02
30/04/2001;09:54:13;Autorizada 043150;094522 ;500;3,01;
30/04/2001;10:02:43;Autorizada 045105;095146 ;1425;8,58;
30/04/2001;10:35:07;Autorizada 001534;100743 ;3127;18,84;127;0,77

4.4. DEVOLUCIÓN DE OPERACIONES

Las dos últimas columnas de la pantalla anterior, "Consultar devoluciones" y "Generar devoluciones", permiten al comercio consultar las devoluciones realizadas y generar devoluciones totales o parciales de las operaciones que se muestran.

Tan sólo los usuarios que accedan al Módulo de Administración con contraseña de perfil administrador están autorizados para realizar devoluciones. Se ha de consultar las operaciones por nº Comercio y nº Terminal (habitualmente el nº 1, terminal en Euros).

Para realizar una devolución parcial o total de la operación seleccionada, se deberá pulsar el botón rojo de la columna "Generar devolución" que corresponda a la operación deseada y, a continuación, aparecerá una página para introducir el importe de devolución. El importe de la devolución no debe sobrepasar el importe de la operación original.

Una vez seleccionado el botón ACEPTAR, se mostrará una página con el comprobante de la devolución, el cual se puede imprimir o archivar.

4.5. CONSULTA DE TOTALES

Pulsando el botón de TOTALES de la parte izquierda de la página principal aparecerá un listado de las últimas 45 sesiones. Seleccionar la sesión deseada y pulsar ACEPTAR.

A continuación aparecerá la pantalla con los importes totales y el número de operaciones.

5. INSTALACIÓN

En esta guía se facilita la información necesaria para que el comercio/empresa, o su servicio de informática, realicen la instalación del TPV virtual en la web del comercio electrónico. La instalación consiste básicamente en introducir en la web unas instrucciones informáticas que ejecuten en remoto el software del TPV virtual residente en un servidor seguro de CatalunyaCaixa. Es recomendable que la instalación de estas instrucciones sea ejecutada por el personal especializado que realiza el mantenimiento de la web del comercio.

Para realizar las primeras pruebas reales durante la fase de instalación se aconseja utilizar **cualquier numeración ficticia de tarjeta de 16 dígitos**. Si la instalación ha sido correcta el mensaje de respuesta del TPV virtual deberá ser "TRANSACCION DENEGADA: TARJETA AJENA". Cuando se utilicen tarjetas reales para efectuar las pruebas, las operaciones tendrán efectos reales tanto para el comercio como para el titular de la tarjeta. En estos casos, es conveniente efectuar las correspondientes transacciones de devolución para deshacer los efectos contables en las respectivas cuentas, al mismo tiempo que se prueban las devoluciones.

En el mensaje hay un campo adicional donde los principales datos relacionados con la compra se transmiten codificados por el algoritmo Hash Sha-1.

Aplicaciones a instalar:

OBLIGATORIO: Un formulario de pago implementado en la web del comercio.

OBLIGATORIO: Algoritmo Hash Sha-1 implementado en el servidor de Internet del comercio.

OPCIONAL: Programa para recibir y procesar la respuesta online a la solicitud de autorización del pago.

5.1. FORMULARIO DE PAGO DE LA WEB DEL COMERCIO

En la página de pago de la web del comercio se deberá incluir un botón para que el comprador lo asocie al pago con tarjeta.

El botón deberá estar vinculado al formulario de pago oculto que se detalla a continuación. Cuando el comprador seleccione este botón, el comercio deberá enviar el formulario de pago de la operación al servidor de CatalunyaCaixa en la siguiente dirección:

https://sis.redsys.es/sis/realizarPago

La ventana o frame donde se abra el TPV Virtual ha de tener barras de desplazamiento vertical y horizontal para poder adaptarse a las diferentes páginas de autenticación que pudieran mostrarse al comprador en procesos posteriores.

Los datos que deberá contener el formulario de pago se encuentran en el ANEXO I.

5.2. OPERACIONES RECURRENTES

Se considera una operación recurrente aquella compra en que se fraccionan los pagos, por ejemplo, pago de subscripciones periódicas o pagos aplazados.

El TPV Virtual de CatalunyaCaixa está homologado para que operaciones recurrentes pagadas con tarjetas Visa o MasterCard a través de Internet en las que se haya realizado una autenticación positiva del titular no se puedan retroceder si éste manifiesta que no las ha realizado.

Para poder procesar operaciones recurrentes se deben solicitar autorizaciones a través del formulario de pago del TPV Virtual, informando campos diferentes según se trate de la transacción para el pago de la primera cuota (Transacción Recurrente) o del resto de cuotas (Transacciones Sucesivas):

NOMBRE DEL CAMPO	OBLIGATORIO	OPCIONAL	NO INFORMAR
Ds_Merchant_Amount	Recurrente / Sucesiva		
Ds_Merchant_Currency	Rec. / Suc.		
Ds_Merchant_Order	Rec. / Suc. (mismo valor para todas las operaciones)		
Ds_Merchant_MerchantCode	Rec. / Suc.		
Ds_Merchant_MerchantURL		Rec. / Suc.	
Ds_Merchant_MerchantName		Rec. / Suc.	
Ds_Merchant_ConsumerLanguage	Rec. / Suc.		
Ds_Merchant_MerchantSignature	Rec. / Suc.		
Ds_Merchant_Terminal	Rec. / Suc.		
Ds_Merchant_MerchantData		Rec. / Suc.	
Ds_Merchant_Transaction_Type	Rec. (valor “5” o “R”) /Suc.(valor “6” o “S”)		
Ds_Merchant_DateFrecuency	Recurrente		Sucesiva
Ds_Merchant_ChargeExpiryDate	Recurrente		Sucesiva
Ds_Merchant_SumTotal	Recurrente		Sucesiva

5.3. LOCALIZACIÓN DE ERRORES

Durante el proceso de instalación, si al enviar el formulario de pago que ejecuta en remoto la aplicación TPV Virtual aparece alguno de los errores de la tabla siguiente implicará que alguno de los parámetros de los campos enviados es erróneo.

Tabla de mensajes que recibe el cliente comprador cuando ocurre un error en la operación, así como su significado.

CÓDIGO	MENSAJE
MSG0000	El sistema está ocupado, inténtelo más tarde

MSG0001	Número de pedido repetido
MSG0002	El Bin de la tarjeta no está dado de alta en FINANET
MSG0003	El sistema está arrancando, inténtelo en unos momentos
MSG0004	Error de Autenticación
MSG0005	No existe método de pago válido para su tarjeta
MSG0006	Tarjeta ajena al servicio
MSG0007	Faltan datos, por favor compruebe que su navegador acepta cookies
MSG0008	Error en datos enviados. Contacte con su comercio.

Para localizar el campo erróneo se deberá ver el código fuente de la página de error y buscar, entre el texto HTML, la cadena "**--SIS**". El valor numérico xxxx adjunto a la instrucción "**<!--SISxxxx:-->**" indicará el tipo de error según la tabla del ANEXO IV.

Asimismo en el ANEXO IV se incluye una segunda tabla con los mensajes que se muestran al titular ante los diferentes errores. Solo se incluyen los textos en castellano, se debe tener en cuenta que estarán traducidos al idioma utilizado por el titular.

5.4. DISEÑO DEL ALGORITMO HASH EN EL SERVIDOR DE INTERNET

Se dotará al comercio de una clave, que se utilizará para firmar los datos aportados por el mismo, pudiendo verificarse no solo la identificación del comercio, sino que los datos no han sido alterados en ningún momento. Se utilizará como protocolo de securización el algoritmo público Hash SHA-1, que garantiza los requisitos mínimos de seguridad en cuanto a la autenticación del origen. La clave se proporcionará para ser incluida en la web del comercio.

Este mismo algoritmo se utilizará para asegurar al comercio la autenticidad de los datos de la respuesta, en caso de que se proporcione URL de notificación por parte del comercio.

El tipo de clave SHA1 no está disponible en versiones de php inferiores a la versión 4.3.0. Si su servidor utiliza alguna versión anterior pónganse en contacto con el servicio técnico de CatalunyaCaixa para encontrar una solución alternativa.

Hay dos posibles casos de cálculo de firma electrónica:

• Para operaciones con Ds_Merchant_TransactionType ≠ 5 o R: La firma electrónica del comercio se deberá calcular de la forma siguiente:

Digest=SHA-1(Ds_Merchant_Amount+Ds_Merchant_Order + Ds_Merchant_MerchantCode + DS_Merchant_Currency + Ds_Merchant_TransactionType + Ds_Merchant_MerchantURL + CLAVE SECRETA)

• Para operaciones con Ds_Merchant_TransactionType = 5 o R (PAGO RECURRENTE INICIAL o PAGO DIFERIDO RECURRENTE): La firma electrónica del comercio se deberá calcular de la forma siguiente:

Digest=SHA-1(Ds_Merchant_Amount + Ds_Merchant_Order + Ds_Merchant_MerchantCode + DS_Merchant_Currency + Ds_Merchant_SumTotal + Ds_Merchant_TransactionType + Ds_Merchant_MerchantURL + CLAVE SECRETA)

Si el comercio no tiene URL de notificación "online", se deja el campo Ds_Merchant_MerchantURL en blanco.

Ejemplo

IMPORTE (Ds_Merchant_Amount) = 1235 (va multiplicado por 100 para ser igual que el Ds_Merchant_Amount).
NÚMERO DE PEDIDO (Ds_Merchant_Order) = 29292929
CÓDIGO COMERCIO (Ds_Merchant_MerchantCode) = 201920191
MONEDA (Ds_Merchant_Currency) = 978
CLAVE SECRETA = h2u282kMks01923kmqpo
Cadena resultado: 123529292929201920191978h2u282kMks01923kmqpo
Resultado SHA-1: c8392b7874e2994c74fa8bea3e2dff38f3913c46

La clave secreta nunca debe ser transmitida, ni debe aparecer en el código fuente de la web del comercio, ni debe ser accesible dentro de la estructura de ficheros de la web. Por ello, el cálculo del algoritmo hash SHA-1 debe implementarse en la parte privada del servidor de Internet del comercio.
Si el comercio reside en un servidor ajeno bajo una fórmula de hosting o similar, deberá ponerse en contacto con la empresa proveedora para que le informe del modo de implementar el algoritmo criptográfico.

CatalunyaCaixa facilita ejemplos de conexión con el TPV en distintos lenguajes de programación.

Referencias SHA-1:
- Estándar de Hash Seguro, FIPS PUB 180-1.
  http://www.itl.nist.gov/fipspubs/fip180-1.htm
  http://csrc.nist.gov/publications/fips/fips180-1/fips180-1.pdf
- Lista de Implementaciones Validadas del SHA-1
  http://csrc.nist.gov/cryptval/dss/dsaval.htm
- Las especificaciones del Estándar del Hash Seguro (Algoritmo SHA-1):
  http://csrc.nist.gov/cryptval/shs.html
- ¿Qué es SHA y SHA-1?
  http://www.rsasecurity.com/rsalabs/faq/3-6-5.html

5.5. RESPUESTA ON-LINE

Si el comercio desea disponer del resultado de los pagos inmediatamente después de su realización, existen cuatro mecanismos de respuesta, que pueden coexistir simultáneamente:

1. Consultando, vía Internet, el **Módulo de Administración**.
   Se podrá consultar, imprimir y exportar a fichero las operaciones de los últimos 45 días.
2. Implementando una solución de **Respuesta on-line**.
   Permite que en el mismo momento en que el titular de la tarjeta recibe la respuesta de la petición de pago con tarjeta, la web del comercio reciba un mensaje con la misma información.
3. Vía **fichero con un listado de operaciones**.
   El fichero se generará periódicamente (normalmente será un fichero diario) y será enviado a una dirección de e-mail de forma cifrada.
4. Vía **consulta SOAP**.
   Permite al comercio realizar una consulta de una operación mediante la tecnología SOAP-XML.

La **respuesta online** es el sistema más utilizado. En caso de querer utilizar fichero con listado de operaciones o consulta SOAP habría que ponerse en contacto con el servicio técnico de CatalunyaCaixa, quien informaría al respecto.

Hay dos posibles vías de recepción de la respuesta on-line, que se pueden combinar entre ellas, utilizando ambas a la vez o una de ellas como secundaria en caso de fallar la otra:

- **Vía e-mail**: recepción de la respuesta a la autorización de pago en la dirección de correo electrónico que el comercio haya indicado al solicitar el alta del TPV virtual.

- Vía URL: recepción de la respuesta en la dirección URL indicada en el formulario de pago. Esta opción requiere de unos sencillos desarrollos informáticos en la web del comercio, tanto para habilitar la recepción de la respuesta como para integrarla dentro de la base de datos del comercio. Solo es válida para comercios instalados con el campo de verificación activo. **Es la opción recomendada**.

Para implementar la respuesta on-line vía URL se tendrá que facilitar en el formulario de petición de pago una URL donde recibir las respuestas (campo Ds_Merchant_MerchantURL). Esta URL será un CGI, Servlet o similar, desarrollado en el lenguaje que se considere adecuado para que el servidor del comercio sea capaz de interpretar la respuesta que le envíe el TPV virtual. **Será una página transparente al usuario** (es decir, no se cargará en el navegador). En ella podrá recibir y recoger los datos de la respuesta on-line i de esta forma introducirlos en su base de datos.

El protocolo utilizado en las respuestas vía URL puede ser http o https, el formato de este mensaje es un formulario HTML, enviado con el método POST, y cuyos campos son los siguientes:

DATO	NOMBRE DEL CAMPO	LONG.	COMENTARIOS
Fecha	Ds_Date	10 A	Fecha de la transacción (DD-MM-AAAA).
Hora	Ds_Hour	5 A	Hora de la transacción (HH:MM).
Importe	Ds_Amount	12 N	Mismo valor que en la petición.
Moneda	Ds_Currency	4 N	Mismo valor que en la petición.
Código de pedido	Ds_Order	12 N	Mismo valor que en la petición.
Código de comercio Código FUC	Ds_MerchantCode	9 N	Mismo valor que en la petición.
Número de terminal	Ds_Terminal	3 N	Mismo valor que en la petición.
Firma para el comercio	Ds_Signature	40 AN	Ver instrucciones al pie de la tabla.
Código de respuesta	Ds_Response	4 N	Ver lista al pie de la tabla.
Tipo de transacción	Ds_TransactionType	1 AN	Mismo valor que en la petición.
Pago seguro	Ds_SecurePayment	1 N	0 – Pago NO seguro 1 – Pago seguro
Datos del comercio	Ds_MerchantData	1024 AN	Información opcional enviada por el comercio en el formulario petición de pago.
País del Titular	Ds_Card_Country	3 N	País de emisión de la tarjeta Ver ANEXO 5 con lista de países
Código de autorización	Ds_AuthorisationCode	6 AN	Código alfanumérico de autorización asignado a la aprobación por la institución autorizadora.
Idioma del Titular	Ds_ConsumerLanguage	3 N	El valor 0, indicará que no se ha determinado el idioma del cliente. (Opcional).
Tipo de tarjeta	Ds_Card_Type	1 AN	C – tarjeta de crédito D – tarjeta de débito

El campo DS_Card_Type puede no venir informado en algunas respuestas, según la entidad emisora de la tarjeta.
En los campos Ds_Currency, Ds_Terminal y Ds_ConsumerLanguage la longitud se considera máxima por lo que no es imprescindible el relleno con ceros a la izquierda.
La firma será generada con los campos exactamente como se envíen.

Igual que en la petición de pago de una compra, la respuesta on-line incluye una firma electrónica que garantizará la integridad de las respuestas.

El algoritmo será el mismo y la fórmula para el cálculo será:

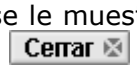
Digest=SHA-1(Ds_ Amount + Ds_ Order + Ds_MerchantCode + Ds_ Currency + Ds _Response + + CLAVE SECRETA)

La conexión utilizada para comunicar la confirmación "on-line" entre el TPV Virtual y el comercio puede ser SSL. Para evitar comunicaciones fraudulentas, opcionalmente el comercio puede activar un filtro que limite la recepción de la confirmación "online" solo desde el TPV Virtual.

El TPV Virtual por defecto puede comunicar a los puertos 80, 443, 8080 y 8081 del comercio. Otros puertos deberán ser consultados al servicio técnico de CatalunyaCaixa.

Una vez que el comercio recibe el formulario, los valores del código de respuesta indican si la operación está aprobada o denegada y, en este caso, el motivo por el que se rechaza. La lista de valores se encuentra en el ANEXO II del presente documento.

5.6. CONTINUIDAD DE LA SESIÓN DEL NAVEGADOR

Una vez el titular de la tarjeta finaliza el proceso de pago y se le muestra la pantalla con el resultado del mismo, esta incluye un botón de 

para que el comprador retorne a la sesión de la web del comercio.

La forma en que continua la sesión del comercio con su cliente irá en función de las instrucciones asociadas al botón de 

. Estas instrucciones, que el titular del comercio habrá comunicado a CatalunyaCaixa en el cuestionario que se le tramita para iniciar el proceso de alta, pueden ser:

- **Instrucción "CERRAR VENTANA"**: Al seleccionar 

se cierra la ventana o frame con el resultado del pago y se continúa la sesión en la página del comercio que permanecía en segundo plano.

- **Instrucción "URL_OK y URL_KO"**: Al seleccionar 

la sesión del navegador continua en la misma ventana de la página de pago, redirigiéndose a una URL que el comercio previamente haya comunicado a CatalunyaCaixa. Esta URL podrá ser diferente si el pago ha sido autorizado (URL_OK) o denegado (URL_KO).
  Hay que tener en cuenta que si el comprador cierra la ventana a través del botón  del navegador, las URL_OK/URL_KO no serán operativas y la sesión continuará en la página del comercio que permanecía en segundo plano.

- **Opción para comercios con RESPUESTA ON-LINE vía URL**: Además de las dos instrucciones anteriores, los comercios que disponen del servicio de RESPUESTA ON-LINE VIA URL la continuidad de la sesión la puede realizar la propia web del comercio, cerrando la ventana de pago en el momento en que se reciba la respuesta on-line.

5.7. ENVÍO DE TRANSACCIONES AL TPV VIRTUAL MEDIANTE XML

Existe la posibilidad de enviar la transacción mediante XML permitiendo automatizar el envío de transacciones, por ejemplo un grupo de devoluciones.

Es muy importante tener en cuenta que este recurso es válido solo para los siguientes tipos de transacciones (Ds_Merchant_TransactionType), ya que al no estar presente el titular no podrá autenticarse:

1 - Preautorización
2 - Confirmación de preautorización
3 - Devolución automática
6 - Transacción sucesiva
8 - Confirmación de autenticación
9 - Anulación de preautorizaciones
A - Pago no seguro sin autenticación
O - Preautorización Diferida
P - Confirmación de Preautorización Diferida
Q - Anulación de Preautorización Diferida
R - Preautorización Diferida Recurrente
S - Confirmación de Preautorización Diferida Recurrente / Transacción Sucesiva

Los tipos 1, A, O, P, Q, R i S no están activados por defecto y los comercios que lo consideren necesario lo tendrán que solicitar a su oficina de CatalunyaCaixa. Todas las operaciones que se envíen mediante este sistema se consideraran NO SEGURAS ya que no puede haber autenticación. Además esta opción requiere que previamente el comercio sea considerado cumplidor del programa PCI-DSS de seguridad en los datos de tarjetas.

La comunicación se realizará mediante un envío del documento XML a la dirección indicada del TPV Virtual. El sistema interpretará el documento XML y realizará las validaciones pertinentes para, a continuación, procesar la operación. Dependiendo del resultado de la operación, se monta un documento XML de respuesta con el resultado de la misma.

El documento XML se transmitirá mediante un envío con POST a la dirección:

Real: https://sis.redsys.es/sis/operaciones

El envío se realizará simulando la petición realizada por un formulario con un único input llamado "entrada". El valor de "entrada" será el documento XML, el cual debe estar en formato x-www-form-urlencoded.

Se definen dos tipos de mensaje en el ANEXO III:

1. DATOSENTRADA: Mensaje de solicitud enviado.
2. RETORNOXML: Respuesta a la petición.

5.8. EJEMPLOS Y SIMULADORES

Una vez el proceso de alta del TPV Virtual esté completado el comercio recibirá vía e-mail los siguientes ficheros de ayuda a la instalación:

→ Un simulador del TPV virtual del comercio formado por:

- Un formulario de pago implementado en HTML.
- Algoritmo Hash Sha-1 implementado en JavaScript.

→ Ejemplos de programación del algoritmo Hash Sha-1 implementados en:

- C
- CGI en C
- Java-JSP
- Java-JSP+Bean
- JavaScript (no recomendado si se instala en la misma web del comercio)
- ASP
- Perl
- PHP

Si el servidor de Internet del comercio necesita de otros lenguajes, el comercio/empresa deberá ponerse en contacto con el Servicio Técnico de Soporte a la Instalación de CatalunyaCaixa.

5.9. SERVICIO TÉCNICO DE SOPORTE A LA INSTALACIÓN

CatalunyaCaixa pone a disposición del comercio/empresa que desee instalar el TPV virtual el Servicio Técnico de Soporte a la Instalación que atenderá, de forma totalmente gratuita, cualquier consulta técnica u operativa sobre su instalación y funcionamiento.

Telf. **902 110 560**

Horario de atención telefónica:

INVIERNO: 16 Septiembre a 30 Junio ➔ Lunes a Jueves 8:00 h.- 18:00 h.
Viernes 8:00 h.- 15:00 h.

VERANO: 1 Julio a 15 Septiembre ➔ Lunes a Viernes 8:00 h.- 15:00 h.

e m@il **soportetpvvirtual@catalunyacaixa.com**

Asimismo para incidencias sobre comunicaciones, inestabilidad del sistema y problemas similares CatalunyaCaixa pone a su disposición el teléfono 902.198747 las 24 horas del día todos los días del año.

ANEXOS

ANEXO I. DATOS DEL FORMULARIO DE PAGO

DATO	NOMBRE DEL CAMPO	LONG.	COMENTARIOS
Importe	Ds_Merchant_Amount	12 N	**Obligatorio.** Las dos últimas posiciones se consideran decimales, excepto en Yenes.
Moneda	Ds_Merchant_Currency	4 N	**Obligatorio.** 978 – Euro 840 – Dólar 826 – Libra Esterlina 392 – Yen 32 – Austral Argentino 124 – Dólar Canadiense 152 – Peso Chileno 170 – Peso Colombiano 356 – Rupia India 484 – Nuevo Peso Mejicano 604 – Nuevos Soles 756 – Franco Suizo 986 – Real Brasileño 937 – Bolívar Venezolano 949 – Lira Turca
Código de pedido	Ds_Merchant_Order	mín. 4N máx.12 AN	**Obligatorio.** Los 4 primeros dígitos deben ser numéricos, para los dígitos restantes solo utilizar los siguientes caracteres ASCII Del 30 = **0** al 39 = **9** Del 65 = **A** al 90 = **Z** Del 97 = **a** al 122 = **z** El código ha de ser diferente de transacciones anteriores.
Descripción del Producto	Ds_Merchant_ProductDescription	Máx.125 AN	**Este campo se mostrará al titular en la pantalla de confirmación de la compra.**
Nombre y apellidos del titular	Ds_Merchant_Titular	Máx. 60 AN	**Este campo se mostrará al titular en la pantalla de confirmación de la compra.**
Identificación de comercio código FUC	Ds_Merchant_MerchantCode	9 N	**Obligatorio.** Código fijo asignado por CatalunyaCaixa.
URL	Ds_Merchant_MerchantURL	250 AN	Obligatorio **si** el comercio tiene notificación "online". URL del comercio que recibirá un post con los datos de la transacción.
URLOK	Ds_Merchant_UrlOK	250 AN	**Opcional.** **Si se envía será utilizado como URLOK, ignorando el configurado en el módulo de administración en caso de tenerlo.**
URLKO	Ds_Merchant_UrlKO	250 AN	**Opcional.** **Si se envía será utilizado como URLKO, ignorando el configurado en el módulo de administración en caso de tenerlo.**
Nombre del comercio	Ds_Merchant_MerchantName	25 AN	**Opcional.** **Será el nombre del comercio que aparecerá en la página de pago del cliente, si lo hubiera.**
Idioma del titular	Ds_Merchant_ConsumerLanguage	3 N	**Opcional.** 0 – Cliente 1 – Castellano 2 – Inglés 3 – Catalán 8 – Sueco 9 – Portugués 10 – Valenciano 11 – Polaco

DATO	NOMBRE DEL CAMPO	LONG.	COMENTARIOS
			4 – Francés 12 – Gallego 5 – Alemán 13 – Euskera 6 – Holandés 7 – Italiano
Firma del comercio	Ds_Merchant_MerchantSignature	40 AN	**Obligatorio.** Ver apartado 5.2. - DISEÑO DEL ALGORITMO HASH EN EL SERVIDOR DE INTERNET
Número de terminal	Ds_Merchant_Terminal	3 N	**Obligatorio.** De forma estándar: 1 – Operaciones en euros (Ds_Merchant_Currency = 978) En caso de querer más terminales se pueden solicitar al servicio técnico de CatalunyaCaixa
Datos del comercio	Ds_Merchant_MerchantData	1024 AN	**Opcional.** Información libre del comercio para ser recibida en la respuesta online (vía URL o e-mail).
Tipo de transacción	Ds_Merchant_TransactionType	1 N	**Opcional (por defecto igual a "0").** 0 – Pago estándar 1 – Preautorización (solo comercios autorizados) 2 – Confirmación de Preautorización 3 – Devolución parcial o total 5 – Transacción recurrente 6 – Transacción Sucesiva 7 – Autenticación 8 – Confirmación de Autenticación 9 – Anulación de Preautorización O – Preautorización Diferida P – Confirmación de Preautorización Diferida Q – Anulación de Preautorización Diferida R – Preautorización Recurrente Diferida S – Confirmación de Preautorización Recurrente Diferida / Transacción Sucesiva de Operaciones Recurrentes
Importe Total	Ds_Merchant_SumTotal	12 N	**Obligatorio. si "Tipo Transacción = 5"** Representa la suma total de los importes de las cuotas. Las dos últimas posiciones son los decimales.
Frecuencia de una transacción recurrente	Ds_Merchant_DateFrecuency	3 N	**Obligatorio. si "Tipo Transacción = 5"** Indica el intervalo mínimo de tiempo, en días, entre el cobro de cuotas en un pago recurrente (ver 4.1.1)
Caducidad de una transacción recurrente	Ds_Merchant_ChargeExpiryDate	10 AN	**Obligatorio si "Tipo Transacción = 5"** Fecha de cobro de la última cuota en un pago recurrente (ver 4.1.1) Formato: AAAA-MM-DD
Código de autorización	Ds_Merchant_AuthorisationCode	6 N	**Opcional.** **Representa el código de autorización necesario para identificar una transacción recurrente sucesiva en las devoluciones de operaciones recurrentes sucesivas.**
Fecha de la operación recurrente sucesiva	Ds_Merchant_TransactionDate	10 AN	**Opcional.** **Formato yyyy-MM-dd. Representa la fecha de la operación recurrente sucesiva, necesaria para identificar la transacción en las devoluciones de operaciones recurrentes sucesivas. Obligatorio para las devoluciones de operaciones recurrentes.**

ANEXO II. TABLA DE CÓDIGOS DE RESPUESTA (Ds_Response)

Códigos de respuesta enviados por el banco emisor de la tarjeta

CODIGOS DE RESPUESTA PARA INDICAR QUE LA TRANSACCION HA SIDO APROBADA		
CODIGO	**DESCRIPCION BREVE**	**COMENTARIO**
000	TRANSACCION APROBADA	Transacción autorizada por el banco emisor de la tarjeta
001	TRANSACCION APROBADA PREVIA IDENTIFICACION DE TITULAR	Código exclusivo para transacciones Verified by Visa o MasterCard SecureCode. - - - - - La transacción ha sido autorizada y, además, el banco emisor nos informa que ha autenticado correctamente la identidad del titular de la tarjeta.
002 - 099	TRANSACCION APROBADA	Transacción autorizada por el banco emisor.

CODIGOS DE RESPUESTA PARA INDICAR QUE LA TRANSACCION HA SIDO DENEGADA		
CODIGO	**DESCRIPCION BREVE**	**COMENTARIO**
101	TARJETA CADUCADA	Transacción denegada porque la fecha de caducidad de la tarjeta que se ha informado en el pago, es anterior a la actualmente vigente.
102	TARJETA BLOQUEDA TRANSITORIAMENTE O BAJO SOSPECHA DE FRAUDE	Tarjeta bloqueada transitoriamente por el banco emisor o bajo sospecha de fraude.
104	OPERACIÓN NO PERMITIDA	Operación no permitida para ese tipo de tarjeta.
106	NUM. INTENTOS EXCEDIDO	Excedido el número de intentos con PIN erróneo.
107	CONTACTAR CON EL EMISOR	El banco emisor no permite una autorización automática. Es necesario contactar telefónicamente con su centro autorizador para obtener una aprobación manual.
109	IDENTIFICACIÓN INVALIDA DEL COMERCIO O TERMINAL	Denegada porque el comercio no está correctamente dado de alta en los sistemas internacionales de tarjetas.
110	IMPORTE INVALIDO	El importe de la transacción es inusual para el tipo de comercio que solicita la autorización de pago.
114	TARJETA NO SOPORTA EL TIPO DE OPERACIÓN SOLICITADO	Operación no permitida para ese tipo de tarjeta.
116	DISPONIBLE INSUFICIENTE	El titular de la tarjeta no dispone de suficiente crédito para atender el pago.
118	TARJETA NO REGISTRADA	Tarjeta inexistente o no dada de alta por el banco emisor.
119	DENEGACION SIN ESPECIFICAR MOTIVO	Operación denegada por banco emisor debido a control al comercio electrónico
125	TARJETA NO EFECTIVA	Tarjeta inexistente o no dada de alta por el banco emisor.
129	ERROR CVV2/CVC2	Código exclusivo para transacciones en las que se solicita el código de 3 dígitos CVV2 (tarj.Visa) o CVC2 (tarj.MasterCard) del reverso de la tarjeta. - - - - - Es erróneo el código CVV2/CVC2 informado por el comprador.
167	CONTACTAR CON EL EMISOR: SOSPECHA DE FRAUDE	Debido a una sospecha de que la transacción es fraudulenta el banco emisor no permite una autorización automática. Es necesario contactar telefónicamente con su centro autorizador para obtener una aprobación manual.
180	TARJETA AJENA AL SERVICIO	Operación no permitida para ese tipo de tarjeta.
181 - 182	TARJETA CON RESTRICCIONES DE DEBITO	Tarjeta bloqueada transitoriamente por el banco emisor.

CODIGOS DE RESPUESTA PARA INDICAR QUE LA TRANSACCION HA SIDO DENEGADA		
CODIGO	**DESCRIPCION BREVE**	**COMENTARIO**
	O CREDITO	
184	ERROR EN AUTENTICACION	Código exclusivo para transacciones Verified by Visa o MasterCard SecureCode. - - - - - La transacción ha sido denegada porque el banco emisor no pudo autenticar debidamente al titular de la tarjeta.
190	DENEGACION SIN ESPECIFICAR EL MOTIVO	Transacción denegada por el banco emisor pero sin que este dé detalles acerca del motivo.
191	FECHA DE CADUCIDAD ERRONEA	Transacción denegada porque la fecha de caducidad de la tarjeta que se ha informado en el pago, no se corresponde con la actualmente vigente.

CODIGOS DE RESPUESTA PARA INDICAR QUE LA TRANSACCION HA SIDO DENEGADA Y QUE, ADEMAS, EL BANCO EMISOR CONSIDERA QUE LA TARJETA ESTA EN UNA SITUACION DE POSIBLE FRAUDE Y, POR ELLO, SOLICITA DE RETENERLA FISICAMENTE O DE ACTIVARLA VIRTUALMENTE EN "LISTAS NEGRAS"		
CODIGO	**DESCRIPCION BREVE**	**COMENTARIO**
201	TARJETA CADUCADA	Transacción denegada porque la fecha de caducidad de la tarjeta que se ha informado en el pago, es anterior a la actualmente vigente. - - - - - Además, el banco emisor considera que la tarjeta está en una situación de posible fraude y, por ello, solicita de retenerla físicamente o de activarla virtualmente en "listas negras".
202	TARJETA BLOQUEDA TRANSITORIAMENTE O BAJO SOSPECHA DE FRAUDE	Tarjeta bloqueada transitoriamente por el banco emisor o bajo sospecha de fraude. - - - - - Además, el banco emisor considera que la tarjeta está en una situación de posible fraude y, por ello, solicita de retenerla físicamente o de activarla virtualmente en "listas negras".
204	OPERACION NO PERMITIDA	Operación no permitida para ese tipo de tarjeta. - - - - - Además, el banco emisor considera que la tarjeta está en una situación de posible fraude y, por ello, solicita de retenerla físicamente o de activarla virtualmente en "listas negras".
207	CONTACTAR CON EL EMISOR	El banco emisor no permite una autorización automática. Es necesario contactar telefónicamente con su centro autorizador para obtener una aprobación manual. - - - - - Además, el banco emisor considera que la tarjeta está en una situación de posible fraude y, por ello, solicita de retenerla físicamente o de activarla virtualmente en "listas negras".
208 - 209	TARJETA PERDIDA O ROBADA	Tarjeta bloqueada por el banco emisor debido a que el titular le ha manifestado que le ha sido robada o perdida. - - - - - *Además, el banco emisor considera que la tarjeta está en una situación de posible fraude y, por ello, solicita de retenerla físicamente o de activarla virtualmente en "listas negras".*

CODIGOS DE RESPUESTA PARA INDICAR QUE LA TRANSACCION HA SIDO DENEGADA Y QUE, ADEMAS, EL BANCO EMISOR CONSIDERA QUE LA TARJETA ESTA EN UNA SITUACION DE POSIBLE FRAUDE Y, POR ELLO, SOLICITA DE RETENERLA FISICAMENTE O DE ACTIVARLA VIRTUALMENTE EN "LISTAS NEGRAS"		
CODIGO	**DESCRIPCION BREVE**	**COMENTARIO**
280	ERROR CVV2/CVC2	Código exclusivo para transacciones en las que se solicita el código de 3 dígitos CVV2 (tarj.Visa) o CVC2 (tarj.MasterCard) del reverso de la tarjeta. - - - - - Es erróneo el código CVV2/CVC2 informado por el comprador. - - - - - Además, el banco emisor considera que la tarjeta está en una situación de posible fraude y, por ello, solicita de retenerla físicamente o de activarla virtualmente en "listas negras".
290	DENEGACION SIN ESPECIFICAR EL MOTIVO	Transacción denegada por el banco emisor pero sin que este dé detalles acerca del motivo. - - - - - Además, el banco emisor considera que la tarjeta está en una situación de posible fraude y, por ello, solicita de retenerla físicamente o de activarla virtualmente en "listas negras".

CODIGOS DE RESPUESTA REFERIDOS A ANULACION O RETROCESION PARCIAL *(Ds_Merchant_TransactionType = 3)*		
CODIGO	**DESCRIPCION BREVE**	**COMENTARIO**
400	ANULACION ACEPTADA	Transacción de anulación o retrocesión parcial aceptada por el banco emisor.
480	NO ENCONTRADA LA OPERACIÓN ORIGINAL O TIME-OUT EXCEDIDO	La anulación o retrocesión parcial no ha sido aceptada porque no se ha localizado la operación original, o bien, porque el banco emisor no ha dado respuesta dentro del time-out predefinido.
481	ANULACION ACEPTADA	Transacción de anulación o retrocesión parcial aceptada por el banco emisor. No obstante, la respuesta del banco emisor se ha recibido con mucha demora, fuera del time-out predefinido.

CODIGOS DE RESPUESTA REFERIDOS A CONCILIACIONES DE PRE-AUTORIZACIONES O PRE-AUTENTICACIONES *(Ds_Merchant_TransactionType = 2 ó 8)*		
CODIGO	**DESCRIPCION BREVE**	**COMENTARIO**
500	CONCILIACION ACEPTADA	La transacción de conciliación ha sido aceptada por el banco emisor.
501 - 503	NO ENCONTRADA LA OPERACION ORIGINAL O TIME-OUT EXCEDIDO	La conciliación no ha sido aceptada porque no se ha localizado la operación original, o bien, porque el banco emisor no ha dado respuesta dentro del time-out predefinido.

CODIGOS DE RESPUESTA REFERIDOS A CONCILIACIONES DE PRE-AUTORITZACIONES DIFERIDAS O PRE-AUTORITZACIONES DIFERIDAS RECURRENTES *(Ds_Merchant_TransactionType = O o R)*		
CODI	**DESCRIPCIÓ BREU**	**COMENTARI**
9928	ANULACIÓN DE PREAUTORITZACIÓN REALIZADA	El sistema ha anulado la preautorización diferida al haber pasado más de 72 horas.

	POR EL SISTEMA	
9929	ANULACIÓN DE PREAUTORITZACIÓN REALIZADA POR EL COMERCIO	La anulación de la preautorización ha sido aceptada

Códigos de respuesta enviados por la propia plataforma de pagos de CATALUNYACAIXA

CODIGOS DE RESPUESTA PARA INDICAR QUE LA TRANSACCION HA SIDO RECHAZADA POR LA PLATAFORMA DE PAGOS DE CATALUNYACAIXA		
CODIGO	**DESCRIPCION BREVE**	**COMENTARIO**
904	COMERCIO NO REGISTRADO EN EL FUC	Hay un problema en la configuración del código de comercio. Contactar con CatalunyaCaixa para solucionarlo.
909	ERROR DE SISTEMA	Error en la estabilidad de la plataforma de pagos de CatalunyaCaixa o en la de los sistemas de intercambio de Visa o MasterCard.
912	EMISOR NO DISPONIBLE	El centro autorizador del banco emisor no está operativo en estos momentos.
913	TRANSMISION DUPLICADA	Se ha procesado recientemente una transacción con el mismo número de pedido (Ds_Merchant_Order).
916	IMPORTE DEMASIADO PEQUEÑO	No es posible operar con este importe.
928	TIME-OUT EXCEDIDO	El banco emisor no da respuesta a la petición de autorización dentro del time-out predefinido.
940	TRANSACCION ANULADA ANTERIORMENTE	Se está solicitando una anulación o retrocesión parcial de una transacción que con anterioridad ya fue anulada.
941	TRANSACCION DE AUTORIZACION YA ANULADA POR UNA ANULACION ANTERIOR	Se está solicitando la confirmación de una transacción con un número de pedido (Ds_Merchant_Order) que se corresponde a una operación anulada anteriormente.
942	TRANSACCION DE AUTORIZACION ORIGINAL DENEGADA	Se está solicitando la confirmación de una transacción con un número de pedido (Ds_Merchant_Order) que se corresponde a una operación denegada.
943	DATOS DE LA TRANSACCION ORIGINAL DISTINTOS	Se está solicitando una confirmación errónea.
944	SESION ERRONEA	Se está solicitando la apertura de una tercera sesión. En el proceso de pago solo está permitido tener abiertas dos sesiones (la actual y la anterior pendiente de cierre).
945	TRANSMISION DUPLICADA	Se ha procesado recientemente una transacción con el mismo número de pedido (Ds_Merchant_Order).
946	OPERACION A ANULAR EN PROCESO	Se ha solicitada la anulación o retrocesión parcial de una transacción original que todavía está en proceso y pendiente de respuesta.
947	TRANSMISION DUPLICADA EN PROCESO	Se está intentando procesar una transacción con el mismo número de pedido (Ds_Merchant_Order) de otra que todavía está pendiente de respuesta.
949	TERMINAL INOPERATIVO	El número de comercio (Ds_Merchant_MerchantCode) o el de terminal (Ds_Merchant_Terminal) no están dados de alta o no son operativos.
950	DEVOLUCION NO PERMITIDA	La devolución no está permitida por regulación.
965	VIOLACIÓN NORMATIVA	Violación de la Normativa de Visa o Mastercard

CODIGOS DE RESPUESTA PARA INDICAR QUE LA TRANSACCION HA SIDO RECHAZADA POR LA PLATAFORMA DE PAGOS DE CATALUNYACAIXA		
CODIGO	**DESCRIPCION BREVE**	**COMENTARIO**
9064	LONGITUD TARJETA INCORRECTA	Nº posiciones de la tarjeta incorrecta
9078	NO EXISTE METODO DE PAGO	Los tipos de pago definidos para el terminal (Ds_Merchant_Terminal) por el que se procesa la transacción, no permiten pagar con el tipo de tarjeta informado.
9093	TARJETA NO EXISTE	Tarjeta inexistente.
9094	DENEGACION DE LOS EMISORES	Operación denegada por parte de los emisoras internacionales
9104	OPER. SEGURA NO ES POSIBLE	Comercio con autenticación obligatoria y titular sin clave de compra segura
9218	NO SE PUEDEN HACER OPERACIONES SEGURAS	La entrada Operaciones no permite operaciones Seguras
9253	CHECK-DIGIT ERRONEO	Tarjeta no cumple con el check-digit (posición 16 del número de tarjeta calculada según algoritmo de Luhn).
9256	PREAUTORITZACION NO HABILITADA EN COMERCIO	El comercio no puede hacer Preautoritzaciones
9257	PREAUT. NO HABILITADA PARA LA TARGETA	La tarjeta no está habilitada para procesar Preautorizaciones
9261/9282	OPERACIÓN SUPERA ALERTA CX	La transacción supera algún limite establecido per CX
9281	SUPERA ALERTAS BLOQUEANTES	La operación excede las alertas bloqueantes, no se puede procesar
9283	SUPERA ALERTAS BLOQUANTES	La operación excede las alertas bloqueantes, no se puede procesar
9912	EMISOR NO DISPONIBLE	El centro autorizador del banco emisor no está operativo en estos momentos.
9913	ERROR EN CONFIRMACION	Error en la confirmación que el comercio envía al TPV Virtual (solo aplicable en la opción de sincronización SOAP)
9914	CONFIRMACION "KO"	Confirmación "KO" del comercio (solo aplicable en la opción de sincronización SOAP)
9915	PAGO CANCELADO	El usuario ha cancelado el pago
9928	AUTORIZACIÓN EN DIFERIDO ANULADA	Anulación de autorización en diferido realizada por el SIS (proceso batch)
9929	AUTORIZACIÓN EN DIFERIDO ANULADA	Anulación de autorización en diferido realizada por el comercio
9997	DOBLE OPERACIÓN SIMULTANEA	Existe una operación previa siendo procesada con el mismo número de tarjeta de forma simultánea.
9998	ESTADO OPERACIÓN: SOLICITADA	Estado temporal mientras la operación se procesa. Cuando la operación termine este código cambiará. Si el cliente cierra el navegador antes de que aparezca la pasarela, éste será el código de error que aparecerá en el módulo.
9999	ESTADO OPERACIÓN: AUTENTICANDO	Estado temporal mientras el TPV realiza la autenticación del titular. Una vez finalizado este proceso el TPV asignará un nuevo código a la operación. Si el cliente cierra el navegador antes de recibir respuesta a la autenticación, éste será el código de error que aparecerá en el módulo.

ANEXO III. MENSAJES XML

1. Especificación del documento DATOSENTRADA.

Este mensaje se envía para solicitar una operación a la plataforma del TPV Virtual:

Versión 1.0 :

```
<!ELEMENT DATOSENTRADA
    (DS_Version,
    DS_MERCHANT_AMOUNT,
    DS_MERCHANT_CURRENCY,
    DS_MERCHANT_ORDER,
    DS_MERCHANT_MERCHANTCODE,
    DS_MERCHANT_MERCHANTURL,
    DS_MERCHANT_MERCHANTNAME ?,
    DS_MERCHANT_CONSUMERLANGUAGE ?,
    DS_MERCHANT_MERCHANTSIGNATURE,
    DS_MERCHANT_TERMINAL,
    DS_MERCHANT_TRANSACTIONTYPE,
    DS_MERCHANT_MERCHANTDATA ?,
    DS_MERCHANT_PAN?,
    DS_MERCHANT_EXPIRYDATE ?,
    DS_MERCHANT_CVV2 ?)>

<!ELEMENT DS_Version (#PCDATA)>
<!ELEMENT DS_MERCHANT_AMOUNT (#PCDATA)>
<!ELEMENT DS_MERCHANT_CURRENCY (#PCDATA)>
<!ELEMENT DS_MERCHANT_ORDER (#PCDATA)>
<!ELEMENT DS_MERCHANT_MERCHANTCODE (#PCDATA)>
<!ELEMENT DS_MERCHANT_MERCHANTURL (#PCDATA)>
<!ELEMENT DS_MERCHANT_MERCHANTNAME (#PCDATA)>
<!ELEMENT DS_MERCHANT_CONSUMERLANGUAGE (#PCDATA)>
<!ELEMENT DS_MERCHANT_MERCHANTSIGNATURE (#PCDATA)>
<!ELEMENT DS_MERCHANT_TERMINAL (#PCDATA)>
<!ELEMENT DS_MERCHANT_TRANSACTIONTYPE (#PCDATA)>
<!ELEMENT DS_MERCHANT_MERCHANTDATA (#PCDATA)>
<!ELEMENT DS_MERCHANT_PAN (#PCDATA)>
<!ELEMENT DS_MERCHANT_EXPIRYDATE (#PCDATA)>
<!ELEMENT DS_MERCHANT_CVV2 (#PCDATA)>
```

Donde:

- DS_Version: Versión de la DTD utilizada para validar el mensaje XML
- DS_MERCHANT_AMOUNT: ver APARTADO 5.1.
- DS_MERCHANT_CURRENCY: ver APARTADO 5.1.
- DS_MERCHANT_ORDER: ver APARTADO 5.1.
- DS_MERCHANT_MERCHANTCODE: ver APARTADO 5.1.
- DS_MERCHANT_MERCHANTURL: ver APARTADO 5.1.
- DS_MERCHANT_MERCHANTNAME: ver APARTADO 5.1.
- DS_MERCHANT_CONSUMERLANGUAGE : ver APARTADO 5.1.
- DS_MERCHANT_MERCHANTSIGNATURE:
  SHA1 de los campos Ds_Merchant_Amount + Ds_Merchant_Order +Ds_Merchant_MerchantCode + DS_Merchant_Currency + *DS_MERCHANT_PAN* + *DS_MERCHANT_CVV2* + DS_MERCHANT_TRANSACTIONTYPE + CLAVE SECRETA.
  DS_MERCHANT_PAN solo se incluirá si se envía en el mensaje.
  DS_MERCHANT_CVV2 solo se incluirá si se envía en el mensaje.
- DS_MERCHANT_TERMINAL: ver APARTADO 5.1.
- DS_MERCHANT_TRANSACTIONTYPE: solo se permiten los tipos:

  1-Preautorización (válido solo si el comercio está autorizado y trabaja en modo no seguro)
  2- Confirmación de preautorización
  3- Devolución Automática
  6- Transacción Sucesiva
  8- Confirmación de Autenticación
  9- Anulaciones de preautorizaciones

A- Pago no seguro sin autenticación (por defecto esta operación no está permitida y solo podrá realizarse previa autorización de CatalunyaCaixa).

- DS_MERCHANT_MERCHANTDATA: ver APARTADO 5.1.
- DS_MERCHANT_PAN : número de tarjeta.
- DS_MERCHANT_EXPIRYDATE : fecha caducidad (AAMM).
- DS_MERCHANT_AUTHORISATIONCODE : solo válido para devoluciones de transacciones recurrentes sucesivas. Ver APARTADO 5.1.
- DS_MERCHANT_TRANSACTIONDATE : solo válido para devoluciones de transacciones recurrentes sucesivas. Ver APARTADO 5.1.
- DS_MERCHANT_CVV2: Código CVV2/CVC2 de la tarjeta (Dato opcional). En caso de que se incluya, se debe añadir a la firma, de la siguiente manera:

firma = SHA1(datos + clave_entidad)

Donde 'datos' es una cadena formada por:

datos=importe + pedido + comercio + moneda
- Si es una autorización o preautorización: datos = datos + tarjeta
- Si además de ser pago tradicional, se envía CVV2:
datos = datos + CVV2

Por último, siempre se le añade el tipo de operación:
datos = datos + tipo_operación

A continuación se muestra un ejemplo del mensaje:

```
<DATOSENTRADA>
        <DS_Version>
        0.1
        </DS_Version>
        <DS_MERCHANT_CURRENCY>
        978
        </DS_MERCHANT_CURRENCY>
        <DS_MERCHANT_MERCHANTURL>
        https://pruebaCom.jsp
</DS_MERCHANT_MERCHANTURL>
<DS_MERCHANT_TRANSACTIONTYPE>
          2
</DS_MERCHANT_TRANSACTIONTYPE>
<DS_MERCHANT_MERCHANTDATA>
          Alfombrilla+para+raton
</DS_MERCHANT_MERCHANTDATA>
<DS_MERCHANT_AMOUNT>
          45
</DS_MERCHANT_AMOUNT>
<DS_MERCHANT_MERCHANTNAME>
          Comercio de Pruebas
</DS_MERCHANT_MERCHANTNAME>
<DS_MERCHANT_MERCHANTSIGNATURE>
          a63dfa507e549936f41f4961ccdace126b8ecdea
</DS_MERCHANT_MERCHANTSIGNATURE>
<DS_MERCHANT_TERMINAL>
          1
</DS_MERCHANT_TERMINAL>
<DS_MERCHANT_MERCHANTCODE>
          999008881
</DS_MERCHANT_MERCHANTCODE>
<DS_MERCHANT_ORDER>
          114532
</DS_MERCHANT_ORDER>
</DATOSENTRADA>
```

2. Especificación del documento RETORNOXML.

Este mensaje es el que la plataforma enviará como resultado de la operación

```
<!ELEMENT RETORNOXML (DS_Version ?,CODIGO,(OPERACION|RECIBIDO ))>
<!ELEMENT DS_Version (#PCDATA)>
<!ELEMENT CODIGO (#PCDATA)>
```

<!ELEMENT OPERACION (Ds_Amount, Ds_Currency, Ds_Order, Ds_Signature, Ds_MerchantCode, Ds_Terminal, Ds_Response, Ds_AuthorisationCode,Ds_TransactionType, Ds_SecurePayment, Ds_Reference ?, Ds_Language ?, Ds_CardNumber ?, Ds_ExpiryDate ?, Ds_MerchantData ?, Ds_MerchantDTD)>

```
<!ELEMENT Ds_Amount (#PCDATA)>
<!ELEMENT Ds_Currency (#PCDATA)>
<!ELEMENT Ds_Order (#PCDATA)>
<!ELEMENT Ds_Signature (#PCDATA)>
<!ELEMENT Ds_MerchantCode (#PCDATA)>
<!ELEMENT Ds_Terminal (#PCDATA)>
<!ELEMENT Ds_Response (#PCDATA)>
<!ELEMENT Ds_AuthorisationCode (#PCDATA)>
<!ELEMENT Ds_TransactionType (#PCDATA)>
<!ELEMENT Ds_SecurePayment (#PCDATA)>
<!ELEMENT Ds_Reference (#PCDATA)>
<!ELEMENT Ds_Language (#PCDATA)>
<!ELEMENT Ds_CardNumber (#PCDATA)>
<!ELEMENT Ds_ExpiryDate (#PCDATA)>
<!ELEMENT Ds_MerchantData (#PCDATA)>
<!ELEMENT RECIBIDO (#PCDATA)>
```

Donde:

- DS_Version: versión de la DTD utilizada para validar el XML.
- CÓDIGO: indica si la operación ha sido correcta o no (no indica si ha sido autorizada, solo si se ha procesado). Un 0 indica que la operación ha sido correcta. En el caso de que sea distinto de 0, tendrá el código del error y no aparecerá la información de la operación.
  CÓDIGO no es Ds_Response una operación puede tener un CÓDIGO = 0 y ser Denegada (Ds_Response distinto de 0).
- Ds_Amount: importe de la operación.
- Ds_Currency: moneda de la operación.
- Ds_Order: pedido de la operación.
- Ds_Signature: firma de la operación, se calcula con los campos.
  Ds_Amount + Ds_Order + Ds_MerchantCode + Ds_Currency + Ds_Response + Ds_CardNumber + Ds_TransactionType + Ds_SecurePayment + Clave.
  El campo Ds_CardNumber solo formará parte de la firma en caso de que se envíe la tarjeta. Si la tarjeta se envía asteriscada, el campo Ds_CardNumber también formará parte de la firma con el valor asteriscado.
- Ds_MerchantCode: código de comercio de la operación.
- Ds_Terminal: número de terminal de la operación.
- Ds_Response: valor que indica el resultado de la operación. Indicará si ha sido autorizada o no. Sus valores posibles son los de PRICE.
- Ds_AuthorisationCode: código de autorización en caso de existir.
- Ds_TransactionType: tipo de operación realizada.
- Ds_MerchantData: ver APARTADO 5.1.
- Ds_SecurePayment: ver APARTADO 5.3.
- Ds_Reference: campo opcional para pago por referencia.
- Ds_Language: indica idioma enviado por el comercio.
- Ds_CardNumber: número de tarjeta de crédito.
- Ds_ExpiryDate: año y mes de caducidad de la tarjeta AAMM.
- RECIBIDO: es una cadena de texto que contiene el XML que el comercio nos envió mediante POST en el campo entrada.

El campo DS_Version solo aparecerá en caso de que la operación haya sido correcta ya que es un valor que nos envía el comercio en caso de no ser correcta el dato irá en el campo RECIBIDO.

El envío del dato OPERACION o RECIBIDO depende de también de que la operación sea correcta o no.

A continuación se muestran tres ejemplos del mensaje:

1- Operación correcta y Autorizada:

```
<RETORNOXML>
        <DS_Version>1.0</DS_Version>
        <CODIGO>0</CODIGO>
```

```
        <OPERACION>
                <Ds_Amount>100</DS_Amount>
            <Ds_Currency>978</DS_Currency>
                <Ds_Order>0001</DS_Order>
                <Ds_Signature>EEFF45687hgth</DS_Signature>
                <Ds_MerchantCode>999008881</DS_MerchantCode>
                <Ds_Terminal>1</DS_Terminal>
                <Ds_Response>0</DS_Response>
                <Ds_AuthorisationCode>222FFF</ Ds_AuthorisationCode>
                <Ds_TransactionType>2</ Ds_TransactionType >
                <Ds_SecurePayment>1</Ds_SecurePayment>
                <Ds_MerchantData>Mis Datos</ Ds_MerchantData>
        </OPERACION>
</RETORNOXML>
```

2 - Operación correcta y denegada (190 - Denegada por la entidad):

```
<RETORNOXML>
        <DS_Version>1.0</ DS_Version >
        <CODIGO>0</CODIGO>
        <OPERACION>
                <Ds_Amount>100</DS_Amount>
            <Ds_Currency>978</DS_Currency>
                <Ds_Order>0001</DS_Order>
                <Ds_Signature>EEFF45687hgth</DS_Signature>
                <Ds_MerchantCode>999008881</DS_MerchantCode>
                <Ds_Terminal>1</DS_Terminal>
                <Ds_Response>190</DS_Response>
                <Ds_AuthorisationCode>222FFF</ Ds_AuthorisationCode>
                <Ds_TransactionType>2 Ds_TransactionType >
                <Ds_SecurePayment>1</Ds_SecurePayment>
                <Ds_MerchantData>Mis Datos</ Ds_MerchantData>
        </OPERACION>
</RETORNOXML>
```

3 - Operación incorrecta (051 - Nº de Pedido Repetido). Nunca será autorizada:

```
<RETORNOXML>
        <CODIGO>SIS0051</CODIGO>
        <RECIBIDO>
                <DATOSENTRADA>
                        <DS_MERCHANT_CURRENCY>
                                978
                        </DS_MERCHANT_CURRENCY>
                        <DS_MERCHANT_MERCHANTURL>
                                https://pruebaCom.jsp
                        </DS_MERCHANT_MERCHANTURL>
                        <DS_MERCHANT_TRANSACTIONTYPE>
                                2
                        </DS_MERCHANT_TRANSACTIONTYPE>
                        <DS_MERCHANT_MERCHANTDATA>
                                Alfombrilla+para+raton
                        </DS_MERCHANT_MERCHANTDATA>
                        <DS_MERCHANT_AMOUNT>
                                45
                        </DS_MERCHANT_AMOUNT>
                        <DS_MERCHANT_MERCHANTNAME>
                                Comercio de Pruebas
                        </DS_MERCHANT_MERCHANTNAME>
                        <DS_MERCHANT_MERCHANTSIGNATURE>
                                a63dfa507e549936f41f4961ccdace126b8ecdea
                        </DS_MERCHANT_MERCHANTSIGNATURE>
                        <DS_MERCHANT_TERMINAL>
                                1
                        </DS_MERCHANT_TERMINAL>
                        <DS_MERCHANT_MERCHANTCODE>
                                999008881
                        </DS_MERCHANT_MERCHANTCODE>
```

```
                        <DS_MERCHANT_ORDER>
                                114532
                        </DS_MERCHANT_ORDER>
                        <DS_Version>
                                1.0
                        </ DS_Version >
                </DATOSENTRADA>
        </RECIBIDO>
</RETORNOXML>
```

ANEXO IV. TABLA DE ERRORES

En la siguiente tabla se enumeran los posibles valores de error que se puede recibir en la respuesta del TPV Virtual, así como el campo al que afecta (si procede) y el significado de cada uno de ellos. Asimismo se especifica el mensaje de error que verá el cliente (comprador) en cada uno de estos errores.

SISxxxx	CAMPO AFECTADO	MOTIVO	MENSAJE
SIS0007		Error al desmontar XML de entrada	MSG0008
SIS0008	Ds_Merchant_MerchantCode	Falta el campo	MSG0008
SIS0009	Ds_Merchant_MerchantCode	Error de formato	MSG0008
SIS0010	Ds_Merchant_Terminal	Falta el campo	MSG0008
SIS0011	Ds_Merchant_Terminal	Error de formato	MSG0008
SIS0014	Ds_Merchant_Order	Error de formato	MSG0008
SIS0015	Ds_Merchant_Currency	Falta el campo	MSG0008
SIS0016	Ds_Merchant_Currency	Error de formato	MSG0008
SIS0018	Ds_Merchant_Amount	Falta el campo	MSG0008
SIS0019	Ds_Merchant_Amount	Error de formato	MSG0008
SIS0020	Ds_Merchant_Signature	Falta el campo	MSG0008
SIS0021	Ds_Merchant_Signature	Campo sin datos	MSG0008
SIS0022	Ds_TransactionType	Error de formato	MSG0008
SIS0023	Ds_TransactionType	Valor desconocido	MSG0008
SIS0024	Ds_ConsumerLanguage	Valor excede de 3 posiciones	MSG0008
SIS0025	Ds_ConsumerLanguage	Error de formato	MSG0008
SIS0026	Ds_Merchant_MerchantCode	Error No existe el comercio / Terminal enviado	MSG0008
SIS0027	Ds_Merchant_Currency	Error moneda no coincide con asignada para ese Terminal.	MSG0008
SIS0028	Ds_Merchant_MerchantCode	Error Comercio/Terminal está dado de baja	MSG0008
SIS0030	Ds_TransactionType	En un pago con tarjeta ha llegado un tipo de operación que no es ni pago ni preautorització	MSG0000
SIS0031	Ds_Merchant_TransactionType	Método de pago no definido	MSG0000
SIS0034		Error en acceso a la Base de datos	MSG0000
SIS0038		Error en JAVA	MSG0000
SIS0040		El comercio / Terminal no tiene ningún método de pago asignado	MSG0008
SIS0041 SIS0042	Ds_Merchant_Signature	Error en el cálculo del algoritmo HASH	MSG0008
SIS0043		Error al realizar la notificación On-line	MSG0008

SISxxxx	CAMPO AFECTADO	MOTIVO	MENSAJE
SIS0046		El Bin de la tarjeta no está dado de alta	MSG0002
SIS0051	Ds_Merchant_Order	Número de pedido repetido	MSG0001
SIS0054	Ds_Merchant_Order	No existe operación sobre la que realizar la devolución	MSG0008
SIS0055	Ds_Merchant_Order	La operación sobre la que se desea realizar la devolución no es una operación válida	MSG0008
SIS0056	Ds_Merchant_Order	La operación sobre la que se desea realizar la devolución no está autorizada	MSG0008
SIS0057	Ds_Merchant_Amount	El importe a devolver supera el permitido	MSG0008
SIS0058		Inconsistencia de datos, en la validación de una confirmación	MSG0008
SIS0059	Ds_Merchant_Order	Error, no existe la operación sobre la que realizar la confirmación	MSG0008
SIS0060	Ds_Merchant_Order	Ya existe una confirmación asociada a la preautorización	MSG0008
SIS0061	Ds_Merchant_Order	La preautorización sobre la que se desea confirmar no está autorizada	MSG0008
SIS0062	Ds_Merchant_Amount	El importe a confirmar supera el permitido	MSG0008
SIS0063 SIS0064 SIS0065		Error en número de tarjeta	MSG0008
SIS0066 SIS0067 SIS0068 SIS0069 SIS0070		Error en caducidad tarjeta	MSG0008
SIS0071		Tarjeta caducada	MSG0000
SIS0072	Ds_Merchant_Order	Operación no anulable	MSG0000
SIS0074	Ds_Merchant_Order	Falta el campo	MSG0008
SIS0075	Ds_Merchant_Order	El valor tiene menos de 4 posiciones o más de 12	MSG0008
SIS0076	Ds_Merchant_Order	El valor no es numérico	MSG0008
SIS0078	Ds_TransactionType	Valor desconocido	MSG0005
SIS0089	Ds_Merchant_ExpiryDate	El valor no ocupa 4 posiciones	MSG0008
SIS0092	Ds_Merchant_ExpiryDate	El valor es nulo	MSG0008
SIS0093		Tarjeta no encontrada en tabla de rangos	MSG0006
SIS0094		La tarjeta no fue autenticada como 3D Secure	MSG0004
SIS0112	Ds_TransactionType	Valor no permitido	MSG0008
SIS0114		Se ha llamado con un GET en lugar de un POST	MSG0000
SIS0115	Ds_Merchant_Order	No existe operación sobre la que realizar el pago de la cuota	MSG0008

SISxxxx	CAMPO AFECTADO	MOTIVO	MENSAJE
SIS0116	Ds_Merchant_Order	La operación sobre la que se desea pagar una cuota no es válida.	MSG0008
SIS0117	Ds_Merchant_Order	La operación sobre la que se desea pagar una cuota no está autorizada	MSG0008
SIS0118	Ds_Merchant_Amount	Se ha excedido el importe total de cuotas que se indicó en la primera operación de una transacción recurrente	MSG0008
SIS0119	Ds_Merchant_DateFrecuency	Error de formato	MSG0008
SIS0120	Ds_Merchant_ChargeExpiryDate	Error de formato	MSG0008
SIS0121	Ds_Merchant_SumTotal	Error de formato	MSG0008
SIS0122	Ds_Merchant_ChargeExpiryDate Ds_Merchant_SumTotal	Error de formato en alguno de los dos campos	MSG0008
SIS0123	Ds_Merchant_ChargeExpiryDate	Se ha excedido la fecha tope que se indicó en la primera operación de una transacción recurrente	MSG0008
SIS0124	Ds_Merchant_DateFrecuency	Se ha excedido la frecuencia mínima que se indicó en la primera operación de una transacción recurrente	MSG0008
SIS0132		La fecha de Confirmación de Autorización no puede superar en más de 7 días a la preautorización	MSG0008
SIS0133		La fecha de confirmación de Autenticación no puede superar en más de 45 días la autenticación previa	MSG0008
SIS0139		El pago recurrente inicial está duplicado	MSG0008
SIS0142		Tiempo excedido para el pago	MSG0000
SIS0198		Importe supera límite permitido para el comercio	MSG0008
SIS0199		El número de operaciones supera el límite permitido para el comercio	MSG0008
SIS0200		El importe acumulado supera el límite permitido para el comercio	MSG0008
SIS0214		El comercio no admite devoluciones	MSG0008
SIS0216		El CVV2 tiene más de tres posiciones	MSG0008
SIS0217		Error de formato en CVV2	MSG0008
SIS0218		La entrada “Operaciones” no permite pagos seguros	MSG0008
SIS0219		El número de operaciones de la tarjeta supera el límite permitido para el comercio	MSG0008
SIS0220		El importe acumulado de la tarjeta supera el límite permitido para el comercio	MSG0008
SIS0221		Error. El CVV2 es obligatorio	MSG0008
SIS0222		Ya existe una anulación asociada a la preautorización	MSG0008
SIS0223		La preautorización que se desea anular no está autorizada	MSG0008

SISxxxx	CAMPO AFECTADO	MOTIVO	MENSAJE
SIS0224		El comercio no permite anulaciones por no tener firma ampliada	MSG0008
SIS0225		No existe operación sobre la que realizar la anulación	MSG0008
SIS0226		Inconsistencia de datos en la validación de una anulación	MSG0008
SIS0227	Ds_Merchant_TransactionDate	Valor no válido	MSG0008
SIS0229		No existe el código de pago aplazado solicitado	MSG0008
SIS0231		No hay formas de pago aplicables	MSG0008
SIS0252		El comercio no permite el envío de tarjeta	MSG0008
SIS0253		La tarjeta no cumple el check-digit	MSG0008
SIS0254		El número de operaciones por IP supera el máximo permitido para el comercio	MSG0008
SIS0255		El importe acumulado por IP supera el límite permitido para el comercio	MSG0008
SIS0256		El comercio no puede realizar preautorizaciones	MSG0008
SIS0257		La tarjeta no permite preautorizaciones	MSG0008
SIS0258		Inconsistencia en datos de confirmación	MSG0008
SIS0261		Operación supera alguna limitación de operatoria definida por CatalunyaCaixa	MSG0008
SIS0270	Ds_Merchant_TransactionType	Tipo de operación no activado para este comercio	MSG0008
SIS0274	Ds_Merchant_TransactionType	Tipo de operación desconocida o no permitida para esta entrada al SIS	MSG0008
SIS0281		Operación supera alguna limitación de operatoria definida por CatalunyaCaixa	MSG0008

Tabla de mensajes que recibe el cliente comprador cuando ocurre un error en la operación, así como su significado.

CÓDIGO	MENSAJE
MSG0000	El sistema está ocupado, inténtelo más tarde
MSG0001	Número de pedido repetido
MSG0002	El Bin de la tarjeta no está dado de alta en FINANET
MSG0003	El sistema está arrancando, inténtelo en unos momentos
MSG0004	Error de Autenticación
MSG0005	No existe método de pago válido para su tarjeta
MSG0006	Tarjeta ajena al servicio
MSG0007	Faltan datos, por favor compruebe que su navegador acepta cookies
MSG0008	Error en datos enviados. Contacte con su comercio.

ANEXO V. LISTA DE CÓDIGOS DE PAISES

004	Afganistán	178	Congo	360	Indonesia
008	Albania	180	Zaire	364	Irán
010	Antártida	184	Cook	368	Iraq
012	Alergia	188	Costa Rica	372	Irlanda
016	Samoa americana	191	Croacia	376	Israel
020	Andorra	192	Cuba	380	Italia
024	Angola	196	Chipre	384	Costa
028	Antigua y Barbuda	203	Chequia	388	Jamaica
031	Azerbaitjan	204	Benín	392	Japón
032	Argentina	208	Dinamarca	398	Kazajstan
036	Australia	212	Dominica	400	Jordania
040	Austria	214	Dominicana	404	Kenya
044	Bahamas	218	Ecuador	408	Corea
048	Bahréin	222	El Salvador	410	Corea
050	Bangladesh	226	Guinea Ecuatorial	414	Kuwait
051	Armenia	230	Etiopía	417	Kirguizistán
052	Barbados	233	Estonia	418	Laos
056	Bélgica	234	Feroe	422	Líbano
060	Bermudas	238	Malvinas	426	Lesoto
064	Bután	242	Fiji	428	Letonia
068	Bolivia	246	Finlandia	430	Liberia
070	Bosnia i Herzegovina	250	Francia	434	Libia
072	Botswana	254	Guayana francesa	438	Liechtenstein
074	Bouvet	258	Polinesia francesa	440	Lituania
076	Brasil	260	Territorio del sur francés	442	Luxemburgo
084	Belice	262	Jibuti	446	Macao
086	Mauricio	266	Gabón	450	Madagascar
090	Salomón	268	Georgia	454	Malawi
092	Vírgenes británicas	270	Gambia	458	Malasia
096	Brunei	280	Alemania	462	Maldivas
100	Bulgaria	288	Ghana	466	Mali
104	Birmania	292	Gibraltar	470	Malta
108	Burundi	296	Kiribati	474	Martinica
112	Bielorrusia	300	Grecia	478	Mauritania
116	Camboya	304	Groenlandia	480	Mauricio
120	Camerún	308	Granada	484	Méjico
124	Canadá	312	Guadalupe	492	Mónaco
132	Cabo Verde	316	Guam	496	Mongolia
136	Caimán	320	Guatemala	498	Moldavia
140	Centro África	324	Guinea	500	Montserrat
144	Sri Lanka	328	Guayana	504	Marruecos
148	Chad	332	Haití	508	Mozambique
152	Chile	334	Heard	512	Omán
156	China	336	Vaticano (Ciudad Estado)	516	Namibia
158	Taiwán	340	Honduras	520	Nauru
162	Christmas	344	Hong Kong	524	Nepal
166	Cocos	348	Hungría	528	Holanda

170	Colombia	352	Islandia	530	Antillas holandesas
174	Comores	356	India	533	Aruba
540	Nueva Caledonia	646	Ruanda	762	Tadjikistan
548	Vanuatu	654	Santa Helena	764	Tailandia
554	Nueva Zelanda	659	Anguila	768	Togo
558	Nicaragua	662	Saint Lucia	776	Tonga
562	Níger	666	Saint Pierre y Miquelón	780	Trinidad y Tobago
566	Nigeria	670	San Vicente y Granadina	784	Emiratos Árabes
570	Niue	674	San Marino	788	Túnez
574	Norfolk	678	São Tomé i Príncipe	792	Turquía
578	Noruega	682	Arabia Saudita	795	Turkmenistán
580	Marianas Septentrionales	686	Senegal	796	Turks i Caicos
581	Minor (Estados Unidos)	690	Seychelles	798	Tuvalu
582	Pacífico	694	Sierra Leona	800	Uganda
583	Micronesia	702	Singapur	804	Ucrania
584	Marshall	703	Eslovaquia	807	Macedonia
586	Pakistán	704	Vietnam	818	Egipto
591	Panamá	705	Eslovenia	826	Reino Unido
598	Papúa-Nova Guinea	706	Somalia	834	Tanzania
600	Paraguay	710	Sudáfrica	840	Estados Unidos
604	Perú	716	Zimbabwe	850	Vírgenes americanas
608	Filipinas	720	Yemen	854	Burkina
612	Pitcairn	722	Tokelau	858	Uruguay
616	Polonia	724	España	860	Uzbekistán
620	Portugal	736	Sudan	862	Venezuela
624	Guinea Bissau	740	Surinam	876	Wallis y Fortuna
626	Timor	744	Svalbard y Jan Mayen	882	Samoa
630	Puerto Rico	748	Suazilandia	886	Yemen
634	Qatar	752	Suecia	891	Yugoslavia
638	Reunión	756	Suiza	894	Zambia
642	Rumania	760	Siria		
643	Rusia				