

TPV Virtual Plus

Manual operativo y de instalación

Índice

1. INTRODUCCIÓN	4
2. ¿QUÉ NECESITO?	8
2.1 ¿Cómo se instala?	9
2.2 ¿Qué debería tener mi web?	9
2.3 ¿Qué reglamentación sobre pagos debo cumplir?	10
3. MEDIDAS DE SEGURIDAD	12
3.1 Velocity checks	13
3.2 Verificación del CVV2	13
3.3 Protocolo de compra segura (CES)	13
3.4 Medidas de seguridad adicionales	14
4. LICENCIA <i>CROSS-BORDER</i>	16
5. ASPECTOS OPERATIVOS	18
5.1 Tipos de transacciones	19
5.2 Solicitud de documentación del pago por parte del comprador	22
5.3 Ventas internacionales	23
5.4 Operativa DCC (Dynamic Currency Conversion)	24
5.5 IUPAY (Aspectos técnicos)	25
6. MÓDULO DE ADMINISTRACIÓN DEL TPV VIRTUAL	27
6.1 Acceso	28
6.2 Usuarios	28
6.3 Consulta y administración de operaciones	29
6.4 Devolución de operaciones	29
6.5 Consulta de totales	30
7. INSTALACIÓN	31
7.1 Gateway “realizarPago”	32
7.1.1 Continuidad de la sesión del navegador	33
7.2 Gateway “entrada XMLEntidad”	34
7.3 Gateway “operaciones”	36
7.4 Gateway “WebService”	40
7.4.1 Mensajes de petición	40
7.4.2 Mensajes de respuesta	41
7.5 Localización de errores	41
7.6 Diseño del algoritmo hash en el servidor de Internet	42
7.6.1 Gateway “realizarPago”	42

7.6.2 Gateways “entradaXMLEntidad” y “operaciones”	42
7.6.3 Gateway “WebService”	43
7.6.4 Recomendaciones generales para el cálculo de la firma	43
7.6.5 Referencias SHA-1	44
7.7 Respuesta online del TPV Virtual al comercio	44
7.7.1 Respuesta online	45
7.7.2 Sincronización SOAP	48
7.8 Pago de suscripciones y pagos exprés	50
7.9. Operativa DCC (Dynamic Currency Conversion)	54
7.9.1 Configuración operativa DCC para entrada ‘webservice’	54
7.9.2 Firma del comercio	57
7.10 Entorno de pruebas	57
7.11 Servicio técnico de soporte a la instalación	58
8. CONSULTA SOAP-XML DE TRANSACCIONES DE TPV VIRTUAL	98
8.1 Cálculo de la firma	60
8.2 Consultas SOAP - Especificación de los mensajes de entrada y de salida	61
8.3 WSDL del servicio	72
8.4 Ejemplo de cliente SOAP	73
8.5 Códigos de error SOAP	74
9. FICHEROS DE INFORMACIÓN PERIÓDICA	77
9.1 Canales para la recepción de los ficheros	79
9.2 Descripción de los ficheros	80
10. PROGRAMAS DE SUPERVISIÓN Y PENALIZACIONES	89
11. PCI-DSS - PROGRAMA DE SEGURIDAD DE DATOS DE TARJETAS	91
11.1 ¿Qué es PCI-DSS?	92
11.2 Objetivos del programa PCI-DSS	92
11.3 Ventajas para los comercios	92
11.4 ¿Quién debe cumplir el programa PCI-DSS?	92
ANEXO I. DATOS DEL FORMULARIO DE PAGO	95
ANEXO II. CÓDIGOS DE ERROR	99
ANEXO III. TABLA CÓDIGOS DE RESPUESTA (DS_RESPONSE)	105
ANEXO IV. CÓDIGOS ISO PAÍSES	113
ANEXO V. CÓDIGOS ISO DIVISAS	117
ANEXO VI. EJEMPLOS ESPECÍFICOS OPERATIVA PAGO DE SUSCRIPCIONES / PAGOS EXPRÉS	121

1.

Introducción

Banco Sabadell es el banco de las mejores empresas y, como tal, es líder en soluciones de cobro al comercio, siempre anticipándose e investigando permanentemente los medios tecnológicos más avanzados.

En la actualidad el comercio por Internet ya no es privativo de un determinado perfil de empresa: pequeños negocios, profesionales, pymes, grandes empresas, etc., cada vez un mayor número de compañías se adentra en el comercio electrónico y demanda **soluciones seguras y adaptables** a su realidad comercial.

Esta realidad requiere, a nuestro juicio, disponer de una tecnología capaz de responder a múltiples requerimientos. En suma, TPV virtuales que puedan servir por igual a las necesidades de cualquier empresa o negocio que opere en la red.

Por todo ello, **Banco Sabadell ha reforzado sus servicios de e-commerce** y dispone de una unidad específica en la que trabajan gestores especializados en plataformas de pagos virtuales y un equipo de *back office* para facilitar a nuestros clientes soluciones diferenciadas y seguras, así como un amplio conjunto de servicios en el ámbito de las ventas por Internet.

Dos tipos de necesidades, dos soluciones TPV

Banco Sabadell ofrece dos tipos de pasarelas de pago, en función de las características del cliente:

- **TPV Virtual.** Es la solución más utilizada y responde con gran eficacia a los requerimientos de negocios y pymes. Esta plataforma se instala fácilmente y ofrece una amplia gama de servicios y prestaciones específicas para el comercio electrónico.
- **TPV Virtual Plus.** Se trata de una solución más sofisticada que está concebida para

empresas con alto volumen de ventas en Internet. Brinda un avanzado conjunto de servicios técnicos y operativos, además del soporte permanente por gestores especializados en pagos *e-commerce*. **El presente manual recoge las descripciones e instrucciones de instalación de los servicios de la solución TPV Virtual Plus.**

Además, Banco Sabadell dispone de una solución adicional denominada **TPV Virtual Organismos**. Se trata de una pasarela de pago específicamente diseñada para satisfacer las necesidades de los organismos e instituciones públicas que deseen ofrecer el servicio de pago de notificaciones, impuestos y tasas, directamente desde su página web.

Soluciones Open Source

Ponemos a su disposición, de manera gratuita, una selección de las mejores herramientas Open Source disponibles para el ámbito del *e-commerce*.

Con ellas, podrá configurar usted mismo su tienda online y gestionar fácilmente su apariencia, usabilidad y funcionalidad, además de integrarla con el TPV Virtual de Banco Sabadell mucho más fácilmente.

Para más información, o para solicitar los manuales de integración, contacte con nuestro servicio técnico (ver apartado 7.11 del manual)

Magento, Prestashop, OsCommerce, Joomla, VirtueMart, Open Cart, Zen Cart, WordPress.

Elementos de seguridad

Ofrecer los máximos elementos de seguridad es una de las prioridades de Banco Sabadell. Por ello, nuestra plataforma integra **CES (Compra Electrónica Segura)** que, bajo los protocolos internacionales Verified by Visa y

MasterCard SecureCode (ambos basados en la tecnología 3D Secure), aporta una alta seguridad y protección en los pagos.

Mediante la aplicación de estos protocolos se consigue la **autenticación del titular** al realizar la compra, es decir, que el cliente se identifique como legítimo titular de la tarjeta que está utilizando.

No obstante, existen establecimientos que prefieren desactivar protocolos CES y sustituirlos por sistemas alternativos de **control del fraude**. En tal caso, basta con que lo soliciten a su gestor del banco, para que realice el correspondiente análisis del comercio e implemente la modificación si lo considera oportuno.

Del mismo modo, y especialmente para los negocios y pymes, el TPV Virtual de Banco Sabadell está configurado con limitaciones de seguridad –*velocity checks*– que validan los intentos repetitivos de compra con la misma tarjeta y/o desde la misma IP, reduciendo significativamente el riesgo de fraude.

Los requerimientos de seguridad son todavía más estrictos en el caso del TPV Virtual Plus, en correspondencia con los altos volúmenes de facturación. En concreto se integran elementos de seguridad adicionales tales como **reglas avanzadas** de gestión del fraude, **informes diarios** de las transacciones dudosas (reclamadas, disputadas o declaradas como ilícitas por los compradores) y acuerdos de **colaboración e integración técnica** con grandes gateways, procesadores y empresas internacionales de *fraud-scrubbing*.

IUPAY, la cartera digital de Banco Sabadell

La plataforma de Banco Sabadell le ofrece el cobro mediante IUPAY, un servicio de cartera digital (wallet) que permite a sus clientes

almacenar de manera muy sencilla todas sus tarjetas de diferentes entidades bancarias. Así, pueden realizar sus compras por Internet de un modo mucho más cómodo y rápido, pero manteniendo todas las garantías de seguridad.

Pago de suscripciones y pagos exprés: mejorando la experiencia del usuario

Los TPV virtuales de Banco Sabadell, admiten las operaciones habituales: autorizaciones, preautorizaciones, autenticaciones, gestión de devoluciones y compras recurrentes.

Pero la verdadera innovación reside en el sistema mediante el cual se almacenan los datos de la tarjeta en la propia pasarela.

La ventaja es obvia: con esta funcionalidad el cliente del comercio introduce los datos de su tarjeta una sola vez en su primera compra, y ya no tiene necesidad de repetir este paso en futuros pagos con el mismo comercio. Con ellos el comercio incrementa la usabilidad de su web (pago exprés) y, también, dispone de una herramienta para el procesamiento de suscripciones u otros pagos periódicos.

Soluciones para la internacionalización

En *e-commerce* el límite es el mundo. Banco Sabadell ha cuidado especialmente este aspecto, integrando soluciones que facilitan la venta fuera de nuestras fronteras:

- El **servicio multdivisa** permite al cliente realizar la compra en **una amplia variedad de monedas locales**, evitando los obstáculos asociados a la conversión de divisas.

- La **operativa DCC** (Dynamic Currency Conversion) habilita la conversión online de la **moneda local al euro**. Esta operativa se pone en marcha tan pronto el TPV Virtual detecta que la tarjeta de compra ha sido emitida en un país fuera de la zona euro.
- Asimismo, la pasarela es **multilinguaje**, tanto para el comercio como para el propio comprador. Actualmente, el TPV Virtual admite operaciones en castellano, catalán, euskera, inglés, francés, alemán, portugués, neerlandés, polaco, italiano y sueco.

Adicionalmente, existen herramientas específicas para el TPV Virtual Plus, que se han desarrollado para maximizar las ventas y simplificar al máximo las transacciones a través de filiales internacionales:

- En muchos países existen **sistemas de pago locales**, distintos a las tarjetas financieras, que tienen un alto nivel de aceptación. Son ventas que no pueden perderse y, por ello, Banco Sabadell mantiene acuerdos internacionales que permiten acceder a un gran número de estos sistemas de pago.
- Si la empresa posee filiales en otros países europeos, gracias a la **licencia transfronteriza (Cross-Border) de Banco Sabadell**, es posible procesar pagos con Visa o MasterCard tanto en comercios españoles como en las filiales. Una sola integración al TPV Virtual Plus permite gestionar todas las ventas.
- **Control en tiempo real** de todas las operaciones.
- **Acceso a los cierres contables**, con disponibilidad permanente de los correspondientes al último año.
- Máxima **simplicidad** en la gestión de devoluciones.
- **Listado de transacciones**, que puede ser descargado en el ordenador, y que incorpora toda la información relevante.
- Para grandes empresas, **integración en la intranet corporativa o en aplicaciones propietarias** y disponibilidad de ficheros mediante FTP y BS Online.

Herramientas *Back Office*

Creemos que la gestión por parte del comercio debe ser sencilla y amigable, pero también completa. El TPV Virtual incorpora un módulo de administración basado en web, diseñado para permitir un manejo sencillo y ofrecer todas las funcionalidades.

2. ¿Qué necesito?

2.1 ¿Cómo se instala?

El primer paso para llevar a cabo la instalación del TPV Virtual de Banco Sabadell es tramitar en su oficina la solicitud de apertura de un contrato de comercio y del alta del TPV Virtual.

Para realizar la contratación de este servicio será necesario que nos facilite algunos datos básicos de su negocio y de su tienda virtual.

Una vez aceptada su solicitud, se le enviará un correo electrónico con las claves de seguridad únicas para su comercio que le permitirán instalar el TPV Virtual. Con el objetivo de facilitar la integración del TPV Virtual en su servidor web y de sincronizar los mecanismos de compra, antes de implementar el TPV Virtual en real, le recomendamos que utilice las claves en entorno de pruebas incluidas en el presente manual.

Ante cualquier duda o consulta, el Servicio Técnico de Soporte al TPV Virtual de Banco Sabadell estará a su disposición para atenderle por correo electrónico o por conversación telefónica.

2.2 ¿Qué debería tener mi web?

Si bien es cierto que la instalación del TPV Virtual no influye en el diseño y las características básicas de la página web de su comercio y la tienda virtual que incluye, sí que hay una serie de requerimientos y recomendaciones que debe tener en cuenta para mejorar la experiencia de compra de sus clientes.

— En la página principal de su web...

La página principal de su web debe incluir una sección en la que se informe acerca de las formas de pago aceptadas y de las condiciones generales de venta y contratación. Debe incluir entre otros, el nombre y CIF de la empresa propietaria de la tienda virtual, y las obligaciones y garantías tanto del comprador como del establecimiento.

— En su catálogo de productos...

En el catálogo de productos de su página web le recomendamos que todos los productos mostrados incluyan información fácilmente visible acerca de la disponibilidad del producto, el plazo de entrega y el precio.

Es importante que dicha información se incluya junto a cada producto en la propia lista del catálogo antes de que el usuario lo seleccione haciendo clic sobre él.

— En su tienda virtual...

Además del catálogo de productos, la tienda virtual de su página web también debe incluir un carrito de la compra donde el comprador vaya almacenando los productos que desea comprar mientras navega por el catálogo.

Al final del proceso, en este espacio se especificarán el producto o productos seleccionados con sus precios y los importes adicionales que compondrán el precio final de la compra,

siempre y cuando sean necesarios (impuestos, gastos de envío, etc.).

— En la solicitud de datos...

Cuando su cliente ya tiene en el “carrito de la compra” la relación de todos los productos que quiere adquirir y los gastos adicionales a desembolsar, deberá aceptar el pedido. En ese momento, la página web de su comercio deberá facilitarle un formulario detallado en el que se le soliciten todos los datos necesarios para cerrar el proceso de venta. Al tratarse de una venta a distancia, su cliente deberá indicar sus datos personales, los datos de entrega de la mercancía y la forma de pago que desea utilizar.

En el momento en que el comprador elije realizar el pago mediante tarjeta de crédito, se activa el TPV Virtual de Banco Sabadell.

2.3 ¿Qué reglamentación sobre pagos debo cumplir?

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 Banco Sabadell.

Esta normativa está recogida en el contrato firmado entre Banco Sabadell y el comercio. Destacamos, especialmente, las siguientes reglas:

- El comercio solo podrá procesar transacciones originadas desde las páginas web que hayan sido debidamente verificadas por Banco Sabadell.
- 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 la mercancía.
- 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 código CVV2 (tres dígitos de seguridad impresos en el reverso de las tarjetas) bajo ninguna circunstancia.

3.

Medidas de seguridad

El TPV Virtual asociado a su comercio se ha configurado con una serie de medidas de seguridad con el objetivo de reducir el riesgo de que se realicen ventas pagadas con tarjetas fraudulentas (robadas, copiadas o utilizadas sin el consentimiento del legítimo titular).

3.1 Velocity checks

Son restricciones de seguridad que bloquean operaciones y comportamientos de compra inusuales.

Como medida adicional de seguridad y prevención del fraude, Banco Sabadell aplicará una serie de límites de seguridad respecto de la operativa del comercio en función de su actividad y del tipo de operativa. Se trata de límites por importe y número de operaciones que han de ajustarse a unos valores que no condicionen las expectativas de venta del comercio, pero que a su vez eviten 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).

Existen límites establecidos en función de los siguientes parámetros:

- Número máximo de operaciones (aceptadas y denegadas) por tarjeta
- Número máximo de operaciones (aceptadas y denegadas) por usuario (dirección IP)
- Importe máximo acumulado por tarjeta
- Importe máximo acumulado por usuario (dirección IP)

Si considera que estos parámetros no se ajustan a la operativa habitual de su comercio, rogamos solicite una modificación a través de su oficina o gestor de Banco Sabadell.

Adicionalmente, también se pueden configurar otras reglas en función de importes, número de operaciones, país de emisión de la tarjeta, país de localización de la IP del comprador, período de uso, etc.

Si considera que se debe implementar alguna de ellas, rogamos lo solicite a través de su oficina o gestor de Banco Sabadell.

3.2 Verificación del CVV2

El CVV2 es un código de tres cifras que está impreso en el reverso de todas las tarjetas financieras. La validación de este código se ha demostrado como una excelente herramienta para limitar el fraude.

El TPV Virtual de Banco Sabadell siempre solicitará en el proceso de pago el código CVV2 y lo validará online con la entidad financiera que haya emitido la tarjeta.

3.3 Protocolo de compra segura (CES)

Para proteger al comercio ante pagos fraudulentos o retrocesiones de los compradores argumentando que ellos no los realizaron, todos los TPV virtuales de Banco Sabadell están homologados a los protocolos de Comercio Electrónico Seguro (CES) de los sistemas de tarjetas Visa (Verified by Visa) y MasterCard (MasterCard SecureCode).

En CES, dentro del proceso de pago, Banco Sabadell requiere al titular de la tarjeta que se autentique *online* con su entidad financiera. El sistema de autenticación es el previamente pactado entre el titular y su banco (contraseña, PIN, envío de un SMS de verificación, etc.).

A tener en cuenta:

- A pesar de que CES aporta seguridad y protección, **si algún comercio virtual dis-**

pone de sistemas alternativos de control del fraude y desea desactivar la compra CES de su TPV Virtual, podrá solicitarlo a su oficina o gestor de Banco Sabadell para que analice el caso e implemente la modificación si procede.

- Habitualmente los sistemas de tarjetas no permiten que las tarjetas llamadas de empresa (Business, Corporate, etc.) puedan llevar a cabo el proceso de autenticación del titular. Por ello, este tipo de tarjetas no son aceptadas por el TPV Virtual. En el caso excepcional de que el comercio considere necesario aceptar tarjetas de empresa, deberá solicitarlo a su oficina de Banco Sabadell, aceptando previa y explícitamente las retrocesiones que de esta operatoria se deriven.
- La autenticación del titular de la tarjeta no exime al comercio de asumir la retrocesión de operaciones producidas por otras causas en las que el cliente argumente que sí realizó la transacción, pero, por ejemplo, reclame que no recibió el servicio o la mercancía pagada. Para defenderse ante dichas retrocesiones, el comercio deberá facilitar a Banco Sabadell documentación donde se demuestre de manera inequívoca que el titular de la tarjeta recibió el producto o servicio contratado.

3.4 Medidas de seguridad adicionales

Para proteger los intereses de su comercio y reducir al máximo el volumen de incidencias, recomendamos que monitorice la actividad de su web por si detecta alguna, o varias, de las siguientes señales sospechosas de fraude:

- En el módulo de administración del TPV Virtual se informa de la dirección IP del comprador y de la numeración de la tarjeta (debidamente enmascarada con asteriscos). Es sospechoso que:
 - _ Un mismo usuario (dirección IP) haya pagado (o haya intentado pagar) con más de dos tarjetas distintas.
 - _ Un mismo usuario (IP) o una misma tarjeta haya realizado múltiples operaciones en un corto período de tiempo.
 - _ Al realizar diferentes compras, un mismo usuario (IP) o una misma tarjeta se haya registrado en la web con datos diferentes.
 - _ Si el TPV ha rechazado la primera operación de la tarjeta, es sospechoso que a continuación se hayan procesado más operaciones con la misma IP o con la misma tarjeta por importes más bajos.
 - _ Operaciones consecutivas con números de tarjetas similares.
- En el mensaje de respuesta (campo “Ds_Response”) o en el módulo de administración del TPV Virtual se informa de si la operación ha sido aceptada (códigos 000 a 099) o denegada (resto de códigos). Los códigos de denegación del 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 deberá bloquear el usuario (identificable mediante dirección IP y datos de registro) para no permitirle la opción de intentar ningún nuevo pago.
- En el mensaje de respuesta se encuentra el campo “Ds_Card_Country” que informa del código ISO del país donde se ha emitido la tarjeta. Mediante la comparación con la dirección IP del comprador se pueden filtrar comportamientos sospechosos de ser fraudulentos (p. ej., una tarjeta emitida en un país pero que opera mediante una IP de otro país diferente).
- En la información de registro del comprador:

- _ Validar los números de teléfono usando directorios públicos de teléfonos.
 - _ Validar que el código del teléfono y/o su prefijo coincide con el área geográfica de la dirección de envío del pedido.
 - _ Validar la correspondencia entre el código postal y la ciudad del envío.
 - _ Validar la dirección de correo electrónico enviando una orden de confirmación.
 - _ Verificar, en datos públicos de redes sociales, los datos de registro del comprador.
- Y también revisar:
 - _ Pedidos con la misma dirección de entrega, pero realizados con múltiples tarjetas.
 - _ Pedidos consistentes en múltiples cantidades del mismo producto.
 - _ Pedidos de importe superior al habitual.
 - _ Pedidos en los que la entrega debe ser urgente, o incluso “para el día siguiente”. Los delincuentes quieren disponer de estos productos obtenidos fraudulentamente tan pronto como sea posible para una probable reventa y no están preocupados por el sobrecoste del envío.
 - _ Para webs no traducidas a idiomas internacionales, que los pagos se realicen con tarjetas extranjeras y/o desde IP internacionales y/o con pedidos para ser enviados a direcciones internacionales.

Adicionalmente a la monitorización de los parámetros anteriores, su comercio puede reducir considerablemente el riesgo de exposición al fraude aplicando controles de operaciones propios para identificar transacciones de alto riesgo. Estos controles pueden ser automáticos (velocity checks) y previos a enviar las solicitudes de autori-

zación a Banco Sabadell, o bien revisiones manuales posteriores al procesamiento de la transacción con Banco Sabadell.

Los protocolos antifraude que implemente deberán estar basados en los datos de registro del usuario (user ID, nombre, teléfono, dirección, correo electrónico, etc.) y, también, en datos de registro del receptor del servicio/ producto (nombre de los viajeros si es agencia de viajes o similar, domicilio de entrega del producto, teléfono de contacto, etc.).

En caso de que la operación no supere todos los controles indicados, el comercio debe rechazar la tarjeta como medio de pago y anular la operación si esta ya se hubiera realizado en el TPV Virtual.

Para minimizar, por tanto, el riesgo de fraude es necesario que los responsables del comercio conozcan estas medidas de seguridad, desarrollen acciones de formación a todos los empleados que gestionen los pagos con tarjeta y verifiquen periódicamente el cumplimiento de estas medidas. 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 Banco Sabadell.

4. Licencia *cross-border*

Banco Sabadell dispone de las licencias *cross-border* emitidas por las dos principales compañías de tarjetas, Visa y MasterCard.

La licencia *cross-border* permite a Banco Sabadell procesar las operaciones de tarjeta que se realicen en las tiendas virtuales de los comercios y empresas con residencia fiscal en el extranjero o de compañías multinacionales españolas con filiales en el extranjero.

Las ventajas para los comercios y empresas que operan en más de un país europeo es evidente: la formalización de un contrato de adquirencia con Banco Sabadell **evitará la complejidad y el coste asociado a la formalización de contratos de adquirencia de tarjetas con bancos locales** de los otros países europeos en los que disponga de tienda virtual.

Visa: área de actuación de la licencia *cross-border*

Comercios y empresas residentes en Alemania, Andorra, Austria, Bélgica, Bulgaria, Chipre, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Gibraltar, Grecia, Groenlandia, Holanda, Hungría, Islandia, Islas Feroe, Irlanda, Israel, Italia, Letonia, Lituania, Luxemburgo, Malta, Noruega, Polonia, Portugal, Reino Unido, República Checa, Rumania, Suecia, Suiza y Turquía.

MasterCard: área de actuación de la licencia *cross-border*

Europa Occidental (Western Europe Region)

Comercios y empresas residentes en Alemania, Andorra, Austria, Bélgica, Bulgaria, Chipre, Ciudad del Vaticano, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Gibraltar, Grecia, Holanda, Hungría, Islandia, Irlanda, Isla de Man, Islas del Canal, Italia,

Letonia, Liechtenstein, Lituania, Luxemburgo, Malta, Mónaco, Noruega, Polonia, Portugal, Rumania, Reino Unido, República Checa, San Marino, Suecia, Suiza y Turquía.

5. Aspectos operativos

5.1 Tipos de transacciones

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 o autorización

(Ds_Merchant_TransactionType = "0")

Se trata del caso más general en el cual la transacción es iniciada por el titular, que está conectado a través de Internet a la página web del comercio durante el proceso de pago. 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 comercio está configurado como CES (Comercio Electrónico Seguro) y el banco del titular de la tarjeta dispone de un sistema de autenticación, se solicitará al titular de la tarjeta, por parte de su banco, la correspondiente prueba de identificación.

La solicitud de autorización se lleva a cabo en tiempo real y comporta un cargo inmediato en la cuenta del titular asociada a la tarjeta (crédito o débito).

Devolución parcial o total

(Ds_Merchant_TransactionType = "3")

Son transacciones contables iniciadas por el comercio, que 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 de Banco Sabadell, que procederá a realizar el cargo correspondiente en la cuenta del comercio.

Preautorización

(Ds_Merchant_TransactionType = "1")

De acuerdo con la normativa de las marcas internacionales de tarjetas, 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 en caso de que, por alguna razón, el comercio no desee 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.

La solicitud de preautorización se lleva a cabo en tiempo real y produce 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 el 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**).

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

Para activar el servicio de preautorización es necesario que el comercio lo solicite explícitamente a su oficina de Banco Sabadell.

Confirmación de preautorización

(Ds_Merchant_TransactionType = "2")

Complementa de forma inseparable la operación anterior.

En esta transacción el titular no está conectado a la web del comercio, y por tanto siempre es iniciada por el comercio.

Debe realizarse en los siete días siguientes a la preautorización original y su importe debe ser menor o igual que el importe de la original.

Esta transacción se trata contablemente, regularizando automáticamente el apunte en la cuenta del titular y enviándose al proceso de liquidación de Banco Sabadell 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, y rechazará la operación en caso de existir algún error.

Anulación de preautorización

(Ds_Merchant_TransactionType = "9")

El titular no está conectado a la web del comercio, y por tanto esta transacción la inicia siempre el comercio. Debe realizarse en los siete días siguientes a la preautorización original.

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

Preautorización diferida

(Ds_Merchant_TransactionType = "0")

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 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 Banco Sabadell.

Confirmación de preautorización diferida

(Ds_Merchant_TransactionType = "P")

Complementa de forma inseparable la operación anterior.

El titular no está conectado a la web del comercio y, por tanto, la transacción la inicia siempre el comercio. Debe realizarse en las 72 horas siguientes a la preautorización original y su importe debe ser EL MISMO que el de la original.

Esta transacción se trata contablemente, regularizando automáticamente el apunte en

la cuenta del titular y enviándose al proceso diario de liquidación de Banco Sabadell 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, y rechazará la operación en caso de existir algún error.

Anulación de preautorización diferida

(Ds_Merchant_TransactionType = "Q")

El titular no está conectado a la web del comercio y, por tanto, la transacción la inicia siempre el comercio. Debe realizarse en las 72 horas siguientes a la preautorización original.

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

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 solo se lleva a cabo la primera parte de la operación; es decir, la autenticación del titular. No se produce, en cambio, la solicitud de autorización, por lo que la transacción no es contable y no provoca retenciones en la cuenta del titular de la tarjeta.

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 de la tarjeta no está conectado a la web del comercio y, por tanto, siempre es iniciada por el comercio.

Su importe puede ser diferente al de la operación original (incluso mayor), y debe realizarse en los 45 días siguientes a la autenticación original.

Esta transacción se trata contablemente, produciendo un apunte en la cuenta del titular de la tarjeta y enviándose al proceso diario de liquidación de Banco Sabadell 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, y la rechazará en caso de existir algún error.

Pago de suscripciones y pagos exprés

(Ds_Merchant_Identifier)

(Ds_Merchant_Group)

(Ds_Merchant_DirectPayment)

Con el objeto de incrementar el ratio de conversión y facilitar en la medida de lo posible el proceso de compra, el TPV Virtual de Banco Sabadell incorpora una funcionalidad innovadora que permite realizar pagos exprés y pago de suscripciones a través de un identificador equivalente al número de tarjeta.

Esta modalidad permite gestionar con mayor facilidad las compras de los clientes habituales, porque no necesitarán introducir los datos de su tarjeta en cada proceso de compra.

El comprador sólo tiene que informar los datos de la tarjeta en la primera compra y en ese momento el comercio recibirá, junto con la respuesta de pago, un identificador para usar en las compras posteriores.

Además, se le informará de la caducidad de la tarjeta y opcionalmente del número de la tarjeta, debidamente enmascarado, es decir, con unos determinados dígitos sustituidos por asteriscos.

Los datos de las tarjetas se almacenan en los servidores de Banco Sabadell y por tanto el comercio evitará tener que cumplir los requerimientos de seguridad PCI-DSS. (ver apartado 11 del presente manual)

En el apartado 7.8 del presente manual, se describen los **requerimientos técnicos para la instalación** en su TPV Virtual de esta modalidad de pago.

Solicite a su oficina o gestor de Banco Sabadell, la activación del servicio de “Pagos de suscripciones y Pagos Exprés”

El Servicio Técnico de Soporte al TPV Virtual de Banco Sabadell estará a su disposición para resolver cualquier duda sobre esta modalidad de pago. Vea los datos de contacto en el apartado 7.11 del manual.

5.2 Solicitud de documentación del pago por parte del comprador

En las compras por Internet normalmente no coincide el momento en el que se realiza la compra con el momento en el que el comprador recibe de su banco el detalle de las operaciones realizadas con la tarjeta de crédito. Si además se da el caso de que el nombre del comercio en el extracto bancario no coincide, o no se puede asociar, con la página web en la que se ha realizado la compra, esto puede ocasionar que el comprador

dude de si realmente ha sido él quien ha realizado esa transacción.

El comprador, por tanto, está facultado para solicitar al comercio la documentación correspondiente que acredite que él ha realizado la compra. El plazo máximo para esta solicitud es de doce meses desde la fecha de la operación.

Hay que tener en cuenta que, cuando un titular de tarjeta solicita una petición de documentación, en muchos casos se trata de un paso previo al envío de un retroceso del importe cargado (chargeback). Para minimizar el porcentaje de retrocesos recibidos (y que pueden incurrir en penalizaciones si sobrepasan las ratios consideradas aceptables por los programas de control de las marcas de tarjetas), es aconsejable que un supervisor del comercio analice las peticiones de documentación recibidas y realice una devolución de aquellas operaciones que, según sus estudios, han podido ser fraudulentas.

En estos casos, **la entidad emisora de la tarjeta podrá solicitar al comercio el envío del comprobante de la operación**. La solicitud se efectúa mediante el envío de una carta física al comercio en la que han de figurar los datos de la transacción. **El comercio está obligado a responder** en un plazo máximo de **siete días hábiles**. La respuesta puede efectuarse mediante fax al número 93 368 72 91 o al siguiente correo electrónico: peticionfotocopias@bancsabadell.com.

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 entregar la mercancía al titular de la tarjeta (bien por imposibilidad

de estar en el lugar y en el tiempo pactado para recibirlo, bien porque se trate de un regalo), se permitirá hacer el envío a una tercera persona. En este caso, debe quedar registrado este supuesto en el formulario de pedido que el cliente realice en el comercio, con la siguiente información:

- Persona autorizada, identificada con nombre y documento de identidad (DNI, pasaporte, etc.). El pedido debe entregarse únicamente a esa persona y el albarán de entrega deberá incluir la firma del receptor así como la anotación conforme se ha comprobado el documento de identidad proporcionado.
- Para recepción en hoteles o similar será necesario identificar el nombre y dirección del hotel, y también el nombre y documento del huésped que lo recibirá. La recepción tiene que estar firmada por un empleado correctamente identificado del hotel y sellada por este. Además, en el comprobante de recepción deberá 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 la 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 de los siguientes datos:

- _ Nombre del comercio
- _ CIF/NIF del comercio
- _ Código del comercio (FUC)
- _ Número de autorización

- _ Fecha de la operación
- _ Número de tarjeta
- _ Dirección de la página web (URL)
- _ Importe de la transacción
- _ Moneda
- _ Nombre del comprador
- _ Descripción del producto comprado
- _ Definición de la política sobre devoluciones que sigue el comercio, o bien indicación de la URL donde los usuarios pueden informarse de ella.

5.3 Ventas internacionales

Si usted cuenta con el TPV Virtual Plus, debe tener en cuenta que en algunos países existen sistemas de pago diferentes a las tarjetas financieras que gozan de un alto nivel de aceptación. Con el objetivo de maximizar sus ventas, Banco Sabadell, a través de acuerdos con empresas internacionales especializadas, le ofrece acceso a un gran número de pagos locales.

Además, Banco Sabadell también dispone de una licencia transfronteriza (Cross-Border) emitida por Visa y MasterCard para poder procesar de comercios españoles y de comercios ubicados en el extranjero. De este modo, una empresa multinacional podrá gestionar las ventas de todas sus filiales situadas en otros países con una sola integración al TPV Virtual Plus.

Si desea que sus productos se puedan adquirir desde prácticamente cualquier lugar del mundo, el TPV Virtual de Banco Sabadell también le ofrece diversas ventajas en este sentido:

Multilinguaje

Adicionalmente, para una mejor universalización del proceso de pago, todas las páginas

del TPV Virtual y mensajes para el comprador están disponibles en los siguientes idiomas: castellano, catalán, valenciano, gallego, euskera, inglés, francés, alemán, portugués, holandés, polaco, italiano y sueco. El campo `Ds_Merchant_ConsumerLanguage` (ver anexo I del manual), le permite seleccionar el idioma de la página de pago del TPV Virtual.

Servicio multdivisa

Podrá dirigirse a sus clientes ofreciéndoles la posibilidad de comprar en su propia moneda local. El servicio multdivisa está disponible para cualquier divisa del mundo. A través del campo `Ds_Merchant_Currency` podrá escoger la divisa en la que se procesará el pago. Puede consultar la lista de divisas en el anexo V del presente manual.

Operativa DCC (Dynamic Currency Conversion)

Gracias a esta opción, cuando el TPV Virtual detecta que la tarjeta que se está utilizando ha sido emitida en un país con moneda diferente al euro, despliega automáticamente una pantalla informativa en la que el usuario puede elegir entre pagar el producto en euros o, mediante una conversión online del importe, en la divisa que se prefiera. En ambos casos, el abono de la operación en su cuenta se realizará siempre en euros y en el importe inicialmente solicitado.

Liquidación multdivisa

Venda sus productos a cualquier lugar del mundo e ingrese en su cuenta el importe en la divisa original del pago. Podrá abrir cuentas en cualquiera de las divisas admitidas a cotización, sin tener que preocuparse por las diferencias de cambio.

En Banco Sabadell le ingresaremos sus ventas en la misma divisa de la transacción original.

5.4 Operativa DCC (Dynamic Currency Conversion)

El TPV Virtual del Banco permite a los titulares de tarjetas Visa o MasterCard emitidas en una divisa diferente del euro, poder pagar sus compras en la misma moneda de la tarjeta. Se trata de una modalidad de cobro que el comercio puede ofrecer a sus clientes.

Características

Esta operativa sólo se puede aplicar a tarjetas Visa o MasterCard emitidas en una divisa diferente del euro.

El funcionamiento es muy simple: Cuando el TPV Virtual detecta automáticamente que la tarjeta es susceptible de operar en modalidad DCC, muestra la siguiente pantalla de selección de moneda:



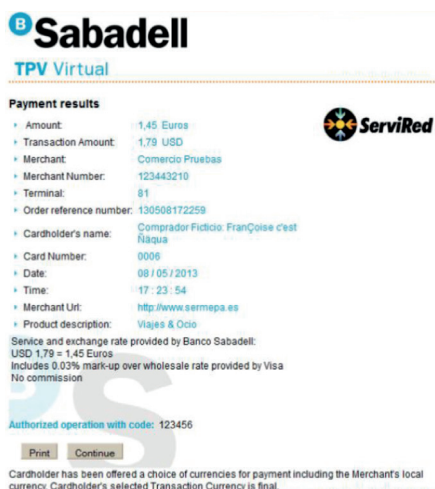
(*) Ejemplo basado en una operación realizada con tarjeta asociada a la divisa USD

En la pantalla se muestra la siguiente información:

- El importe de la operación en euros. Si el cliente escoge esta modalidad, la transacción se realizará en la divisa de la cuenta de abono.
- El importe de la operación en la divisa de la tarjeta. En este caso la transacción se realizará en la moneda original de la tarjeta. La pantalla incluye el mark up, o diferencial

sobre el fixing que se aplicará, y el importe definitivo de la operación, ya que ni el banco del cliente ni Visa o MasterCard podrán aplicar ninguna otra comisión.

A la vista de la pantalla, el cliente deberá elegir libremente si opta por efectuar el pago en euros o en la divisa de la tarjeta. A continuación el TPV Virtual muestra la siguiente pantalla de recibo de la transacción:



Sabadell
TPV Virtual

Payment results

- Amount: 1.45 Euros
- Transaction Amount: 1.79 USD
- Merchant: Comercio Puebas
- Merchant Number: 123443210
- Terminal: 81
- Order reference number: 130508172259
- Cardholder's name: Comprador Ficticio: Françoise c'est Nique
- Card Number: 0006
- Date: 08 / 05 / 2013
- Time: 17 : 23 : 54
- Merchant Url: <http://www.sermepa.es>
- Product description: Viajes & Ocio

Service and exchange rate provided by Banco Sabadell:
USD 1,79 = 1,45 Euros
Includes 0.03% mark-up over wholesale rate provided by Visa
No commission

Authorized operation with code: 123456

Print Continue

Cardholder has been offered a choice of currencies for payment including the Merchant's local currency. Cardholder's selected Transaction Currency is final.

Con independencia de la elección del cliente, la liquidación al comercio se realizará en euros. En la liquidación al comercio figurará: el nominal de la operación y la diferencia entre la comisión de descuento que aplicamos al comercio por operar con el TPV y la bonificación pactada con el comercio por operar en la modalidad DCC.

Ventajas para el titular de la tarjeta:

- El titular de la tarjeta, en el momento de realizar la compra, conoce el importe exacto que le adeudará el banco de su país por la operación.
- El banco del titular de la tarjeta no puede aplicar ninguna comisión por cambio de

divisas, la transacción se realiza en la moneda original de la tarjeta.

Ventajas para el establecimiento:

- Posibilidad de ofrecer un servicio a su cliente que le permite conocer de antemano el importe de la operación.
- Obtiene una bonificación sobre la comisión de descuento por operar con el TPV en las operaciones realizadas con multidivisa.
- A diferencia de la modalidad Multidivisa, en la que se deben actualizar diariamente los precios del catálogo de productos, en la modalidad DCC la conversión se realiza de forma automática.

A modo de ejemplo, se incluye en el apartado 7.9 del presente manual, la información técnica, así como los mensajes de petición de pago, confirmación y respuesta DCC.

El Servicio Técnico de Soporte al TPV Virtual de Banco Sabadell estará a su disposición para resolver cualquier duda referente al servicio DCC. Vea los datos de contacto en el apartado 7.11 del manual.

5.5 IUPAY (Aspectos técnicos)

IUPAY es el servicio de cartera digital (wallet) apto para aquellos comercios que hayan obtenido la certificación PCI-DSS (ver capítulo 11 del manual), y que por tanto pueden capturar y almacenar los datos de la tarjeta. Estos comercios podrán realizar una llamada directa al módulo IUPAY sin pasar por la página de pago del Banco.

Dado que IUPAY necesita operar con el navegador del comprador, las entradas 'WebService' y 'operaciones', ambas Host to Host, no admiten IUPAY.

Para activar IUPAY es necesario utilizar la entrada 'entradaXMLEntidad' (ver capítulo 7 del manual).

La implementación técnica es muy simple, y solamente es necesario incorporar en el formulario de pago que los comercios envían actualmente, un nuevo campo que se denomina `Ds_Merchant_PayMethod`.

Los valores posibles del nuevo campo son los siguientes:

- **`Ds_Merchant_PayMethod = "T"`** para que la llamada de pago realice la validación de la tarjeta informada en el mensaje. Es la opción aplicable para aquellos clientes que escojan en la web el pago con tarjetas, por que tal como ya ocurre en la actualidad, la web capture la tarjeta y envíe al Banco un mensaje de pago contra la tarjeta capturada.

- **`Ds_Merchant_PayMethod = "O"`** para que la llamada de pago active el módulo IUPAY del cliente, con la cartera digital de tarjetas que tenga incorporadas.

El Servicio Técnico de Soporte al TPV Virtual de Banco Sabadell estará a su disposición para resolver cualquier duda referente al servicio IUPAY. Vea los datos de contacto en el apartado 7.11 del manual.

6. Módulo de administración del TPV virtual

6.1 Acceso

El TPV Virtual de Banco Sabadell incluye el acceso a un módulo de administración de las operaciones realizadas. El acceso a esta intranet se realiza mediante una página web y ofrece infinidad de ventajas para la gestión de su negocio.

El módulo de administración ofrece un control en tiempo real de todas las ventas realizadas.

Además de consultar las operaciones realizadas, siempre que lo necesite también podrá tener un control de los cierres contables, gestionar la devolución de los pagos que no sean correctos y visualizar las transacciones que no se han finalizado correctamente, obteniendo información sobre el error o motivo de denegación.

Podrá acceder al módulo de administración del comercio en las siguientes direcciones web:

- Entorno de pruebas:
<https://sis-t.REDSYS.es:25443/canales>
- Entorno real:
<https://sis.REDSYS.es/canales>

Le aparecerá una página donde tendrá que introducir el código de usuario y la contraseña de administrador, previamente facilitados por Banco Sabadell, así como el idioma en el que desea operar con el módulo de administración.

6.2 Usuarios

Las gestiones correspondientes al alta de nuevos usuarios y modificación de los perfiles de acceso las podrá realizar desde el apartado “Usuarios” del módulo de administración del TPV Virtual. Además podrá modificar su contraseña por otra que le sea más fácil de recordar o que considere más segura.

Se pueden asignar dos perfiles distintos a los nuevos usuarios que sean dados de alta:

1. **Perfil informativo:** solo 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.

El apartado “Usuarios” del módulo de administración incluye las siguientes opciones:

1. **Contraseña:** permite modificar la contraseña de acceso del usuario.
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 correo electrónico del comercio especificado.

Además, en función del tipo de consultas que se permita realizar a los usuarios, el administrador podrá dar de alta dos tipos de usuarios:

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

6.3 Consulta y administración de operaciones

El apartado “Consultas” del módulo de administración le permite consultar los datos de las operaciones autorizadas o denegadas de su comercio de los últimos **365 días** na-

turales. Para localizar una operación debe introducir una fecha de inicio y una fecha de fin del período que desea consultar.

Las consultas de operaciones en el módulo de administración están restringidas a períodos de un mes. Si se necesita consultar periodos más extensos, se deberán realizar consultas consecutivas de periodos de treinta días.

Para una mayor rapidez en la búsqueda, si conoce el número de referencia de la transacción, lo puede introducir y accederá de forma inmediata al detalle de esa operación.

Cuando haya introducido los parámetros de búsqueda y haya pulsado el botón “ACEPTAR” aparecerá una pantalla donde se relacionarán las operaciones coincidentes con los parámetros de búsqueda.

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

Los códigos de respuesta que se muestran en el campo “Resultado núm. autorización o código de respuesta”, tanto para operaciones aprobadas como denegadas, se corresponden con los definidos en el Anexo III - Tabla de códigos de respuesta.

6.4 Devolución de operaciones

El módulo de administración del TPV Virtual permite al comercio consultar y generar las devoluciones totales o parciales de las operaciones que se han procesado.

Exclusivamente los usuarios que accedan al módulo de administración con contraseña de perfil administrador están autorizados para realizar devoluciones.

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 la devolución. El importe de la devolución no deberá sobrepasar nunca el importe de la operación original.

En el caso de operativa DCC (Dinamic Currency Conversión) u operativa multidivisa, se deberá introducir el importe en la moneda del terminal.

Cuando se haya aceptado la devolución, se mostrará una página de ticket de devolución, que se puede imprimir o archivar si se desea.

Aquellos comercios que realicen operativa de preautorizaciones, autenticaciones, o preautorizaciones en diferido, podrán generar confirmaciones y anulaciones de las mismas desde el módulo de administración del TPV Virtual.

6.5 Consulta de totales

El módulo de administración del TPV Virtual permite al comercio la consulta de los totales procesados.

Pulsando el botón “Totales” de la parte izquierda de la página principal aparecerá un listado de las últimas 45 sesiones. Se deberá seleccionar la sesión deseada y pulsar “Aceptar”.

A continuación aparecerá la pantalla con los importes totales y el número de operaciones correspondientes a la sesión seleccionada.

Existe la opción de realizar la consulta de totales con desglose (por marca de tarjeta) o sin desglose (360 últimas sesiones).

7. Instalación

El presente manual del TPV Virtual le ofrece la información necesaria para que usted o su departamento informático realicen la instalación del TPV Virtual en la web de su tienda virtual. La instalación es simple y 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 Banco Sabadell.

Se recomienda que esta instalación sea llevada a cabo por las personas que se encargan de forma habitual del mantenimiento del sitio web del comercio y que, con anterioridad a la utilización en real del TPV Virtual, se realicen las pruebas necesarias en el entorno de pruebas del TPV Virtual.

El TPV Virtual de Banco Sabadell admite diversas modalidades en el procesamiento de operaciones de los comercios. Cada modalidad comporta una configuración diferente del sistema.

- **Gateway “realizarPago”**: se trata de una conexión en lenguaje HTML y es la modalidad común en el procesamiento de operaciones. Se utiliza cuando no es necesario que los comercios tengan acceso a los datos de las tarjetas. La instalación en el sistema informático del comercio es simple y consiste en introducir las instrucciones para que las transacciones con tarjeta se ejecuten a través del TPV Virtual en los servidores seguros de Banco Sabadell.
- **Gateway “entradaXMLEntidad”**: en este caso el envío de la transacción se realizará simulando la petición realizada por un formulario con un único input llamado “entrada”. El valor de “entrada” será el documento XML, que debe estar en el formato x-www-form-urlencoded.

Este formulario será enviado a través de un POST y ello permitirá que el comercio pueda capturar los datos de la tarjeta.

Este sistema también permite procesar transacciones 3D Secure.

- **Gateway “operaciones”**: se trata de una conexión HOST-HOST que funciona como una conversación XML. Se utiliza para enviar reembolsos, suscripciones y otras operaciones donde el titular de la tarjeta no está presente y, por tanto, no puede autenticarse.

En caso de que el comercio no desee obtener los datos de las tarjetas y, por tanto, quiera evitar el cumplimiento de la normativa PCI-DSS, deberá utilizar la opción “Gateway realizarPago”.

- **Gateway “WebService”**: el TPV Virtual WebService es un producto que permite a los comercios tener integrado el TPV Virtual dentro de su propia aplicación web. Esta operativa no acepta comercios que posean métodos de pago con autenticación del titular por parte de la entidad emisora de la tarjeta.

7.1 Gateway “realizarPago”

Lenguaje de programación	HTML
Permite autenticación del titular (3D Secure)	SÍ
Permite al comercio capturar datos de la tarjeta	NO

La página de pago de la web del comercio debe incluir un botón para que el comprador lo identifique con la modalidad de pago con tarjeta.

En el momento en que el cliente pulse el botón de pago, el comercio rellenará un formulario web con los datos de la transacción, cuya descripción técnica detallada figura en el Anexo I del presente manual, y lo enviará a la siguiente dirección:

- » Entorno de pruebas: <https://sis-t.redsys.es:25443/sis/realizarPago>
- » Entorno real: <https://sis.redsys.es/sis/realizarPago>

La ventana o frame donde se abra el TPV Virtual deberá tener barras de desplazamiento para poder adaptarse a las diferentes páginas de autenticación que pudieran mostrarse al titular en los procesos posteriores.

El titular de la tarjeta que vaya a efectuar la compra en el comercio introducirá los datos de la tarjeta directamente en el TPV Virtual ubicado en la página segura de Banco Sabadell, y por tanto el comercio no tendrá acceso a los datos de la tarjeta del comprador.

En el mensaje existe un campo adicional donde los principales datos relacionados con la compra se transmiten de forma securizada mediante el algoritmo hash SHA-1. (Ver apartado 7.6)

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.

7.1.1 Continuidad de la sesión del navegador

Una vez que el titular de la tarjeta ha finalizado el proceso de pago, se le muestra la pantalla con el resultado del mismo; esta

pantalla debe incluir el botón “Cerrar” para que el comprador retorne a la sesión de la web del comercio.

La forma en que continúe la sesión del comercio con su cliente irá en función de las instrucciones asociadas al botón “Cerrar”. Estas instrucciones, que el titular del comercio habrá comunicado a Banco Sabadell en el cuestionario que se le tramita para iniciar el proceso de alta, pueden ser:

- **Instrucción “CERRAR VENTANA”:** al seleccionar “Cerrar” se cerrará la ventana o frame con el resultado del pago y se continuará la sesión en la página del comercio que permanecía en segundo plano.
- **Instrucciones “URL_OK” y “URL_KO”:** al seleccionar “Cerrar” la sesión del navegador continuará en la misma ventana de la página de pago, redirigiéndose a una URL que el comercio previamente haya comunicado a Banco Sabadell. 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 del navegador, las URL_OK/URL_KO no estarán operativas y la sesión continuará en la página del comercio que permanecía en segundo plano.

- **Opción para comercios con RESPUESTA ONLINE VÍA URL:** además de las dos instrucciones anteriores, para los comercios que disponen del servicio de RESPUESTA ONLINE VÍA 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 *online*.

El TPV Virtual incluye fuertes validaciones y controles para detectar posibles errores en la entrada de datos. Si se produce algún error en la entrada de datos, se generará un código de error y no se permitirá continuar

con la operación. Dependiendo del error producido, el mensaje mostrado al titular será diferente. La descripción técnica detallada de los diferentes mensajes de error se incluye en el Anexo II del presente manual.

7.2 Gateway “entrada XMLEntidad”

Lenguaje de programación (single input)	XML
Permite autenticación del titular (3D Secure)	SÍ
Permite al comercio capturar datos de la tarjeta	SÍ

La comunicación de los datos de la transacción 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 montará un documento XML de respuesta con el resultado de la misma.

La descripción técnica detallada de los datos del documento XML figura en el Anexo I del presente manual.

El formulario de compra a través de TPV Virtual se compondrá de un único input llamado “entrada”. El valor de “entrada” será el documento XML, el cual debe estar en formato x-www-form-urlencoded. Dicho formulario se enviará mediante un POST. El comercio facilitará la información de la compra a la siguiente dirección del servidor web:

- » Entorno de pruebas: <https://sis-t.redsys.es:25443/sis/entradaXMLEntidad>
- » Entorno real: <https://sis.redsys.es/sis/entradaXMLEntidad>

La ventana o *frame* donde se abra el TPV Virtual debe tener barras de desplazamiento para poder adaptarse a las diferentes páginas de autenticación que pudieran mostrarse al titular en los procesos posteriores.

Es importante destacar que esta modalidad requiere el cumplimiento de los requerimientos del programa de seguridad PCI-DSS. (Ver apartado 11 del presente manual)

Se han definido dos tipos de documentos XML:

- “DATOSENTRADA”: se trata del documento enviado por el TPV Virtual en la petición de pago.
- “NOTIFICACIONXML”: se trata del documento de respuesta que envía la plataforma de pago en la notificación online.

A continuación se describe el código de ambos mensajes:

Mensaje XML “DATOSENTRADA”

```
<!ELEMENT DATOSENTRADA
(DS_VERSION,
DS_MERCHANT_AMOUNT,
DS_MERCHANT_CURRENCY,
DS_MERCHANT_ORDER,
DS_MERCHANT_MERCHANTCODE,
DS_MERCHANT_MERCHANTURL?,
DS_MERCHANT_URLOK?,
DS_MERCHANT_URLKO?,
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?,
DS_MERCHANT_SUMTOTAL ?,
DS_MERCHANT_DATEFREQUENCY ?,
DS_MERCHANT_CHARGEEXPIRYDATE ?,
DS_MERCHANT_AUTHORISATIONCODE ?,
DS_MERCHANT_TRANSACTIONDATE ?)>
<!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_URLOK (#PCDATA)>
<!ELEMENT DS_MERCHANT_URLKO (#PCDATA)>
<!ELEMENT DS_MERCHANT_MERCHANTNAME (#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)>
<ELEMENT DS_MERCHANT_DATEFREQUENCY (#PCDATA)>
<ELEMENT DS_MERCHANT_CHARGEEXPIRYDATE (#PCDATA)>
<ELEMENT DS_MERCHANT_AUTHORISATIONCODE (#PCDATA)>
<ELEMENT DS_MERCHANT_TRANSACTIONDATE (#PCDATA)>
<ELEMENT DS_MERCHANT_SUMTOTAL (#PCDATA)>

```

Donde:

- DS_VERSION: versión del mensaje.
- DS_MERCHANT_AMOUNT: ver Anexo I.
- DS_MERCHANT_CURRENCY: ver Anexo I.
- DS_MERCHANT_ORDER: ver Anexo I.
- DS_MERCHANT_MERCHANTCODE: ver Anexo I.
- DS_MERCHANT_MERCHANTURL: ver Anexo I.
- DS_MERCHANT_URLOK: ver Anexo I.
- DS_MERCHANT_URLKO: ver Anexo I.
- DS_MERCHANT_MERCHANTNAME: ver Anexo I.
- DS_MERCHANT_MERCHANTSIGNATURE: ver apartado 7.6.
- DS_MERCHANT_TERMINAL: ver Anexo I.
- DS_MERCHANT_TRANSACTIONTYPE: ver Anexo I.
- DS_MERCHANT_MERCHANTDATA: ver Anexo I.
- DS_MERCHANT_PAN: ver Anexo I.
- DS_MERCHANT_EXPIRYDATE: ver Anexo I.
- DS_MERCHANT_CVV2: ver Anexo I.
- DS_MERCHANT_DATEFREQUENCY: ver Anexo I.
- DS_MERCHANT_CHARGEEXPIRYDATE: ver Anexo I.
- DS_MERCHANT_AUTHORISATIONCODE: ver Anexo I.
- DS_MERCHANT_TRANSACTIONDATE: ver Anexo I.
- DS_MERCHANT_SUMTOTAL: ver Anexo I.

A continuación se muestra un ejemplo del mensaje:

```

<DATOSENTRADA>
<DS_VERSION>1.999008881</DS_VERSION>
<DS_MERCHANT_CURRENCY>978</DS_MERCHANT_
CURRENCY>
<DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_
TRANSACTIONTYPE>
<DS_MERCHANT_AMOUNT>45</DS_MERCHANT_AMOUNT>
<DS_MERCHANT_MERCHANTCODE>999008881</DS_
MERCHANT_MERCHANTCODE>
<DS_MERCHANT_TERMINAL>1</DS_MERCHANT_TERMINAL>
<DS_MERCHANT_ORDER>112545</DS_MERCHANT_ORDER>
<DS_MERCHANT_PAN>4548812049400004</DS_MERCHANT_
PAN>
<DS_MERCHANT_EXPIRYDATE>1205</DS_MERCHANT_
EXPIRYDATE>
<DS_MERCHANT_CVV2>123</DS_MERCHANT_CVV2>
<DS_MERCHANT_MERCHANTSIGNATURE>
</DATOSENTRADA>

```

(La longitud de los campos “Ds_Merchant_Currency”, “Ds_Merchant_Terminal” y “Ds_Merchant_ConsumerLanguage” se considera

máxima, por lo que no es imprescindible el relleno con ceros a la izquierda; la firma ha de ser generada con los campos exactamente como se envíen).

Mensaje XML “NOTIFICACIONXML”

Como respuesta a la petición realizada, el SIS devolverá al comercio un documento XML con el resultado de la petición.

Este documento de respuesta se introducirá de igual manera en un formulario, dentro de un campo denominado “datos”, después de haberlo pasado a formato x-www-form-urlencoded.

```

Versión 1.<fuc_comercio>
<ELEMENT NOTIFICACIONXML
(Ds_Version,
Ds_Amount,
Ds_Currency,
Ds_Order,
Ds_MerchantCode,
Ds_Terminal,
Ds_Response,
Ds_MerchantData?,
Ds_SecurePayment,
Ds_Card_Number,
Ds_ExpiryDate,
Ds_Card_Country,
Ds_TransactionType,
Ds_AuthorisationCode,
Ds_Signature,
Ds_ErrorCode ?)>

```

```

<ELEMENT Ds_Version (#PCDATA)>
<ELEMENT Ds_Amount (#PCDATA)>
<ELEMENT Ds_Currency (#PCDATA)>
<ELEMENT Ds_Order (#PCDATA)>
<ELEMENT Ds_MerchantCode (#PCDATA)>
<ELEMENT Ds_Terminal (#PCDATA)>
<ELEMENT Ds_Response (#PCDATA)>
<ELEMENT Ds_MerchantData (#PCDATA)>
<ELEMENT Ds_SecurePayment (#PCDATA)>
<ELEMENT Ds_Card_Number (#PCDATA)>
<ELEMENT Ds_ExpiryDate (#PCDATA)>
<ELEMENT Ds_Card_Country (#PCDATA)>
<ELEMENT Ds_TransactionType (#PCDATA)>
<ELEMENT Ds_AuthorisationCode (#PCDATA)>
<ELEMENT Ds_Signature (#PCDATA)>
<ELEMENT Ds_ErrorCode (#PCDATA)>

```

Donde:

- Ds_Version: versión de la DTD para validar el mensaje XML.
- Ds_Amount: importe de la operación.
- Ds_Currency: moneda de la operación.
- Ds_Order: pedido de la operación.
- Ds_Signature: ver apartado 7.6, Diseño del algoritmo hash en

- el servidor de Internet.
- 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 que se indican en el Anexo III.
- Ds_AuthorisationCode: código de autorización en el caso de que exista.
- Ds_TransactionType: tipo de la operación realizada. Ver tabla del apartado 7.7.
- Ds_MerchantData: ver tabla del apartado 7.7.
- Ds_SecurePayment: ver tabla del apartado 7.7.
- Ds_Card_Number: número de tarjeta.
- Ds_ExpiryDate: año y mes de caducidad de la tarjeta AAMM.
- Ds_Card_Country: país de la tarjeta.
- Ds_ErrorCode: campo opcional que aparecerá en el caso de que se detecte un error en el procesamiento de la operación.

A continuación se muestra un ejemplo del mensaje:

```
<NOTIFICACIONXML>
  <Ds_Version>1.XXX</Ds_Version>
  <Ds_Amount>100</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>
  <Ds_Order>0001</Ds_Order>
  <Ds_MerchantCode>999008881</Ds_MerchantCode>
  <Ds_Terminal>1</Ds_Terminal>
  <Ds_Response>0</Ds_Response>
  <Ds_MerchantData>Mis Datos</Ds_MerchantData>
  <Ds_SecurePayment>1</Ds_SecurePayment>
  <Ds_Card_Number>99999999999999999999</Ds_Card_Number>
  <Ds_ExpiryDate>0204</Ds_ExpiryDate>
  <Ds_TransactionType>0</Ds_TransactionType>
  <Ds_AuthorisationCode>222FFF</Ds_AuthorisationCode>
  <Ds_Signature>.....</Ds_Signature>
</NOTIFICACIONXML>
```

Al igual que en el apartado 7.6 se explica el procedimiento de cálculo de la firma que protege los datos de la transacción que el comercio ha generado, en caso de que éste desee recibir una respuesta online a las peticiones, el sistema le proporcionará una firma que garantiza a su vez la integridad de las respuestas.

El TPV Virtual por defecto puede comunicar a los puertos 80, 443, 8080 y 8081 del comercio. Para otros puertos deberá ser consultado.

Una vez que el comercio recibe el formulario, el código de respuesta (Ds_Response) indicará si la transacción ha sido aceptada o rechazada, y en este último caso se indicará

el motivo del rechazo. El Anexo III del presente documento detalla los valores del código de respuesta (Ds_Response).

El TPV Virtual incluye fuertes validaciones y controles para detectar posibles errores en la entrada de datos. Si se produce algún error en la entrada de datos, se generará un código de error y no se permitirá continuar con la operación. Dependiendo del error producido, el mensaje mostrado al titular será diferente. La descripción técnica detallada de los diferentes mensajes de error se incluye en el Anexo II del presente manual.

7.3 Gateway “operaciones”

Lenguaje de programación	XML
Permite autenticación del titular (3D Secure)	NO
Permite al comercio capturar datos de la tarjeta	SÍ

Se trata de una conexión HOST-HOST que funciona como una conversación XML. Se utiliza para enviar devoluciones, suscripciones y otras operaciones donde el titular de la tarjeta no está presente y, por tanto, no puede autenticarse.

En caso de que el comercio no desee obtener los datos de las tarjetas y, por tanto, quiera evitar el cumplimiento de la normativa PCI-DSS, deberá utilizar la opción “Gateway realizarPago”.

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
- 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
- L - Transacción “Tarjeta archivo inicial” (suscripciones y pago exprés)
- M - Transacciones “Tarjetas archivo sucesivas” (suscripciones y pago exprés)

Exceptuando los tipos 3 y 8, el resto no están activados por defecto. Los comercios que los consideren necesarios deberán solicitar su activación a su oficina o gestor de Banco Sabadell. Todas las operaciones que se envíen mediante este sistema se consideraran NO SEGURAS ya que no existe autenticación del titular de la tarjeta.

Los tipos 1, A, O y L que se procesen mediante este protocolo requerirán que el comercio solicite directamente al comprador su número de tarjeta y caducidad. Los comercios que los consideren necesarios deberán solicitar su activación a su oficina o gestor de Banco Sabadell. Además esta opción requiere que previamente el comercio haya cumplimentado los cuestionarios del programa PCI-DSS de seguridad en los datos de tarjetas. Ver apartado 11 del presente manual.

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 montará un documento XML de respuesta con el resultado de la misma.

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

- » Entorno de pruebas: <https://sis-t.REDSYS.es:25443/sis/operaciones>
- » Entorno 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 deberá estar en formato x-www-form-urlencoded.

A continuación se describen las especificaciones de los dos posibles tipos de mensajes:

- a. DATOSENTRADA: mensaje de solicitud enviado.
- b. RETORNOXML: respuesta a la petición.

a. Especificación del documento DATOSENTRADA

Este mensaje se enviará 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 Anexo I - Datos del formulario de pago.

– DS_MERCHANT_CURRENCY: ver Anexo I - Datos del formulario de pago.

– DS_MERCHANT_ORDER: ver Anexo I - Datos del formulario de pago.

– DS_MERCHANT_MERCHANTCODE: ver Anexo I - Datos del formulario de pago.

– DS_MERCHANT_MERCHANTURL: ver Anexo I - Datos del formulario de pago.

– DS_MERCHANT_MERCHANTNAME: ver Anexo I - Datos del formulario de pago.

– DS_MERCHANT_CONSUMERLANGUAGE: ver Anexo I - Datos del formulario de pago.

– DS_MERCHANT_MERCHANTSIGNATURE: SHA-1 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 Anexo I - Datos del formulario de pago.

– 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.
- 8 - Confirmación de autenticación.
- 9 - Anulaciones de preautorizaciones.

A - Pago no seguro sin autenticación.

O - Preautorización diferida.

P - Confirmación de preautorización diferida.

Q - Anulación de preautorización diferida.

L - Transacción "Tarjeta archivo inicial" (suscripciones y pago exprés).

M - Transacciones "Tarjetas archivo sucesivas" (suscripciones y pago exprés).

– DS_MERCHANT_MERCHANTDATA: ver Anexo I - Datos del formulario de pago.

– DS_MERCHANT_PAN: número de tarjeta.

– DS_MERCHANT_EXPIRYDATE: fecha caducidad (AAMM).

– DS_MERCHANT_AUTHORISATIONCODE: solo válido para devoluciones de transacciones recurrentes sucesivas.

– DS_MERCHANT_TRANSACTIONDATE: solo válido para devoluciones de transacciones recurrentes sucesivas.

– 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 = SHA-1 (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>
a63dfa507e549936f41f4961cddace126b8ecdea
</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>
```

b. 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 que se indican en el Anexo III.
- Ds_AuthorisationCode: código de autorización en caso de existir.
- Ds_TransactionType: tipo de operación realizada.
- Ds_MerchantData: ver tabla del apartado 7.7.
- Ds_SecurePayment: ver tabla del apartado 7.7.
- Ds_Reference: campo opcional para pago por referencia.
- Ds_Language: indica el 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>EEFF45687hgh</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>EEFF45687hgh</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 - Núm. 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>
a63dfa507e549936f41f4961codace126b8ecdea
</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>

```

7.4 Gateway “WebService”

Lenguaje de programación	XML
Permite autenticación del titular (3D Secure)	NO
Permite al comercio capturar datos de la tarjeta	SÍ

El TPV Virtual WebService permite a los comercios tener integrado el TPV Virtual dentro de su propia aplicación web. Este tipo de conexión al TPV Virtual a través de WebService no se permite en aquellos comercios que posean métodos de pago seguros, que solicitan autenticación del titular por parte de la entidad emisora de la tarjeta.

La conexión al TPV Virtual se realizará mediante el envío de una petición vía WebService a la siguiente dirección:

- » Entorno de pruebas: <https://sis-t.redsys.es:25443/sis/services/SerClsWSEntrada>
- » Entorno real: <https://sis.redsys.es/sis/services/SerClsWSEntrada>

La plataforma de pago interpretará esta petición y realizará las validaciones necesarias

para, a continuación, procesar la operación. Dependiendo del resultado de la operación, se construye un documento XML de respuesta con el resultado de la misma.

Para poder realizar la compra a través del TPV Virtual WebService, es necesario intercambiar una serie de datos, tanto en los mensajes de petición como en los mensajes de respuesta.

7.4.1 Mensajes de petición

Podemos diferenciar tres tipos de peticiones:

- Peticiones de pago (con envío de datos de tarjeta)
- Peticiones de confirmación
- Peticiones de devolución

En cada tipo varía la estructura del mensaje y los parámetros que se envían/reciben. A continuación explicamos cada tipo con los parámetros necesarios y mostramos un ejemplo de cada caso.

Mensaje de petición de pago

Los datos necesarios que debe incluir el mensaje para enviar al TPV Virtual WebService en formato XML una petición de pago y sus características técnicas, se describen en el Anexo I del presente manual.

A continuación se detalla un ejemplo de cómo utilizar esos datos en los mensajes de petición de pago.

```

<DATOSENTRADA>
<DS_MERCHANT_AMOUNT>145</DS_MERCHANT_AMOUNT>
<DS_MERCHANT_ORDER>050911523002</DS_MERCHANT_ORDER>
<DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
<DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
<DS_MERCHANT_PAN>4548810000000000</DS_MERCHANT_PAN>
<DS_MERCHANT_CVV2>123</DS_MERCHANT_CVV2>
<DS_MERCHANT_TRANSACTIONTYPE>A</DS_MERCHANT_TRANSACTIONTYPE>
<DS_MERCHANT_TERMINAL>999</DS_MERCHANT_TERMINAL>

```

```
<DS_MERCHANT_EXPIRYDATE>1212</DS_MERCHANT_
EXPIRYDATE>
<DS_MERCHANT_MERCHANTSIGNATURE>22809e232ae
8c1b6996c9934530bc75b03b3c767</DS_MERCHANT_
MERCHANTSIGNATURE>
</DATOSENTRADA>
```

Mensaje de petición de confirmación/devolución

Los datos necesarios que debe incluir el mensaje para enviar al TPV Virtual WebService en formato XML una petición de confirmación/devolución y sus características técnicas, se describen en el Anexo I del presente manual.

A continuación se detalla un ejemplo de cómo utilizar esos datos en los mensajes de petición de pago.

```
<DATOSENTRADA>
  <DS_MERCHANT_AMOUNT>145</DS_MERCHANT_AMOUNT>
  <DS_MERCHANT_ORDER>050911523002</DS_MER-
  CHANT_ORDER>
  <DS_MERCHANT_MERCHANTCODE>999008881</DS_MER-
  CHANT_MERCHANTCODE>
  <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CU-
  RRENCY>
  <DS_MERCHANT_TRANSACTIONTYPE>3</DS_MERCHANT_
  TRANSACTIONTYPE>
  <DS_MERCHANT_TERMINAL>999</DS_MERCHANT_TER-
  MINAL>
  <DS_MERCHANT_MERCHANTSIGNATURE>df66905b10a84
  8ddfa80b202aedcd6b172533cc0</DS_MERCHANT_MER-
  CHANTSIGNATURE>
</DATOSENTRADA>
```

7.4.2 Mensajes de respuesta

Los datos y las características técnicas que se recibirán en el mensaje de respuesta, tras una petición al TPV Virtual WebService, en formato XML, se detallan en el apartado 7.7 del presente manual.

Así mismo se incluye un ejemplo de cómo utilizar esos datos en los mensajes de respuesta.

Ejemplo de mensaje de respuesta de la operación

```
<RETORNOXML>
  <CODIGO>0</CODIGO>
```

```
<OPERACION>
  <Ds_Amount>145</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>
  <Ds_Order>050911523002</Ds_Order>
  <Ds_Signature>702676D44A56D722EAE1FBF16F74
  D58C6EA2D27</Ds_Signature>
  <Ds_MerchantCode>999008881</Ds_MerchantCode>
  <Ds_Terminal>999</Ds_Terminal>
  <Ds_Response>0000</Ds_Response>
  <Ds_AuthorisationCode>758688</Ds_Authorisation-
  Code>
  <Ds_TransactionType>A</Ds_TransactionType>
  <Ds_SecurePayment>0</Ds_SecurePayment>
  <Ds_Language>1</Ds_Language>
  <Ds_MerchantData>
  </Ds_MerchantData>
  <Ds_Card_Country>826</Ds_Card_Country>
  </OPERACION>
</RETORNOXML>
```

Ejemplo de mensaje de respuesta de la operación de devolución

```
<RETORNOXML>
  <CODIGO>0</CODIGO>
  <OPERACION>
    <Ds_Amount>145</Ds_Amount>
    <Ds_Currency>978</Ds_Currency>
    <Ds_Order>102113140002</Ds_Order>
    <Ds_Signature>BAAC6FA0EA24821B7CAB7D6A9875
    BC8BE3C1562</Ds_Signature>
    <Ds_MerchantCode>297124299</Ds_MerchantCode>
    <Ds_Terminal>1</Ds_Terminal>
    <Ds_Response>0900</Ds_Response>
    <Ds_AuthorisationCode>487603</Ds_Authorisation-
    Code>
    <Ds_TransactionType>3</Ds_TransactionType>
    <Ds_SecurePayment>0</Ds_SecurePayment>
    <Ds_Language>1</Ds_Language>
    <Ds_MerchantData>
    </Ds_MerchantData>
    <Ds_Card_Country>724</Ds_Card_Country>
  </OPERACION>
</RETORNOXML>
```

7.5 Localización de errores

El TPV Virtual incluye fuertes validaciones y controles para detectar posibles errores en la entrada de datos. Es posible que durante la instalación del TPV Virtual, en el momento de envío del formulario de pago, alguno de los parámetros de los campos del formulario sea erróneo. Si se produce algún error en la entrada de datos, se generará un código de error y no se permitirá continuar con la operación.

Dependiendo del error producido, el mensaje mostrado al titular será diferente. La des-

cripción técnica detallada de los diferentes mensajes de error se incluye en el Anexo II del presente manual. En el citado documento anexo se enumeran los posibles valores de error que se pueden recibir en la respuesta del TPV Virtual, así como el campo al que afectan (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.

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 “<!--sisxxx:-->” indicará el tipo de error según la tabla adjunta del Anexo II.

7.6 Diseño del algoritmo hash en el servidor de Internet

Banco Sabadell 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.

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 SHA-1 no está disponible en versiones de php inferiores a la versión 5.0. Si su servidor utiliza alguna versión anterior pónganse en contacto con el servicio técnico de Banco Sabadell para encontrar una solución alternativa.

La forma de cálculo del algoritmo difiere según sea la modalidad de pago escogida.

7.6.1 Gateway “realizarPago”

En este caso la firma electrónica del comercio se deberá calcular concatenando el valor de los siguientes campos (salvo que alguno sea de valor nulo, en cuyo caso no se considerará en la firma) incluyendo al final la clave secreta de encriptación:

```
Digest=SHA-1(Ds_Merchant_Amount+Ds_Merchant_Order +
Ds_Merchant_MerchantCode +
Ds_Merchant_Currency + Ds_Merchant_TransactionType +
Ds_Merchant_MerchantURL + SECRET
CODE)
```

Si el comercio no tiene URL de notificación online, se deberá dejar 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: c8392b7874e2994c74fa8bea3e-
2dff38f3913c46
```

7.6.2 Gateways “entradaXMLEntidad” y “operaciones”

En este caso la firma electrónica del comercio se deberá calcular concatenando el valor de los siguientes campos (salvo que alguno sea de valor nulo, en cuyo caso no se considerará en la firma) incluyendo al final la clave secreta de encriptación:

```
Digest = SHA-1(Ds_Merchant_Amount + Ds_Merchant_Order
+ Ds_Merchant_MerchantCode+
Ds_Merchant_Currency + Ds_Merchant_Pan + Ds_Mer-
chant_MerchantURL(1) + Ds_Merchant_CVV2 (2) +
Ds_Merchant_TransactionType + SECRET CODE)
```

(1) Solo para “entradaXMLgateway”

(2) Solo si se facilita el código CVV2

Es imprescindible destacar que está totalmente prohibido almacenar los datos del CVV2. Por este motivo no se debe grabar el

CVV2 en el momento de calcular la firma de la transacción.

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) =
999008881
MONEDA (Ds_Merchant_Currency) = 978
NÚMERO DE TARJETA (Ds_Merchant_Pan) =
4548812049400004
URL del COMERCIO (Ds_Merchant_MerchantURL) = http://
www.redsys.es
CLAVE SECRETA = h2u282kMks01923kmqpo
Cadena resultado: 12352929292920192019197845488
10000000003
Resultado SHA-1: 8cbd9137533846152fc3b8921d909742e-
6b87f8e
```

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.

Forma de cálculo en el documento “RETORNOXML”:

```
Ds_Signature= SHA-1 (Ds_Amount + Ds_Order + Ds_Mer-
chantCode + Ds_Currency + Ds_Response +
Ds_Merchant_Pan + Ds_TransactionType + Ds_SecurePayment
+ SECRET CODE)
El valor (Ds_Merchant_Pan) formará parte de la firma solo si
se envía el número de tarjeta. Adicionalmente, si el número
de tarjeta se informa con un asterisco, el campo (Ds_Mer-
chant_Pan) formará parte de la firma con el valor de asterisco.
```

7.6.3 Gateway “WebService”

La firma electrónica del comercio, en los mensajes de petición de pago al TPV Virtual, se deberá calcular concatenando el valor de los siguientes campos (salvo que alguno sea de valor nulo, en cuyo caso no se considerará en la firma) incluyendo al final la clave secreta de encriptación:

```
Ds_Merchant_Amount + Ds_Merchant_Order + Ds_Merchant_
Merchantcode + Ds_Merchant_Currency + Ds_Merchant_Pan
+ Ds_Merchant_Cvv2 + Ds_Merchant_Transactiontype + Clave
Secreta
```

Ejemplo:

```
IMPORTE (Ds_Merchant_Amount) = 145 (va multiplicado
por 100)
NÚMERO DE PEDIDO (Ds_Merchant_Order) =
050911523002
```

```
CÓDIGO COMERCIO (Ds_Merchant_MerchantCode) =
999008881
MONEDA (Ds_Merchant_Currency) = 978
NÚMERO DE TARJETA (Ds_Merchant_Pan) =
4548810000000000
CVV2 = 123
Tipo de transacción = A
CLAVE SECRETA = qwertyasdf0123456789
Cadena resultado: 14505091152300299900888197845
48810000000000123Aqwertyasdf0123456789
Resultado SHA-1: 22809e232ae8c1b6996c9934530b-
c75b03b3c767
```

La firma electrónica del comercio, en los mensajes de petición de confirmación/devolución al TPV Virtual, se deberá calcular concatenando el valor de los siguientes campos (salvo que alguno sea de valor nulo, en cuyo caso no se considerará en la firma) incluyendo al final la clave secreta de encriptación:

```
Ds_Merchant_Amount + Ds_Merchant_Order + Ds_Mer-
chant_Merchantcode + Ds_Merchant_Currency + Ds_Mer-
chant_Transactiontype + Clave Secreta
```

Ejemplo:

```
IMPORTE (Ds_Merchant_Amount) = 145 (va multiplicado
por 100)
NÚMERO DE PEDIDO (Ds_Merchant_Order) =
050911523002
CÓDIGO COMERCIO (Ds_Merchant_MerchantCode) =
999008881
MONEDA (Ds_Merchant_Currency) = 978
Tipo de transacción = 3
CLAVE SECRETA = qwertyasdf0123456789
Cadena resultado: 1450509115230029990088819783
qwertyasdf0123456789
Resultado SHA-1: df66905b10a848ddfa80b202aedcd6b-
172533cc0
```

7.6.4 Recomendaciones generales para el cálculo de la firma

Una vez que se ha generado la firma no se deben modificar los datos de la petición de ningún modo, ya que el TPV Virtual los utiliza para validarla. Si los datos que se envían al TPV Virtual no son exactamente los que se utilizaron para generar la firma, se generará un error y no se podrá continuar la compra.

El **importe** vendrá multiplicado por 100, sin decimales y sin ceros a la izquierda, salvo en el caso de los yenes, que no tienen decimales.

El **número de pedido** será diferente en cada

transacción y las cuatro primeras posiciones tienen que ser numéricas.

Hay que verificar que la **clave** que se está utilizando para hacer la firma es la que está asignada al comercio y comprobar el entorno (pruebas o real) en el que está realizando la petición de compra.

NOTA IMPORTANTE:

- La clave secreta nunca debe ser revelada a terceros, 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.
- 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.

7.6.5 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/ds-aval.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>

7.7 Respuesta online del TPV Virtual al comercio

Esta opción está disponible para aquellos comercios que necesitan, para su gestión, una verificación inmediata de las transacciones realizadas a través del TPV Virtual.

Existen varios mecanismos de respuesta que pueden coexistir de forma simultánea. Se trata de los siguientes:

1. Consulta directa de las transacciones por Internet mediante el acceso al **módulo de administración del TPV Virtual**.
2. Implementación de una solución de **respuesta online**.

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. Sincronización vía SOAP

Permite al comercio realizar una consulta de una operación mediante la tecnología SOAP/XML.

4. Recepción de datos vía XML

Esta modalidad está disponible en exclusiva para las modalidades “Gateway-entradaXMLEntidad”, “Gateway-operaciones” y “Gateway-WebService”.

A continuación se amplía la información correspondiente a los casos de “Respuesta online” y “Sincronización vía SOAP”, teniendo en cuenta que el modo de “Respuesta online” es el sistema más utilizado.

7.7.1 Respuesta online

Existen dos modos de recepción de la respuesta online, que se pueden combinar entre ellos, utilizando ambos a la vez o uno de ellos como secundario en caso de fallar el otro:

– **Notificación al correo electrónico del comercio:**

La respuesta a la autorización de pago se recibirá en la dirección de correo electrónico que el comercio haya indicado al solicitar el alta del TPV Virtual.

– **Notificación HTTP:**

La respuesta a la autorización de pago se recibirá en la dirección URL (Ds_Merchant_MerchantURL) indicada en el formulario de pago. Esta opción requiere unos sencillos desarrollos informáticos en la web del comercio. **Es la opción recomendada ya que garantiza la respuesta de forma inmediata.**

Para implementar la respuesta *online* vía notificación HTTP se debe facilitar en el formulario de petición de pago una URL en la que se recibirán 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. La URL no se cargará en el navegador y, por tanto, no será visible para el usuario. En ella se podrán recibir y recoger los datos de la respuesta online y de esta forma introducirlos en la base de datos del comercio.

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 DATO	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.
Número 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_Merchant_MerchantData	1024 AN	Información opcional enviada por el comercio en el formulario de petición de pago.

DATO	NOMBRE DEL DATO	LONG.	COMENTARIOS
País del titular	Ds_Card_Country	3 N	País de emisión de la tarjeta. Ver Anexo IV con la 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	0 - Cliente 1 - Castellano 2 - Inglés 3 - Catalán 4 - Francés 5 - Alemán 6 - Neerlandés 7 - Italiano 8 - Sueco 9 - Portugués 10 - Valenciano 11 - Polaco 12 - Gallego 13 - Euskera
Tipo de tarjeta	Ds_Card_Type	1 AN	C - Tarjeta de crédito D - Tarjeta de débito

(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 envían).

De la misma manera que en la petición de pago de una compra, la respuesta online incluye una firma electrónica que garantizará la integridad de las respuestas.

El algoritmo será el mismo y la fórmula a tener en cuenta 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 online 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. Para otros puertos se deberá consultar al servicio técnico de Banco Sabadell.

Una vez que el comercio recibe el formulario, los valores del campo “Código de respuesta” (Ds_Response) indican si la operación está aprobada o denegada y, en este caso, el motivo por el que se ha denegado. El Anexo III incluye la tabla de códigos de respuesta.

El TPV Virtual efectúa el envío de las notificaciones online para las operaciones de compra autorizadas y denegadas por la entidad emisora de la tarjeta, así como en aquellas situaciones en las que el proceso de compra ha sido interrumpido al haberse producido uno de los siguientes errores:

SIS0051 -> Pedido repetido. Se envía notificación con código 913.

SIS0078 -> Método de pago no disponible para su tarjeta. Se envía notificación con código 118.

SIS0093 -> Tarjeta no válida. Se envía notificación con código 180.

SIS0094 -> Error en la llamada al MPI sin controlar. Se envía notificación con código 184.

SIS0218 -> El comercio no permite preautorización por la entrada XML.

SIS0256 -> El comercio no puede realizar preautorizaciones.

7.7.2 Sincronización SOAP

Este método de sincronización permite al comercio recibir una notificación de la transacción en un servicio SOAP. Si el comercio no tiene privilegios para activar este permiso con su usuario, deberá solicitar la activación a través de Banco Sabadell. Esta sincronización es una notificación en sí, por lo que no tiene sentido rellenar el campo de notificación online, ya que no se tomará en cuenta.

Si la opción “Sincronización SOAP” está habilitada para un comercio significará que el TPV Virtual enviará las notificaciones para

operaciones de autorización, preautorización y autenticación como peticiones SOAP a un servicio que tendrá publicado el comercio. Para el resto de operaciones las notificaciones se realizarán de forma síncrona y según la opción elegida en la configuración del comercio para las notificaciones online.

La principal particularidad de esta notificación es que el TPV Virtual espera una respuesta a la notificación antes de presentar el resultado de la operación al titular que está realizando la compra. En el caso en que el comercio devuelva una respuesta con valor KO o se produzca un error durante el proceso de notificación, el SIS anulará la operación y presentará al titular un recibo con el resultado KO, es decir, el TPV Virtual supedita el resultado de la operación a la respuesta que obtenga del comercio en la notificación.

La URL del router al que se conectará el TPV Virtual y donde estará publicado el servicio SOAP deberá enviarla el comercio en el parámetro “Ds_Merchant_MerchantURL” del formulario de entrada al TPV Virtual. Este campo es el que actualmente se está utilizando para la notificación http.

El servicio SOAP que tienen que publicar los comercios debe tener las siguientes características:

- a. El servicio deberá llamarse “InotificacionSIS” y ofrecer un método llamado “procesaNotificacionSIS”. Este método estará definido con un parámetro de entrada tipo cadena XML y otro parámetro de salida del mismo tipo. Para más información, se adjunta un fichero WSDL a partir del cual se puede construir el esqueleto del servidor y que servirá para definir los tipos de datos que se intercambiarán entre cliente y servidor, de cara a facilitar la comunicación.

- b. El formato de los mensajes que se intercambiarán en este servicio deberán ajustarse a la siguiente DTD:

– Mensaje de notificación enviado desde el SIS con los datos de la operación correspondiente:

```
<ELEMENT Message (Request, Signature)>
<ELEMENT Request (Fecha, Hora, Ds_SecurePayment,
Ds_Amount, Ds_Currency, Ds_Order, Ds_MerchantCode,
Ds_Terminal, Ds_Response, Ds_MerchantData?, Ds_
TransactionType, Ds_ConsumerLanguage, Ds_ErrorCode?,
Ds_CardCountry?, Ds_AuthorisationCode?)>
<!ATTLIST Request Ds_Version CDATA #REQUIRED>
<ELEMENT Fecha (#PCDATA)>
<ELEMENT Hora (#PCDATA)>
<ELEMENT Ds_SecurePayment (#PCDATA)>
<ELEMENT Ds_Amount (#PCDATA)>
<ELEMENT Ds_Currency (#PCDATA)>
<ELEMENT Ds_Order (#PCDATA)>
<ELEMENT Ds_MerchantCode (#PCDATA)>
<ELEMENT Ds_Terminal (#PCDATA)>
<ELEMENT Ds_Response (#PCDATA)>
<ELEMENT Ds_MerchantData (#PCDATA)>
<ELEMENT Ds_TransactionType (#PCDATA)>
<ELEMENT Ds_ConsumerLanguage (#PCDATA)>
<ELEMENT Ds_ErrorCode (#PCDATA)>
<ELEMENT Ds_CardCountry (#PCDATA)>
<ELEMENT Ds_AuthorisationCode (#PCDATA)>
<ELEMENT Signature (#PCDATA)>
```

Para generar el valor del campo “Signature” en el mensaje de notificación del comercio aplicaremos un SHA-1 a la cadena resultante de concatenar el mensaje <Request ...>...</Request> con la clave del comercio.

Ejemplo:

El siguiente mensaje:

```
<Message>
<Request Ds_Version="0.0">
  <Fecha>01/04/2003</Fecha>
  <Hora>16:57</Hora>
  <Ds_SecurePayment>1</Ds_SecurePayment>
  <Ds_Amount>345</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>
  <Ds_Order>165446</Ds_Order>
  <Ds_MerchantCode>999008881</Ds_MerchantCode>
  <Ds_Terminal>001</Ds_Terminal>

  <Ds_Card_Country>724</Ds_Card_Country>
  <Ds_Response>0000</Ds_Response>
  <Ds_MerchantData>Alfombrilla para raton</Ds_
MerchantData>
  <Ds_TransactionType>1</Ds_TransactionType>
  <Ds_ConsumerLanguage>1</Ds_ConsumerLanguage>
</Request>
</Message>
```

La firma se calculará así (siendo la clave secreta qwertyasdf0123456789):

firma = SHA-1 (

```
<Request
Ds_Version="0.0"><Fecha>01/04/2003</Fecha><Hora>16:57</
Hora><Ds_SecurePayment>1</Ds_SecurePayment><Ds_
Amount>345</Ds_Amount><Ds_Currency>978</Ds_
Currency><Ds_Order>165446</Ds_Order><Ds_MerchantCo-
de>999008881</Ds_MerchantCode><Ds_Terminal>001</
Ds_Terminal><Ds_Card_Country>724</Ds_Card_Country><Ds_
Response>0000</Ds_Response><Ds_MerchantData>Alfombrilla
para raton</Ds_MerchantData><Ds_TransactionType>1</Ds_
TransactionType><Ds_ConsumerLanguage>1</Ds_ConsumerLang-
uage></Request>qwertyasdf0123456789
)
Resultado = c0026a953d4b4d52c360751bdd8476de311d36e
```

– Mensaje de respuesta del comercio a la notificación:

```
<ELEMENT Message (Response, Signature)>
<ELEMENT Response (Ds_Response_Merchant)>
<!ATTLIST Response Ds_Version CDATA #REQUIRED>
<ELEMENT Ds_Response_Merchant (#PCDATA)>
<ELEMENT Signature (#PCDATA)>
```

Los posibles valores que podrá tomar la etiqueta “Ds_Response_Merchant” serán:

- » OK, cuando la notificación se ha recibido correctamente.
- » KO, cuando se ha producido algún error.

Para generar el valor del campo “Signature” en el mensaje de respuesta del comercio aplicaremos un SHA-1 a la cadena resultante de concatenar el mensaje <Response>...</Response> (es importante hacerlo tal y como se recibe desde el TPV Virtual) con la clave del comercio.

Ejemplos de mensajes intercambiados en una notificación con sincronización SOAP:

– Mensaje de notificación enviado desde el TPV Virtual:

```
<Message>
<Request Ds_Version="0.0">
<Fecha>01/04/2003</Fecha>
<Hora>16:57</Hora>
<Ds_SecurePayment>1</Ds_SecurePayment>
<Ds_Amount>345</Ds_Amount>
<Ds_Currency>978</Ds_Currency>
<Ds_Order>165446</Ds_Order>
<Ds_MerchantCode>999008881</Ds_MerchantCode>
<Ds_Terminal>001</Ds_Terminal>
```

```
<Ds_Card_Country>724</Ds_Card_Country>
<Ds_Response>0000</Ds_Response>
<Ds_MerchantData>Alfombrilla para raton</Ds_
MerchantData>
<Ds_TransactionType>1</Ds_TransactionType>
<Ds_ConsumerLanguage>1</Ds_ConsumerLanguage>
</Request>
<Signature>efc52623500b6174af3216190373ba35360
e99d5</Signature>
</Message>
```

– Mensaje de respuesta desde el comercio al SIS:

```
<Message>
<Response Ds_Version="0.0">
<Ds_Response_Merchant>OK</Ds_Response_Merchant>
</Response>
<Signature>adb300af20b477f6438a3f9fb671b3d9afe
cb444</Signature>
</Message>
```

WSDL para el servicio InotificacionSIS

Los comercios que deseen desarrollar un servicio SOAP deben ajustarse a esta WSDL. A partir de ella, mediante herramientas de generación automática de código, se puede desarrollar el esqueleto del servidor SOAP de forma cómoda y rápida.

La WSDL que debe cumplir el servicio SOAP desarrollado por el cliente es la siguiente:

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions name="InotificacionSIS"
targetNamespace="https://sis.redsys.es/sis/
InotificacionSIS.wsdl" xmlns:xs="http://www.w3.org/2001/
XMLSchema
xmlns:tns="https://sis.REDSYS.es/sis/InotificacionSIS.
wsdl" xmlns:soapenc="http://schemas.xmlsoap.org/
soap/encoding/" xmlns:soap="http://schemas.xmlsoap.
org/wsdl/soap/
xmlns="http://schemas.xmlsoap.org/wsdl/">
<message name="procesaNotificacionSISRequest">
<part name="XML" type="xs:string"/>
</message>
<message name="procesaNotificacionSISResponse">
<part name="return" type="xs:string"/>
</message>
<portType name="InotificacionSISPortType">
<operation name="procesaNotificacionSIS">
<input message="tns:procesaNotificacionSISRequest"/>
<output message="tns:procesaNotificacionSISResp
onse"/>
</operation>
</portType>
<binding name="InotificacionSISBinding" type="tns:Inotif
icacionSISPortType">
<soap:binding style="rpc" transport="http://schemas.
xmlsoap.org/soap/http"/>
<operation name="procesaNotificacionSIS">
<soap:operation
```

```
soapAction="urn:InotificacionSIS#procesaNotifica
cionSIS" style="rpc"/>
<input>
<soap:body use="encoded"
encodingStyle="http://schemas.xmlsoap.org/soap/
encoding/
namespace="InotificacionSIS"/>
</input>
<output>
<soap:body use="encoded"
encodingStyle="http://schemas.xmlsoap.org/soap/
encoding/
namespace="InotificacionSIS"/>
</output>
</operation>
</binding>
<service name="InotificacionSISService">
<port name="InotificacionSIS" binding="tns:Inotif
icacionSISBinding">
<soap:address
location="http://localhost/WebServiceSIS/InotificacionSIS.
asmx"/>
</port>
</service>
</definitions>
```

7.8 Pago de suscripciones y pagos exprés

Con el objeto de incrementar el ratio de conversión y facilitar en la medida de lo posible el proceso de compra, el TPV Virtual de Banco Sabadell incorpora una funcionalidad innovadora que permite realizar pagos exprés y pago de suscripciones a través de un identificador equivalente al número de tarjeta.

Esta modalidad permite gestionar con mayor facilidad las compras de los clientes habituales, porque no necesitarán introducir los datos de su tarjeta en cada proceso de compra. El comprador sólo tiene que informar los datos de la tarjeta en la primera compra y en ese momento el comercio recibirá, junto con la respuesta de pago, un identificador para usar en las compras posteriores. Además, se le informará de la caducidad de la tarjeta y opcionalmente del número de la tarjeta, debidamente enmascarado, es decir, con unos determinados dígitos sustituidos por asteriscos.

Los datos de las tarjetas se almacenan en los servidores de Banco Sabadell y por lo

tanto el comercio evitará tener que cumplir los requerimientos de seguridad PCI-DSS. (Ver capítulo 11.)

• Operativa para el primer pago:

El comercio solicita un pago al TPV Virtual. Junto con los datos necesarios para el pago, se envía un nuevo parámetro para solicitar la generación de un identificador asociado a los datos de la tarjeta. Esta petición se puede realizar por cualquiera de las entradas al TPV Virtual ('realizarPago', 'entradaXMLentidad', 'operaciones' o 'WebService').

Si el comercio no ha enviado la tarjeta, el TPV Virtual se encargará de solicitarla al titular junto con la fecha de caducidad y el CVV2.

El TPV Virtual procesa la solicitud de pago y almacena los datos de tarjeta asociados a una referencia generada internamente. Sólo se generará la referencia si el pago es autorizado.

El TPV Virtual devuelve el identificador y la fecha de caducidad junto con la respuesta del pago, para que el comercio pueda utilizarla con posterioridad. Opcionalmente también se puede configurar el comercio para que en el mensaje de respuesta se incluya el número de tarjeta debidamente enmascarado.

Dependiendo del tipo de conexión utilizado por el comercio, la referencia se devolverá por los siguientes medios:

i. **Para la entradas 'realizarPago' y 'entradaXMLentidad':** se devolverá la referencia y la fecha de caducidad en la notificación On-Line y en la URL OK.

ii. **Para la entradas 'operaciones' y 'WebService':** se devolverá la referencia y la fecha de caducidad en la respuesta de las operaciones autorizadas.

• Operativa para los pagos posteriores:

Una vez que el comercio ya dispone de una referencia, podrá utilizarla en los pagos posteriores en lugar de enviar la tarjeta y la caducidad. El esquema de funcionamiento sería el siguiente:

- Nuevo pago: el comercio solicita un pago al TPV Virtual y para ello envía el identificador que Banco Sabadell ha facilitado en el primer pago.
- La operativa de pagos exprés /pago de suscripciones, es válida para cualquier tipo de transacción (Ds_Merchant_TransactionType).
- Opcionalmente el comercio también podrá indicar si quiere mostrar o no pantallas adicionales (DCC, Fraccionamiento y Autenticación).
- El comercio puede utilizar cualquier entrada de las actuales al TPV Virtual ('realizarPago', 'entradaXMLentidad', 'operaciones' o 'WebService').
- El TPV Virtual valida el identificador asociado al comercio y recupera los datos de la tarjeta.
- Una vez que ha localizado los datos de la tarjeta, el TPV Virtual procede a realizar el pago. En caso de que se haya indicado que no se muestren pantallas, el pago se realizará sin mostrar las pantallas de DCC ni de fraccionamiento y sin usar ningún método de pago seguro. La fecha de caducidad sólo se incluye en la respuesta si el comercio está configurado para ello.

Para aquellos casos en los que el comercio, al solicitar un pago al TPV Virtual, no haya solicitado la creación de un identificador, o estuviera utilizando la anterior modalidad de Banco Sabadell, denominada 'Tarjeta en Archivo', será posible la opción de crear un identificador a posteriori. Para ello Banco Sabadell dispone de un proceso batch llamado

GenerarReferencias, a través del cual podrá filtrar las operaciones para las cuales quiere crear los identificadores.

El Anexo VI del presente manual recoge los ejemplos específicos de utilización de la funcionalidad Pago de suscripciones y pagos Exprés, para cada una de modalidades de procesamiento de operaciones en el TPV Virtual de Banco Sabadell.

Restricciones

Para que un comercio utilice esta operativa debe tener en cuenta las siguientes restricciones:

- i. El número de identificador se asociará también al número de comercio que ha realizado la solicitud. Si el comercio desea que este identificador pueda ser usada por otros comercios, estos deberán estar configurados previamente formando un grupo. Para la creación de grupos, es necesario solicitarlo a su gestor habitual en Banco Sabadell.
- ii. Los datos de la tarjeta se mantendrán hasta la fecha de validez de su caducidad.
- iii. La validez del identificador estará limitada a la fecha de caducidad de la tarjeta y será devuelta siempre en la respuesta cuando se pida un nuevo identificador. En el resto de casos sólo se devolverá en la respuesta para los comercios que estén configurados para ello.
- iv. Sólo se podrán indicar que no se muestren pantallas en el caso de que se use una referencia válida. Cuando se pide generar un nuevo identificador y en cualquier otro caso, no se puede indicar que no se muestren pantallas.

El resto de parámetros necesarios para un pago bajo esta modalidad, no varía con respecto a un pago normal.

• Ds_Merchant_Identifier

Este parámetro se utilizará para manejar la referencia asociada a los datos de tarjeta. Es un campo alfanumérico de un máximo de 40 posiciones cuyo valor es generado por el TPV Virtual.

1ª Petición: en la primera petición para que el comercio solicite la generación de una nueva referencia debe enviar el valor "REQUIRED". El TPV Virtual devolverá el identificador generado asociado a la tarjeta en un parámetro con este mismo nombre. Además el TPV Virtual devolverá siempre la fecha de caducidad, que irá en el parámetro **Ds_ExpiryDate**. Como ya hemos indicado anteriormente ambos parámetros se devolverán en la Notificación on-line, URL OK o respuesta a WebService dependiendo de la conexión utilizada por el comercio.

El parámetro Ds_Merchant_Identifier **se debe incluir en la cadena de cálculo de la firma Hash** (ver apartado 7.6.4 del presente manual). Se debe concatenar al final de la cadena de datos y antes del valor de la clave o del parámetro Ds_Merchant_Group si este existe.

2ª Petición y sucesivas: el comercio deberá enviar la referencia en el parámetro Ds_Merchant_Identifier y no facilitar datos de tarjeta. La fecha de caducidad sólo se incluirá en la respuesta si el comercio está configurado para ello.

El parámetro Ds_Merchant_Identifier **se debe incluir en la cadena de cálculo de la firma Hash** (ver apartado 7.6.4 del presente manual). Se debe concatenar al final de la cadena de datos y antes del valor de la clave o del parámetro Ds_Merchant_Group si este existe o del parámetro Ds_Merchant_DirectPayment si este existe y el parámetro Ds_MerchantGroup no existe.

- **Ds_Merchant_Group**

Este parámetro permite asociar una referencia a un conjunto de comercios. Es un parámetro opcional numérico de un máximo de 9 posiciones. Si se utiliza este parámetro, la referencia estará asociada al código de grupo en lugar de al código de comercio.

El grupo de comercios debe estar previamente definido en el TPV Virtual. Para la creación de grupos, es necesario solicitarlo a su gestor habitual en Banco Sabadell.

Si una referencia se asocia a un grupo de comercios, posteriormente la podrán utilizar cada uno de los comercios de forma individual.

Este parámetro **se debe incluir en la cadena de cálculo de la firma Hash** (ver apartado 7.6.4 del presente manual). Se debe concatenar justo detrás del parámetro Ds_Merchant_Identifier y antes del valor de la clave o del parámetro Ds_Merchant_DirectPayment si este existe.

- **Ds_Merchant_DirectPayment**

Este parámetro funciona como un flag que indica si hay que mostrar pantallas adicionales (DCC, Fraccionamiento y Autenticación). Es un parámetro opcional que tan sólo puede tomar los valores “true” o “false”. Si se utiliza con el valor “true”, no se mostrarán pantallas adicionales (DCC, Fraccionamiento y Autenticación) durante el pago y se debe utilizar conjuntamente con el parámetro Ds_Merchant_Identifier conteniendo una referencia válida. Si no se utiliza o se utiliza con el valor de “false”, el pago se hará de manera normal y se mostrarán todas las pantallas adicionales (DCC, Fraccionamiento y Autenticación) que se requieran dependiendo de la configuración del comercio.

Este parámetro **se debe incluir en la cadena de cálculo de la firma Hash** (ver apartado 7.6.4 del presente manual). Se debe concatenar justo detrás del parámetro Ds_Merchant_Group (si este existe) y antes del valor de la clave.

Migración de identificadores

(Exclusivo para comercios que anteriormente utilizaban la modalidad de pago 'Tarjeta en Archivo')

Un comercio puede continuar utilizando la operativa de Tarjeta En Archivo existente hasta este momento o comenzar a utilizar la modalidad de pagos por referencia.

En algunos casos, el comercio deseará utilizar la nueva operativa para operaciones anteriores. Para ello se ha desarrollado un proceso de migración de identificadores desde la operativa de Tarjeta en Archivo a la nueva operativa de pagos exprés / pago de suscripciones.

La migración de las referencias se realizará mediante una solicitud expresa a su gestor habitual en Banco Sabadell. Una vez procesada la solicitud, el comercio dispondrá de un fichero con los siguientes datos por operación:

- Código de comercio
- N° de terminal
- Fecha de operación
- Código de pedido operación original
- Referencia generada y registrada para la tarjeta de la operación original

Con este fichero el comercio podrá actualizar sus sistemas de cara a utilizar las referencias.

Ejemplo de fichero con identificadores

Comercio;Terminal;Pedido;Fecha;Identificador
999008881;1;130211123726;2013-02-11-12.37.27.381; 7490da446dee0a...25b6bd52e086c3181

999008881;1;130211123739;2013-02-11
12.37.40.429;d5ac083cb97d183...548f16
8c32c7bb5ab7d

7.9. Configuración operativa DCC

El TPV Virtual de Banco Sabadell permite a los titulares de tarjetas Visa o MasterCard emitidas en una divisa diferente del euro, poder pagar sus compras en la misma moneda de la tarjeta. Ver detalles en el apartado 5.4 del presente manual.

A continuación se detallarán las características adicionales de carácter técnico que se requieren para la configuración de la operativa DCC en el TPV Virtual del comercio. Hay que destacar, no obstante, que únicamente se requiere configurar el TPV Virtual, en caso que el comercio utilice la entrada 'WebService' descrita el apartado 7.4 del presente manual.

En el caso de utilizar la entrada 'Operaciones', no es posible configurar la operativa DCC dado que el comercio en ningún momento cede al Banco la sesión del navegador y por tanto no podemos mostrar las pantallas de selección de moneda de DCC ni el recibo de compra de DCC.

Para las entradas 'RealizarPago' y 'EntradaXMLEntidad', no es necesario realizar ninguna configuración. Las pantallas de selección de moneda de DCC y el recibo de compra de DCC, aparecerán de forma automática si el TPV Virtual detecta que se está realizando una transacción con tarjetas Visa o MasterCard emitidas en una divisa diferente del euro.

7.9.1 Configuración operativa DCC para entrada 'webservice'

1. Mensaje de petición inicial de pago

Las características del mensaje de petición inicial de pago (1. Petición de Pago) son las

mismas que se recogen en el apartado 7.4.1 del presente manual. En este tipo de mensaje no se requiere ninguna codificación especial para activar la operativa DCC.

2. Mensaje de respuesta DCC

A continuación se describen los datos específicos necesarios que se recibirán en los mensajes de respuesta DCC del TPV Virtual (2. Respuesta monedas DCC):

DATO	LONGITUD/TIPO	DESCRIPCIÓN
Moneda	3 / N	Obligatorio. Valor del identificador de la moneda
litMoneda	- / A	Obligatorio. Literal asociado a la moneda.
litMonedaR	3 / R	Obligatorio. Literal reducida asociado a la moneda.
cambio	- / N	Obligatorio. Valor del cambio de la moneda.
importe	- / N	Obligatorio. Importe en la moneda.
checked	true / false	Obligatorio. Indica divisa comprobada.
margenDCC	- / N	Obligatorio. Margen DCC aplicado por la entidad al importe.
nombreEntidad	- / A	Obligatorio. Nombre de la entidad bancaria que aplica el DCC.
DS_MERCHANT_SESION	- / AN	Obligatorio. Identificador de la sesión para continuar la operación en operativas DCC.

Tipo A: caracteres ASCII del 65 = A al 90 = Z y del 97 = a al 122 = z.

Tipo N: caracteres ASCII del 30 = 0 al 39 = 9.

Ejemplo de respuesta DCC

```
<RETORNOXML>
<CODIGO>0</CODIGO>
<DCC>
<moneda>826</moneda>
<litMoneda>POUND STERLING</litMoneda>
<litMonedaR>GBP</litMonedaR>
<cambio>1.413788</cambio>
<importe>1.03</importe>
<checked>true</checked>
</DCC>
<DCC>
<moneda>978</moneda>
<litMoneda>Euros</litMoneda>
<importe>1.45</importe>
</DCC>
```

```
<margenDCC>2.5</margenDCC>
<nombreEntidad>SIN CAPTURA</nombreEntidad>
<DS_MERCHANT_SESION>vXYIxTsfkVJ6ZL82vJ48Lvm</
DS_MERCHANT_SESION>
</RETORNOXML>
```

3. Mensaje de confirmación DCC

A continuación se describen los datos específicos necesarios para enviar una petición de confirmación DCC (3. Confirmación moneda DCC):

DATO	LONGITUD/TIPO	DESCRIPCIÓN
Sis_Divisa	16/A-N	Obligatorio. Dos valores separados por #. El primero es el identificador de la moneda, el segundo el importe en dicha moneda.
DS_MERCHANT_SESION		Obligatorio. Identificador de la sesión para continuar la operación en operativas DCC.

Tipo A: caracteres ASCII del 65 = A al 90 = Z y del 97 = a al 122 = z.

Tipo N: caracteres ASCII del 30 = 0 al 39 = 9.

Ejemplo de mensaje de confirmación de moneda DCC

```
< DATOSENTRADA >
<DS_MERCHANT_ORDER>050911523002</DS_MERCHANT_ORDER>
<DS_MERCHANT_MERCHANTCODE>999008881</DS_MERCHANT_MERCHANTCODE>
<Sis_Divisa>826#1.03</Sis_Divisa>
<DS_MERCHANT_SESION>vXYIxtsfkVJ6ZL82vJ48Lvm</DS_MERCHANT_SESION>
<DS_MERCHANT_TERMINAL>999</DS_MERCHANT_TERMINAL>
<DS_MERCHANT_MERCHANTSIGNATURE>b7a9dcc79fd1146f315ad3461a5a2009850cc375</DS_MERCHANT_MERCHANTSIGNATURE>
</ DATOSENTRADA >
```

```
<moneda>826</moneda>
<litMoneda>POUND STERLING</litMoneda>
<litMonedaR>GBP</litMonedaR>
<cambio>1.413788</cambio>
<importe>1.03</importe>
<checked>true</checked>
</DCC>
<DCC>
<moneda>978</moneda>
<litMoneda>Euros</litMoneda>
<importe>1.45</importe>
</DCC>
<margenDCC>2.5</margenDCC>
<nombreEntidad>SIN CAPTURA</nombreEntidad>
<DS_MERCHANT_SESION>vXYIxtsfkVJ6ZL82vJ48Lvm</DS_MERCHANT_SESION>
</RETORNOXML>
```

4. Mensaje de respuesta

Las características del mensaje de respuesta (4. Respuesta de pago) son las que están definidas en el apartado 7.4.2 del presente manual. En este tipo de mensaje no se requiere ninguna codificación especial para activar la operativa DCC.

5. Mensaje de consulta DCC

El mensaje de consulta DCC se generará con los datos anteriormente descritos en un XML que se mandará al método consultaDCC. Esta consulta es solamente informativa.

Ejemplo de mensaje de consulta DCC

```
<RETORNOXML>
<CODIGO>0</CODIGO>
<DCC>
```

6. Mensaje de respuesta de consulta DCC

El mensaje de consulta DCC se generará con los datos anteriormente descritos en un XML que se mandará al método consultaDCC.

Ejemplo de mensaje de respuesta consulta DCC

```
<RETORNOXML>
<CODIGO>0</CODIGO>
<DCC>
<moneda>826</moneda>
<litMoneda>POUND STERLING</litMoneda>
<litMonedaR>GBP</litMonedaR>
<cambio>1.413788</cambio>
<importe>1.03</importe>
<checked>true</checked>
</DCC>
<DCC><moneda>978</moneda>
<importe>1.45</importe>
</DCC>
<margenDCC>2.5</margenDCC>
<nombreEntidad>LA CAIXA </nombreEntidad>
</RETORNOXML>
```

7.9.2 Firma del comercio

Peticiones de confirmación DCC

En el caso de que se requiera realizar una segunda petición al TPV Virtual WebService, debido a que se admita DCC en la operativa, la firma se calculará de la siguiente manera:

```
DS_MERCHANT_ORDER + DS_MERCHANT_MERCHANTCODE +  
Sis_Divisa + DS_MERCHANT_SESION + SECRET KEY  
Order = 050911523002  
Merchant = 999008881  
Currency and Amount = 826#1.03  
Session Id. = vXYIxTsfkVJ6ZL82vJ48LvM  
SECRET KEY=qwertyasdf0123456789
```

```
Chain Result:  
050911523002999008881826#1.03vXYIxTsfkVJ6ZL82vJ48L  
vmqwertyasdf0123456789  
SHA-1 Result:  
b7a9dcc79fd1146f315ad3461a5a2009850cc375
```

Peticiones de consulta de DCC

La firma electrónica del comercio se deberá calcular concatenando el valor de los siguientes campos (salvo que sea alguno de valor nulo en cuyo caso no se considerará en la firma) incluyendo al final la clave secreta de encriptación:

```
DS_MERCHANT_AMOUNT + DS_MERCHANT_ORDER + DS_MER-  
CHANT_MERCHANTCODE + DS_MERCHANT_CURRENCY + SE-  
CRET KEY  
Amount = 145 (it is multiplied by 100)  
Order = 050911523002  
Merchant = 999008881  
Currency = 978  
SECRET KEY = qwertyasdf0123456789
```

```
Chain result:  
145050911523002999008881978qwertyasdf0123456789  
SHA-1 result:  
32e9820a3b3b19e5b51b0847e13defa47d5443a
```

7.10 Entorno de pruebas

El entorno de pruebas permite realizar las pruebas necesarias para verificar el correcto funcionamiento del sistema antes de la utilización en real del TPV Virtual del comercio. Dicho entorno es idéntico al real, pero sin que los pagos realizados tengan una validez contable.

Las claves del entorno de pruebas que le facilitamos a continuación son comunes para otros clientes de Banco Sabadell. Si desea disponer de unas claves de pruebas exclusivas para su comercio, rogamos lo solicite al Servicio Técnico de Soporte a la Instalación del TPV Virtual de Banco Sabadell.

Los parámetros del entorno de prueba son los que se describen a continuación.

1. URL para el envío de las órdenes de pago:

Entrada “realizarpago (HTML)”:

<https://sis-t.redsys.es:25443/sis/realizarPago>

Entrada “operaciones (XML)”:

<https://sis-t.redsys.es:25443/sis/operaciones>

Entrada “XMLentidad (XML)”:

<https://sis-t.redsys.es:25443/sis/entradaXMLentidad>

Entrada “WebService (XML)”:

<https://sis-t.redsys.es:25443/sis/services/SerCIsWSEntrada>

2. Número de comercio
(Ds_Merchant_MerchantCode):
327234688
3. Clave secreta
(Ds_Merchant_MerchantSignature):
qwertyasdf0123456789
4. Terminales (Ds_Merchant_Terminal):
 - 001 - Para pagos en EUROS (Ds_MerchantCurrency = 978) de comercios bajo protocolo CES (Comercio Electrónico Seguro –VERIFIED BY Visa y MasterCard SecureCode–)
 - 002 - Para pagos en EUROS (Ds_MerchantCurrency = 978) de comercios bajo protocolo No-CES (pagos considerados NO seguros)

5. Tarjeta aceptada:

- 4548 8120 4940 0004, caducidad 12/17, código CVV2: 123
- En modo de compra segura (CES), en la que se requiera autenticación del comprador, el código de identificación personal (CIP) es: 123456

Para pagos CES en los que se requiera autenticación del comprador, el código de identificación personal (CIP) es 123.

6. URL módulo de administración:

<https://sis-t.redsys.es:25443/canales/>

7. Acceso al módulo de administración:

» Para terminal 001 (CES):

Usuario: 327234688-001
Contraseña: 123456a

» Para terminal 002 (NO CES):

Usuario: 327234688-002
Contraseña: 123456a

7.11 Servicio técnico de soporte a la instalación

Para ofrecer todo el soporte necesario durante el proceso de alta e instalación del TPV Virtual de Banco Sabadell, ponemos a su disposición un servicio de soporte especializado:

Horario del servicio:

De lunes a domingo de 8 h a 22 h

Teléfono: 902 365 650 (opc. 2)

Correo electrónico:

tpvvirtual@bancsabadell.com

Soporte técnico VIP

Adicionalmente, y para aquellos clientes que, bien por características técnicas o comerciales, requieran atención técnica urgente y/o de carácter preferencial, ponemos a su disposición un servicio VIP de soporte técnico.

Consulte a su gestor *e-commerce*, las condiciones para acceder a este servicio.

Correo electrónico:

ServicioTPVirtualPlus@bancsabadell.com

Asimismo, solo en los casos de **incidencias sobre comunicaciones, inestabilidad del sistema y similares, rogamos contacte al teléfono 902 198 747, en activo las 24 horas del día**, todos los días del año (servicio de soporte prestado por la empresa RedSys).

8. Consulta SOAP-XML de transacciones de TPV virtual

SOAP es un estándar de protocolo basado en XML que permite la comunicación con los servicios web. SOAP proporciona un mecanismo sencillo y uniforme para el envío de mensajes XML a otra aplicación.

A continuación se describen los pasos a seguir para utilizar el servicio web de consultas SOAP de transacciones de cara a realizar consultas de las operaciones realizadas por un comercio, independientemente de que estas hayan sido respondidas al mismo. Por tanto, el servicio de consultas online ofrece la posibilidad de obtener información de todas las operaciones que se han iniciado.

Existen varios tipos de **consultas: por transacción y por monitor**, masivas o no.

La consulta por transacción permite obtener información de un determinado tipo de operaciones (p. ej., autorización) correspondiente a un pedido.

La consulta por monitor permite obtener información de todos los tipos de operaciones (p. ej., autorización y devolución) asociados a un número de pedido.

Estas operaciones pueden hacerse **simples** (para una sola fecha) o **masivas** (entre un rango de fechas).

Los posibles valores de una consulta por transacción son:

```
<Ds_TransactionType> = 0 (Operación de pago normal)
<Ds_TransactionType> = 1 (Preautorización sin confirmar)
<Ds_TransactionType> = 4 (Pago por referencia)
<Ds_TransactionType> = 7 (Preautenticación)
<Ds_TransactionType> = A (Pago no seguro sin autenticación)
```

La especificación de los mensajes de entrada y de salida del servicio se describe en el apartado 8.2 del presente manual.

El servicio de acceso a la gestión de tarjetas está implementado con la tecnología SOAP-XML, Simple Object Access Protocol (SOAP). SOAP es un protocolo estándar, basado en XML, que permite la comunicación de los

servicios web. SOAP facilita un mecanismo simple y consistente para que una aplicación pueda enviar mensajes XML a otra aplicación. Para la utilización de dicho servicio será necesario usar esta tecnología.

Este servicio permite que de manera simple y fiable el terminal pueda realizar una petición de operación con las tarjetas.

El solicitante del servicio hará una petición al proveedor del servicio que devolverá el resultado de la misma.

Es necesario implementar un cliente SOAP que hará la llamada al método encargado de iniciar la transacción (ver ejemplo en el apartado 8.4 del presente manual).

El cliente SOAP tiene que enviar un XML al Servicio de Acceso al Servicio Web que contendrá los datos de la operación a realizar. Éste retornará otro XML de respuesta. Estos XML deben cumplir el XML-SCHEMA en los términos que se describen en el presente manual.

8.1 Cálculo de la firma

Debido al carácter confidencial de los datos enviados en los mensajes, se hace necesario proteger dichos datos de manera que ninguna persona externa pueda modificar los mismos y confundir a alguna de las dos partes implicadas en el sistema.

A parte de la seguridad inherente que proporciona SOAP en el envío de los mensajes, es necesario añadir una firma a los mensajes que identifique a las dos partes en la transacción. Para calcular la firma, se utiliza una clave secreta compartida entre el comercio y Banco Sabadell.

Los datos que se incluyen en la firma son una cadena con el mensaje enviado (los datos que hay entre las etiquetas <version...> </version>) y la clave secreta compartida entre

Banco Sabadell y el comercio.

Así, para el cálculo de la firma de envío se utilizarán los siguientes datos:

Datos del XML de envío + clave del comercio.

Digest=SHA-1(“<version...</version>” + clave del comercio).

Dado el mensaje siguiente:

```
<Version Ds_Version="0.0">
  <Message>
    <Monitor>
      <Ds_MerchantCode>999008881</Ds_
        MerchantCode><Ds_Terminal>1</Ds_Terminal>
      <Ds_Order>113847</Ds_Order>
      <Ds_Merchant_Data>datos</Ds_Merchant_Data>
    </Monitor>
  </Message>
</Version>
```

y siendo la clave del comercio la cadena “qwertyasdf0123456789”, la firma es la resultante de realizar el siguiente cálculo:

```
Digest=SHA-1(<Version Ds_Version="0.0"><Message><Monitor><
Ds_MerchantCode>999008881</Ds_MerchantCode><Ds_Terminal>1</Ds_Terminal>
<Ds_Order>113847</Ds_Order><Ds_Merchant_Data>datos</Ds_Merchant_Data></Monitor></Message></
Version>qwertyasdf0123456789)
```

Obteniéndose el valor

571b2d002c878ddb241fc542c7b-
6d46262bbb7cb.

Para el cálculo de la firma de respuesta se utilizarán los siguientes datos, al igual que en la firma de entrada:

Datos del XML de respuesta + clave del comercio.

Digest=SHA-1(“<version...</version>” + clave del comercio).

8.2 Consultas SOAP - Especificación de los mensajes de entrada y de salida

En este apartado se describe mediante un XML-SCHEMA el detalle de los mensajes de entrada y salida del servicio web de consultas de transacciones.

Hay varios tipos de mensajes de envío:

1. Mensaje de tipo **Transaction (simple)**: permite obtener información de un determinado tipo de operaciones (p. ej., autorización) correspondiente a un pedido.
2. Mensaje de tipo **Monitor (simple)**: permite obtener información de todos los tipos de operaciones (p. ej., autorización y devolución) asociados a un mismo número de pedido.
3. Mensaje de tipo **Transaction (masivo)**: permite obtener un listado de un determinado tipo de operaciones que se han generado sobre el comercio, en un rango de tiempo determinado.
4. Mensaje de tipo **Monitor (masivo)**: permite obtener un listado de todas las operaciones en el comercio y terminal indicados en un rango de tiempo.
5. Mensaje de tipo **Detail**: permite tener información del detalle de una operación determinada.

Este es el XML-SCHEMA que deben cumplir los mensajes enviados al servicio de consulta de transacciones:

```
<schema targetNamespace="http://www.w3.org/namespaces/"
xmlns:t="http://www.w3.org/namespaces/"
xmlns="http://www.w3.org/2001/XMLSchema" elementFormD
efault="unqualified"
attributeFormDefault="unqualified">
  <element name="Messages">
    <complexType>
      <sequence>
        <element ref="t:Version"/>
        <element ref="t:Signature"/>
      </sequence>
    </complexType>
  </element>
  <element name="Version">
    <complexType>
      <sequence maxOccurs="unbounded">
        <element ref="t:Message"/>
      </sequence>
      <attribute name="Ds_Version" type="string"
        use="required"/>
    </complexType>
  </element>
  <element name="Message">
    <complexType>
      <choice>
```

```

        <element ref="t:Transaction"/>
        <element ref="t:Monitor"/>
        <element ref="t:Detail"/>
        <element ref="t:TransactionMasiva"/>
        <element ref="t:MonitorMasiva"/>
        <sequence minOccurs="0"
            maxOccurs="unbounded">
            <element ref="t:Response"/>
        </sequence>
        <element ref="t:ErrorMsg"/>
    </choice>
</complexType>
</element>
<element name="Transaction">
    <complexType>
        <sequence>
            <element ref="t:Ds_MerchantCode"/>
            <element ref="t:Ds_Terminal"/>
            <element ref="t:Ds_Order"/>
            <element ref="t:Ds_TransactionType"/>
            <element ref="t:Ds_Merchant_Data"
                minOccurs="0"/>
        </sequence>
    </complexType>
</element>
<element name="TransactionMasiva">
    <complexType>
        <sequence>
            <element ref="t:Ds_MerchantCode"/>
            <element ref="t:Ds_Terminal"/>
            <element ref="t:Ds_TransactionType"/>
            <element ref="t:Ds_Fecha_inicio"/>
            <element ref="t:Ds_Fecha_fin"/>
        </sequence>
    </complexType>
</element>
<element name="Monitor">
    <complexType>
        <sequence>
            <element ref="t:Ds_MerchantCode"/>
            <element ref="t:Ds_Terminal"/>
            <element ref="t:Ds_Order"/>
            <element ref="t:Ds_Merchant_Data"
                minOccurs="0"/>
        </sequence>
    </complexType>
</element>
<element name="MonitorMasiva">
    <complexType>
        <sequence>
            <element ref="t:Ds_MerchantCode"/>
            <element ref="t:Ds_Terminal"/>
            <element ref="t:Ds_Fecha_inicio"/>
            <element ref="t:Ds_Fecha_fin"/>
        </sequence>
    </complexType>
</element>
<element name="Detail">
    <complexType>
        <sequence>
            <element ref="t:Ds_MerchantCode"/>
            <element ref="t:Ds_Terminal"/>
            <element ref="t:Ds_Order"/>
            <element ref="t:Ds_TransactionType"/>
            <element ref="t:Ds_Merchant_Data"
                minOccurs="0"/>
        </sequence>
    </complexType>

```

```

</element>
<element name="Response">
    <complexType>
        <sequence>
            <element ref="t:Ds_MerchantCode"/>
            <element ref="t:Ds_Terminal"/>
            <element ref="t:Ds_Order"/>
            <element ref="t:Ds_TransactionType"/>
            <element ref="t:Ds_Date"/>
            <element ref="t:Ds_Hour"/>
            <element ref="t:Ds_State"/>
            <element ref="t:Ds_Currency"/>
            <choice minOccurs="0">
                <sequence>
                    <element ref="t:Ds_CardNumber"/>
                    <element ref="t:Ds_ExpiryDate"/>
                </sequence>
                <element ref="t:Ds_TelephoneNumber"/>
            </choice>
            <element ref="t:Ds_SecurePayment"/>
            <element ref="t:Ds_State"/>
            <element ref="t:Ds_Response" minOccurs="0"/>
            <element ref="t:Ds_Merchant_Data"
                minOccurs="0"/>
            <element ref="t:Ds_CardCountry" minOccurs="0"/>
            <element ref="t:Ds_CardType" minOccurs="0"/>
            <element ref="t:Ds_AuthorisationCode"
                minOccurs="0"/>
        </sequence>
    </complexType>
</element>
<element name="Ds_MerchantCode">
    <simpleType>
        <restriction base="int">
            <minInclusive value="1"/>
            <maxInclusive value="999999999"/>
        </restriction>
    </simpleType>
</element>
<element name="Ds_Terminal">
    <simpleType>
        <restriction base="short">
            <minInclusive value="1"/>
            <maxInclusive value="999"/>
        </restriction>
    </simpleType>
</element>
<element name="Ds_Order">
    <simpleType>
        <restriction base="string">
            <minLength value="1"/>
            <maxLength value="12"/>
        </restriction>
    </simpleType>
</element>
<element name="Ds_TransactionType">
    <simpleType>
        <restriction base="string">
            <length value="1"/>
        </restriction>
    </simpleType>
</element>
<element name="Ds_Merchant_Data" type="string"/>
<element name="Ds_Fecha_fin" type="string"/>

```

```

element name="Ds_Fecha_inicio" type="string"/>
<element name="Ds_Date">
  <complexType mixed="true"/>
</element>
<element name="Ds_Hour">
  <complexType mixed="true"/>
</element>
<element name="Ds_Amount" type="long"/>
<element name="Ds_Currency" type="short"/>
<element name="Ds_CardNumber">
  <simpleType>
    <restriction base="string">
      <minLength value="13"/>
      <maxLength value="19"/>
    </restriction>
  </simpleType>
</element>
<element name="Ds_ExpiryDate">
  <simpleType>
    <restriction base="string">
      <length value="4"/>
    </restriction>
  </simpleType>
</element>
<element name="Ds_TelephoneNumber" type="int"/>
<element name="Ds_SecurePayment">
  <simpleType>
    <restriction base="short">
      <minInclusive value="0"/>
      <maxInclusive value="1"/>
    </restriction>
  </simpleType>
</element>
<element name="Ds_State" type="string"/>
<element name="Ds_Response" type="int"/>
<element name="ErrorMsg">
  <complexType>
    <sequence>
      <element ref="t:Ds_ErrorCode"/>
    </sequence>
  </complexType>
</element>
<element name="Ds_ErrorCode">
  <complexType mixed="true"/>
</element>
<element name="Signature" type="string"/>
<element name="Ds_CardCountry">
  <simpleType>
    <restriction base="short">
      <minInclusive value="1"/>
      <maxInclusive value="999"/>
    </restriction>
  </simpleType>
</element>
<element name="Ds_CardType">
  <simpleType>
    <restriction base="string">
      <length value="1"/>
    </restriction>
  </simpleType>
</element>
<element name="Ds_AuthorisationCode">
  <simpleType>
    <restriction base="string">
      <minLength value="0"/>
      <maxLength value="6"/>

```

```

    </restriction>
  </simpleType>
</element>
</schema>

```

Los posibles campos que se envían en el mensaje de petición mantienen el formato que se indica en la creación de cada uno de los mensajes.

DATO	NOMBRE DEL DATO	Long. / Tipo	COMENTARIOS
Identificación de comercio: código FUC	Ds_MerchantCode	9 / N	Obligatorio. Código FUC asignado al comercio.
Número de terminal	Ds_Terminal	3 / N	Obligatorio. Número de terminal que le asignará su banco. 3 se considera su longitud máxima
Número de pedido	Ds_Order	12 / A-N	Obligatorio. Los 4 primeros dígitos deben ser numéricos, para los dígitos restantes solo se deben utilizar los siguientes caracteres ASCII: Del 30 = 0 al 39 = 9 Del 65 = A al 90 = Z Del 97 = a al 122 = z
Tipo de transacción	Ds_TransactionType	1 / A-N	Campo obligatorio para el comercio para indicar qué tipo de transacción es. Los posibles valores son: 0 - Autorización 1 - Preautorización 4 - Pago referencia 7 - Autenticación A - Pago tradicional
Datos del comercio	Ds_Merchant_Data	1024 / A-N	Campo opcional para el comercio para ser incluido en los datos enviados por la respuesta online al comercio si se ha elegido esta opción.
Fecha de inicio	Ds_Fecha_inicio	26 / A-N	La fecha tendrá un formato : aaaa-MM-dd-HH.mm.ss.xxxxxx. Un ejemplo para el 1 de diciembre a las 12:05 AM sería: 2009-12-01-12.05.00.000000.
Fecha de fin	Ds_Fecha_fin	26 / A-N	La fecha tendrá un formato : aaaa-MM-dd-HH.mm.ss.xxxxxx. Un ejemplo para el 1 de diciembre a las 12:05 AM sería: 2009-12-01-12.05.00.000000.

Como salida podemos encontrar en el XML los campos que nos permiten tener la información solicitada en la consulta:

DATO	NOMBRE DEL DATO	Long. / Tipo	COMENTARIOS
Identificación de comercio: código FUC	Ds_MerchantCode	9 / N	Obligatorio. Código FUC asignado al comercio.
Número de terminal	Ds_Terminal	3 / N	Obligatorio. Número de terminal que le asignará su banco. 3 se considera su longitud máxima.
Número de pedido	Ds_Order	12 / A-N	Obligatorio. Los 4 primeros dígitos deben ser numéricos, para los dígitos restantes solo se deben utilizar los siguientes caracteres ASCII: Del 30 = 0 al 39 = 9 Del 65 = A al 90 = Z Del 97 = a al 122 = z
Tipo de transacción	Ds_TransactionType	1 / A-N	Campo obligatorio para el comercio para indicar qué tipo de transacción es. Los posibles valores son: 0 - Autorización 1 - Preautorización 4 - Pago referencia 7 - Autenticación A - Pago tradicional
Datos del comercio	Ds_Merchant_Data	1024 / A-N	Campo opcional para el comercio para ser incluido en los datos enviados por la respuesta online al comercio si se ha elegido esta opción.
Número de autorización	Ds_AuthorisationCode	6 / A-N	Código alfanumérico de autorización asignado a la aprobación de la transacción por la institución autorizadora.
Fecha	Ds_Date	26 / A-N	La fecha del sistema en la que se ha realizado la operación. Ejemplo: 2009-09-14-11.59.59.999999.

Hora	Ds_Hour	26 / A-N	La fecha del sistema en la que se ha realizado la operación. Ejemplo: 2009-09-14-11.59.59.999999.
Importe	Ds_Amount	Núm.	El importe de la operación.
Moneda	Ds_Currency	3 / Núm.	Código de moneda. Los más usados son: 978 = euros 840 = dólares 826 = libras 392 = yenes
Núm. tarjeta	Ds_CardNumber	14-16 / Núm.	(Depende de la configuración del comercio).
Tipo tarjeta	Ds_CardType	1 / Núm.	C = crédito D = débito - -> sin determinar
Pago seguro	Ds_SecurePayment	1 / Núm.	0 - Si el pago NO es seguro. 1 - Si el pago es seguro.
Estado	Ds_State	1 / A-N	Estado de la transacción. Posibles valores: P: en proceso F: finalizada T: sin respuesta E: operaciones con error de formato. S: solicitada. I: incidencia especial. W: estado temporal.
Error	Ds_ErrorCode	71 / A-N	Código de error. (Solo en mensaje de error). Ver errores en la tabla de errores.
Código de respuesta	Ds_Response	4 / Núm.	Ver la tabla siguiente.

Como salida podemos encontrar en el XML los campos que nos permiten tener la información solicitada en la consulta:

CODIGO	SIGNIFICADO
0000 a 0099	Transacción autorizada para pagos y preautorizaciones.
0900	Transacción autorizada para devoluciones y confirmaciones.
101	Tarjeta caducada.
102	Tarjeta en excepción transitoria o bajo sospecha de fraude.
104/9104	Operación no permitida para esa tarjeta o terminal.
116	Disponible insuficiente.
118	Tarjeta no registrada.
129	Código de seguridad (CVV2/CVC2) incorrecto.
180	Tarjeta ajena al servicio.
184	Error en la autenticación del titular.
190	Denegación sin especificar motivo.
191	Fecha de caducidad errónea.
202	Tarjeta en excepción transitoria o bajo sospecha de fraude con retirada de tarjeta.
912/9912	Emisor no disponible.
Cualquier otro valor	Transacción denegada.

Nota: solo en el caso de las preautenticaciones (preautorizaciones separadas) se devuelve un 0 si está autorizada y el titular se autentica, y un 1, si está autorizada y el titular no se autentica.

En base a este XML-SCHEMA, podemos mostrar varios ejemplos para poder comprobar los datos de entrada y de salida de los XML.

Los campos “tarjeta” y “fecha de caducidad” vendrán en función de la configuración del comercio. En el ejemplo se muestran, pero

no son obligatorios y no aparecerán a no ser que se especifique dentro de la configuración definida en el comercio.

1 - Monitor simple

Mensaje envío ej.:

```
<Messages>
  <Version Ds_Version="0.0">
    <Message>
      <Monitor>
        <Ds_MerchantCode>999008881</Ds_MerchantCode>
        <Ds_Terminal>1</Ds_Terminal>
        <Ds_Order>09102612333</Ds_Order>
        <Ds_Merchant_Data>El merchant data</Ds_Mer-
          chant_Data>
```

```

    </Monitor>
  </Message>
</Version>
<Signature>2a5fecc4f3d41274f5345503d580ac65dd7
be801</Signature>
</Messages>

```

Mensaje respuesta ej.:

```

<Messages>
  <Version Ds_Version="0.0">
    <Message>
      <Response>
        <Ds_MerchntCode>999008881</Ds_Mer-
        chantCode>
        <Ds_Terminal>1</Ds_Terminal>
        <Ds_Order>09102613337</Ds_Order>
        <Ds_TransactionType>0</Ds_TransactionType>
        <Ds_Date>2009-10-26</D_Date>
        <Ds_Hour>12:33:37</Ds_Hour>
        <Ds_Amount>145</Ds_Amount>
        <Ds_Currency>978</DsCurrency>
        <Ds_CardNumber>4548810000000003</
        Ds_CardNumber>
        <Ds_CardType>C</Ds_Cardtype>
        <Ds_ExpiryDate>1212</Ds_ExpiryDate>
        <Ds_SecurePayment>1</Ds_SecurePayment>
        <D_State>F</Ds_State>
        <Ds_Response>0</Ds_Response>
        <Ds_Merchant_Data>El merchant daa</
        Ds_Merchant_Data>
      </Response>
    </Message>
  </Version>
  <Signature>1eb3770ba531c7ecfcb557f623d6b06a149c
  52f</Signature>
</Messages>

```

Nota: Los campos "Ds_CardNumber" y "Ds_ExpiryDate" dependen de la configuración del comercio.

2 - Transacción simple

Mensaje envío ej.:

```

<Messages>
  <Version Ds_Version="0.0">
    <Message>
      <Transaction>
        <Ds_MerchantCode>999008881</Ds_MerchantCo-
        de>
        <Ds_Terminal>1</Ds_Terminal>
        <Ds_Order>091026123337</Ds_Order>
        <Ds_TransactionType>0</Ds_TransactionType>
        <Ds_Merchant_Data>El merchant data</Ds_Mer-
        chant_Data>
      </Transaction>
    </Message>
  </Version>
  <Signature>f44ae1b30659c3441b52c1cd0e14f55ae
  4c76082</Signature>
</Messages>

```

Mensaje respuesta ej.:

```

<Messages>
  <Version Ds_Version="0.0">

```

```

    <Message>
      <Response>
        <Ds_MerchantCode>999008881</Ds_Mer-
        chantCode>
        <Ds_Terminal>1</Ds_Terminal>
        <Ds_Order>091026123337</Ds_Order>
        <Ds_TransactionType>0</Ds_TransactionType>
        <Ds_Date>2009-10-26</Ds_Date>
        <Ds_Hour>12:33:37</Ds_Hour>
        <Ds_Amount>145</Ds_Amount>
        <Ds_Currency>978</Ds_Currency>
        <Ds_CardNumber>4548810000000003</Ds_CardNumber>
        <Ds_CardType>C</Ds_CardType>
        <Ds_ExpiryDate>1212</Ds_ExpiryDate>
        <Ds_SecurePayment>1</Ds_SecurePayment>
        <Ds_State>F</Ds_State>
        <Ds_Response>0</Ds_Response>
        <Ds_Merchant_Data>El merchant data</
        Ds_Merchant_Data>
      </Response>
    </Message>
  </Version>
  <Signature>1eb3770ba531c7ecfcb557f623d6b06a149
  c52f</Signature>
</Messages>

```

NOTA: Los campos "Ds_CardNumber" y "Ds_ExpiryDate" dependen de la configuración del comercio.

3 - Monitor masivo

Mensaje envío ej.:

```

<Messages>
  <Version Ds_Version="0.0">
    <Message>
      <MonitorMasiva>
        <Ds_MerchantCode>999008881</Ds_Mer-
        chantCode>
        <Ds_Terminal>1</Ds_Terminal>
        <Ds_Fecha_inicio>
        2009-09-10-00.00.000000
        </Ds_Fecha_inicio>
        <Ds_Fecha_fin>
        2009-09-14-11.59.59.999999
        </Ds_Fecha_fin>
      </MonitorMasiva>
    </Message>
  </Version>
  <Signature>7b1df6940c00271a2f47fb2de2353487f6430066
  </Signature>
</Messages>

```

Mensaje respuesta ej.:

```

<Messages>
  <Version Ds_Version="0.0">
    <Message>
      <Response>
        <Ds_MerchantCode>999008881</Ds_Mer-
        chantCode>
        <Ds_Terminal>1</Ds_Terminal>
        <Ds_Order>090910132731</Ds_Order>
        <Ds_TransactionType>0</Ds_Transaction-
        Type>
        <Ds_Date>2009-09-10</Ds_Date>
        <Ds_Hour>13:27:32</Ds_Hour>

```

```

<Ds_Amount>145</Ds_Amount>
<Ds_Currency>978</Ds_Currency>
<Ds_SecurePayment>0</Ds_SecurePay-
ment>
<Ds_State>S</Ds_State>
</Response>
<Response>
  <Ds_MerchantCode>999008881</Ds_Mer-
chantCode>
  <Ds_Terminal>1</Ds_Terminal>
  <Ds_Order>090910135448</Ds_Order>
  <Ds_TransactionType>1</Ds_Transaction-
Type>
  <Ds_Date>2009-09-10</Ds_Date>
  <Ds_Hour>13:55:11</Ds_Hour>
  <Ds_Amount>145</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>

  <Ds_CardNumber>4548810000000003</
Ds_CardNumber>
  <Ds_CardType>null</Ds_CardType>
  <Ds_ExpiryDate>0909</Ds_ExpiryDate>
  <Ds_SecurePayment>0</Ds_SecurePay-
ment>
  <Ds_State>F</Ds_State>
  <Ds_Response>0</Ds_Response>
</Response>
<Response>
  <Ds_MerchantCode>999008881</Ds_Mer-
chantCode>
  <Ds_Terminal>1</Ds_Terminal>
  <Ds_Order>090911113431</Ds_Order>
  <Ds_TransactionType>0</Ds_Transaction-
Type>
  <Ds_Date>2009-09-11</Ds_Date>
  <Ds_Hour>11:34:32</Ds_Hour>
  <Ds_Amount>145</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>
  <Ds_SecurePayment>0</Ds_SecurePay-
ment>
  <Ds_State>S</Ds_State>
</Response>
<Response>
  <Ds_MerchantCode>999008881</Ds_Mer-
chantCode>
  <Ds_Terminal>1</Ds_Terminal>
  <Ds_Order>090911113550</Ds_Order>
  <Ds_TransactionType>0</Ds_Transaction-
Type>
  <Ds_Date>2009-09-11</Ds_Date>
  <Ds_Hour>11:35:51</Ds_Hour>
  <Ds_Amount>145</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>
  <Ds_SecurePayment>0</Ds_SecurePay-
ment>
  <Ds_State>S</Ds_State>
</Response>
<Response>
  <Ds_MerchantCode>999008881</Ds_Mer-
chantCode>
  <Ds_Terminal>1</Ds_Terminal>
  <Ds_Order>090911113851</Ds_Order>
  <Ds_TransactionType>0</Ds_Transaction-
Type>
  <Ds_Date>2009-09-11</Ds_Date>
  <Ds_Hour>11:38:52</Ds_Hour>
  <Ds_Amount>145</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>

```

```

<Ds_CardNumber>4548030000000008</
Ds_CardNumber>
<Ds_CardType>null</Ds_CardType>
<Ds_ExpiryDate>0909</Ds_ExpiryDate>
<Ds_SecurePayment>0</Ds_SecurePay-
ment>
<Ds_State>A</Ds_State>
</Response>
<Response>
  <Ds_MerchantCode>999008881</Ds_Mer-
chantCode>
  <Ds_Terminal>1</Ds_Terminal>
  <Ds_Order>090911114406</Ds_Order>
  <Ds_TransactionType>0</Ds_Transaction-
Type>
  <Ds_Date>2009-09-11</Ds_Date>
  <Ds_Hour>11:44:43</Ds_Hour>
  <Ds_Amount>145</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>

  <Ds_CardNumber>4548030000000008</
Ds_CardNumber>
  <Ds_CardType>null</Ds_CardType>
  <Ds_ExpiryDate>0909</Ds_ExpiryDate>
  <Ds_SecurePayment>0</Ds_SecurePay-
ment>
  <Ds_State>A</Ds_State>
</Response>
<Response>
  <Ds_MerchantCode>999008881</Ds_Mer-
chantCode>
  <Ds_Terminal>1</Ds_Terminal>
  <Ds_Order>090911114836</Ds_Order>
  <Ds_TransactionType>0</Ds_Transaction-
Type>
  <Ds_Date>2009-09-11</Ds_Date>
  <Ds_Hour>11:48:37</Ds_Hour>
  <Ds_Amount>145</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>

  <Ds_CardNumber>4548030000000008</
Ds_CardNumber>
  <Ds_CardType>null</Ds_CardType>
  <Ds_ExpiryDate>0909</Ds_ExpiryDate>
  <Ds_SecurePayment>0</Ds_SecurePay-
ment>
  <Ds_State>A</Ds_State>
</Response>
<Response>
  <Ds_MerchantCode>999008881</Ds_Mer-
chantCode>
  <Ds_Terminal>1</Ds_Terminal>
  <Ds_Order>090914090801</Ds_Order>
  <Ds_TransactionType>0</Ds_Transaction-
Type>
  <Ds_Date>2009-09-14</Ds_Date>
  <Ds_Hour>09:08:02</Ds_Hour>
  <Ds_Amount>145</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>

  <Ds_CardNumber>4940198000000007</
Ds_CardNumber>
  <Ds_CardType>null</Ds_CardType>
  <Ds_ExpiryDate>1212</Ds_ExpiryDate>
  <Ds_SecurePayment>0</Ds_SecurePay-
ment>
  <Ds_State>A</Ds_State>

```

```

</Response>
<Response>
  <Ds_MerchantCode>999008881</Ds_Mer-
    chantCode>
  <Ds_Terminal>1</Ds_Terminal>
  <Ds_Order>1234567890</Ds_Order>
  <Ds_TransactionType>1</Ds_Transaction-
    Type>
  <Ds_Date>2009-09-10</Ds_Date>
  <Ds_Hour>13:27:40</Ds_Hour>
  <Ds_Amount>145</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>

  <Ds_CardNumber>4548810000000003</
    Ds_CardNumber>
  <Ds_CardType>null</Ds_CardType>
  <Ds_ExpiryDate>0909</Ds_ExpiryDate>
  <Ds_SecurePayment>0</Ds_SecurePay-
    ment>
  <Ds_State>F</Ds_State>
  <Ds_Response>0</Ds_Response>
</Response>
<Response>
  <Ds_MerchantCode>999008881</Ds_Mer-
    chantCode>
  <Ds_Terminal>1</Ds_Terminal>
  <Ds_Order>1234567890</Ds_Order>
  <Ds_TransactionType>2</Ds_Transaction-
    Type>
  <Ds_Date>2009-09-10</Ds_Date>
  <Ds_Hour>13:28:28</Ds_Hour>
  <Ds_Amount>145</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>

  <Ds_CardNumber>4548810000000003</
    Ds_CardNumber>
  <Ds_CardType>null</Ds_CardType>
  <Ds_ExpiryDate>0909</Ds_ExpiryDate>
  <Ds_SecurePayment>0</Ds_SecurePay-
    ment>
  <Ds_State>F</Ds_State>
  <Ds_Response>900</Ds_Response>
</Response>
<Response>
  <Ds_MerchantCode>999008881</Ds_Mer-
    chantCode>
  <Ds_Terminal>1</Ds_Terminal>
  <Ds_Order>1234567890</Ds_Order>
  <Ds_TransactionType>3</Ds_Transaction-
    Type>
  <Ds_Date>2009-09-10</Ds_Date>
  <Ds_Hour>13:29:53</Ds_Hour>
  <Ds_Amount>145</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>

  <Ds_CardNumber>4548810000000003</
    Ds_CardNumber>
  <Ds_CardType>null</Ds_CardType>
  <Ds_ExpiryDate>0909</Ds_ExpiryDate>
  <Ds_SecurePayment>0</Ds_SecurePay-
    ment>
  <Ds_State>F</Ds_State>
  <Ds_Response>900</Ds_Response>
</Response>
<Response>
  <Ds_MerchantCode>999008881</Ds_Mer-
    chantCode>
  <Ds_Terminal>1</Ds_Terminal>
  <Ds_Order>1234567890</Ds_Order>
  <Ds_TransactionType>3</Ds_Transaction-
    Type>
  <Ds_Date>2009-09-10</Ds_Date>
  <Ds_Hour>13:30:43</Ds_Hour>
  <Ds_Amount>1</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>

  <Ds_CardNumber>4548810000000003</
    Ds_CardNumber>
  <Ds_CardType>null</Ds_CardType>
  <Ds_ExpiryDate>0909</Ds_ExpiryDate>
  <Ds_SecurePayment>0</Ds_SecurePay-
    ment>
  <Ds_State>F</Ds_State>
  <Ds_Response>900</Ds_Response>
</Response>
<Response>
  <Ds_MerchantCode>999008881</Ds_Mer-
    chantCode>
  <Ds_Terminal>1</Ds_Terminal>
  <Ds_Order>1234567890</Ds_Order>
  <Ds_TransactionType>3</Ds_Transaction-
    Type>
  <Ds_Date>2009-09-10</Ds_Date>
  <Ds_Hour>13:38:00</Ds_Hour>
  <Ds_Amount>2</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>

  <Ds_CardNumber>4548810000000003</
    Ds_CardNumber>
  <Ds_CardType>null</Ds_CardType>
  <Ds_ExpiryDate>0909</Ds_ExpiryDate>
  <Ds_SecurePayment>0</Ds_SecurePay-
    ment>
  <Ds_State>F</Ds_State>
  <Ds_Response>900</Ds_Response>
</Response>
</Message>
</Version>
<Signature>44c8a04b33c4feeb8bc5bbb8796263075862
44c4</Signature>
</Messages>

Nota: Los campos "Ds_CardNumber" y "Ds_ExpiryDate" dependen
de la configuración del comercio.

4 - Transacción masiva

Mensaje envío ej.:

<Messages>
  <Version Ds_Version="0.0">
    <Message>
      <TransactionMasiva>
        <Ds_MerchantCode>999008881</Ds_Mer-
          chantCode>
        <Ds_Terminal>1</Ds_Terminal>
        <Ds_TransactionType>0</Ds_Transaction-
          Type>
        <Ds_Fecha_ini-
          cio>2009-09-10-00.00.00.000000</Ds_Fe-
            cha_inicio>
        <Ds_Fecha_fin>2009-09-14-
          11.59.59.999999</Ds_Fecha_fin>
      </TransactionMasiva>
    </Message>
  </Version>
</Messages>

```

```

</Version>
<Signature>f40a4de448f4539a423582d02be1303bd86c
f4a0</Signature>
</Messages>

```

Mensaje respuesta ej.:

```

<Messages>
  <Version Ds_Version="0.0">
    <Message>
      <Response>
        <Ds_MerchantCode>999008881</Ds_Mer-
        chantCode>
        <Ds_Terminal>1</Ds_Terminal>
        <Ds_Order>090911113431</Ds_Order>
        <Ds_TransactionType>0</Ds_TransactionType>
        <Ds_Date>2009-09-11</Ds_Date>
        <Ds_Hour>11:34:32</Ds_Hour>
        <Ds_Amount>145</Ds_Amount>
        <Ds_Currency>978</Ds_Currency>
        <Ds_SecurePayment>0</Ds_SecurePay-
        ment>
        <Ds_State>S</Ds_State>
      </Response>
    </Message>
    <Response>
      <Ds_MerchantCode>999008881</Ds_Mer-
      chantCode>
      <Ds_Terminal>1</Ds_Terminal>
      <Ds_Order>090911113550</Ds_Order>
      <Ds_TransactionType>0</Ds_TransactionType>
      <Ds_Date>2009-09-11</Ds_Date>
      <Ds_Hour>11:35:51</Ds_Hour>
      <Ds_Amount>145</Ds_Amount>
      <Ds_Currency>978</Ds_Currency>
      <Ds_SecurePayment>0</Ds_SecurePay-
      ment>
      <Ds_State>S</Ds_State>
    </Response>
  </Messages>
  <Response>
    <Response>
      <Ds_MerchantCode>999008881</Ds_Mer-
      chantCode>
      <Ds_Terminal>1</Ds_Terminal>
      <Ds_Order>090911113851</Ds_Order>
      <Ds_TransactionType>0</Ds_TransactionType>
      <Ds_Date>2009-09-11</Ds_Date>
      <Ds_Hour>11:38:52</Ds_Hour>
      <Ds_Amount>145</Ds_Amount>
      <Ds_Currency>978</Ds_Currency>
      <Ds_SecurePayment>0</Ds_SecurePay-
      ment>
      <Ds_State>A</Ds_State>
    </Response>
  </Response>
  <Response>
    <Ds_MerchantCode>999008881</Ds_Mer-
    chantCode>
    <Ds_Terminal>1</Ds_Terminal>
    <Ds_Order>090911114406</Ds_Order>
    <Ds_TransactionType>0</Ds_TransactionType>
    <Ds_Date>2009-09-11</Ds_Date>
    <Ds_Hour>11:44:43</Ds_Hour>
    <Ds_Amount>145</Ds_Amount>
    <Ds_Currency>978</Ds_Currency>
    <Ds_SecurePayment>0</Ds_SecurePay-
    ment>
    <Ds_State>A</Ds_State>
  </Response>
</Response>

```

```

<Ds_CardNumber>4548030000000008</
Ds_CardNumber>
<Ds_CardType>null</Ds_CardType>
<Ds_ExpiryDate>0909</Ds_ExpiryDate>
<Ds_SecurePayment>0</Ds_SecurePay-
ment>
<Ds_State>A</Ds_State>
</Response>
<Response>
  <Ds_MerchantCode>999008881</Ds_Mer-
  chantCode>
  <Ds_Terminal>1</Ds_Terminal>
  <Ds_Order>090911114836</Ds_Order>
  <Ds_TransactionType>0</Ds_TransactionType>
  <Ds_Date>2009-09-11</Ds_Date>
  <Ds_Hour>11:48:37</Ds_Hour>
  <Ds_Amount>145</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>
  <Ds_CardNumber>4548030000000008</
  Ds_CardNumber>
  <Ds_CardType>null</Ds_CardType>
  <Ds_ExpiryDate>0909</Ds_ExpiryDate>
  <Ds_SecurePayment>0</Ds_SecurePay-
  ment>
  <Ds_State>A</Ds_State>
</Response>
<Response>
  <Ds_MerchantCode>999008881</Ds_Mer-
  chantCode>
  <Ds_Terminal>1</Ds_Terminal>
  <Ds_Order>090914090801</Ds_Order>
  <Ds_TransactionType>0</Ds_TransactionType>
  <Ds_Date>2009-09-14</Ds_Date>
  <Ds_Hour>09:08:02</Ds_Hour>
  <Ds_Amount>145</Ds_Amount>
  <Ds_Currency>978</Ds_Currency>
  <Ds_CardNumber>4940198000000007</
  Ds_CardNumber>
  <Ds_CardType>null</Ds_CardType>
  <Ds_ExpiryDate>1212</Ds_ExpiryDate>
  <Ds_SecurePayment>0</Ds_SecurePay-
  ment>
  <Ds_State>A</Ds_State>
</Response>
</Message>
</Version>
<Signature>a5a38ed7336808b7695363ebec2879e2e41
9e7b4</Signature>
</Messages>

```

Nota: Los campos "Ds_CardNumber" y "Ds_ExpiryDate" dependen de la configuración del comercio.

5 - Transacción Detail

Mensaje envío ej.:

```

<Messages>
  <Version Ds_Version="0.0">
    <Message>
      <Detail>
        <Ds_MerchantCode>999008881
        </Ds_MerchantCode>
        <Ds_Terminal>16</Ds_Terminal>

```

```

<Ds_Order>100511114713</Ds_Order>
<Ds_TransactionType>0</Ds_TransactionType>
<Ds_Merchant_Data>El merchant data</
Ds_Merchant_Data>
</Detail>
</Message>
</Version>
<Signature>5b808cc7cbfea755600ff226b22107307dd1
1d29</Signature>
</Messages>

```

Mensaje respuesta ej.:

```

<Messages>
  <Version Ds_Version="0.0">
    <Message>
      <Response>
        <Ds_MerchantCode>999008881</Ds_Mer-
        chantCode>
        <Ds_Terminal>16</Ds_Terminal>
        <Ds_Order>100511114713</Ds_Order>
        <Ds_TransactionType>0</Ds_TransactionType>
        <Ds_Date>2010-05-11</Ds_Date>
        <Ds_Hour>11:47:15</Ds_Hour>
        <Ds_Amount>12244</Ds_Amount>
        <Ds_Currency>978</Ds_Currency>
        <Ds_SecurePayment>1</Ds_SecurePayment>
        <Ds_State>F</Ds_State>
        <Ds_Response>0</Ds_Response>
        <Ds_Merchant_Data>El merchant data</
        Ds_Merchant_Data>
        <Ds_AuthorisationCode>050197</Ds_Autho-
        risationCode>
      </Response>
    </Message>
  </Version>
  <Signature>1bb5122958b0c4234df5f15d3e8a1c1961
  ec8626</Signature>
</Messages>

```

6 - Ejemplo de respuesta con error:

En este caso error de firma.

```

<Messages>
  <Version Ds_Version="0.0">
    <Message>
      <ErrorMsg>
        <Ds_ErrorCode>SIS0034</Ds_ErrorCode>
      </ErrorMsg>
    </Message>
  </Version>
</Messages>

```

8.3 WSDL del servicio

Las URL de los servicios web del TPV Virtual son las siguientes:

Entorno de pruebas:

<https://sis-t.redsys.es:25443/apl-SOAP/rpcrouter>

Entorno real:

<https://sis.redsys.es/aplSOAP/rpcrouter>

Estas URL se utilizarán como punto de destino del servicio.

Las URL con la WSDL disponible se encuentran en estas direcciones:

Entorno de pruebas:

<https://sis-t.redsys.es:25443/sis/wSDL/SerCisConsultasSIS.wsdl>

Entorno real:

<https://sis.redsys.es/sis/wSDL/SerCisConsultasSIS.wsdl>

La WSDL que describe el servicio de consulta de transacciones del SIS es la siguiente:

```

<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions
  name="SerCisConsultasSIS"
  targetNamespace="http://tempuri.org/"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:xsd=http://www.w3.org/2001/XMLSchema
  xmlns:tns="http://tempuri.org/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:soap="http://schemas.xmlsoap.org/soap/">
  <wsdl:message name="procesaMensajeRecibidoResponse">
    <wsdl:part name="return" type="xsd:string"/>
  </wsdl:message>

  <wsdl:message name="procesaMensajeRecibidoRequest">
    <wsdl:part name="Mensaje" type="xsd:string"/>
  </wsdl:message>

  <wsdl:portType name="SerCisConsultasSISPortType">
    <wsdl:operation name="procesaMensajeRecibido">
      <wsdl:input message="tns:procesaMensajeRecibidoRequest"/>
      <wsdl:output message="tns:procesaMensajeRecibidoResponse"/>
    </wsdl:operation>
  </wsdl:portType>

  <wsdl:binding name="SerCisConsultasSISBinding"
    type="tns:SerCisConsultasSISPortType">
    <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="procesaMensajeRecibido">
      <soap:operation soapAction="urn:mensajeríaCIBERPAC#procesaMensajeRecibido"/>
    <wsdl:input>
      <soap:body use="encoded"
        encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
        namespace="urn:mensajeríaCIBERPAC"/>
    </wsdl:input>
    <wsdl:output>
      <soap:body use="encoded"

```

```

        encodingStyle="http://schemas.xmlsoap.org/soap/
        encoding/"
        namespace="urn:mensajeríaCIBERPAC"/>
    </wsdl:output>
</wsdl:operation>
</wsdl:binding>

<wsdl:service name="SerCisConsultasSISService">
<wsdl:port name="SerCisConsultasSISPort"
    binding="tns:SerCisConsultasSISBinding">
    <soap:address location="https://sis.redsys.es/aplSOAP/
    rpcrouter"/>
</wsdl:port>
</wsdl:service>

</wsdl:definitions>

```

8.4 Ejemplo de cliente SOAP

A continuación se detalla un ejemplo de cliente SOAP realizado en JAVA. El cliente SOAP debe llevar a cabo los siguientes pasos:

- Indicar la URL del servicio SOAP al que quiere acceder

URL url = new URL
 ("https://sis.redsys.es/aplSOAP/
 rpcrouter");

- Crear un objeto del tipo SOAPMappingRegistry:

SOAPMappingRegistry smr = new SOAPMappingRegistry();

Crear un objeto del tipo Call con los siguientes datos:

SOAPMappingRegistry (anteriormente creado)

TargetObjectURI. URN del servicio de mensajería.

MethodName. Método al que se quiere acceder.

EncodingStyleURI. Constante.

- Vector con los parámetros de la consulta

Por ejemplo:

```

Call call = new Call();
call.setSOAPMappingRegistry(smr);
call.setTargetObjectURI("urn:mensajeríaCIBERPAC");
call.setMethodName("procesaMensajeRecibido");

```

```

call.setEncodingStyleURI(Constants.NS_URI_SOAP_ENC);
Vector params = new Vector();
params.addElement(new Parameter("Mensaje", String.class, xml_doc, null));
call.setParams(params);
-
Realizar invoke con la URL del servicio SOAP que retornará un objeto "Response"
Response resp=null;
resp = call.invoke(url, "");
Parameter ret = resp.getReturnValue();
Object value = ret.getValue();

```

EJEMPLO CLIENTE SOAP JAVA (SERVLET)

```

import java.io.*;
import javax.servlet.*;
import javax.servlet.http.*;

import java.io.*;
import java.net.*;
import org.apache.soap.*;
import org.apache.soap.messaging.*;
import org.apache.soap.transport.*;
import org.apache.soap.util.xml.*;
import org.apache.soap.encoding.*;
import org.apache.soap.encoding.soapenc.*;
import org.apache.soap.rpc.*;

public class SerSviCIBERPAC extends HttpServlet
{
    public void doPost(HttpServletRequest req, HttpServletResponse res)
    throws ServletException, IOException
    {
        String respuesta = "";
        try
        {
            String xml_doc = req.getParameter("eIXMLEnvio");
            respuesta = ejecutaCallRPCStyle(xml_doc);
        }
        catch(Exception e)
        {
            e.printStackTrace();
        }
    }

    public String ejecutaCallRPCStyle(String xml_doc) throws
    ServletException, IOException
    {
        String respuesta = "";

        String encodingStyleURI = Constants.NS_URI_SOAP_ENC;
        URL url = new URL("https://sis.redsys.es/aplSOAP/rpcrouter");
        SOAPMappingRegistry smr = new SOAPMappingRegistry();
        Call call = new Call();
        call.setSOAPMappingRegistry(smr);
        call.setTargetObjectURI("urn:mensajeríaCIBERPAC");
        call.setMethodName("procesaMensajeRecibido");
        call.setEncodingStyleURI(encodingStyleURI);
        Vector params = new Vector();
        params.addElement(new Parameter("Mensaje", String.class, xml_doc, null));
        call.setParams(params);
        Response resp=null;
        try
        {

```

```

    resp = call.invoke(url, "");
}
catch (SOAPException e)
{
    e.printStackTrace();
}
if (!resp.generatedFault())
{
    Parameter ret = resp.getReturnValue();
    Object value = ret.getValue();
    respuesta = (String) value;
}
else
{

```

```

    Fault fault = resp.getFault();
    respuesta = fault.getFaultString();
}
return (respuesta);
}
}

```

8.5 Códigos de error SOAP

El servicio SOAP de consulta de transacciones tiene sus propios códigos de error, que se describen a continuación.

ERROR	DESCRIPCIÓN
XML0000	Errores varios en el proceso del XML-String recibido.
XML0001	Error en la generación del DOM a partir del XML-String recibido y la DTD definida.
XML0002	No existe el elemento “Message” en el XML-String recibido.
XML0003	El tipo de “Message” en el XML-String recibido tiene un valor desconocido o inválido en la petición.
XML0004	No existe el elemento “Ds_MerchantCode” en el XML-String recibido.
XML0005	El elemento “Ds_MerchantCode” viene vacío en el XML-String recibido.
XML0006	El elemento “Ds_MerchantCode” tiene una longitud incorrecta en el XML-String recibido.
XML0007	El elemento “Ds_MerchantCode” no tiene formato numérico en el XML-String recibido.
XML0008	No existe el elemento “Ds_Terminal” en el XML-String recibido.

XML0009	El elemento “Ds_Terminal” viene vacío en el XML-String recibido.
XML0010	El elemento “Ds_Terminal” tiene una longitud incorrecta en el XML-String recibido.
XML0011	El elemento “Ds_Terminal” no tiene formato numérico en el XML-String recibido.
XML0012	No existe el elemento “Ds_Order” en el XML-String recibido.
XML0013	El elemento “Ds_Order” viene vacío en el XML-String recibido.
XML0014	El elemento “Ds_Order” tiene una longitud incorrecta en el XML-String recibido.
XML0015	El elemento “Ds_Order” no tiene sus 4 primeras posiciones numéricas en el XML-String recibido.
XML0016	No existe el elemento “Ds_TransactionType” en el XML-String recibido.
XML0017	El elemento “Ds_TransactionType” viene vacío en el XML-String recibido.
XML0018	El elemento “Ds_TransactionType” tiene una longitud incorrecta en el XML-String recibido.
XML0019	El elemento “Ds_TransactionType” no tiene formato numérico en el XML-String recibido.
XML0020	El elemento “Ds_TransactionType” tiene un valor desconocido o inválido en un mensaje “Transaction”.
XML0021	No existe el elemento “Signature” en el XML-String recibido.
XML0022	El elemento “Signature” viene vacío en el XML-String recibido.

XML0023	La firma no es correcta.
XML0024	No existen operaciones en TZE para los datos solicitados.
XML0025	El XML de respuesta está mal formado.
XML0026	No existe el elemento “Ds_fecha_inicio” en el XML-String recibido.
XML0027	No existe el elemento “Ds_fecha_fin” en el XML-String recibido.

9.

Ficheros de información periódica

Banco Sabadell ha creado un sistema de ficheros con información sobre la operativa de tarjetas de crédito y débito realizada en los comercios. Se trata de los siguientes tipos de ficheros:

- Fichero de operaciones
- Fichero de retrocesiones
- Fichero de fraude confirmado
- Fichero de peticiones de documentación

Los ficheros se generan todos los días de lunes a viernes, siempre que no sean festivos estatales.

Fichero de operaciones

Este fichero informa sobre las operaciones procesadas por el comercio y que han sido contabilizadas en su cuenta financiera.

No se detallan las operaciones procesadas en el día, sino las operaciones liquidadas.

La suma de las operaciones relacionadas coincide con el importe abonado diariamente en la cuenta financiera del comercio.

Fichero de retrocesiones

Las retrocesiones de operaciones (chargebacks) son el instrumento que tiene el titular de la tarjeta para solicitar, a través de su entidad financiera (banco emisor), la devolución del importe de dicha compra. Estas retrocesiones se han de ajustar a las normativas de la correspondiente marca de tarjeta (Visa o MasterCard).

Banco Sabadell verifica la adecuación de los chargebacks recibidos a dichas reglas, representando directamente al banco emisor aquellas retrocesiones que considera que no se ajustan a derecho y cargando en la cuenta del comercio las que procedan. En algunos casos puede ser necesario para Banco Sabadell solicitar al establecimiento

documentación, ya sea para evaluar la posibilidad de realizar una representación o para documentar dicha representación, y así tener más posibilidades de éxito. En estos supuestos el comercio recibirá una petición de documentación que deberá responder según se describe en el apartado 5.2 del presente manual.

Banco Sabadell informa de los chargebacks recibidos, sean cargados en cuenta o no, para que el establecimiento conozca aquellos clientes que están solicitando retrocesiones. De esta manera el departamento de seguridad del comercio se podrá poner en contacto con ellos, cancelar sus suscripciones, añadirlos a sus listas negras, o llevar a cabo cualquier otra medida que considere necesaria. Este fichero, por tanto, no tiene carácter contable, tan solo informativo.

Fichero de fraude confirmado

El fraude confirmado es la herramienta que tiene el banco emisor para notificar que una operación ha sido objeto de fraude (no la ha realizado ni autorizado el titular de la tarjeta).

Esta notificación es absolutamente independiente de la existencia de un chargeback previo o posterior, o de si éste se ha cargado al comercio o si se ha representado. Es un método para notificar que la transacción no la ha realizado el titular de la tarjeta, de manera que Visa/MasterCard puedan detectar aquellos comercios que procesan un alto índice de operaciones fraudulentas.

Un índice elevado de fraude confirmado es un indicador de que el comercio está realizando una actividad fraudulenta, o bien de que está sufriendo un ataque por parte de compradores ilícitos y no ha implementado los mecanismos necesarios para reducirlo.

Si este nivel es muy superior al permitido o se presenta durante varios meses seguidos,

las marcas de tarjetas exigen la cancelación del contrato con el establecimiento y, en ocasiones, lo sancionan con importantes penalizaciones económicas.

De la misma forma que en el fichero de chargebacks, Banco Sabadell genera un fichero diario con las operaciones de fraude confirmado que han sido reportadas por las diferentes marcas de tarjetas. Este fichero, igual que el anterior, es únicamente informativo y no tiene datos contables. Su finalidad es informar al establecimiento de aquellas tarjetas con las que se está realizando fraude para que, en consecuencia, su departamento de seguridad se pueda poner en contacto con los clientes afectados, cancelar sus cuentas, añadirlos a sus listas negras o llevar a cabo cualquier otra medida que considere necesaria.

Fichero de peticiones de documentación

La solicitud de documentación es una opción que tiene el titular de la tarjeta y el banco emisor para comprobar la bondad de una operación, ya sea porque no recuerda la compra, porque no la reconoce o por cualquier otro motivo que considere.

Toda persona que realice una compra (presencial o no) mediante una tarjeta financiera tiene derecho a realizar una solicitud al comercio de la documentación que justifica el pago. Esta solicitud se debe normalmente a que el propietario de la tarjeta no se acuerda de la operación, o quiere tener más datos de la misma, 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.

Esta documentación se solicita para realizar la defensa o representación de una operación, y deberá ser proporcionada obligatoriamente si se quiere evitar la retrocesión.

El comercio está obligado a presentarla dentro de un plazo de siete días hábiles, siguiendo las instrucciones que se detallan en el apartado 5.2 del presente manual.

9.1 Canales para la recepción de los ficheros

Los ficheros se pueden obtener por los siguientes canales:

- BS Online
- FTP

BS Online

El comercio se conecta al servicio de banca a distancia del grupo Banco Sabadell y descarga el fichero que contiene las operaciones liquidadas desde la última descarga que hizo el cliente.

Si un día no se realiza la descarga, las operaciones quedan acumuladas para la siguiente descarga.

Para obtener esta información, el comercio debe tener contratado el servicio de banca a distancia.

FTP

Una vez finalizado el proceso diario de abono a comercios del grupo Banco Sabadell, los ficheros quedan disponibles en un recurso accesible. El cliente se conecta y los transfiere a su sistema mediante FTPS.

Para acceder a esta información, el cliente debe solicitarlo a su oficina y proporcionar los datos siguientes:

- Datos de contacto (nombre, correo electrónico y teléfono) del responsable técnico del comercio.
- Dirección IP del servidor que accederá al recurso de Banco Sabadell.

9.2 Descripción de los ficheros

A continuación se describe el contenido de cada uno de los ficheros disponibles:

9.2.1 Fichero de operaciones

Registro de cabecera de fichero

DATO	FORMATO	DESCRIPCIÓN
Tipo de registro	XX	10
Fecha proceso	DD-MM-AAAA	Fecha del proceso de liquidación
Fecha inicio	DD-MM-AAAA	Fecha desde la que se informan operaciones
Fecha final	DD-MM-AAAA	Fecha hasta la que se informan operaciones
Relleno	X(179)	

Registro de cabecera de remesa

DATO	FORMATO	DESCRIPCIÓN
Tipo de registro	XX	00
Contrato	9(15)	Número del contrato del comercio
Comercio	9(10)	Número FUC del comercio
Cuenta	9(20)	CCC de la cuenta del comercio
Oficina	9(4)	Oficina gestora del comercio
Fecha proceso	DD-MM-AAAA	Fecha del proceso de liquidación
Fecha inicio	DD-MM-AAAA	Fecha desde la que se informan operaciones
Fecha final	DD-MM-AAAA	Fecha hasta la que se informan operaciones
Relleno	X(130)	

Registro de operación

DATO	FORMATO	DESCRIPCIÓN
Tipo de registro	XX	01
Valor	DD-MM-AAAA	Fecha de valoración abono
Remesa	9(10)	Número de la remesa
Factura	X(12)	Número de la factura
Oficina remesa	9(4)	Oficina de la remesa
Tarjeta	9999+++++9999	Número de la tarjeta
Marca de la tarjeta	X	V - Visa M - Master (incluye Maestro) O - Otra
Clase de tarjeta	X	Reservado para uso futuro
Modalidad de pago	X	C - Crédito D - Débito
Entidad emisora tarjeta	X	P - Banco Sabadell N - Nacional sistema Servired R - Nacional resto sistemas E - Internacional zona euro I - Internacional resto X - Otra
Fecha operación	DD-MM-AAAA	Fecha de la operación
Hora operación	HHMMSS	Hora de la operación
Autorización	9(6)	Número de la autorización
Tipo operación	XX	05 – Venta (realizada por el comercio) 06 – Devolución (realizada por el comercio) 15 – Cancelación de chargeback (representación del comercio) 16 – Chargeback (reclamación del titular de la tarjeta)
Captura operación	XXX	ON - Online OFF - Offline
Importe operación	9 enteros 2 decimales	Importe nominal de la operación
Signo operación	X	+ Abono - Cargo

Tasa descuento	3 enteros 2 decimales	Porcentaje de descuento
Importe descuento	7 enteros 2 decimales	Importe del descuento
Signo descuento	X	+ Abono - Cargo
Importe líquido	11 enteros 2 decimales	Importe nominal - descuento
Signo líquido	X	+ Abono - Cargo
TPV	9(13)	Número del TPV
Relleno	X(38)	
Divisa comercio	X(3)	Divisa de liquidación al comercio
Número de pedido	9(12)	Número de la operación
Código razón	X(4)	Código de razón en <i>chargeback</i>
Relleno	XX	
Importe original	11 enteros 2 decimales	Importe en la divisa original (si es distinta de euro)
Signo original	X	+ Abono - Cargo
Divisa original	X(3)	Divisa de liquidación a titular tarjeta
Relleno	X	

Registro de cola de comercio

DATO	FORMATO	DESCRIPCIÓN
Tipo de registro	XX	99
Relleno	X(25)	
Operaciones	9(9)	Número de operaciones del comercio
Importe	11 enteros 2 decimales	Importe total de las operaciones del comercio
Signo	X	+ Abono - Cargo
Relleno	X(161)	

Registro de cola de fichero

DATO	FORMATO	DESCRIPCIÓN
Tipo registro	XX	90
Comercios	9(9)	Número de comercios del archivo
Relleno	X(25)	
Operaciones	9(9)	Número de operaciones del archivo
Importe	11 enteros 2 decimales	Importe total de operaciones del archivo
Signo	X	+ Abono - Cargo
Relleno	X(152)	

9.2.2 Fichero de retrocesiones

El fichero contiene un único tipo de registro, con los datos separados por el carácter punto y coma (;) y cuyo formato es el siguiente:

DATO	DESCRIPCIÓN
Tipo de registro	CB
Comercio	Número FUC del comercio
Fecha recepción	Fecha de recepción del chargeback
Tarjeta	9999++++++9999
Importe retrocesión	Importe retrocedido
Divisa retrocesión	Divisa de la retrocesión
Fecha operación	Fecha de la operación original
Hora operación	Hora de la operación original
Fecha remesa	Fecha de la remesa de la operación original
Remesa	Número de la remesa de la operación original
Factura	Número de la factura de la operación original
Importe operación	Importe de la operación original
Divisa operación	Divisa de la operación original

Número de pedido	Número de la operación original
Tipo incidencia	06 - Retrocesión 16 - Anulación de retrocesión
Código razón	Código de razón de la retrocesión (ver tabla)
Número de orden	Número de orden de la retrocesión
Texto	Texto que acompaña a la retrocesión recibida

Tabla CÓDIGO DE MOTIVO de la retrocesión

CÓDIGO DE RAZÓN	DESCRIPCIÓN
4501	Operación inválida.
4502	Disputa de titular.
4503	Tarjeta caducada.
4506	Importe o número de tarjeta incorrectos.
4510	Abono procesado como cargo.
4512	Operación duplicada.
4513	Abono no recibido.
4514	Operación fraudulenta (AMD).
4515	Transacción no finalizada.
4516	Petición de fotocopia no contestada.
4517	Petición de fotocopia ilegible.
4521	Operación no autorizada.
4522	Autorización denegada.
4523	Tarjeta inexistente.
4524	Error en suma.
4525	Pagado por otros medios.
4526	Fraude. Operación no reconocida por el titular.
4527	Fraude en entorno presencial.

4531	Disputa del titular.
4532	Mercancía defectuosa o la mercancía no es la especificada.
4534	Transacciones múltiples no autorizadas.
4535	Tarjeta incluida en el archivo de excepciones.
4536	Presentación de la operación fuera de plazo.
4538	Depósito por reserva de alojamiento.
4544	Operación recurrente cancelada.
4545	Código de moneda incorrecto.
4546	Fraude en entorno no presencial.
4547	Tarjeta incluida en el archivo de excepciones.
4549	Número de tarjeta incorrecto.
4550	Titular no reconoce op. en teléfono.
4551	La moneda de la transacción no está incorporada.
4554	Efectivo no recibido.
4555	Servicios no prestados o mercancía no recibida.
4556	La mercancía no es como la especificada.
4753	Operación no conciliada.
4762	Banda magnética de la tarjeta falsificada.
4801	Solicitud de recibo sin confirmar envío en IPM (4516).
4857	Transacciones múltiples no autorizadas.
4859	Servicios no prestados.
4863	Transacción no reconocida por el titular.
4870	Operación no reconocida por el titular-tarjeta chip.
4871	Operación no realizada por el titular.
4896	Importe superior al límite en terminal de importe limitado.
4901	Documentación requerida no recibida en representación.
4902	La documentación de la representación es ilegible.
4903	La documentación facilitada es incompleta o inválida.
4908	Operación no autorizada.
4924	Tarjeta incluida en el archivo de excepciones.

9.2.3 Fichero de fraude confirmado

El fichero contiene un único tipo de registro, con los datos separados por el carácter punto y coma (;), y cuyo formato es el siguiente:

DATO	DESCRIPCIÓN
Tipo de registro	FC.
Comercio	Número FUC del comercio.
Fecha reporte	Fecha de reporte del fraude confirmado.
Tarjeta	9999+++++++9999.
Importe fraude	Importe del fraude.
Divisa fraude	Divisa del fraude.
Fecha operación	Fecha de la operación original.
Hora operación	Hora de la operación original.
Fecha remesa	Fecha de la remesa de la operación original.
Remesa	Número de la remesa de la operación original.
Factura	Número de la factura de la operación original.
Importe operación	Importe de la operación original.
Divisa operación	Divisa de la operación original.
Número de pedido	Número de la operación original.
4524	Error en suma.
4525	Pagado por otros medios.
4526	Fraude. Operación no reconocida por el titular.
4527	Fraude en entorno presencial.
4531	Disputa del titular.
4532	Mercancía defectuosa o la mercancía no es la especificada.

9.2.4 Fichero de solicitudes de documentación

El fichero contiene un único tipo de registro cuyo formato es el siguiente:

DATO	FORMATO	DESCRIPCIÓN
Fecha proceso	DD-MM-AAAA	Día del proceso.
FUC	9(10)	Número FUC del comercio.
Comercio	X(10)	Nombre reducido del comercio.
Teléfono	9(9)	Teléfono del comercio.
Relleno	XX	
Fecha liquidación	DD-MM-AA	Fecha de liquidación.
Relleno	X	
Remesa	9(10)	Número de la remesa.
Relleno	X	
Factura	9(12)	Número de la factura.
Relleno	X(4)	
Fecha operación	DD-MM-AA	Fecha de la operación.
Relleno	X	
Tarjeta	9999+++++++9999	Número de la tarjeta.
Importe operación	11 enteros 2 decimales	Importe de la operación.
Divisa	X	Divisa (E = euro).
Adicional	X(30)	Información adicional.
Relleno	X(10)	

10.

Programas de supervisión y penalizaciones

Las marcas de tarjetas Visa y MasterCard disponen de programas de supervisión y control de las retrocesiones (chargebacks) que reciben los comercios. En dichos programas se establecen las correspondientes penalizaciones a aquellos comercios que exceden el porcentaje máximo permitido de retrocesiones.

Se aplicarán penalizaciones a los comercios que superen las cincuenta operaciones de retrocesión, y durante dos meses consecutivos el porcentaje de devoluciones de cargos recibido supere el 1% de las transacciones del mes anterior.

Además, se han establecido programas para identificar a los comerciantes que, a pesar de no exceder los parámetros citados anteriormente, que dan lugar a la imposición de penalizaciones, reciben ratios cercanas de operaciones retrocedidas.

Los parámetros de alerta son los siguientes:

- Comercios que superen las cincuenta operaciones de retrocesión y el porcentaje de devoluciones de cargos sea superior al 0,5% de las transacciones del mes anterior.

Los parámetros de alerta no implican necesariamente que el comerciante sea penalizado, sino que obligan a que el comerciante dé explicaciones y esté obligado a enviar un plan de acción para demostrar que está tomando todas las medidas necesarias para evitar que los altos volúmenes de operaciones retrocedidas se repitan en el futuro.

Si el plan de acción enviado por el comerciante es considerado como insuficiente por las compañías de tarjetas, estas pueden solicitar que se imponga una sanción consistente en la suspensión temporal de hasta un mes de procesamiento de tarjetas.

Si un comerciante aparece en varias ocasiones en un archivo de advertencia, se podrán

tomar medidas más severas, incluida la exclusión del comercio de la plataforma de pagos con tarjetas. Por esta razón, a pesar de que no existe una sanción directa, es necesario considerar los parámetros de alerta máxima como los valores máximos aceptables para el comercio.

11.

PCI-DSS - programa de seguridad de datos de tarjetas

11.1 ¿Qué es PCI-DSS?

PCI Data Security Standard (PCI-DSS) es un estándar de seguridad desarrollado con el objetivo de reducir el fraude relacionado con tarjetas de crédito e incrementar la seguridad de los datos almacenados en las mismas. Este estándar es de obligado cumplimiento para todas aquellas empresas que procesen, transmitan o almacenen información de tarjetas de crédito, como puede ser el número de tarjeta PAN, la fecha de caducidad, el CVV y demás información privilegiada.

Su finalidad es la reducción del fraude relacionado con las tarjetas de crédito e incrementar la seguridad de estos datos.

Este programa de seguridad ha sido creado por las principales empresas de tarjetas: Visa Internacional, MasterCard Worldwide, American Express, JCB y Discover Financial Services, y en la actualidad es gestionado, revisado y actualizado por el PCI Security Standards Council (<https://www.pcisecuritystandards.org/>).

11.2 Objetivos del programa PCI-DSS

- Mejorar el nivel de seguridad de los pagos realizados mediante tarjetas, promoviendo la existencia de un entorno de pago seguro para la información.
- Garantizar la protección de la información de titulares de tarjetas.
- Minimizar el riesgo de posibles intrusiones no autorizadas, o compromiso de la información de cuentas y tarjetas.
- Incrementar la confianza de los titulares de tarjetas en las transacciones realizadas con tarjetas.
- Luchar contra la suplantación y otros fraudes que se producen en Internet

11.3 Ventajas para los comercios

- Promover la integridad del comercio y aumentar la confianza de los consumidores en el negocio.
- Incrementar las ventas como consecuencia del aumento de la confianza de los consumidores.
- Proteger al comercio de posibles pérdidas de ingresos, investigaciones no deseadas y costos legales.
- Reducir el riesgo reputacional del comercio como resultado de una fuga de información de clientes.
- Reducir las disputas de los titulares de tarjetas y los costes asociados a transacciones fraudulentas resultantes de fugas de información.
- Prevenir el robo masivo de información de clientes.
- Facilitar la adopción de estándares de seguridad válidos a nivel global.

11.4 ¿Quién debe cumplir el programa PCI-DSS?

El programa PCI es de obligado cumplimiento para todas aquellas empresas que procesen, transmitan o almacenen información de tarjetas de crédito o débito, como el número de tarjeta PAN, la fecha de caducidad, el CVV y demás información privilegiada.

Si el comercio ya tiene un certificado válido que demuestre que cumple con los requerimientos del programa, deberá proporcionar a Banco Sabadell una copia del correspondiente certificado acreditativo.

Las compañías de tarjetas han dividido a los comercios en cuatro categorías para el cumplimiento de la normativa PCI en función

del volumen y tipo de transacción procesadas. Estas categorías son las siguientes:

Nivel	Criterio	Obligaciones	Entidad supervisora
1	– Cualquier comercio que procese más de 6 millones de transacciones anuales, con independencia del canal. – Cualquier comercio que haya sufrido un ataque informático que podría haber comprometido la información de tarjetas. – Cualquier comerciante que a criterio de Visa o MasterCard se considere de nivel 1. – Cualquier IPSP (Internet Services Payment Provider) con independencia del número de transacciones procesadas.	– Auditoría anual por parte de un QSA (Quality Security Assessor). – Escaneo de vulnerabilidad de red trimestral con un ASV (Approved Scanning Providers).	– Consultor independiente de seguridad, o la propia empresa si está firmado por un representante de la compañía de seguridad. – Especialista de la compañía de seguridad.
2	– Cualquier comercio que procese más de un millón y menos de 6 millones de transacciones anuales, con independencia del canal.	– Cuestionario anual de autoevaluación (SAQ). – Escaneo de vulnerabilidad de red trimestral con un ASV (Approved Scanning Providers).	– El propio comercio. – Especialista de la compañía de seguridad.
3	– Cualquier comercio que procese más de 20.000 y menos de un millón de transacciones anuales, con independencia del canal.	– Escaneo de vulnerabilidad de red trimestral con un ASV (Approved Scanning Providers).	– Especialista de la compañía de seguridad.
4	– Resto de comercios.	– Cuestionario anual de autoevaluación (SAQ).	– El propio comercio.

Las obligaciones que se indican en el cuadro son de obligado cumplimiento para los comercios. Se trata de las siguientes:

- Auditoría anual por parte de un QSA.
- Escaneo de vulnerabilidad de red trimestral con un ASV (Approved Scanning Providers).
- Cuestionario anual de autoevaluación (SAQ).

Auditoría anual por parte de un QSA

Un asesor de seguridad cualificado (QSA) de Visa o MasterCard lleva a cabo una audi-

toría in situ, de carácter anual, para revisar los sistemas del comercio con el objeto de evaluar la seguridad de los sistemas informáticos implicados en el procesamiento de los datos de las tarjetas (hardware, software y netware). El comercio es responsable de la contratación de este servicio de auditoría a cualquiera de las auditoras certificadas por PCI. Banco Sabadell puede proporcionarle una lista de diferentes servicios de auditoría especializados.

Escaneo de vulnerabilidad de red trimestral con un ASV (Approved Scanning Providers)

Se trata de controles de carácter trimestral que son realizados por empresas certificadas por Visa o MasterCard en calidad de asesor de seguridad cualificado (QSA) o de Approved Scanning Providers (ASV).

El comercio es responsable de la contratación de este servicio a cualquiera de las compañías certificadas por PCI. Banco Sabadell puede proporcionarle una lista de diferentes servicios de auditoría especializados.

Cuestionario anual de autoevaluación (SAQ)

Se le conoce en España como AIS y se trata de un cuestionario de carácter anual sobre la arquitectura del sistema informático del comercio y sobre la forma de procesar y almacenar los datos de las tarjetas.

En el sitio web oficial PCI Security Standards Council hay enlaces a los cuestionarios e instrucciones y documentos de apoyo que le ayudarán a decidir el modelo de cuestionario que debe cumplimentar su empresa.

<https://www.pcisecuritystandards.org/saq/index.shtml>

https://www.pcisecuritystandards.org/pdfs/pci_dss_saq_instr_guide.pdf

Además, para su información, adjuntamos el enlace a la lista de compañías certificadas por PCI para evaluar y validar el cumplimiento de las normas de seguridad PCI.

https://www.pcisecuritystandards.org/approved_companies_providers/index.php

Anexo I.

Datos del formulario de pago

DATO	NOMBRE DEL CAMPO	LONGITUD	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 El TPV Virtual de Banco Sabadell permite operar con 184 divisas. Puede consultar la lista completa de las divisas permitidas en el Anexo V. Las más utilizadas son: 978 - EURO 840 - USD 826 - GBP 392 - JPY 756 - CHF 124 - CAD
Número de pedido	Ds_Order	mín. 4N máx.12 AN Para "Tarjeta en Archivo" el campo debe ser máx. 10 posiciones. El TPV Virtual añadirá 2 posiciones más para indicar el número de orden del pago	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.
Número de comercio. Código FUC	Ds_Merchant_MerchantCode	9 N	Obligatorio. Código fijo asignado por Banco Sabadell.
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 4 – Francés 5 – Alemán 6 – Holandés 7 – Italiano 8 – Sueco 9 – Portugués 10– Valenciano 11 – Polaco 12 – Gallego 13 – Euskera
Firma del comercio	Ds_Merchant_MerchantSignature	40 AN	Obligatorio. Ver apartado 7.6. - 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 Banco Sabadell
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 (exclusivo 'Gateway RealizarPago' y 'XMLentidad') 1 – Preautorización 2 – Confirmación de Preautorización 3 – Devolución parcial o total 7 – Autenticación 8 – Confirmación de Autenticación 9 – Anulación de Preautorización A – Pago sin autenticación (exclusivo 'Gateway Operaciones' y 'WebService') L – Tarjeta en Archivo Inicial (PSuscripciones/PExprés) M – Tarjeta en Archivo Sucesiva (PSuscripciones/PExprés) O – Preautorización Diferida P – Confirmación de Preautorización Diferida Q – Anulación de Preautorización Diferida
Código de autorización	Ds_Merchant_AuthorisationCode	6 N	Opcional.

Identificador	Ds_Merchant_Identifier	Max. 40 AN	El valor del campo es obligatorio para el primer pago. Para segundo pago y sucesivos, el valor será el identificador que el Banco ha facilitado en el mensaje de respuesta del primer pago.
Grupo de comercios	Ds_Merchant_Group	Max. 9 N	Opcional. Permite asociar una referencia a un conjunto de comercios.
Pantallas adicionales	Ds_Merchant_DirectPayment	'True' or 'false'	Opcional. Este parámetro funciona como un flag que indica si hay que mostrar pantallas adicionales (DCC, Fraccionamiento, Autenticación, etc.)
Método de Pago	Ds_Merchant_PayMethod	1 AN	T - Pago con Tarjeta O - Pago mediante IUPAY

A continuación se describen los campos relacionados con los datos de la tarjeta, dada la posibilidad de que puedan ser capturados por el comerciante. Estos nuevos campos sólo tendrán que ser enviados por los comer-

ciantes que capturan los datos de la tarjeta. (Esta posibilidad comporta el cumplimiento de los requisitos del programa de seguridad de PCI-DSS, tal como se describe en el apartado 1.1 del presente manual).

DATO	NOMBRE DEL CAMPO	LONGITUD	COMENTARIOS
Número de tarjeta	Ds_Merchant_Pan	16-19 N	Obligatorio para todas las operaciones (*) Para aquellas que no requieren tarjeta, como las devoluciones, se enviará rellena a 99999999999999999999
Fecha de caducidad	Ds_Merchant_ExpiryDate	4 N	Obligatorio para todas las operaciones (*) Para aquellas que no requieren tarjeta, como las devoluciones, se enviará rellena a 9901 por defecto. Tiene el formato AAMM.
CVV2	Ds_Merchant_CVV2	3 N	Opcional Código CVV2/CVC2 de la tarjeta enviada (*)

(*) Los tipos de transacciones 2 / 3 / 6 / 8 / 9 / P / Q no requieren que se informe el número de tarjeta, fecha de caducidad y CVV2. En estos casos, el campo (Ds_Merchant_Order) debe ser el mismo de la transacción original.

Anexo II.

Códigos de error

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 preautorización	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	Ds_Merchant_Signature	Error en el cálculo del algoritmo HASH	MSG0008
SIS0042			
SIS0043		Error al realizar la notificación on-line	MSG0008
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 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
SIS0079		Error al realizar el pago con tarjeta	MSG0008
SIS0081		La sesión es nueva, se han perdido los datos almacenados	MSG0008
SIS0089		El valor de Ds_Merchant_ExpiryDate no ocupa 4 posiciones	MSG0008
SIS0092		El valor de Ds_Merchant_ExpiryDate 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
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
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 anulación asociada a la preautorización	MSG0008
SIS0223		La preautorización que se desea anular no está autorizada	MSG0008
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
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 Banco Sabadell	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 TPV Virtual.	MSG0008
SIS0281		Operación supera alguna limitación de operatoria definida por Banco Sabadell.	MSG0008
SIS0296		Error al validar los datos de la operación "Tarjeta en Archivo (PSuscripciones/PExprés)" inicial.	MSG0008
SIS0297		Superado el número máximo de operaciones (99 oper. o 1 año) para realizar transacciones sucesivas de "Tarjeta en Archivo (PSuscripciones/PExprés)". Se requiere realizar una nueva operación de "Tarjeta en Archivo Inicial" para iniciar el ciclo..	MSG0008
SIS0298		El comercio no permite realizar operaciones de Pago con Referencia	MSG0008
SIS0319		El comercio no pertenece al grupo especificado en Ds_Merchant_Group	MSG0008
SIS0321		La referencia indicada en Ds_Merchant_Identifier no está asociada al comercio	MSG0008
SIS0322		Error de formato en Ds_Merchant_Group	MSG0008
SIS0325		Se ha pedido no mostrar pantallas pero no se ha enviado ninguna referencia de tarjeta	MSG0008

En la siguiente tabla se relacionan los mensajes que la página de pago muestra al titular de la tarjeta compradora ante los diferentes errores que se puedan producir.

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 III.

Tabla códigos respuesta (ds_response)

A) CODIGOS PARA TRANSACCIONES APROBADAS

CÓDIGO	TÍTULO	DESCRIPCIÓN
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.

B) CODIGOS PARA TRANSACCIONES DENEGADAS

b.1.) Transacciones denegadas por motivos genéricos

CÓDIGO	TÍTULO	DESCRIPCIÓN
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 BLOQUEADA 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 banco emisor.
119	TRANSACCIÓN DENEGADA	Transacción denegada. Contactar con el Banco.

125	TARJETA NO EFECTIVA	Tarjeta inexistente o no dada de alta por banco emisor.
129	ERROR CVV2/CVC2	El código CVV2/CVC2 (los tres dígitos del reverso de la tarjeta) informado por el comprador es erróneo.
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 O CREDITO	Tarjeta bloqueada transitoriamente por el banco emisor.
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.

b.2.) Transacciones denegadas por motivos en los que el banco emisor de la tarjeta considera que existen indicios de fraude.

CÓDIGO	TÍTULO	DESCRIPCIÓN
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.
202	TARJETA BLOQUEADA 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.
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.
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.

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.
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. El código CVV2/CVC2 informado por el comprador es erróneo. Además, el banco emisor considera que la tarjeta está en una situación de posible fraude.
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.

C) CODIGOS REFERIDOS A ANULACIONES O DEVOLUCIONES

(Ds_Merchant_TransactionType = 3) SOLICITADAS POR EL COMERCIO)

CÓDIGO	TÍTULO	DESCRIPCIÓN
400	ANULACION ACEPTADA	Transacción de anulación o retrocesión parcial aceptada por el banco emisor.
480	NO SE ENCUENTRA 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.

D) CODIGOS REFERIDOS A CONCILIACIONES DE PRE-AUTORIZACIONES O PRE-AUTENTICACIONES (Ds_Merchant_TransactionType = 2, 8, 0 o R)

CÓDIGO	TÍTULO	DESCRIPCIÓN
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.

9928	ANULACIÓN DE PREAUTORIZACIÓN REALIZADA POR EL SISTEMA	El sistema ha anulado la preautorización diferida al haber pasado más de 72 horas.
9929	ANULACIÓN DE PREAUTORIZACIÓN REALIZADA POR EL COMERCIO	La anulación de la preautorización ha sido aceptada

E) CODIGOS DE ERROR ENVIADOS POR LA PROPIA PLATAFORMA DE PAGOS DE BANCO SABADELL

CÓDIGO	TÍTULO	DESCRIPCIÓN
904	COMERCIO NO REGISTRADO EN EL FUC	Hay un problema en la configuración del código de comercio. Contactar con Banco Sabadell para solucionarlo.
909	ERROR DE SISTEMA	Error en la estabilidad de la plataforma de pagos de Banco Sabadell 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
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
9142	TIEMPO LÍMITE DE PAGO SUPERADO	El titular de la tarjeta no se ha autenticado durante el tiempo máximo permitido.
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	PREAUTORIZACIONES NO HABILITADAS	La tarjeta no puede hacer Preautorizaciones
9261	LÍMITE OPERATIVO EXCEDIDO	La transacción excede el límite operativo establecido por Banco Sabadell
9283	SUPERA ALERTAS BLOQUANTES	La operación excede las alertas bloqueantes, no se puede procesar
9281	SUPERA ALERTAS BLOQUEANTES	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
9994	IUPAY: TARJETA NO SELECCIONADA	El comprador no ha seleccionado la tarjeta dentro del time-out predefinido.
9997	TRANSACCIÓN SIMULTÁNEA	En el TPV Virtual se está procesando de forma simultánea otra operación con la misma tarjeta.
9998	ESTADO OPERACIÓN: SOLICITADA	Estado temporal mientras la operación se procesa. Cuando la operación termine este código cambiará.
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.

Anexo IV. Códigos ISO países

Anexo IV. Códigos ISO países.

004	Afganistán	152	Chile	276	Alemania
008	Albania	156	China	288	Ghana
012	Argelia	158	Taiwán	292	Gibraltar
016	Samoa Americana	162	Isla de Navidad	296	Kiribati
020	Andorra	166	Islas Cocos	300	Grecia
024	Angola	170	Colombia	304	Groenlandia
028	Antigua y Barbuda	174	Comoras	308	Granada
031	Azerbaiyán	175	Mayotte	312	Guadalupe
032	Argentina	178	República del Congo	316	Guam
036	Australia	180	Rep. Dem. del Congo	320	Guatemala
040	Austria	184	Islas Cook	324	Guinea
044	Bahamas	188	Costa Rica	328	Guyana
048	Baréin	191	Croacia	332	Haití
050	Bangladés	192	Cuba	334	Islas Heard y McDonald
051	Armenia	196	Chipre	336	Ciudad del Vaticano
052	Barbados	203	República Checa	340	Honduras
056	Bélgica	204	Benín	344	Hong Kong
060	Bermudas	208	Dinamarca	348	Hungría
064	Bután	212	Dominica	352	Islandia
068	Bolivia	214	República Dominicana	356	India
070	Bosnia y Herzegovina	218	Ecuador	360	Indonesia
072	Botsuana	222	El Salvador	364	Irán
074	Isla Bouvet	226	Guinea Ecuatorial	368	Irak
076	Brasil	231	Etiopía	372	Irlanda
084	Belice	232	Eritrea	376	Israel
086	Territorio Británico del Océano Índico	233	Estonia	380	Italia
090	Islas Salomón	234	Islas Feroe	384	Costa de Marfil
092	Islas Vírgenes Británicas	238	Islas Malvinas	388	Jamaica
096	Brunéi	239	Islas Georgias y Sandwich del Sur	392	Japón
100	Bulgaria	242	Fiji	398	Kazajistán
104	Birmania	246	Finlandia	400	Jordania
108	Burundi	248	Aland	404	Kenia
112	Bielorrusia	250	Francia	408	Corea del Norte
116	Camboya	254	Guayana Francesa	410	Corea del Sur
120	Camerún	258	Polinesia Francesa	414	Kuwait
124	Canadá	260	Territorios Australes Franceses	417	Kirguistán
132	Cabo Verde	262	Yibuti	418	Laos
136	Islas Caimán	266	Gabón	422	Líbano
140	República Centroafricana	268	Georgia	426	Lesoto
144	Sri Lanka	270	Gambia	428	Letonia
148	Chad	275	Estado de Palestina	430	Liberia

Anexo IV. Códigos ISO países.

434	Libia	585	Palaos	728	Sudán del Sur
438	Liechtenstein	586	Pakistán	729	Sudán
440	Lituania	591	Panamá	732	República Árabe Saharaui Democrática
442	Luxemburgo	598	Papúa Nueva Guinea	740	Surinam
446	Macao	600	Paraguay	744	Svalbard y Jan Mayen
450	Madagascar	604	Perú	748	Suazilandia
454	Malawi	608	Filipinas	752	Suecia
458	Malasia	612	Islas Pitcairn	756	Suiza
462	Maldivas	616	Polonia	760	Siría
466	Malí	620	Portugal	762	Tayikistán
470	Malta	624	Guinea-Bisáu	764	Tailandia
474	Martinica	626	Timor Oriental	768	Togo
478	Mauritania	630	Puerto Rico	772	Tokelau
480	Mauricio	634	Catar	776	Tonga
484	México	638	Reunión	780	Trinidad y Tobago
492	Mónaco	642	Rumania	784	Emiratos Árabes Unidos
496	Mongolia	643	Rusia	788	Túnez
498	Moldavia	646	Ruanda	792	Turquía
499	Montenegro	652	San Bartolomé	795	Turkmenistán
500	Montserrat	654	Santa Helena, A. y T.	796	Islas Turcas y Caicos
504	Marruecos	659	San Cristóbal y Nieves	798	Tuvalu
508	Mozambique	660	Anguila	800	Uganda
512	Omán	662	Santa Lucía	804	Ucrania
516	Namibia	663	San Martín	807	República de Macedonia
520	Nauru	666	San Pedro y Miquelón	818	Egipto
524	Nepal	670	San Vicente y las Granadinas	826	Reino Unido
528	Países Bajos	674	San Marino	831	Guernsey
531	Curazao	678	Santo Tomé y Príncipe	832	Jersey
533	Aruba	682	Arabia Saudita	833	Isla de Man
540	Nueva Caledonia	686	Senegal	834	Tanzania
548	Vanuatu	688	Serbia	840	Estados Unidos
554	Nueva Zelanda	690	Seychelles	850	Islas Vírgenes de los Estados Unidos
558	Nicaragua	694	Sierra Leona	854	Burkina Faso
562	Níger	702	Singapur	858	Uruguay
566	Nigeria	703	Eslovaquia	860	Uzbekistán
570	Niue	704	Vietnam	862	Venezuela
574	Norfolk	705	Eslovenia	876	Wallis y Futuna
578	Noruega	706	Somalia	882	Samoa
580	Islas Marianas del Norte	710	Sudáfrica	887	Yemen
583	Micronesia	716	Zimbabue	894	Zambia
584	Islas Marshall	724	España		

Anexo V.

Códigos ISO divisas

Anexo V. Códigos ISO divisas.

Afgani	AFN	971	El Salvador Colon	SVC	222
Algerian Dinar	DZD	12	Ethiopian Birr	ETB	230
Angola Kwanza	AON	24	Euro	EUR	978
Argentine Peso	ARS	32	European Currency UN	XEU	954
Armenian Dram	AMD	51	Falkland Islands Pound	FKP	238
Aruban Guilder	AWG	533	Fiji Dollar	FJD	242
Australian Dollar	AUD	36	Forint	HUF	348
Azerbaijani Manat	AZN	944	Ghana Cedi	GHC	288
Bahamian Dollar	BSD	44	Gibraltar Pound	GIP	292
Bahraini Dinar	BHD	48	Gourde	HTG	332
Baht	THB	764	Guarani	PYG	600
Balboa	PAB	590	Guinea Franc	GNF	324
Barbados Dollar	BBD	52	Guinea-Bissau Peso	GWP	624
Belarussian Ruble	BYR	974	Guyana Dollar	GYD	328
Belize Dollar	BZD	84	Hong Kong Dollar	HKD	344
Bellarussian Ruble	BYB	112	Hryvnia	UAH	980
Bermudian Dollar	BMD	60	Iceland Krona	ISK	352
Bolivar Fuerte	VEF	937	Indian Rupee	INR	356
Boliviano	BOB	68	Iraqi Dinar	IQD	368
Brazilian Real	BRL	986	Jamaican Dollar	JMD	388
Brunei Dollar	BND	96	Jordanian Dinar	JOD	400
Bulgarian Lev	BGN	975	Karbovanet	UAK	804
Burundi Franc	BIF	108	Kenyan Shilling	KES	404
Canadian Dollar	CAD	124	Kina	PGK	598
Cape Verde Escudo	CVE	132	Kip	LAK	418
Cayman Islands Dollar	KYD	136	Koruna	CSK	200
Cedi	GHS	936	Kroon	EEK	233
CFA Franc BCEAO	XOF	952	Kuwaiti Dinar	KWD	414
CFA Franc BEAC	XAF	950	Kwacha	MWK	454
CFP Franc	XPF	953	Kwacha	ZMW	967
Chilean Peso	CLP	152	Kwanza	AOA	973
Chinese Renminbi	CNH	157	Kyat	MMK	104
Chinese Renminbi	CNX	158	Lari	GEL	981
Colombian Peso	COP	170	Latvian Lats	LVL	428
Comoro Franc	KMF	174	Lebanese Pound	LBP	422
Congolese Franc	CDF	976	Lek	ALL	8
Convertible Marks	BAM	977	Lempira	HNL	340
Cordoba Oro	NIO	558	Leone	SLL	694
Costa Rican Colon	CRC	188	Liberian Dollar	LRD	430
Croatian Kuna	HRK	191	Libyan Dinar	LYD	434
Cruzeiro	BRC	76	Lilangeni	SZL	748
Cuban Peso	CUP	192	Lithuanian Litas	LTL	440
Cyprus Pound	CYP	196	Loti	LSL	426
Czech Koruna	CZK	203	Malagassy Franc	MGF	450
Dalasi	GMD	270	Malagasy Ariary	MGA	969
Danish Krone	DKK	208	Malaysian Ringgit	MYR	458
Denar	MKD	807	Mali	MLF	466
Dinar	BAM	70	Maltese Lira	MTL	470
Djibouti Franc	DJF	262	Manat	TMM	795
Dobra	STD	678	Manat	TMT	934
Dominican Peso	DOP	214	Mauritius Rupee	MUR	480
Dong	VND	704	Metical	MZN	943
East Caribbean Dollar	XCD	951	Mexican Peso	MXN	484
Egyptian Pound	EGP	818	Moldovan Leu	MDL	498

Anexo V. Códigos ISO divisas.

Moroccan Dirham	MAD	504	Singapore Dollar	SGD	702
Naira	566	556	Slovenian Tolar	SIT	705
Naira	NGN	566	Solomon Islands Dollar	SBD	90
Nakfa	ERN	232	Som	KGS	417
Namibia Dollar	NAD	516	Somali Shilling	SOS	706
Nepalese Rupee	NPR	524	Somoni	TJS	972
Netherlands Antillian Guilder	ANG	532	Sri Lanka Rupee	LKR	144
New Israeli Sheqel	ILS	376	Sudan Airlines	SDA	737
New Leu	RON	946	Sudanese Pound	SDP	736
New Taiwan Dollar	TWD	901	Surinam Dollar	SRD	968
New Zealand Dollar	NZD	554	Swedish Krona	SEK	752
Ngultrum	BTN	64	Swiss Franc	CHF	756
Norwegian Krone	NOK	578	Syrian Pound	SYP	760
Nuevo Sol	PEN	604	Tajik Ruble	TJR	762
Ouguiya	MRO	478	Taka	BDT	50
Pa'anga	TOP	776	Tala	WST	882
Pacific Island	PCI	582	Tanzanian Shilling	TZS	834
Pakistan Rupee	PKR	586	Tenge	KZT	398
Pataca	MOP	446	Timor Escudo	TPE	626
Peseta Convertible	ESB	995	Trinidad and Tobago Dollar	TTD	780
Peso Uruguayo	UYU	858	Tugrik	MNT	496
Philippine Peso	PHP	608	Tunisian Dinar	TND	788
Pound Sterling	GBP	826	Turkish Lira	PTL	793
Pula	BWP	72	Turkish Lira	TRY	949
Qatari Rial	QAR	634	UAE Dirham	AED	784
Quetzal	GTQ	320	Uganda Shilling	UGX	800
Rand	ZAR	710	US Dollar	USD	840
Rial Omani	OMR	512	Uzbekistan Sum	UZS	860
Riel	KHR	116	Vatu	VUV	548
Rowanda Franc	RWF	646	Won	KRW	410
Rufiyaa	MVR	462	Yemeni Dinar	YDD	720
Rupiah	IDR	360	Yemeni Rial	YER	886
Russian Ruble	RUB	643	Yen	JPY	392
Saint Helena Pound	SHP	654	Yuan Renminbi	CNY	156
Saudi Riyal	SAR	682	Yugoslavian New Dian	NTZ	536
Serbian Dinar	CSD	891	Zambian Kwacha	ZMK	894
Serbian Dinar	RSD	941	Zimbabwe Dollar	ZWD	716
Seychelles Rupee	SCR	690	Zloty	PLN	985

Anexo VI.

Ejemplos específicos

Pago de suscripciones y

Pagos Exprés

El presente Anexo recoge los ejemplos específicos de utilización de la funcionalidad Pago de Suscripciones / Pagos Exprés, para cada una de modalidades de procesamiento de operaciones en el TPV Virtual de Banco Sabadell

A continuación se incluyen varios ejemplos basados en un comercio que utilice la entrada “**realizarPago**” al SIS.

•Ejemplo 1:

Pago con petición de nuevo identificador

Se hace un pago y se añade el parámetro Ds_Merchant_Identifier con el valor REQUIRED para que se genere un identificador nuevo y se devuelva en la notificación junto con la fecha de caducidad. El identificador estará asociado al comercio indicado por el parámetro Ds_Merchant_MerchantCode.

Datos a enviar en la petición:

Ds_Merchant_MerchantCode=999008881
Ds_Merchant_Terminal=1
Ds_Merchant_Currency=978
Ds_Merchant_TransactionType=0
Ds_Merchant_Amount=100
Ds_Merchant_Order=112545

Ds_Merchant_Identifier=REQUIRED

Ds_Merchant_MerchantURL=<URL de notificación>
Ds_Merchant_MerchantSignature=<firma incluyendo el valor REQUIRED en la cadena de firma justo antes del valor de la clave>.

Respuesta en notificación on-line

Si la operación es autorizada, la notificación On-Line y la URL OK incluirán los nuevos parámetros con el valor del identificador generado y la caducidad de la tarjeta a modo de caducidad del identificador. El resto de los campos de la notificación no varían ni tampoco el cálculo de su firma.

Un ejemplo de identificador sería el siguiente:

Ds_Merchant_Identifier=a091f0f9f0aaf0506930dda4a6974f1df4a0d9c1

Ds_ExpiryDate=1412

•Ejemplo 2:

Pago con identificador

Se hace un pago y se añade el parámetro Ds_Merchant_Identifier con el valor del identificador a utilizar. En este caso, se podría usar el parámetro Ds_Merchant_DirectPayment con valor ‘true’ y el comportamiento sería el mismo.

Datos a enviar en la petición:

Ds_Merchant_MerchantCode=999008881
Ds_Merchant_Terminal=1
Ds_Merchant_Currency=978
Ds_Merchant_TransactionType=0
Ds_Merchant_Amount=100
Ds_Merchant_Order=112546<No tiene que ser el mismo de la operación original>
Ds_Merchant_Identifier=a091f0f9f0aaf0506930dda4a6974f1df4a0d9c1
Ds_Merchant_MerchantURL=<URL de notificación>
Ds_Merchant_MerchantSignature=<firma incluyendo el valor a091f0f9f0aaf0506930dda4a6974f1df4a0d9c1 en la cadena de firma justo antes del valor de la clave>.

•Ejemplo 3:

Pago con petición de nuevo identificador y código de grupo

Se hace un pago y se añade el parámetro Ds_Merchant_Identifier con el valor REQUIRED para que se genere un identificador nuevo y se devuelva en la notificación junto con la fecha de caducidad. El identificador estará asociado al grupo de comercios que se indique en el campo Ds_Merchant_Group.

Datos a enviar en la petición:

Ds_Merchant_MerchantCode=999008881
Ds_Merchant_Terminal=1

```
Ds_Merchant_Currency=978
Ds_Merchant_TransactionType=0
Ds_Merchant_Amount=100
Ds_Merchant_Order=112545
Ds_Merchant_Identifier=REQUIRED
Ds_Merchant_Group=777888991
Ds_Merchant_MerchantURL=<URL de notificación>
Ds_Merchant_MerchantSignature=<firma incluyendo el valor
REQUIRED777888991 en la cadena de firma justo antes del
valor de la clave >.
```

Respuesta en notificación on-line

Si la operación es autorizada, la notificación On-Line y la URL OK incluirán los nuevos parámetros con el valor del identificador generado y la caducidad de la tarjeta a modo de caducidad del identificador. El resto de los campos de la notificación no varían ni tampoco el cálculo de su firma.

Un ejemplo de identificador sería el siguiente:

```
Ds_Merchant_
Identifier=a091f0f9f0aaf0506930dda4a6974f1df4a0d9c1
Ds_ExpiryDate=1412
```

•Ejemplo 4:

Pago con identificador asociado a un grupo

Se hace un pago y se añade el parámetro Ds_Merchant_Identifier con el valor del identificador a utilizar y el campo Ds_Merchant_Group con el ID de grupo. En este caso, se podría usarse el parámetro Ds_Merchant_DirectPayment con valor 'true' y el comportamiento sería el mismo.

Datos a enviar en la petición:

```
Ds_Merchant_MerchantCode=999008881
Ds_Merchant_Terminal=1
Ds_Merchant_Currency=978
Ds_Merchant_TransactionType=0
Ds_Merchant_Amount=100
Ds_Merchant_Order=112546
Ds_Merchant_
Identifier=a091f0f9f0aaf0506930dda4a6974f1df4a0d9c1
Ds_Merchant_Group=777888991
Ds_Merchant_MerchantURL=<URL de notificación>
Ds_Merchant_MerchantSignature=<firma incluyendo el valor
a091f0f9f0aaf0506930dda4a6974f1df4a0d9c1777888991
en la cadena de firma justo antes del valor de la clave>.
```

•Ejemplo 5:

Pago con identificador y flag para no mostrar pantallas

Se hace un pago y se añaden los parámetros Ds_Merchant_Identifier con el valor del identificador a utilizar y Ds_Merchant_DirectPayment con el valor "true".

Datos a enviar en la petición:

```
Ds_Merchant_MerchantCode=999008881
Ds_Merchant_Terminal=1
Ds_Merchant_Currency=978
Ds_Merchant_TransactionType=0
Ds_Merchant_Amount=100
Ds_Merchant_Order=112546 <No tiene que ser el mismo de la
operación original>
Ds_Merchant_
Identifier=a091f0f9f0aaf0506930dda4a6974f1df4a0d9c1
Ds_Merchant_MerchantURL=<URL de notificación>
Ds_Merchant_DirectPayment=true
Ds_Merchant_MerchantSignature=<firma incluyendo el valor
a091f0f9f0aaf0506930dda4a6974f1df4a0d9c1true en la
cadena de firma justo antes del valor de la clave>.
```

•Ejemplo 6:

Pago con petición de nuevo identificador por entrada Web Service

Se hace un pago y se añade el elemento XML<DS_MERCHANT_IDENTIFIER> con el valor REQUIRED para que se genere un identificador nuevo y se devuelva en la respuesta XML junto con la fecha de caducidad. La referencia estará asociada al grupo de comercios que se indique en el elemento<DS_MERCHANT_GROUP>, si se define. En la petición original no se debe enviar el elemento <DS_MERCHANT_DIRECTPAYMENT>.

XML de petición:

```
<DATOSENTRADA>
<DS_Version>1.0</DS_Version>
<DS_MERCHANT_AMOUNT>200</DS_MERCHANT_
AMOUNT>
<DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CUR-
RENCY>
<DS_MERCHANT_MERCHANTURL>http://sis-d.redsys.es/
sis/reciboSoap.jsp</DS_MERCHANT_MERCHANTURL>
<DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_
TRANSACTIONTYPE>
<DS_MERCHANT_MERCHANTDATA>Alfombrilla</DS_MER-
```

```

CHANT_MERCHANTDATA>
<DS_MERCHANT_MERCHANTNAME>Comercio de Pruebas</
DS_MERCHANT_MERCHANTNAME>
<DS_MERCHANT_MERCHANTSIGNATURE>A0D5ACA3487D-
6FC8F0F37FCEB11883E26278C1C</DS_MERCHANT_
MERCHANTSIGNATURE>
<DS_MERCHANT_TERMINAL>22</DS_MERCHANT_TERMI-
NAL>
<DS_MERCHANT_MERCHANTCODE>079940722</DS_MER-
CHANT_MERCHANTCODE>
<DS_MERCHANT_ORDER>1305092720</DS_MERCHANT_
ORDER>
<DS_MERCHANT_PAN>4548810000000003</DS_MER-
CHANT_PAN>
<DS_MERCHANT_EXPIRYDATE>4912</DS_MERCHANT_EX-
PIRYDATE>
<DS_MERCHANT_CVV2>123</DS_MERCHANT_CVV2>
<DS_MERCHANT_IDENTIFIER>REQUIRED</DS_MERCHANT_
IDENTIFIER>
<DS_MERCHANT_GROUP>999008881</DS_MERCHANT_
GROUP>
</DATOSENTRADA>

```

Cálculo de la firma (con SHA-1 completo ampliado):
 Signature = DS_MERCHANT_AMOUNT + DS_MERCHANT_ORDER
 + DS_MERCHANT_MERCHANTCODE + DS_MERCHANT_
 CURRENCY + DS_MERCHANT_PAN + DS_MERCHANT_
 MERCHANTURL + DS_MERCHANT_CVV2 + DS_MERCHANT_
 TRANSACTIONTYPE + DS_MERCHANT_IDENTIFIER +
 DS_MERCHANT_GROUP + clave_secreta

Si suponemos que el valor de "clave_secreta" es
 qwertyasdf0123456789:

Data for signature = 200130509272007994072297845
 48810000000003http://sis-d.redsys.es/sis/reciboSoap.
 jsp1230REQUIRED999008881qwertyasdf0123456789

NOTA: Si alguno de los parámetros que se incluyen en la cadena de firma no se envía en la petición XML, no se debe considerar tampoco para la cadena de firma.

Respuesta XML

Si la operación es autorizada, el XML de respuesta incluirá los nuevos parámetros con el valor del identificador generado y la caducidad de la tarjeta a modo de caducidad de la referencia. En la notificación Online también se enviarán estos datos. El resto de los campos de la respuesta no varían ni tampoco el cálculo de su firma.

Un ejemplo de respuesta XML sería el siguiente:

```

<RETORNOXML>
<CODIGO>0</CODIGO>
<Ds_Version>1.0</Ds_Version>

```

```

<OPERACION>
<Ds_Amount>200</Ds_Amount>
<Ds_Currency>978</Ds_Currency>
<Ds_Order>1305092720</Ds_Order>
<Ds_Signature>7F8265CA61A47E0FCAF09B0D6B41C-
FAC6536ECBF</Ds_Signature>
<Ds_MerchantCode>079940722</Ds_MerchantCode>
<Ds_Terminal>22</Ds_Terminal>
<Ds_Response>0000</Ds_Response>
<Ds_AuthorisationCode>678905</Ds_AuthorisationCode>
<Ds_TransactionType>0</Ds_TransactionType>
<Ds_SecurePayment>0</Ds_SecurePayment>
<Ds_Language>1</Ds_Language>
<Ds_ExpiryDate>4912</Ds_ExpiryDate>
<Ds_Merchant_Identifier>3695d14811d31fa5fe3be1b-
98f3606be576328d5</Ds_Merchant_Identifier>
<Ds_Merchant_Group>999008881</Ds_Merchant_Group>
<Ds_MerchantData>Alfombrilla</Ds_MerchantData>
<Ds_Card_Country>724</Ds_Card_Country>
</OPERACION>
</RETORNOXML>

```

• Ejemplo 7: Pago usando un identificador por entrada Web Service

Se hace un pago y se añade el elemento XML<DS_MERCHANT_IDENTIFIER>con el valor de la referencia a utilizar. En este caso, se podría usar el elemento XML<DS_MERCHANT_DIRECTPAYMENT> con valor 'true' y no aplicaría DCC (en caso de haberlo).

XML de petición:

```

<DATOSENTRADA>
<DS_Version>1.0</DS_Version>
<DS_MERCHANT_AMOUNT>200</DS_MERCHANT_
AMOUNT>
<DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CUR-
RENCY>
<DS_MERCHANT_MERCHANTURL>http://sis-d.redsys.es/
sis/reciboSoap.jsp</DS_MERCHANT_MERCHANTURL>
<DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_
TRANSACTIONTYPE>
<DS_MERCHANT_MERCHANTDATA>Alfombrilla</DS_MER-
CHANT_MERCHANTDATA>
<DS_MERCHANT_MERCHANTNAME>Comercio de Pruebas</
DS_MERCHANT_MERCHANTNAME>
<DS_MERCHANT_MERCHANTSIGNATURE>A0D5ACA3487D-
6FC8F0F37FCEB11883E26278C1C</DS_MERCHANT_
MERCHANTSIGNATURE>
<DS_MERCHANT_TERMINAL>22</DS_MERCHANT_TERMI-
NAL>
<DS_MERCHANT_MERCHANTCODE>079940722</DS_MER-
CHANT_MERCHANTCODE>
<DS_MERCHANT_ORDER>1305092720</DS_MERCHANT_
ORDER>
<DS_MERCHANT_PAN>4548810000000003</DS_MER-
CHANT_PAN>
<DS_MERCHANT_EXPIRYDATE>4912</DS_MERCHANT_EX-
PIRYDATE>
<DS_MERCHANT_CVV2>123</DS_MERCHANT_CVV2>

```

```
<DS_MERCHANT_IDENTIFER>REQUIRED</DS_MERCHANT_IDENTIFER>
<DS_MERCHANT_GROUP>999008881</DS_MERCHANT_GROUP>
</DATOSENTRADA>
```

Cálculo de la firma (con SHA-1 completo ampliado):

Signature = DS_MERCHANT_AMOUNT + DS_MERCHANT_ORDER + DS_MERCHANT_MERCHANTCODE + DS_MERCHANT_CURRENCY + DS_MERCHANT_MERCHANTURL + DS_MERCHANT_TRANSACTIONTYPE + DS_MERCHANT_IDENTIFER + DS_MERCHANT_GROUP + DS_MERCHANT_DIRECTPAYMENT + clave_secreta

Si suponemos que el valor de "clave_secreta" es qwertyasdf0123456789:

Data for signature = 2001305095351079940722978http://sis-d.redsys.es/sis/reciboSoap.
jsp02e0817473e1ad57c3cb9dd78be14c645f2df5945

NOTA: Si alguno de los parámetros que se incluyen en la cadena de firma no se envía en la petición XML, no se debe considerar tampoco para la cadena de firma (en este caso, no se han enviado los campos DS_MERCHANT_GROUP y DS_MERCHANT_DIRECTPAYMENT por lo que no se ha considerado en la firma).

Respuesta XML

Si la operación es autorizada, el XML de respuesta incluirá también el parámetro con el valor del identificador enviado. En la notificación Online también se enviará este dato. El resto de los campos de la respuesta no varían ni tampoco el cálculo de su firma.

Un ejemplo de respuesta XML sería el siguiente:

```
<RETORNOXML>
<CODIGO>0</CODIGO>
<Ds_Version>1.0</Ds_Version>
<OPERACION>
<Ds_Amount>200</Ds_Amount>
<Ds_Currency>978</Ds_Currency>
<Ds_Order>1305095351</Ds_Order>
<Ds_Signature>A859865855BFE738D0E701B89C63CF49C160472F</Ds_Signature>
<Ds_MerchantCode>079940722</Ds_MerchantCode>
<Ds_Terminal>22</Ds_Terminal>
<Ds_Response>0000</Ds_Response>
<Ds_AuthorisationCode>325299</Ds_AuthorisationCode>
<Ds_TransactionType>0</Ds_TransactionType>
<Ds_SecurePayment>0</Ds_SecurePayment>
```

```
<Ds_Language>1</Ds_Language>
<Ds_MerchantIdentifier>2e0817473e1ad57c3cb9dd78be14c645f2df5945</Ds_MerchantIdentifier>
<Ds_MerchantData>Alfombrilla</Ds_MerchantData>
<Ds_Card_Country>724</Ds_Card_Country>
</OPERACION>
</DATOSENTRADA>
```

•Ejemplo 8: Pago con petición de nuevo identificador por entrada "operaciones"

Se hace un pago y se añade el elemento XML <DS_MERCHANT_IDENTIFER> con el valor REQUIRED para que se genere un identificador nuevo y se devuelva en la respuesta XML junto con la fecha de caducidad. La referencia estará asociada al grupo de comercios que se indique en el elemento <DS_MERCHANT_GROUP>, si se define. En la petición original no se debe enviar el elemento <DS_MERCHANT_DIRECTPAYMENT>.

XML de petición:

```
<DATOSENTRADA>
  <DS_Version>1.0</DS_Version>
  <DS_MERCHANT_AMOUNT>200</DS_MERCHANT_AMOUNT>
  <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CURRENCY>
  <DS_MERCHANT_MERCHANTURL>http://sis-d.redsys.es/sis/reciboSoap.jsp</DS_MERCHANT_MERCHANTURL>
  <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_TRANSACTIONTYPE>
  <DS_MERCHANT_MERCHANTDATA>Alfombrilla</DS_MERCHANT_MERCHANTDATA>
  <DS_MERCHANT_MERCHANTNAME>Comercio de Pruebas</DS_MERCHANT_MERCHANTNAME>
  <DS_MERCHANT_MERCHANTSIGNATURE>80C97C4CEAA4DC9F42812F2DB190B9A87B91DED7</DS_MERCHANT_MERCHANTSIGNATURE>
  <DS_MERCHANT_TERMINAL>22</DS_MERCHANT_TERMINAL>
  <DS_MERCHANT_MERCHANTCODE>079940722</DS_MERCHANT_MERCHANTCODE>
  <DS_MERCHANT_ORDER>1305092044</DS_MERCHANT_ORDER>
  <DS_MERCHANT_CLIENTIP>172.16.132.79</DS_MERCHANT_CLIENTIP>
  <DS_MERCHANT_PAN>4916710000000017</DS_MERCHANT_PAN>
  <DS_MERCHANT_EXPIRYDATE>4912</DS_MERCHANT_EXPIRYDATE>
  <DS_MERCHANT_CVV2>123</DS_MERCHANT_CVV2>
  <DS_MERCHANT_IDENTIFER>REQUIRED</DS_MERCHANT_IDENTIFER>
  <DS_MERCHANT_GROUP>999008881</DS_MERCHANT_GROUP>
</DATOSENTRADA>
```

Cálculo de la firma (con SHA-1 completo ampliado):

```
Signature = DS_MERCHANT_AMOUNT + DS_MERCHANT_ORDER
+ DS_MERCHANT_MERCHANTCODE + DS_MERCHANT_
CURRENCY + DS_MERCHANT_PAN + DS_MERCHANT_CVV2
+ DS_MERCHANT_TRANSACTIONTYPE + DS_MERCHANT_
IDENTIFIER + DS_MERCHANT_GROUP + clave_secreta
```

Si suponemos que el valor de "clave_secreta" es
qwertyasdf0123456789:

Datos para firma =

```
200130509204407994072297849167100000000171230
REQUIRED999008881
```

NOTA: Si alguno de los parámetros que se incluyen en la cadena de firma no se envía en la petición XML, no se debe considerar tampoco para la cadena de firma.

Respuesta XML

Si la operación es autorizada, el XML de respuesta incluirá los nuevos parámetros con el valor del identificador generado y la caducidad de la tarjeta a modo de caducidad de la referencia. En la notificación Online también se enviarán estos datos. El resto de los campos de la respuesta no varían ni tampoco el cálculo de su firma. Si la operación es autorizada, el XML de respuesta incluirá los nuevos parámetros con el valor del identificador generado y la caducidad de la tarjeta a modo de caducidad de la referencia. En la notificación Online también se enviarán estos datos. El resto de los campos de la respuesta no varían ni tampoco el cálculo de su firma.

Un ejemplo de respuesta XML sería el siguiente:

```
<?xml version='1.0' encoding='ISO-8859-1' ?>
<RETORNOMXML>
  <CODIGO>0</CODIGO>
  <Ds_Version>1.0</Ds_Version>
  <OPERACION>
    <Ds_Amount>200</Ds_Amount>
    <Ds_Currency>978</Ds_Currency>
    <Ds_Order>1305092044</Ds_Order>
    <Ds_Signature>5C9309C99EEF8A4E852A31CF-
F9825A4142B37D79</Ds_Signature>
    <Ds_MerchantCode>079940722</Ds_MerchantCode>
    <Ds_Terminal>22</Ds_Terminal>
    <Ds_Response>0000</Ds_Response>
    <Ds_AuthorisationCode>325300</Ds_AuthorisationCode>
    <Ds_TransactionType>0</Ds_TransactionType>
```

```
<Ds_SecurePayment>0</Ds_SecurePayment>
<Ds_Language>1</Ds_Language>
<Ds_ExpiryDate>4912</Ds_ExpiryDate>
<Ds_Merchant_Identifier>f7461007009513beb1f45baf0be-
ff2b11b96c162</Ds_Merchant_Identifier>
<Ds_Merchant_Group>999008881</Ds_Merchant_Group>
<Ds_MerchantData>Alfombrilla</Ds_MerchantData>
<Ds_Card_Country>724</Ds_Card_Country>
</OPERACION>
```

• Ejemplo 9: Pago usando un identificador por entrada "operaciones"

Se hace un pago y se añade el elemento XML <DS_MERCHANT_IDENTIFIER> con el valor del identificador a utilizar. En este caso, se podría usar el elemento XML <DS_MERCHANT_DIRECTPAYMENT> con valor 'true' y no aplicaría DCC (en caso de haberlo).

XML de petición:

```
<DATOSENTRADA>
  <DS_Version>1.0</DS_Version>
  <DS_MERCHANT_AMOUNT>200</DS_MERCHANT_
  AMOUNT>
  <DS_MERCHANT_CURRENCY>978</DS_MERCHANT_
  CURRENCY>
  <DS_MERCHANT_MERCHANTURL>http://sis-d.redsys.es/
  sis/reciboSoap.jsp</DS_MERCHANT_MERCHANTURL>
  <DS_MERCHANT_TRANSACTIONTYPE>0</DS_MERCHANT_
  TRANSACTIONTYPE>
  <DS_MERCHANT_MERCHANTDATA>Alfombrilla</DS_MER-
  CHANT_MERCHANTDATA>
  <DS_MERCHANT_MERCHANTNAME>Comercio de Pruebas</
  DS_MERCHANT_MERCHANTNAME>
  <DS_MERCHANT_MERCHANTSIGNATURE>14E8284634B-
  8CDFBA9C0ACA01CD259F7A6349D2E</DS_MERCHANT_
  MERCHANTSIGNATURE>
  <DS_MERCHANT_TERMINAL>22</DS_MERCHANT_
  TERMINAL>
  <DS_MERCHANT_MERCHANTCODE>079940722</DS_MER-
  CHANT_MERCHANTCODE>
  <DS_MERCHANT_ORDER>1305093030</DS_MERCHANT_
  ORDER>
  <DS_MERCHANT_CLIENTIP>172.16.132.79</DS_MER-
  CHANT_CLIENTIP>
  <DS_MERCHANT_IDENTIFIER>32539c31f319d3ad-
  67de24ed8fc5ec92e2c4124a</DS_MERCHANT_IDENTI-
  FIER>
  <DS_MERCHANT_DIRECTPAYMENT>true</DS_MERCHANT_
  DIRECTPAYMENT>
</DATOSENTRADA>
```

Cálculo de la firma (con SHA-1 completo ampliado):

```
Signature = DS_MERCHANT_AMOUNT + DS_MERCHANT_ORDER
+ DS_MERCHANT_MERCHANTCODE + DS_MERCHANT_
CURRENCY + DS_MERCHANT_TRANSACTIONTYPE +
DS_MERCHANT_IDENTIFIER + DS_MERCHANT_GROUP +
DS_MERCHANT_DIRECTPAYMENT + clave_secreta
```

Si suponemos que el valor de "clave_secreta" es
qwertyasdf0123456789:

Datos para firma =

2001305093030 079940722978032539c31f319d3ad67de
24ed8fc5ec92e2c4124atrue

NOTA: Si alguno de los parámetros que se incluyen en la cadena de firma no se envía en la petición XML, no se debe considerar tampoco para la cadena de firma (en este caso, no se ha enviado el campo DS_MERCHANT_GROUP por lo que no se ha considerado en la firma).

Respuesta XML

Si la operación es autorizada, el XML de respuesta incluirá también el parámetro con el valor del identificador enviado. En la notificación Online también se enviará este dato. El resto de los campos de la respuesta no varían ni tampoco el cálculo de su firma.

Un ejemplo de respuesta XML sería el siguiente:

```
<?xml version='1.0' encoding="ISO-8859-1" ?>
<RETORNOXML>
  <CODIGO>0</CODIGO>
  <Ds_Version>1.0</Ds_Version>
  <OPERACION>
    <Ds_Amount>200</Ds_Amount>
    <Ds_Currency>978</Ds_Currency>
    <Ds_Order>1305093030</Ds_Order>
    <Ds_Signature>384BB9675FEE4D88358079FCCC16B-
C2940B6F7AF</Ds_Signature>
    <Ds_MerchantCode>079940722</Ds_MerchantCode>
    <Ds_Terminal>22</Ds_Terminal>
    <Ds_Response>0000</Ds_Response>
    <Ds_AuthorisationCode>325302</Ds_AuthorisationCode>
    <Ds_TransactionType>0</Ds_TransactionType>
    <Ds_SecurePayment>0</Ds_SecurePayment>
    <Ds_Language>1</Ds_Language>
    <Ds_Merchant_Identifier>32539c31f319d3ad67de24ed8f-
c5ec92e2c4124a</Ds_Merchant_Identifier>
    <Ds_MerchantData>Alfombrilla</Ds_MerchantData>
    <Ds_Card_Country>724</Ds_Card_Country>
  </OPERACION>
</RETORNOXML>
```