TPV Virtual

Manual operativo y de instalación

Sabadell

Índice

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, pero ofrece una amplia gama de servicios y prestaciones específicas para el comercio electrónico.

El presente manual recoge las descripciones e instrucciones de instalación de los servicios de la solución TPV Virtual.

- **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 eCommerce. Esta solución se define en un manual adicional al presente. Si los pagos en su comercio necesitan de los servicios de TPV Virtual Plus, solicite el manual a su oficina o gestor de Banco Sabadell.

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 OpenSource 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 Para más información, o para solicitar los manuales de integración, contacte con nuestro servicio técnico (ver apartado 6.9 del manual).

Prestashop, Magento, Wordpress Woocommerce, OsCommerce, Zencart, Opencart, Wordpress E-Commerce y Virtuemart (Joomla).

Elementos de seguridad

Ofrecer los máximos elementos de seguridad es una de las prioridades de Banco Sabadell. Entre ellos, 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, **reportes 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*.

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 multidivisa** 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** (Dinamic 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 **multilenguaje**, 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.

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.

- **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.

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?

Según requisitos de las marcas de tarjetas (Visa y MasterCard) y del Banco de España, se requiere que cualquier tienda on-line con TPV virtual disponga de:

1. Carrito de compra o similar dónde los compradores soliciten la compra del producto o servicio. Para ello Banco Sabadell requerirá que la web esté accesible y permita una prueba de compra (en caso de páginas web en construcción, el comercio deberá facilitar acceso a su entorno de pruebas).

2. El “Aviso Legal” (o apartado similar) deberá contener el nombre comercial, identificación (CIF), domicilio social y datos de contacto del comercio.

3. En “Términos y Condiciones (o apartado similar) se debe incluir la política de devoluciones.

4. En el caso de que el comercio trabaje con un proveedor de servicios de pago, éste debe estar autorizado previamente por Banco Sabadell.

5. El domicilio y país del establecimiento deben aparecer en alguna de las páginas a las que el titular accede durante el proceso de pago (debe estar visible y nunca enlazable a una web externa).

Los requisitos anteriores serán validados por el equipo de Banco Sabadell durante el proceso de alta del tpv virtual. En caso de que alguno no esté implementado, nos pondremos en contacto con el comercio para su modificación. **Para evitar demoras, rogamos que el comercio verifique que dispone de los requisitos anteriores en el proceso de alta**.

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 autorización 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.
Aspectos operativos

4.1 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, quien 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")

NOTA: 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 dentro del período de tiempo máximo establecido por cada marca de tarjeta. 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 dentro del período de tiempo máximo establecido por cada marca de tarjeta y su importe debe ser menor, igual o un 15% superior al 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 el período de tiempo que establezcan las marcas de tarjetas.

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 = "O")

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

Si transcurrido el período de tiempo establecido por las marcas de la tarjeta 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 dentro del periodo de tiempo máximo establecido por cada marca de tarjeta 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 menor, igual, o mayor en un 15% al importe de la operación original, 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.

Operativa "Tarjeta en Archivo" para el 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 ma- yor 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.

En el apartado 6.8 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 6.9.2 del manual.

4.2 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 (charge-back). Para minimizar el porcentaje de charge-backs 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 fraude.

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 figuran 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 librar la mercancía al titular de tarjeta (bien por imposibilidad de estar en el lugar y en tiempo pactado para recibirlo, bien porque se trate de un regalo) se permitirá hacer el envío a una tercera

persona. En este caso, debería quedar registrado este supuesto en el formulario de pedido que el cliente realizó en el comercio, con la siguiente información:

- Persona autorizada, identificada con nombre y documento de identidad (DNI, Pasaporte, etc.). El pedido se ha de entregar únicamente a esa persona y el albarán de entrega debería de incluir la firma del receptor así como la anotación conforme se ha comprobado el documento de identidad proporcionado.

- 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 ha de recibir. La recepción ha de estar firmada por un empleado correctamente identificado del hotel y sellado por este. Además, en el comprobante de recepción debería constar que se ha comprobado que el receptor de la mercancía está alojado en el hotel.

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

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

_ Nombre del comercio

_ CIF/NIF del comercio

_ Código del comercio (FUC)

_ Número de autorización

_ Fecha 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.

4.3 Descriptor Flexible

Esta funcionalidad permite al comercio añadir información adicional sobre la operación que se está realizando con el fin de ayudar al titular de la tarjeta a identificar la compra en el extracto de operaciones realizadas con la tarjeta y, a la vez, evita posibles retrocesos al comercio.

Para activar esta funcionalidad, el comercio debe contactar con el Servicio Técnico de Soporte TPV Virtual de Banco Sabadell (apartado 6.9).

4.4 Operativa Importe 0

La operativa de Importe 0 permite al comercio validar la autenticidad de una tarjeta contra el emisor sin aplicar ningún cargo. Con carácter adicional, el comercio podrá solicitar la generación de una referencia para la tarjeta mientras se valida la misma.

Utilización de la operativa de Importe 0

Para utilizar la operativa de Importe 0 el comercio tiene tres opciones para construir la petición:

1. Construir la petición informado los parámetros que obedecen a los datos de tarjeta:

– Ds_Merchant_Amount = 0

– Ds_Merchant_Pan

– Ds_Merchant_ExpiryDate

– Ds_Merchant_Cvv2 (Opcional en función de la configuración del comercio)

2. Construir la petición informado los parámetros que obedecen a los datos de tarjeta y a la generación de referencia:

– Ds_Merchant_Amount = 0

– Ds_Merchant_Pan

– Ds_Merchant_ExpiryDate

– Ds_Merchant_Cvv2 (Opcional en función de la configuración del comercio)

– Ds_Merchant_Identifier = REQUIRED

3. Construir la petición informado el parámetro de generación de referencia:

– Ds_Merchant_Amount = 0

– Ds_Merchant_Identifier = REQUIRED

Esta última opción implica que el cliente tiene que estar presente durante la operación ya que deberá introducir los datos de tarjeta en la pantalla.

Ejemplo de petición y respuesta WS

A continuación se presenta un ejemplo en el que se solicita la generación de una referencia para la tarjeta mientras se valida la misma.

Petición

```
<REQUEST>
<DATOSENTRADA>
<DS_MERCHANT_MERCHANTCODE>999008881</
DS_MERCHANT_MERCHANTCODE>
<DS_MERCHANT_TERMINAL>871</DS_MERCHANT_
TERMINAL>
<DS_MERCHANT_AMOUNT>0</DS_MERCHANT_AMOU-
NT>
<DS_MERCHANT_ORDER>1467310037</DS_MER-
CHANT_ORDER>
<DS_MERCHANT_CURRENCY>978</DS_MERCHANT_
CURRENCY>
<DS_MERCHANT_PAN>491671******0017</
DS_MERCHANT_PAN>
<DS_MERCHANT_EXPIRYDATE>****</DS_MERCHANT_
EXPIRYDATE>
<DS_MERCHANT_CVV2>***</DS_MERCHANT_CVV2>
<DS_MERCHANT_TRANSACTIONTYPE>0</DS_MER-
CHANT_TRANSACTIONTYPE>
<DS_MERCHANT_IDENTIFIER>REQUIRED</DS_MER-
CHANT_IDENTIFIER>
</DATOSENTRADA>
<DS_SIGNATUREVERSION>HMAC_SHA256_V1</
DS_SIGNATUREVERSION>
<DS_SIGNATURE>0n95/3kZl9xl3/dz3/
h08yktiFxZRWK3m0IGcmR8+qA=</DS_SIGNATURE>
</REQUEST>
```

Respuesta

```
<RETORNOXML>
<CODIGO>0</CODIGO>
<OPERACION>
<Ds_Amount>0</Ds_Amount>

<Ds_Currency>978</Ds_Currency>
<Ds_Order>1467310037</Ds_Order>
<Ds_Signature>Xsj3sTYPOXtTO+eWogyLs1RxG5UI9VvZA
wRxB7AQ8fY=</Ds_Signature>
<Ds_MerchantCode>999008881</Ds_MerchantCode>
<Ds_Terminal>871</Ds_Terminal>
<Ds_Response>0000</Ds_Response>
<Ds_AuthorisationCode>446616</Ds_Authorisation-
Code>
<Ds_TransactionType>0</Ds_TransactionType>
<Ds_SecurePayment>0</Ds_SecurePayment>
<Ds_Language>1</Ds_Language>
<Ds_ExpiryDate>****</Ds_ExpiryDate>
<Ds_Merchant_Identifier>f30e9f8196cfa0616705fd5eb
ef39d9ab4ee5f38
</Ds_Merchant_Identifier>
<Ds_MerchantData></Ds_MerchantData>
<Ds_Card_Country>724</Ds_Card_Country>
</OPERACION>
</RETORNOXML>
```

5.
Módulo de administración del TPV virtual

5.1 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/bsabadell
- Entorno real: https://sis.REDSYS.es/canales/bsabadell

Se recomienda utilizar el navegador **Internet Explorer** para acceder, puesto que algunas funcionalidades solo son compatibles con este navegador.

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

5.2 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. Datos de usuario: permite modificar los datos de contacto del propio usuario.

2. Gestión usuarios: permite realizar todas las funciones de consulta, alta, baja y modificación de usuarios de comercios.

3. Alta usuario: permite generar de forma automática, a partir de un código de comercio y número de terminal, un usuario de acceso al módulo de administración con unas características o permisos establecidos por defecto y enviar los datos de dicho usuario al email del comercio especificado.

4. Cambiar contraseña: permite modificar la contraseña de acceso del usuario.

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 determinado.
2. **Comercio**: para gestionar las operaciones

realizadas por todos los terminales de un comercio.

5.3 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** naturales. Para ello deberá introducir una fecha de inicio y fin del período que desea consultar para localizar una operación.

Las consultas de operaciones en el módulo de administración están restringidas a períodos de 1 mes. Si se necesita consultar periodos más extensos deberán realizar consultas consecutivas de periodos de 31 días.

Para una mayor rapidez en la búsqueda, si conoce el número de pedido 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 BUSCAR 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 Nº Autorización o código de respuesta", tanto para operaciones aprobadas como denegadas, se corresponden con los definidos en tabla del apartado "6.4 Respuesta Online" del presente manual.

5.4 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. Se podrán realizar devoluciones de las operaciones realizadas en los últimos 365 días naturales.

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

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 ticket de devolución pudiendo imprimir o archivar si se desea.

Aquellos comercios que realicen operativa de preautorizaciones, pre-autenticaciones o preautorizaciones en diferido, podrán ge-

nerar confirmaciones y anulaciones de las mismas desde el módulo de administración del TPV Virtual.

5.5 Consulta de totales

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

Pulsando el botón de '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.

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

6.
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.

En el mensaje hay un campo adicional de seguridad donde los principales datos relacionados con la compra se transmiten codificados por el algoritmo Hash Sha-256.

6.1 Formulario de pago de la web del comercio

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

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

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

El formulario de pago deberá mostrarse siempre en una ventana distinta, donde se visualice la url anteriormente indicada, de forma que el comprador pueda identificar que se encuentra en el entorno de pago de Banco Sabadell.

Para comercios CES, **la ventana donde se abra el TPV Virtual ha de tener barras de desplazamiento vertical y horizontal** para poder adaptarse a las diferentes páginas de autenticación que pudieran mostrarse al comprador en procesos posteriores.

A continuación se indican los datos que deberá contener el formulario de pago:

DATO	NOMBRE DEL CAMPO	COMENTARIOS
Versión de firma	Ds_SignatureVersion	Constante que indica la versión de firma que se está utilizando.
Datos de la operación	Ds_MerchantParameters	Cadena en formato JSON con todos los parámetros de la petición codificada en Base 64
Firma	Ds_Signature	Resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior.

Para la creación del campo **Ds_MerchantParameters**, deberán utilizarse todos los campos marcados como obligatorio en la tabla que se muestra a continuación. El resto de campos son opcionales y podrán incluirse si el comercio lo desea.

DATO	NOMBRE DEL CAMPO	LONG.	COMENTARIOS
Número de comercio. Código FUC	Ds_Merchant_ MerchantCode	9 N	**Obligatorio**. Código fijo asignado por Banco Sabadell.
Número de terminal	Ds_MerchantParameters	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. Número de terminal que le asignará su banco. Tres se considera su longitud máxima
Número de pedido	Ds_Merchant_Order	Mín. 4N Máx. 12 AN Para “Tarjeta en Archivo” el campo debe ser máx.10 posiciones, ya que el TPV Virtual añadirá 2 posiciones más para indicar el número de orden	**Obligatorio**. Los 4 primeros dígitos deben ser numéricos, para los dígitos restantes Sólo utilizar los siguientes caracteres ASCII Del30=0al39=9 Del65=Aal90=Z Del97=aal122=z El código ha de ser diferente de transacciones anteriores.
Importe	Ds_Merchant_ Amount	12 N	**Obligatorio**. Las dos últimas posiciones se consideran decimales, excepto en Yenes.
Moneda	Ds_Merchant_Currency	4 N	**Obligatorio**. 978 – EURO 840 – USD 826 – GBP 392 – JPY 756 – CHF 124 – CAD 4 se considera su longitud máxima

Tipo de transacción	Ds_Merchant_ TransactionType	1 N	**Obligatorio**. 0 - Pago estándar 1 - Preautorización 2 - Confirmación de Preautorización 3 - Devolución parcial o total 7 - Autenticación 8 - Confirmación de Autenticación 9 - Anulación de Preautorización L - Tarjeta en Archivo Inicial M - Tarjeta en Archivo Sucesiva O - Preautorización Diferida P - Confirmación de Preautorización Diferida Q - Anulación de Preautorización Diferida
Descripción del Producto	Ds_Merchant_ ProductDescription	Máx. 125 AN	Opcional. 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	Opcional. Este campo se mostrará al titular en la pantalla de confirmación de la compra.
URL	Ds_Merchant_ MerchantURL	250 AN	Obligatorio si el comercio tiene notificación “online”. URL del comercio que recibirá una comunicacion en segundo plano (vía post) con los datos de la transacción.
URLOK	Ds_Merchant_UrlOK	250 AN	**Opcional**. URL donde se redirigirá al titular cuando pulse en el botón “Continuar” o “Cerrar”, una vez la operación haya finalizado.
URLKO	Ds_Merchant_UrlKO	250 AN	**Opcional**. URL donde se redirigirá al titular cuando pulse en el botón “Continuar” o “Cerrar”, una vez la operación haya finalizado.
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 12 – Gallego 7– Italiano 2 – Inglés 3 – Catalán 4 – Francés 5 – Alemán 6 – Holandés 1 – Castellano 13 – Euskera 8 – Sueco 9 – Portugués 10 – Valenciano 11 – Polaco

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).
Código de autorización	Ds_Merchant_ Authorisation-Code	6 N	Opcional.
Identificador	Ds_Merchant_ Identifier	Max. 40 AN	Campo exclusivo de pago por referencia. El valor del campo es obligatorio para el primer pago. Para segundo pago y sucesivos, el valor será el identificador queel Banco ha facilitado en el mensaje de respuesta del primerpago.
Grupo de comercios	Ds_Merchant_ Group	Max. 9 N	Campo exclusivo de pago por referencia. Opcional. Permite asociar una referencia a un conjunto de comercios.
Pantallas adicionales	Ds_Merchant_Di-rectPayment	True' or 'false'	Campo exclusivo de pago por referencia. Opcional. Este parámetro funciona como un flag que indica si se no deben mostrarse pantallas adicionales (DCC, Fraccionamiento, Autenticación, etc.)

Ejemplo de formulario de envío de petición

A continuación se muestra un ejemplo del formulario de petición de pago:

Ejemplo de formulario de pago **sin envío** de datos de tarjeta:

```
<form id="form1" method="post" action="https://sis-t.
redsys.es:25443/sis/realizarPago" target="_blank">
<input type="hidden" name="Ds_SignatureVersion"
value="HMAC_SHA256_V1" />
<input type="hidden" name="Ds_MerchantParameters"
value="eyJEU19NRVJDSEFOVF9BTU9VTlQiOiIxNDUiLCJE-
U19NRVJDSEFOVF9PUkRFUiI6MTQ2Mjc5NjIwMiwiRFNfTUV
SQ0hBTlRfTUVSQ0hBTlRDT0RFIjoiMzI3MjM0Njg4IiwiRFNf-
TUVSQ0hBTlRfQ1VSUkVOQ1kiOiI5NzgiLCJEU19NRVJDSE-
FOVF9UUkFOU0FDVElPTlRZUEUiOiIwIiwiRFNfTUVSQ0hBTl-
RfVEVSTUlOQUwiOiIxIiwiRFNfTUVSQ0hBTlRfTUVSQ0hBTl-
RVUkwiOiJodHRwOlwvXC93d3cud2ViZGVsY29tZXJjaW8u-
Y29tXC91cmxkZW5vdGlmaWNhY2lvbi5waHAiLCJEU-
19NRVJDSEFOVF9VUkxPSyI6Imh0dHA6XC9cL3d3d-
y53ZWJkZWxjb21lcmNpby5jb21cL3VybG9rLnBocCIsIkR-
TX01FUkNIQU5UX1VSTEtPIjoiaHR0cDpcL1wvd3d3LndlYmRl-
bGNvbWVyY2lvLmNvbVwvdXJsa28ucGhwIn0=" />
<input type="hidden" name="Ds_Signature" value="arbjAns
wMyybenZIBKqxS8Fdw4nSWRdRXfmTPhHZkJg=" />
</form>
```

Ejemplo de formulario de pago **con envío** de datos de tarjeta:

```
<form id="form1" method="post" action="https://sis-t.
redsys.es:25443/sis/realizarPago" target="_blank">
<input type="hidden" name="Ds_SignatureVersion"
value="HMAC_SHA256_V1" />
<input type="hidden" name="Ds_MerchantParameters"
value="eyJEU19NRVJDSEFOVF9BTU9VTlQiOiIxNDUi-
LCJEU19NRVJDSEFOVF9PUkRFUiI6MTQ2Mjc5NTk1M-
SwiRFNfTUVSQ0hBTlRfTUVSQ0hBTlRDT0RFIjoiMzI3
MjM0Njg4IiwiRFNfTUVSQ0hBTlRfQ1VSUkVOQ1kiOiI5NzgiL-
CJEU19NRVJDSEFOVF9UUkFOU0FDVElPTlRZUEUiOiIwIiwiR-
FNfTUVSQ0hBTlRfVEVSTUlOQUwiOiIxIiwiRFNfTUVSQ0hBTl-
RfTUVSQ0hBTlRVUkwiOiJodHRwOlwvXC93d3cud2ViZGVs-
Y29tZXJjaW8uY29tXC91cmxkZW5vdGlmaWNhY2lvbi5wa-
HAiLCJEU19NRVJDSEFOVF9VUkxPSyI6Imh0dHA6XC-
9cL3d3dy53ZWJkZWxjb21lcmNpby5jb21cL3VybG9rL-
nBocCIsIkRTX01FUkNIQU5UX1VSTEtPIjoiaHR0cDp-
cL1wvd3d3LndlYmRlbGNvbWVyY2lvLmNvbVwvdXJsa28u-
cGhwIiwiRFNfTUVSQ0hBTlRfUEFOIjoiNDUOODgxMjA0O-
TQwMDAwNCIsIkRTX01FUkNIQU5UX0VYUEISWURB-
VEUiOiIxNjEyIiwiRFNfTUVSQ0hBTlRfQ1ZWMiI6IjEyMyJ9" />
<input type="hidden" name="Ds_Signa-
ture" value="wLirBHcT3mc01WmwuE2/
qy1cL6o46D+eJjlp5dih/40=" />
</form>
```

Para facilitar la integración del comercio, a continuación se explica de forma detallada

los pasos a seguir para montar el formulario de petición de pago.

6.1.1 Identificar la versión de algoritmo de firma a utilizar

En la petición se debe identificar la versión concreta de algoritmo que se está utilizando para la firma. Actualmente se utiliza el valor **HMAC_SHA256_V1** para identificar la versión de todas las peticiones, por lo que este será el valor del parámetro **Ds_SignatureVersion**, tal y como se puede observar en el ejemplo de formulario mostrado anteriormente.

6.1.2 Generar la cadena de datos de la petición

Se debe generar una cadena con todos los datos de la petición en formato JSON. JSON es un formato abierto de intercambio de datos basado en texto. Al igual que el XML está diseñado para ser legible e independiente de la plataforma tecnológica. La codificación de datos en JSON es muy ligera por lo que es ideal para intercambio de datos en aplicaciones Web.

El nombre de cada parámetro debe indicarse en mayúsculas o con estructura "CamelCase" (Por ejemplo: DS_MERCHANT_AMOUNT o Ds_Merchant_Amount). La lista de parámetros que se pueden incluir en la petición se describen en el apartado **6.1 Formulario de pago de la web del comercio**. A continuación se muestra un ejemplo del objeto JSON de una petición:

Ejemplo **sin envío** de datos de tarjeta:

{"DS_MERCHANT_AMOUNT":"145","DS_MERCHANT_ORDER":1462796202,"DS_MERCHANT_MERCHANTCODE":"327234688","DS_MERCHANT_CURRENCY":"978","DS_MERCHANT_TRANSACTIONTYPE":"0","DS_MERCHANT_TERMINAL":"1","DS_MERCHANT_MERCHANTURL":"http:\/\/www.webdelcomercio.com\/urldenotificacion.php","DS_MERCHANT_URLOK":"http:\/\/www.webdelcomercio.com\/urlok.php","DS_MERCHANT_URLKO":"http:\/\/www.webdelcomercio.com\/urlko.php"}

Ejemplo **con envío** de datos de tarjeta:

{"DS_MERCHANT_AMOUNT":"145","DS_MERCHANT_ORDER":1462795951,"DS_MERCHANT_MERCHANTCODE":"327234688","DS_MERCHANT_CURRENCY":"978","DS_MERCHANT_TRANSACTIONTYPE":"0","DS_MERCHANT_TERMINAL":"1","DS_MERCHANT_MERCHANTURL":"http:\/\/www.webdelcomercio.com\/urldenotificacion.php","DS_MERCHANT_URLOK":"http:\/\/www.webdelcomercio.com\/urlok.php","DS_MERCHANT_URLKO":"http:\/\/www.webdelcomercio.com\/urlko.php","DS_MERCHANT_PAN":"4548812049400004","DS_MERCHANT_EXPIRYDATE":"1612","DS_MERCHANT_CVV2":"533"}

Una vez montada la cadena JSON con todos los campos, es necesario codificarla en BASE64 sin retornos de carro para asegurarnos de que se mantiene constante y no es alterada en su paso por el navegador del cliente/comprador.

A continuación se muestra el objeto JSON que se acaba de mostrar codificado en BASE64:

Ejemplo JSON codificado **sin envío** de datos de tarjeta:

eyJEU19NRVJDSEFOVF9BTU9VTlQiOiIxNDUiLCJEU19NRVJDSEFOVF9PUkRFUiI6MTQ2Mjc5NjIwMiwiRFNfTUVSQ0hBTlRfTUVSQ0hBTlRDT0RFljoiMzI3MjM0Njg4IiwiRFNfTUVSQ0hBTlRfQ1VSUkVOQ1kiOiI5NzgiLCJEU19NRVJDSEFOVF9UUkFOU0FDVElPTlRZUEUiOiIwIiwiRFNfTUVSQ0hBTlRfVEVSTUlOQUwiOiIxIiwiRFNfTUVSQ0hBTlRfTUVSQ0hBTlRVUkwiOiJodHRwOlwvXC93d3cud2ViZGVsY29tZXJjaW8uY29tXC91cmxva28ucGhwIiwiRFNfTUVSQ0hBTlRfTUVSQ0hBTlRfVVJMT0siOiJodHRwOlwvXC93d3cud2ViZGVsY29tZXJjaW8uY29tXC91cmxrby5waHAiLCJEU19NRVJDSEFOVF9VUkxPSyI6Imh0dHA6XC9cL3d3dy53ZWJkZWxjb21lcmNpby5jb21cL3VybG9rLnBocCIsIkRTX01FUkNIQU5UX1VSTEtPIjoiaHR0cDpcL1wvd3d3LndlYmRlbGNvbWVyY2lvLmNvbVwvdXJsa28ucGhwIn0=

Ejemplo JSON codificado **con envío** de datos de tarjeta:

eyJEU19NRVJDSEFOVF9BTU9VTlQiOiIxNDUiLCJEU19NRVJDSEFOVF9PUkRFUiI6MTQ2Mjc5NTk1MSwiRFNfTUVSQ0hBTlRfTUVSQ0hBTlRDT0RFljoiMzI3MjM0Njg4IiwiRFNfTUVSQ0hBTlRfQ1VSUkVOQ1kiOiI5NzgiLCJEU19NRVJDSEFOVF9UUkFOU0FDVElPTlRZUEUiOiIwIiwiRFNfTUVSQ0hBTlRfVEVSTUlOQUwiOiIxIiwiRFNfTUVSQ0hBTlRfTUVSQ0hBTlRVUkwiOiJodHRwOlwvXC93d3cud2ViZGVsY29tZXJjaW8uY29tXC91cmxva28ucGhwIiwiRFNfTUVSQ0hBTlRfTUVSQ0hBTlRfVVJMT0siOiJodHRwOlwvXC93d3cud2ViZGVsY29tZXJjaW8uY29tXC91cmxrby5waHAiLCJEU19NRVJDSEFOVF9VUkxPSyI6Imh0dHA6XC9cL3d3dy53ZWJkZWxjb21lcmNpby5jb21cL3VybG9rLnBocCIsIkRTX01FUkNIQU5UX1VSTEtPIjoiaHR0cDpcL1wvd3d3LndlYmRlbGNvbWVyY2lvLmNvbVwvdXJsa28ucGhwIn0=

La cadena resultante de la codificación en BASE64 del JSON creado será el valor del

parámetro Ds_MerchantParameters, tal y como se puede observar en el ejemplo de formulario mostrado al inicio de este apartado.

6.1.3 Identificar la clave a utilizar para la firma

Para calcular la firma es necesario utilizar una clave específica para cada terminal. La clave de comercio que debe utilizar es la que recibió a través de SMS desde Banco Sabadell.

NOTA IMPORTANTE: Esta clave debe ser almacenada en el servidor del comercio de la forma más segura posible para evitar un uso fraudulento de la misma. El comercio es responsable de la adecuada custodia y mantenimiento en secreto de dicha clave.

6.1.4 Firmar los datos de la petición

Una vez se ha creado la cadena de datos a firmar y la clave específica del terminal se debe calcular la firma siguiendo los siguientes pasos:

1. Se genera una clave específica por operación. Para obtener la clave derivada a utilizar en una operación se debe realizar un cifrado 3DES entre la clave del comercio, la cual debe ser previamente decodificada en BASE 64, y el valor del número de pedido de la operación (Ds_Merchant_Order).

2. Se calcula el HMAC SHA256 del valor del parámetro Ds_MerchantParameters y la clave obtenida en el paso anterior.

3. El resultado obtenido se codifica en BASE 64, y el resultado de la codificación será el valor del parámetro Ds_Signature, tal y como se puede observar en el ejemplo de formulario mostrado al inicio del apartado 3.

6.1.5 Utilización de librerías de ayuda

En los apartados anteriores se ha descrito la forma de enviar la petición de pago utilizando conexión por la entrada **Realizar Pago** y el sistema de firma basado en HMAC SHA256. En este apartado se explica cómo se utilizan las librerías disponibles en PHP, JAVA y .NET para facilitar los desarrollos y la generación de los campos del formulario de pago. El uso de las librerías suministradas por Banco Sabadell es opcional, si bien simplifican los desarrollos a realizar por el comercio.

6.1.5.1 Librería PHP

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería PHP proporcionada por Banco Sabadell:

1. Importar el fichero principal de la librería, tal y como se muestra a continuación:

```
include("./apiRedsys.php");
```

El comercio debe decidir si la importación desea hacerla con la función "include" o "required", según los desarrollos realizados.

2. Definir un objeto de la clase principal de la librería, tal y como se muestra a continuación:

```
$miObj = new RedsysAPI;
```

3. Calcular el parámetro **Ds_MerchantParameters**. Para llevar a cabo el cálculo de este parámetro, inicialmente se deben añadir todos los parámetros de la petición de pago que se desea enviar.

   Importante: no existe un orden específico a la hora de añadir los parámetros, por lo que se podrán incluir en el orden que se desee.

   Ejemplo de parámetros **sin envío** de datos de tarjeta:

```
$miObj->setParameter("DS_MERCHANT_AMOUNT",
$importe);
$miObj->setParameter("DS_MERCHANT_ORDER",
strval($numPedido));
$miObj->setParameter("DS_MERCHANT_MERCHANTCO-
DE", $merchantCode);
$miObj->setParameter("DS_MERCHANT_CURRENCY",
$moneda);
$miObj->setParameter("DS_MERCHANT_TRANSACTION-
TYPE", $transactionType);
$miObj->setParameter("DS_MERCHANT_TERMINAL",
$terminal);
$miObj->setParameter("DS_MERCHANT_MERCHAN-
TURL", $merchantURL);
$miObj->setParameter("DS_MERCHANT_URLOK",
$urlOK);
$miObj->setParameter("DS_MERCHANT_URLKO",
$urlKO);
```

Ejemplo de parámetros **con envío** de datos de tarjeta:

```
$miObj->setParameter("DS_MERCHANT_AMOUNT",
$importe);
$miObj->setParameter("DS_MERCHANT_ORDER",
strval($numPedido));
$miObj->setParameter("DS_MERCHANT_MERCHANTCO-
DE", $merchantCode);
$miObj->setParameter("DS_MERCHANT_CURRENCY",
$moneda);
$miObj->setParameter("DS_MERCHANT_TRANSACTION-
TYPE", $transactionType);
$miObj->setParameter("DS_MERCHANT_TERMINAL",
$terminal);
$miObj->setParameter("DS_MERCHANT_MERCHAN-
TURL", $merchantURL);
$miObj->setParameter("DS_MERCHANT_URLOK",
$urlOK);
$miObj->setParameter("DS_MERCHANT_URLKO",
$urlKO);
$miObj->setParameter("DS_MERCHANT_PAN", $numTar-
jeta);
$miObj->setParameter("DS_MERCHANT_EXPIRYDATE",
$fechaCaducidad);
$miObj->setParameter("DS_MERCHANT_CVV2", $cvv2);
```

Por último, para calcular el parámetro **Ds_MerchantParameters**, se debe llamar a la función de la librería "createMerchantParameters()", tal y como se muestra a continuación:

```
$params = $miObj->createMerchantParameters();
```

4. Calcular el parámetro **Ds_Signature**. Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería "createMerchantSignature()"con la clave de comercio facilitada, tal y como se muestra a continuación:

```
$clave = 'sq7HjrUOBfKmC576ILgskD5srU870gJ7';
$firma = $miObj->createMerchantSignature($clave);
```

5. Una vez obtenidos los valores de los parámetros **Ds_MerchantParameters** y **Ds_Signature**, se debe rellenar el formulario de pago con dichos valores, tal y como se muestra a continuación:

```
<form name="form" action="https://sis-t.redsys.
es:25443/sis/realizarPago"
method="POST" target="_blank">
  <input type="hidden" name="Ds_SignatureVersion"
  value="<HMAC_SHA256_V1>"/>
  <input type="hidden" name="Ds_MerchantParame-
  ters" value="<?php echo $params; ?>"/>
  <input type="hidden" name="Ds_Signature"
  value="<?php echo $Signature; ?>" />
  <input type="submit" value="Realizar Pago" />
</form>
```

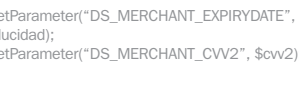
6.1.5.2 Librería JAVA

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería JAVA proporcionada por Banco Sabadell:

1. Importar la librería, tal y como se muestra a continuación:

```
<%@page import="sis.redsys.api.ApiMacSha256"%>
```

   El comercio debe incluir en la vía de construcción del proyectotodas las librerías (JARs) que se proporcionan:



2. Definir un objeto de la clase principal de la librería, tal y como se muestra a continuación:

```
ApiMacSha256 apiMacSha256 = new ApiMacSha256();
```

3. Calcular el parámetro **Ds_MerchantParameters**. Para llevar a cabo el cálculo de este parámetro, inicialmente se deben añadir todos los parámetros de la petición de pago que se desea enviar.

   Importante: no existe un orden específico a la hora de añadir los parámetros, por lo que se podrán incluir en el orden que se desee.

Ejemplo de parámetros **sin envío** de datos de tarjeta:

```
apiMacSha256.setParameter("DS_MERCHANT_AMOUNT", importe);
apiMacSha256.setParameter("DS_MERCHANT_ORDER", numPedido);
apiMacSha256.setParameter("DS_MERCHANT_MERCHANTCODE", merchantCode);
apiMacSha256.setParameter("DS_MERCHANT_CURRENCY", moneda);
apiMacSha256.setParameter("DS_MERCHANT_TRANSACTIONTYPE", transactionType);apiMacSha256.
setParameter("DS_MERCHANT_TERMINAL", terminal);
apiMacSha256.setParameter("DS_MERCHANT_MERCHANTURL", merchantURL);
apiMacSha256.setParameter("DS_MERCHANT_URLOK", urlOK)
apiMacSha256.setParameter("DS_MERCHANT_URLKO", urlKO);
```

Ejemplo de parámetros **con envío** de datos de tarjeta:

```
apiMacSha256.setParameter("DS_MERCHANT_AMOUNT", importe);
apiMacSha256.setParameter("DS_MERCHANT_ORDER", numPedido);
apiMacSha256.setParameter("DS_MERCHANT_MERCHANTCODE", merchantCode);
apiMacSha256.setParameter("DS_MERCHANT_CURRENCY", moneda);
apiMacSha256.setParameter("DS_MERCHANT_TRANSACTIONTYPE", transactionType);
apiMacSha256.setParameter("DS_MERCHANT_TERMINAL", terminal);
apiMacSha256.setParameter("DS_MERCHANT_MERCHANTURL", merchantURL);
apiMacSha256.setParameter("DS_MERCHANT_URLOK", urlOK);
apiMacSha256.setParameter("DS_MERCHANT_URLKO", urlKO);
apiMacSha256.setParameter("DS_MERCHANT_PAN", numTarjeta);
apiMacSha256.setParameter("DS_MERCHANT_EXPIRYDATE", expiryDate);
apiMacSha256.setParameter("DS_MERCHANT_CVV2", cvv2);
```

Por último se debe llamar a la función de la librería "createMerchantParameters()", tal y como se muestra a continuación:

```
String params = apiMacSha256.createMerchantParameters();
```

4. Calcular el parámetro **Ds_Signature**. Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería "createMerchantSignature()"con la clave de comercio facilitada, tal y como se muestra a continuación:

```
String clave = "sq7HjrUOBfKmC576ILgskD5srU870gJ7";
String firma = apiMacSha256.
createMerchantSignature(clave);
```

5. Una vez obtenidos los valores de los parámetros **Ds_MerchantParameters** y **Ds_Signature**, se debe rellenar el formulario de pago con los valores obtenidos, tal y como se muestra a continuación:

```
<form action="https://sis-t.redsys.es:25443/sis/
realizarPago"
method="POST" target="_blank">
<input type="hidden" name="Ds_SignatureVersion"
value="HMAC_SHA256_V1" />
<input type="hidden" name="Ds_MerchantParameters"
value="<%= params %>" />
<input type="hidden" name="Ds_Signature"
value="<%= firma %>" />
<input type="submit" value="Realizar Pago" />
</form>
```

6.1.5.3 Librería .NET

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería .NET proporcionada por Redsys:

1. Importar la librería RedsysAPI y Newronsoft. Json en su proyecto.
2. Calcular el parámetro **Ds_MerchantParameters**. Para llevar a cabo el cálculo de este parámetro, inicialmente se deben añadir todos los parámetros de la petición de pago que se desea enviar.

   Importante: no existe un orden específico a la hora de añadir los parámetros, por lo que se podrán incluir en el orden que se desee.

   Ejemplo de parámetros **sin envío** de datos de tarjeta:

```
//Creación del objeto
RedsysAPI r = new RedsysAPI();

//Se incluyen los parámetros
r.SetParameter("DS_MERCHANT_AMOUNT",importe);
r.SetParameter("DS_MERCHANT_ORDER",numPedido);
r.SetParameter("DS_MERCHANT_
MERCHANTCODE",merchantCode);
r.SetParameter("DS_MERCHANT_CURRENCY",moneda);
r.SetParameter("DS_MERCHANT_TRANSACTIONTYPE",
transactionType);
r.SetParameter("DS_MERCHANT_TERMINAL",terminal);
r.SetParameter("DS_MERCHANT_
MERCHANTURL",merchantURL);
```

```
r.SetParameter("DS_MERCHANT_URLOK",urlOK);
r.SetParameter("DS_MERCHANT_URLKO",urlKO);
```

Ejemplo de parámetros **con envío** de datos de tarjeta:

```
//Creación del objeto
RedsysAPI r = new RedsysAPI();

//Se incluyen los parámetros
r.SetParameter("DS_MERCHANT_AMOUNT",importe);
r.SetParameter("DS_MERCHANT_ORDER",numPedido);
r.SetParameter("DS_MERCHANT_
MERCHANTCODE",merchantCode);
r.SetParameter("DS_MERCHANT_CURRENCY",moneda);
r.SetParameter("DS_MERCHANT_TRANSACTIONTYPE",
transactionType);
r.SetParameter("DS_MERCHANT_TERMINAL",terminal);
r.SetParameter("DS_MERCHANT_
MERCHANTURL",merchantURL);
r.SetParameter("DS_MERCHANT_URLOK",urlOK);
r.SetParameter("DS_MERCHANT_URLKO",urlKO);
r.SetParameter("DS_MERCHANT_PAN",numTarjeta);
r.SetParameter("DS_MERCHANT_
EXPIRYDATE",expiryDate);
r.SetParameter("DS_MERCHANT_CVV2",cvv2);
```

Por último se debe llamar a la función de la librería "createMerchantParameters()", tal y como se muestra a continuación:

```
string signature = r.createMerchantSignature(clave);
Ds_Signature.Value = signature;
```

3. Calcular el parámetro **Ds_Signature**. Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería "createMerchantSignature()" con la clave de comercio facilitada, tal y como se muestra a continuación:

```
string signature = r.createMerchantSignature(clave);
Ds_Signature.Value = signature;
```

4. Una vez obtenidos los valores de los parámetros **Ds_MerchantParameters** y **Ds_Signature**, se debe rellenar el formulario de pago con los valores obtenidos, tal y como se muestra a continuación:

```
<form action=" https://sis-t.redsys.es:25443/sis/
realizarPago" method="post">

<input runat="server" type="text" id="Ds_Signature_
Version" name="Ds_SignatureVersion" value="HMAC_
SHA256_V1" />

<input runat="server" type="hidden" id="Ds_Mer-
chantParameters"

name="Ds_MerchantParameters" value="eyJEU19NRVJ-
DSEFOVF9BTU9VTlQiOiIxNDUiLCJEU19NRVJDSEFOV
F9PUkRFUiI6MTQ2Mjc5NjIwMiwiRFNfTUVSQ0hBTlRf-
TUVSQ0hBTlRDT0RFIjoiMzI3MjM0Njg4IiwiRFNf-TUVS-
Q0hBTlRfQ1VSUkVOQ1kiOiI5NzgiLCJEU19NRVJDSEFO-
VF9UUkFOU0FDVElPTIRZUEUiOiIwIiwiRFNfTUVSQ0hBTl-
RfVEVSTUlOQUwiOiIxIiwiRFNfTUVSQ0hBTlRfTUVSQ0hBTl-
RVUkwiOiJodHRwOlwvXC93d3cud2ViZGVsY29tZXJjaW8u-
Y29tXC91cmxkZW5vdGlmaWNhY2lvbi5waHAiLCJEU-
19NRVJDSEFOVF9VUkxPSyI6Imh0dHA6XC9cL3d3d-
y53ZWJkZWxjb21lcmNpby5jb21cL3VybG9rLnBoc-
CIsIkRTX01FUkNIQU5UX1VSTEtPIjoiaHR0cDp-
cL1wvd3d3LndlYmRlbGNvbWVyY2lvLmNvbVwvdXJsa28u-
cGhwIn0=" />

<input runat="server" type="hidden" id="Ds_Signature"
name="Ds_Signature" value="arbjAns wMyybenZIBKqxS-
8Fdw4nSWRdRXfmTPhHZkJg=" />

<input id="Submit1" runat="server" type="submit"
value="Realizar Pago" />

</form>
```

6.2 Recepción de la notificación *on-line*

La notificación on-line es una función opcional que permite a la tienda web recibir el resultado de una transacción de forma *on-line* y en tiempo real, una vez que el comprador ha completado el proceso en el TPV Virtual.

El comercio debe capturar **y validar todos los parámetros junto a la firma** de la notificación on-line de forma previa a cualquier ejecución en su servidor.

La utilización de las librerías de ayuda proporcionadas por Banco Sabadell se expone en los siguientes subapartados y dependerá del tipo de notificación configurada.

6.2.1 Sincronización síncrona y asíncrona

En los apartados anteriores se ha descrito la forma de crear peticiones de pago utilizando conexión por la entrada **Realizar Pago** y el sistema de firma basado en HMAC SHA256. En este apartado se explica cómo se utilizan las librerías disponibles PHP, JAVA y .NET para facilitar los desarrollos **para la recepción de los parámetros de la notificación on-line y la validación de la firma**. El uso de las librerías suministradas por Banco Sabadell es opcional, si bien simplifican los desarrollos a realizar por el comercio.

Para que la notificación on-line pueda ser recibida correctamente por el servidor del comercio, deberá cumplir con los siguientes requisitos:

- La url debe ser accesible desde internet
- No debe pedir usuario y contraseña
- No debe redireccionar a terceras páginas
- Debe estar preparada para recibir los parámetros vía POST.

Es posible que por cuestiones de seguridad desee limitar el acceso a su servidor para que solo se realicen conexiones autorizadas. Si es el caso, a continuación le facilitamos las IP's de los servidores de notificación desde donde se realizarán las comunicaciones on-line:

195.76.9.117
195.76.9.149
193.16.243.13
193.16.243.173
195.76.9.187
195.76.9.222
194.224.159.47
194.224.159.57

6.2.1.1 Gestión de la notificación

6.2.1.1.1 Librería PHP

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería PHP proporcionada por Banco Sabadell:

1. Importar el fichero principal de la librería, tal y como se muestra a continuación:

```
include("./apiRedsys.php");
```

   El comercio debe decidir si la importación desea hacerla con la función "include" o "required", según los desarrollos realizados.

2. Definir un objeto de la clase principal de la librería, tal y como se muestra a continuación:

```
$miObj = new RedsysAPI;
```

3. Capturar los parámetros de la notificación on-line:

```
$version = $_POST["Ds_SignatureVersion"];
$params = $_POST["Ds_MerchantParameters"];
$firmaRecibida = $_POST["Ds_Signature"];
```

4. Validar el parámetro **Ds_Signature**. Para llevar a cabo la validación de este parámetro se debe calcular la firma y compararla con el parámetro **Ds_Signature** capturado. Para ello se debe llamar a la función de la librería "createMerchantSignatureNotif()" con la clave de comercio facilitada y el parámetro **Ds_MerchantParameters** capturado, tal y como se muestra a continuación:

```
$clave = 'sq7HjrU0BfKmC576ILgskD5srU870gJ7';
$firmaCalculada = $miObj->createMerchantSignatureNot
if($clave,$params);
```

   Una vez hecho esto, ya se puede validar si el valor de la firma enviada coincide con el valor de la firma calculada, tal y como se muestra a continuación:

```
if ($firmaCalculada === $firmaRecibida)
{
//FIRMA OK. Realizar tareas de servidor.
}
else
{
//FIRMA KO. Error, firma inválida.
}
```

   Una vez se ha realizado la llamada a la función "createMerchantSignatureNotif()", se puede obtener el valor de cualquier parámetro que sea susceptible de incluirse en la notificación on-line, tal y como se muestra en el apartado **6.3 Respuesta online**. Para llevar a cabo la obtención del valor de un parámetro se debe llamar a la función "getParameter()" de la librería con el nombre de parámetro, tal y como se muestra a continuación para obtener el código de respuesta:

```
$codigoResp = $miObj->getParameter("Ds_Response");
```

NOTA IMPORTANTE: Para garantizar la seguridad y el origen de las notificaciones el comercio debe llevar a cabo la validación de la firma recibida y de todos los parámetros que se envían en la notificación.

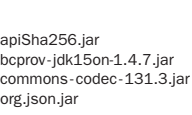
6.2.1.1.2 Librería JAVA

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería JAVA proporcionada por Banco Sabadell:

1. Importar la librería, tal y como se muestra a continuación:

```
<%@page import="sis.redsys.api.ApiMacSha256"%>
```

   El comercio debe incluir en la vía de construcción del proyecto todas las librerías(JARs) que se proporcionan:



2. Definir un objeto de la clase principal de la librería, tal y como se muestra a continuación:

```
ApiMacSha256 apiMacSha256 = new ApiMacSha256();
```

3. Capturar los parámetros de la notificación on-line:

```
String version = request.getParameter("Ds_Signature-
Version");
String params = request.getParameter("Ds_MerchantPa-
rameters");
String signatureRecibida = request.getParameter("Ds_
Signature");
```

4. Validar el parámetro **Ds_Signature**. Para llevar a cabo la validación de este parámetro se debe calcular la firma y compararla con el parámetro **Ds_Signature** capturado. Para ello se debe llamar a la función de la librería "createMerchantSignatureNotif()" con la clave de comercio facilitada y el parámetro **Ds_MerchantParameters** capturado, tal y como se muestra a continuación:

```
String clave = "sq7HjrUOBfKmC576ILgskD5srU870gJ7";
String signatureCalculada = apiMacSha256.createMerch
antSignatureNotif(clave, params);
```

   Una vez hecho esto, ya se puede validar si el valor de la firma enviada coincide con el valor de la firma calculada, tal y como se muestra a continuación:

```
if (signatureCalculada.equals(signatureRecibida))
{
System.out.println("FIRMA OK. Realizar tareas en el
servidor");
}
else
{
System.out.println("FIRMA KO. Firma inválida");
```

   Una vez se ha realizado la llamada a la función "createMerchantSignatureNotif()", se puede obtener el valor de cualquier parámetro que sea susceptible de incluirse en la notificación on-line, tal y como se muestra en el apartado **6.3 Respuesta online**. Para llevar a cabo la obtención del valor de un parámetro se debe llamar a la función "getParameter()" de la librería con el nombre de parámetro, tal y como se muestra a continuación para obtener el código de respuesta:

```
String codigoResuesta = apiMacSha256.
getParameter("Ds_Response");
```

NOTA IMPORTANTE: Para garantizar la seguridad y el origen de las notificaciones el comercio debe llevar a cabo la validación de la firma recibida y de todos los parámetros que se envían en la notificación.

6.2.1.1.3 Librería .NET

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería JAVA proporcionada por Redsys:

1. Importar la librería RedsysAPI y Newronsoft. Json en su proyecto.

2. Capturar los parámetros de la notificación on-line:

```
//Creación del objeto
RedsysAPI r = new RedsysAPI();
```

```
// Obtener la variable Ds_SignatureVersion vía POST
        if (Request.Form["Ds_SignatureVersion"] != null)
        {
        version = Request.Form["Ds_SignatureVersion"];
        }
        // Obtener la variable Ds_MerchantParameters
        vía POST
        if (Request.Form["Ds_MerchantParameters"]
        != null)
        {
        parms = Request.Form["Ds_MerchantParame-
        ters"];
        }
        // Obtener la variable Ds_Signature vía POST
        if (Request.Form["Ds_Signature"] != null)
        {
        firmaRecibida = Request.Form["Ds_Signature"];
        }
```

NOTA IMPORTANTE: Para garantizar la seguridad y el origen de las notificaciones el comercio debe llevar a cabo la validación de la firma recibida y de todos los parámetros que se envían en la notificación.

5. Validar el parámetro **Ds_Signature**. Para llevar a cabo la validación de este parámetro se debe calcular la firma y compararla con el parámetro **Ds_Signature** capturado. Para ello se debe llamar a la función de la librería "createMerchantSignatureNotif()" con la clave de comercio facilitada y el parámetro **Ds_MerchantParameters** capturado, tal y como se muestra a continuación:

```
string clave = "sq7HjrU0BfKmC576ILgskD5srU870gJ7";
string notif = r.createMerchantSignatureNotif(clave, data);
```

Una vez hecho esto, ya se puede validar si el valor de la firma enviada coincide con el valor de la firma calculada, tal y como se muestra a continuación:

```
if (notif.Equals(firmaRecibida) && notif != "")
{
//FIRMA OK. Realizar tareas de servidor
}
else
{
//FIRMA KO. Error, firma inválida.
}
```

Una vez se ha realizado la llamada a la función "createMerchantSignatureNotif()", se puede obtener el valor de cualquier parámetro que sea susceptible de incluirse en la notificación on-line, tal y como se muestra en el apartado **6.3 Respuesta online**. Para llevar a cabo la obtención del valor de un parámetro se debe llamar a la función "getParameter()" de la librería con el nombre de parámetro, tal y como se muestra a continuación para obtener el código de respuesta:

```
codigoRespuesta = r.GetParameter("Ds_Response");
```

NOTA IMPORTANTE: Para garantizar la seguridad y el origen de las notificaciones el comercio debe llevar a cabo la validación de la firma recibida y de todos los parámetros que se envían en la notificación.

6.3 Retorno del control de la navegación

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 pueden ser:

- **Instrucción "CERRAR VENTANA"**: al seleccionar "Cerrar" se cerrará la ventana 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).

El comercio debe capturar y validar, en caso de que el comercio tenga activado el retorno

de los parámetros de la operación a través de la URL, los parámetros del retorno de control de navegación previo a cualquier ejecución en su servidor, si bien no es recomendable realizar ninguna acción en el servidor a través de estas URL, debido a que el propio cliente podría modificar los valores de la respuesta.

La utilización de las librerías de ayuda proporcionadas por Banco Sabadell para la captura y validación de los parámetros del retorno de control de navegación, se expone a continuación.

6.3.1 Utilización de librerías de ayuda

En los apartados anteriores se ha descrito la forma de acceso al SIS utilizando conexión por la entrada **Realizar Pago** En este apartado se explica cómo se utilizan las librerías disponibles PHP, JAVA y .NET para facilitar los desarrollos para la recepción de los parámetros para la recepción de los parámetros del retorno de control de navegación. El uso de las librerías suministradas por Banco Sabadell es opcional, si bien simplifican los desarrollos a realizar por el comercio.

6.3.1.1 Librería PHP

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería PHP proporcionada por Banco Sabadell:

1. Importar el fichero principal de la librería, tal y como se muestra a continuación:

```
include("./apiRedsys.php");
```

El comercio debe decidir si la importación desea hacerla con la función "include" o "required", según los desarrollos realizados.

2. Definir un objeto de la clase principal de la librería, tal y como se muestra a continuación:

```
$miObj = new RedsysAPI;
```

3. Capturar los parámetros de la notificación on-line:

```
$version = $_GET["Ds_SignatureVersion"];
$params = $_ GET["Ds_MerchantParameters"];
$firmaRecibida = $_ GET["Ds_Signature"];
```

NOTA IMPORTANTE: Es importante llevar a cabo la validación de todos los parámetros que se envían en la comunicación. Para actualizar el estado del pedido de forma on-line NO debe usarse esta comunicación, sino la notificación on-line descrita en los otros apartados, ya que el retorno de la navegación depende de las acciones del cliente en su navegador.

4. Validar el parámetro **Ds_Signature**. Para llevar a cabo la validación de este parámetro se debe calcular la firma y compararla con el parámetro Ds_Signature capturado. Para ello se debe llamar a la función de la librería "createMerchantSignatureNotif ()"con la clave de comercio facilitada y el parámetro Ds_MerchantParameters capturado, tal y como se muestra a continuación:

```
$clave = 'sq7HjrUOBfKmC576ILgskD5srU870gJ7';
$firma = $miObj->createMerchantSignatureNotif($clav
e,$datos);
```

Una vez hecho esto, ya se puede validar si el valor de la firma enviada coincide con el valor de la firma calculada, tal y como se muestra a continuación:

```
if ($signatureCalculada == $signatureRecibida)
{
//FIRMA OK. Realizar tareas de servidor
}
else
{
//FIRMA KO. Error, firma inválida.
}
```

Una vez se ha realizado la llamada a la función "decodeMerchantParameters()",

se puede obtener el valor de cualquier parámetro que sea susceptible de incluirse en la notificación on-line, tal y como se muestra en el apartado **6.3 Respuesta online**. Para llevar a cabo la obtención del valor de un parámetro se debe llamar a la función "getParameter()" de la librería con el nombre de parámetro, tal y como se muestra a continuación para obtener el código de respuesta:

```
$codigoRespuesta = $miObj –>getParameter("Ds_Response");
```

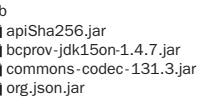
6.3.1.2 Librería JAVA

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería JAVA proporcionada por Banco Sabadell:

1. Importar la librería, tal y como se muestra a continuación:

   ```
   <%@page import="sis.redsys.api.ApiMacSha256"%>
   ```

   El comercio debe incluir en la vía de construcción del proyecto todas las librerías(JARs) que se proporcionan:

2. Definir un objeto de la clase principal de la librería, tal y como se muestra a continuación:

   ```
   ApiMacSha256 apiMacSha256 = new ApiMacSha256();
   ```

3. Capturar los parámetros del retorno de control de navegación:

   ```
   String version = request.getParameter("Ds_Signature-
   Version");
   String params = request.getParameter("Ds_MerchantPa-
   rameters");
   String signatureRecibida = request.getParameter("Ds_
   Signature");
   ```

5. Validar el parámetro **Ds_Signature**. Para llevar a cabo la validación de este parámetro se debe calcular la firma y compararla con el parámetro **Ds_Signature** capturado. Para ello se debe llamar a la función de la librería "createMerchantSignatureNotif()"con la clave de comercio facilitada y el parámetro **Ds_MerchantParameters** capturado, tal y como se muestra a continuación:

   ```
   String clave = "sq7HjrU0BfKmC576ILgskD5srU870gJ7";
   String signatureCalculada = apiMacSha256.createMerch
   antSignatureNotif(clave, params);
   ```

   Una vez hecho esto, ya se puede validar si el valor de la firma enviada coincide con el valor de la firma calculada, tal y como se muestra a continuación:

   ```
   if (signatureCalculada.equals(signatureRecibida))
   {
   System.out.println("FIRMA OK. Realizar tareas en el
   servidor");
   }
   else
   {
   System.out.println("FIRMA KO. Firma inválida");
   }
   ```

   Una vez se ha realizado la llamada a la función "decodeMerchantParameters()", se puede obtener el valor de cualquier parámetro que sea susceptible de incluirse en la retorno de control de navegación, tal y como se muestra en el apartado 6.3 Respuesta online.. Para llevar a cabo la obtención del valor de un parámetro se debe llamar a la función "getParameter()" de la librería con el nombre de parámetro, tal y como se muestra a continuación para obtener el código de respuesta:

   ```
   String codigoRespuesta = ApiMacSha256.
   getParameter("DS_Response");
   ```

   NOTA IMPORTANTE: Es importante llevar a cabo la validación de todos los parámetros que se envían en la comunicación. Para actualizar el estado del pedido de forma on-line NO debe usarse esta comunicación, sino la notificación on-line descrita en los otros apartados, ya que el retorno de la

navegación depende de las acciones del comprador en su navegador.

6.3.1.3 Librería .NET

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería .NET proporcionada por Redsys:

1. Importar la librería, tal y como se muestra a continuación:

```
Using RedsysAPIPrj;
```

2. Definir un objeto de la clase principal de la librería, tal y como se muestra a continuación:

```
RedsysAPI r = new RedsysAPI();
```

3. Capturar los parámetros del retorno de control de navegación:

```
string version = Request.QueryString["Ds_Signature-
Version"];
string parms = Request.QueryString["Ds_MerchantPa-
rameters"];
string firmaRecibida = Request.QueryString["Ds_Sig-
nature"];
```

NOTA IMPORTANTE: Es importante llevar a cabo la validación de todos los parámetros que se envían en la comunicación. Para actualizar el estado del pedido de forma on-line NO debe usarse esta comunicación, sino la notificación on-line descrita en los otros apartados, ya que el retorno de la navegación depende de las acciones del titular en su navegador.

4. Validar el parámetro **Ds_Signature**. Para llevar a cabo la validación de este parámetro se debe calcular la firma y compararla con el parámetro **Ds_Signature** capturado. Para ello se debe llamar a la función de la librería "createMerchantSignatureNotif()" con la clave de comercio facilitada y el parámetro **Ds_MerchantParameters** capturado, tal y como se muestra a continuación:

```
string clave = "sq7HjrU0BfKmC576ILgskD5srU870gJ7";
string firmaCalculada = r.createMerchantSignatureNotif(
clave, parms);
```

Una vez hecho esto, ya se puede validar si el valor de la firma enviada coincide con el valor de la firma calculada, tal y como se muestra a continuación:

```
If (firmaRecibida == firma Calculada)
{
//FIRMA OK. Mostrar mensaje en la URLOK
}
Else
{
//FIRMA KO. Mostrar mensaje en la URLKO
}
```

6.4 Localización de errores

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.

Para localizar el error se deben seguir los siguientes pasos:

1. En la barra de tareas de la página del navegador, deberá pulsar el botón Ver > Código fuente.
2. Una vez que tenemos el código fuente abierto buscar el error que se ha producido. En la barra de tareas del bloc de notas: Edición > Buscar.
3. Introducir en la caja de texto "buscar" el siguiente literal: SIS0.
4. Aparecerá un literal del tipo: <!–SIS0051:–>.
5. De este modo tendremos identificado el error que se ha producido.

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

ERROR	DESCRIPCIÓN
SIS0007	Error al desmontar el XML de entrada o error producido al acceder mediante un sistema de firma antiguo teniendo configurado el tipo de clave HMAC SHA256
SIS0008	Error falta Ds_Merchant_MerchantCode
SIS0009	Error de formato en Ds_Merchant_MerchantCode
SIS0010	Error falta Ds_Merchant_Terminal
SIS0011	Error de formato en Ds_Merchant_Terminal
SIS0014	Error de formato en Ds_Merchant_Order
SIS0015	Error falta Ds_Merchant_Currency
SIS0016	Error de formato en Ds_Merchant_Currency
SIS0017	Error no se admiten operaciones en pesetas
SIS0018	Error falta Ds_Merchant_Amount
SIS0019	Error de formato en Ds_Merchant_Amount
SIS0020	Error falta Ds_Merchant_MerchantSignature
SIS0021	Error la Ds_Merchant_MerchantSignature viene vacía
SIS0022	Error de formato en Ds_Merchant_TransactionType
SIS0023	Error Ds_Merchant_TransactionType desconocido
SIS0024	Error Ds_Merchant_ConsumerLanguage tiene mas de 3 posiciones
SIS0025	Error de formato en Ds_Merchant_ConsumerLanguage
SIS0026	Error No existe el comercio / terminal enviado
SIS0027	Error Moneda enviada por el comercio es diferente a la que tiene
SIS0028	Error Comercio / terminal está dado de baja
SIS0030	Error en un pago con tarjeta ha llegado un tipo de operación que no es ni pago ni preautorización
SIS0031	Método de pago no definido
SIS0033	Error en un pago con móvil ha llegado un tipo de operación que no es ni pago ni preautorización
SIS0034	Error de acceso a la Base de Datos
SIS0037	El número de teléfono no es válido
SIS0038	Error en java
SIS0040	Error el comercio / terminal no tiene ningún método de pago asignado
SIS0041	Error en el cálculo de la HASH de datos del comercio.
SIS0042	La firma enviada no es correcta
SIS0043	Error al realizar la notificación on-line
SIS0046	El bin de la tarjeta no está dado de alta
SIS0051	Error número de pedido repetido
SIS0054	Error no existe operación sobre la que realizar la devolución
SIS0055	Error existe más de un pago con el mismo número de pedido
SIS0056	La operación sobre la que se desea devolver no está autorizada
SIS0057	El importe a devolver supera el permitido

SIS0058	Inconsistencia de datos, en la validación de una confirmación
SIS0059	Error no existe operación sobre la que realizar la confirmación
SIS0060	Ya existe una confirmación asociada a la preautorización
SIS0061	La preautorización sobre la que se desea confirmar no está autorizada
SIS0062	El importe a confirmar supera el permitido
SIS0063	Error. Número de tarjeta no disponible
SIS0064	Error. El número de tarjeta no puede tener más de 19 posiciones
SIS0065	Error. El número de tarjeta no es numérico
SIS0066	Error. Mes de caducidad no disponible
SIS0067	Error. El mes de la caducidad no es numérico
SIS0068	Error. El mes de la caducidad no es válido
SIS0069	Error. Año de caducidad no disponible
SIS0070	Error. El Año de la caducidad no es numérico
SIS0071	Tarjeta caducada
SIS0072	Operación no anulable
SIS0074	Error falta Ds_Merchant_Order
SIS0075	Error el Ds_Merchant_Order tiene menos de 4 posiciones o más de 12
SIS0076	Error el Ds_Merchant_Order no tiene las cuatro primeras posiciones numéricas
SIS0077	Error el Ds_Merchant_Order no tiene las cuatro primeras posiciones numéricas. No se utiliza
SIS0078	Método de pago no disponible
SIS0079	Error al realizar el pago con tarjeta
SIS0080	Error al tomar los datos de pago con tarjeta desde el XML
SIS0081	La sesión es nueva, se han perdido los datos almacenados
SIS0084	El valor de Ds_Merchant_Conciliation es nulo
SIS0085	El valor de Ds_Merchant_Conciliation no es numérico
SIS0086	El valor de Ds_Merchant_Conciliation no ocupa 6 posiciones
SIS0089	El valor de Ds_Merchant_ExpiryDate no ocupa 4 posiciones
SIS0092	El valor de Ds_Merchant_ExpiryDate es nulo
SIS0093	Tarjeta no encontrada en la tabla de rangos
SIS0094	La tarjeta no fue autenticada como 3D Secure
SIS0097	Valor del campo Ds_Merchant_CComercio no válido
SIS0098	Valor del campo Ds_Merchant_CVentana no válido
SIS0112	Error El tipo de transacción especificado en
SIS0113	Excepción producida en el servlet de operaciones
SIS0114	Error, se ha llamado con un GET en lugar de un POST
SIS0115	Error no existe operación sobre la que realizar el pago de la cuota

SIS0116	La operación sobre la que se desea pagar una cuota no es una operación válida
SIS0117	La operación sobre la que se desea pagar una cuota no está autorizada
SIS0118	Se ha excedido el importe total de las cuotas
SIS0119	Valor del campo Ds_Merchant_DateFrecuency no válido
SIS0120	Valor del campo Ds_Merchant_ChargeExpiryDate no válido
SIS0121	Valor del campo Ds_Merchant_SumTotal no válido
SIS0122	Valor del campo Ds_Merchant_DateFrecuency o no Ds_Merchant_SumTotal tiene formato incorrecto
SIS0123	Se ha excedido la fecha tope para realizar transacciones
SIS0124	No ha transcurrido la frecuencia mínima en un pago recurrente sucesivo
SIS0126	Operación denegada para evitar duplicidades.
SIS0132	La fecha de Confirmación de Autorización no puede superar en mas de 7 días a la de Preautorización.
SIS0133	La fecha de Confirmación de Autenticación no puede superar en mas de 45 días a la de Autenticación Previa.
SIS0139	Error el pago recurrente inicial está duplicado
SIS0142	Tiempo excedido para el pago
SIS0197	Error al obtener los datos de cesta de la compra en operación tipo pasarela
SIS0198	Error el importe supera el límite permitido para el comercio
SIS0199	Error el número de operaciones supera el límite permitido para el comercio
SIS0200	Error el importe acumulado supera el límite permitido para el comercio
SIS0214	El comercio no admite devoluciones
SIS0216	Error Ds_Merchant_CVV2 tiene más de 3 posiciones
SIS0217	Error de formato en Ds_Merchant_CVV2
SIS0218	El comercio no permite operaciones seguras por la entrada /operaciones
SIS0219	Error el número de operaciones de la tarjeta supera el límite permitido para el comercio
SIS0220	Error el importe acumulado de la tarjeta supera el límite permitido para el comercio
SIS0221	Error el CVV2 es obligatorio
SIS0222	Ya existe una anulación asociada a la preautorización
SIS0223	La preautorización que se desea anular no está autorizada
SIS0224	El comercio no permite anulaciones por no tener firma ampliada
SIS0225	Error no existe operación sobre la que realizar la anulación
SIS0226	Inconsistencia de datos, en la validación de una anulación
SIS0227	Valor del campo Ds_Merchant_TransactionDate no válido
SIS0229	No existe el código de pago aplazado solicitado
SIS0230	El comercio no permite pago fraccionado
SIS0231	No hay forma de pago aplicable para el cliente
SIS0252	El comercio no permite el envío de tarjeta
SIS0253	La tarjeta no cumple el check-digit

SIS0254	El número de operaciones de la IP supera el límite permitido por el comercio
SIS0255	El importe acumulado por la IP supera el límite permitido por el comercio
SIS0256	El comercio no puede realizar preautorizaciones
SIS0257	Esta tarjeta no permite operativa de preautorizaciones
SIS0258	Inconsistencia de datos, en la validación de una confirmación
SIS0261	Operación detenida por superar el control de restricciones en la entrada al SIS
SIS0270	El comercio no puede realizar autorizaciones en diferido
SIS0274	Tipo de operación desconocida o no permitida por esta entrada al SIS
SIS0295	Se ha denegado una operación que fue enviada en el mismo minuto para evitar duplic.
SIS0296	Error al validar los datos de la operación de Tarjeta en Archivo Inicial.
SIS0297	Número de operaciones sucesivas de tarjeta en archivo superado.
SIS0298	El comercio no permite realizar operaciones de Tarjeta en Archivo o Pago por referencia.
SIS0319	El comercio no pertenece al grupo especificado en Ds_Merchant_Group
SIS0321	La referencia indicada en Ds_Merchant_Identifier no está asociada al comercio
SIS0322	Error de formato en Ds_Merchant_Group
SIS0323	Faltan parámetros CustomerMobile y CustomerMail
SIS0324	Imposible enviar enlace al titular
SIS0325	Se ha pedido no mostrar pantallas pero no se ha enviado ninguna referencia de tarjeta
SIS0327	No se ha indicado teléfono o email en la petición Phone & Sell
SIS0330	El enlace para el pago ha caducado.
SIS0331	La operación no tiene un estado válido o no existe.
SIS0333	No está configurado el wallet solicitado (V.Me, Master)
SIS0334	Operación detenida por superar el control de restricciones de seguridad del TPV Virtual
SIS0429	Error en la versión enviada por el comercio en el parámetro Ds_SignatureVersion
SIS0430	Error al decodificar el parámetro Ds_MerchantParameters
SIS0431	Error del objeto JSON que se envía codificado en el parámetro Ds_MerchantParameters
SIS0432	Error FUC del comercio erróneo
SIS0433	Error Terminal del comercio erróneo
SIS0434	Error ausencia de número de pedido en la operación enviada por el comercio
SIS0435	Error en el cálculo de la firma
SIS0436	Error en la construcción del elemento padre <REQUEST>
SIS0437	Error en la construcción del elemento <DS_SIGNATUREVERSION>
SIS0438	Error en la construcción del elemento <DATOSENTRADA>
SIS0439	Error en la construcción del elemento <DS_SIGNATURE>
SIS0444	Este error se produce cuando el comercio ya ha migrado a la firma HMAC SHA256 y envía una transacción con la firma antigua

SIS0448	Se ha realizado una operación con tarjeta DINERS, pero el comercio no tiene habilitado este tipo de tarjeta. Para habilitarla, deberá contactar directamente con Diners Club.
SIS0449	Se ha enviado el tipo de transacción “A” y el comercio no tiene activado la operatividad con este tipo de transacción.
SIS0450	Se ha enviado el tipo de transacción “A” con una tarjeta American Express y el comercio no tiene activado la operatividad con este tipo de transacción.
SIS0451	Se ha enviado el tipo de transacción “A” y el comercio no tiene activado la operatividad con este tipo de transacción.
SIS0452	Se ha utilizado una tarjeta 4B y el comercio no admite este tipo de tarjeta.
SIS0453	Se ha utilizado una tarjeta JCB y el comercio no admite este tipo de tarjeta.
SIS0454	Se ha utilizado una tarjeta American Express y el comercio no admite este tipo de tarjeta.
SIS0455	Método de pago no disponible
SIS0456	Método de pago no seguro (Visa) no disponible
SIS0457	Se ha utilizado una tarjeta comercial y el comercio no admite este tipo de tarjeta. Para habilitarlo, deberá contactar con su oficina gestora.
SIS0458	Se ha utilizado una tarjeta comercial y el comercio no admite este tipo de tarjeta. Para habilitarlo, deberá contactar con su oficina gestora.
SIS0459	Se ha utilizado una tarjeta JCB y el comercio no admite este tipo de tarjeta.
SIS0460	Se ha utilizado una tarjeta American Express y el comercio no admite este tipo de tarjeta.
SIS0461	Se ha utilizado una tarjeta American Express y el comercio no admite este tipo de tarjeta.
SIS0462	Error, se ha enviado una petición segura a través de Host to Host.
SIS0463	Método de pago no disponible
SIS0464	Se ha utilizado una tarjeta comercial y el comercio no admite este tipo de tarjeta. Para habilitarlo, deberá contactar con su oficina gestora.
SIS0465	Se ha lanzado una petición de pago no segura y el comercio no admite pagos no seguros.

6.5 Respuesta online

Existen cuatro mecanismos de respuesta para los comercios que deseen disponer del resultado de los pagos inmediatamente después de su realización. Los cuatro mecanismos, que pueden coexistir de forma simultánea son:

1. Consulta a través de Internet del **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. Recepción de **fichero con un listado de operaciones**.

   El fichero se generará periódicamente (normalmente será un fichero diario) y será enviado a BS Online para que el comercio lo pueda descargar.

4. **Consulta vía SOAP.**

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

La **respuesta online** es el sistema más utilizado. En caso de querer utilizar un fichero con el listado de operaciones o consulta SOAP es necesario ponerse en contacto con el servicio técnico de Banco Sabadell, quien facilitará las instrucciones necesarias.

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

- **Vía e-mail**:

  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.

- **Vía URL**:

  La respuesta a la autorización de pago se recibirá en la dirección URL indicada en el formulario de pago. Esta opción requiere de unos sencillos desarrollos informáticos en la web del comercio, tanto para habilitar la recepción de la respuesta como para integrarla dentro de la base de datos del comercio. Esta opción es válida únicamente para comercios instalados con el campo de verificación activo. Es la opción recomendada.

Para implementar la respuesta online vía URL se debe facilitar en el formulario de petición de pago, una URL donde 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 CAMPO	COMENTARIOS
Versión de firma	Ds_SignatureVersion	Constante que indica la versión de firma que se está utilizando.
Datos de la operación	Ds_MerchantParameters	Cadena en formato JSON con todos los parámetros de la petición codificada en Base 64
Firma	Ds_Signature	Resultado del HMAC SHA256 de la cadena JSON codificada en Base 64 enviada en el parámetro anterior.

Para acceder a los datos de la operación, los datos deberán ser desencriptados. Esta desencriptación se realiza en el momento en el que se genera la firma de notificación, tal y como se indica en los ejemplos.

DATO	NOMBRE DEL CAMPO	LONG/TIPO	COMENTARIOS
Fecha	Ds_Date	dd/mm/yyyy	Fecha de la transacción
Hora	Ds_Hour	HH:mm	Hora de la transacción
Importe	Ds_Amount	12 / Núm.	Mismo valor que en la petición.
Moneda	Ds_Currency	4 / Núm.	Mismo valor que en la petición. 4 se considera su longitud máxima.
Número de pedido	Ds_Order	12 / A-N.	Mismo valor que en la petición.
Identificación de comercio: código FUC	Ds_MerchantCode	9 / N.	Mismo valor que en la petición.

Terminal	Ds_Terminal	3 / Núm.	Número de terminal que le asignará su banco. 3 se considera su longitud máxima.
Código de respuesta	Ds_Response	4 / Núm.	Ver tabla siguiente (Posibles valores del Ds_Response).
Datos del comercio	Ds_MerchantData	1024 / A-N	Información opcional enviada por el comercio en el formulario de pago.
Pago Seguro	Ds_SecurePayment	1 / Núm.	0 – Si el pago NO es seguro 1 – Si el pago es seguro
Tipo de operación	Ds_TransactionType	1 / A-N	Tipo de operación que se envió en el formulario de pago
País del titular	Ds_Card_Country	3/Núm	País de emisión de la tarjeta. Ver Anexo I con la lista de países.
Código de autorización	Ds_AuthorisationCode	6/ A-N	Opcional: Código alfanumérico de autorización asignado a la aprobación de la transacción por la institución autorizadora.
Idioma del titular	Ds_ConsumerLanguage	3 / Núm	Opcional: El valor 0, indicará que no se ha determinado el idioma del cliente. (opcional). 3 se considera su longitud máxima.
Tipo de Tarjeta	Ds_Card_Type	1 / A-N	Opcional: Valores posibles: C – Crédito D - Débito
Número de tarjeta	Ds_Card_Number	15-19/A-N	Opcional: El valor de esta variable será el número de tarjeta asteriscado. Esta variable por defecto no se encuentra activada.

Referencia	Ds_Merchant_Identifier	40/A-N	Referencia generada en la petición de pago por referencia. Esta variable solo se enviará si se ha activado la operativa de pago por referencia
Fecha de caducidad	Ds_ExpiryDate	4 / N	Fecha de caducidad de la tarjeta. Esta variable solo se enviará si se ha activado la operativa de pago por referencia

(En los campos "Ds_Currency", "Ds_Terminal" y "Ds_ConsumerLanguage" la longitud se considera máxima, por lo que no es imprescindible el relleno con ceros a la izquierda. La firma será generada con los campos exactamente como se envíen).

La conexión utilizada para comunicar la confirmación online entre el TPV Virtual y el comercio debe ser TLS 1.1 o superior en el caso de que se utilice un certificado de seguridad (https). 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.

A continuación se indica la lista completa de códigos disponibles:

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 BLOQUEDA TRANSITORIAMENTE O BAJO SOSPECHA DE FRAUDE	Tarjeta bloqueada transitoriamente por el banco emisor o bajo sospecha de fraude.
104	OPERACIÓN NO PERMITIDA	Operación no permitida para ese tipo de tarjeta.
106	NUM. INTENTOS EXCEDIDO	Excedido el número de intentos con PIN erróneo.
107	CONTACTAR CON EL EMISOR	El banco emisor no permite una autorización automática. Es necesario contactar telefónicamente con su centro autorizador para obtener una aprobación manual.
109	IDENTIFICACIÓN INVALIDA DEL COMERCIO O TERMINAL	Denegada porque el comercio no está correctamente dado de alta en los sistemas internacionales de tarjetas.
110	IMPORTE INVALIDO	El importe de la transacción es inusual para el tipo de comercio que solicita la autorización de pago.
114	TARJETA NO SOPORTA EL TIPO DE OPERACIÓN SOLICITADO	Operación no permitida para ese tipo de tarjeta.
116	DISPONIBLE INSUFICIENTE	El titular de la tarjeta no dispone de suficiente crédito para atender el pago.
118	TARJETA NO REGISTRADA	Tarjeta inexistente o no dada de alta por banco emisor.
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 BLOQUEDA TRANSITORIAMENTE O BAJO SOSPECHA DE FRAUDE	Tarjeta bloqueada transitoriamente por el banco emisor o bajo sospecha de fraude. Además, el banco emisor considera que la tarjeta está en una situación de posible fraude.
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, O 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 PREAUTORITZACIÓN REALIZADA POR EL SISTEMA	El sistema ha anulado la preautorización diferida al haber pasado más de 72 horas.
9929	ANULACIÓN DE PREAUTORITZACIÓN 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
9126	OPERACIÓN DENEGADA PARA EVITAR DUPLICIDADES	
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	PREAUTORITZACIONES 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
9334	DENEGACIÓN POR FILTROS DE SEGURIDAD	La alerta ha sido bloqueada por filtros de seguridad
9912	EMISOR NO DISPONIBLE	El centro autorizador del banco emisor no está operativo en estos momentos.
9913	ERROR EN CONFIRMACION	Error en la confirmación que el comercio envía al TPV Virtual (solo aplicable en la opción de sincronización SOAP)
9914	CONFIRMACION “KO”	Confirmación “KO” del comercio (solo aplicable en la opción de sincronización SOAP)
9915	PAGO CANCELADO	El usuario ha cancelado el pago
9928	AUTORIZACIÓN EN DIFERIDO ANULADA	Anulación de autorización en diferido realizada por el SIS (proceso batch)
9929	AUTORIZACIÓN EN DIFERIDO ANULADA	Anulación de autorización en diferido realizada por el comercio
9997	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.

6.6 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*.

6.7 Certificados SSL para la notificación online

Para los comercios que deseen cifrar sus conexiones hacia la pasarela de pagos, deben tener en cuenta que existen requisitos acerca de los certificados de seguridad.

Estos requisitos son los siguientes:

1.El certificado tiene que estar en la lista de certificados admitidos por Redsys

2. Se soporta 1.1 y 1.2

3. Los cipher suites que se aceptan son los siguientes:

SSL_RSA_WITH_AES_256_CBC_SHA256
SSL_RSA_WITH_AES_256_CBC_SHA
SSL_RSA_WITH_AES_128_CBC_SHA256
SSL_RSA_WITH_AES_128_CBC_SHA
SSL_RSA_WITH_AES_256_GCM_SHA384
SSL_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_FIPS_WITH_3DES_EDE_CBC_SHA

Adicionalmente, si se detecta un error del tipo "handshake" es necesario definir correctamente los parámetros ServerName y ServerAlias (opcional):

ServerName HYPERLINK "http://mi.dominio.com" mi.dominio.com

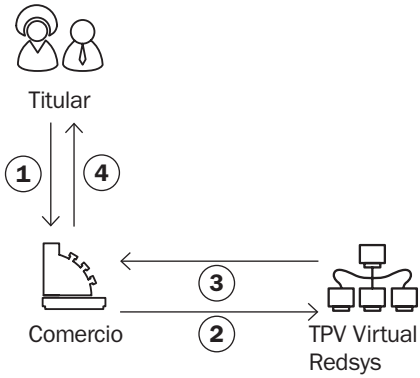
ServerAlias HYPERLINK “http://misegundo.dominio.com” misegundo.dominio.com (opcional)

ServerAlias HYPERLINK “http://mitercer.dominio.com” mitercer.dominio.com (opcional)

Para obtener la lista con los últimos certificados admitidos, contacte con el servicio tecnico, o también puede descargárselo desde el Módulo de Administración del TPV Virtual.

6.8 Envío de peticiones a través de Web Service

El siguiente esquema presenta el flujo general de una operación realizada con el Web Service TPV Virtual.



1. El titular selecciona los productos en el comercio.
2. El comercio envía los datos del pago al TPV Virtual.
3. Una vez finalizado el pago, el TPV Virtual informa del resultado al comercio.
4. El comercio devuelve la información del resultado del pago al titular.

6.8.1 Envío de petición al TPV Virtual

Como se muestra en el paso 2 del esquema anterior, el comercio debe enviar al TPV Virtual los datos de la petición de pago vía Web Service con codificación UTF-8.Para ello el Web Service tiene publicados varios métodos sobre los cuales operan los TPV Virtuales. El método “**trataPeticion**”, permite la realización de operaciones a través del Web Service , para lo cual se debe construir un XML que incluye los datos de la petición de pago. La descripción exacta de esta petición XML se presenta mediante el fichero WSDL en el Anexo 5 (Web Service de petición de pago - WSDL) del apartado Anexos del presente documento.

Esta petición de pago debe enviarse a las siguientes URLs dependiendo de si se quiere realizar una operación de pruebas u operacioens reales. No obstante, las comunicaciones realizadas por Web Service deben ser realizadas a través del protocolo TLS 1.2.

Entorno de pruebas:

https://sis-t.redsys.es:25443/sis/services/SerClsWSEntrada

Entorno de producción:

https://sis.redsys.es/sis/services/SerClsWSEntrada

URLs de WSDL del servicio:

Entorno de pruebas:

https://sis-t.redsys.es:25443/sis/services/SerClsWSEntrada/wsdl/SerClsWSEntrada.wsdl

Entorno de producción:

https://sis.redsys.es/sis/services/SerClsWSEntrada/wsdl/SerClsWSEntrada.wsdl

Una vez enviada la petición el TPV Virtual la interpretará y realizará las validaciones

necesarias para, a continuación, procesar la operación, tal y como se muestra en el paso 3del esquema anterior. Dependiendo del resultado de la operación, se construye un documento XML de respuesta con el resultado de la misma con codificación UTF-8.

6.8.1.1 Mensaje de petición de pago Web Service

Para que el comercio pueda realizar la petición a través del Web Service de Banco Sabadell, es necesario intercambiar una serie de datos, tanto en los mensajes de petición como en los mensajes de respuesta.

La estructura del mensaje siempre será la misma, estableciendo como raíz del mismo el elemento **<REQUEST>**. En su interior siempre deben encontrarse tres elementos que hacen referencia a:

- Datos de la petición de pago. Elemento identificado por la etiqueta <**DATOSENTRADA**>.
- Versión del algoritmo de firma. Elemento identificado por la etiqueta <**DS_SIGNATUREVERSION**>.
- Firma de los datos de la petición de pago. Elemento identificado por la etiqueta <**DS_SIGNATURE**>.

A continuación se muestra un ejemplo de un mensaje de petición de pago:

```
<REQUEST>
<DATOSENTRADA>
<DS_MERCHANT_AMOUNT>145</DS_MERCHANT_
AMOUNT>
<DS_MERCHANT_ORDER>151029142229</DS_MER-
CHANT_ORDER>
<DS_MERCHANT_MERCHANTCODE>327234688</
DS_MERCHANT_MERCHANTCODE>
<DS_MERCHANT_CURRENCY>978</DS_MERCHANT_
CURRENCY>
<DS_MERCHANT_PAN>4548812049400004</
DS_MERCHANT_PAN>
<DS_MERCHANT_EXPIRYDATE>1512</DS_MERCHANT_
EXPIRYDATE>
<DS_MERCHANT_CVV2>285</DS_MERCHANT_CVV2>
<DS_MERCHANT_TRANSACTIONTYPE>A</DS_MER-
CHANT_TRANSACTIONTYPE>
<DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TER-
MINAL>
</DATOSENTRADA>
   <DS_SIGNATUREVERSION>HMAC_SHA256_V1</
DS_SIGNATUREVERSION>
   <DS_SIGNATURE>2YW19YQ8rb/0LLav79Y5L24Yw04
5KxN5hme27605WxY=</DS_SIGNATURE>
</REQUEST>
```

Para facilitar la integración del comercio, a continuación se explica de forma detallada los pasos a seguir para montar el mensaje de petición de pago.

6.8.1.2 Montar la cadena de datos de la petición

Se debe generar una cadena con todos los datos de la petición en formato XML dando como resultado el elemento <**DATOSENTRADA**>.

Se debe tener en cuenta que existen varios tipos de peticiones y según el tipo varía la estructura del mensaje y los parámetros que se envían y reciben.

Podemos diferenciar tres tipos de peticiones:

- Peticiones de pago (con envío de datos de tarjeta). En el Anexo 1 (Peticiones de pago) del apartado Anexos del presente documento, se presentan los parámetros necesarios para este tipo de petición incluyendo un ejemplo.
- Peticiones de Confirmación/Devolución. En el Anexo 3 (Peticiones de Confirmación/Devolución) del apartado Anexos del presente documento, se presentan los parámetros necesarios para este tipo de petición incluyendo un ejemplo.

Para comercios que utilicen operativas especiales como el “Pago por referencia” (Pago 1-Clic), deberán incluir los campos específicos de este tipo de operativa en el elemento <DATOSENTRADA>. Estos campos se incluyen en el punto 6.1.

6.8.1.3 Identificar la versión de algoritmo de firma a utilizar

En la petición se debe identificar la versión concreta de algoritmo que se está utilizando para la firma. Actualmente se utiliza el valor **HMAC_SHA256_V1** para identificar la versión de todas las peticiones, por lo que este será el valor del elemento <**DS_SIGNATUREVERSION**>, tal y como se puede observar en el ejemplo de mensaje mostrado al inicio del apartado 3.

6.8.1.4 Identificar la clave a utilizar para la firma

Para calcular la firma es necesario utilizar una clave específica para cada terminal. La clave de comercio que debe utilizar es la que recibió a través de SMS desde Banco Sabadell.

NOTA IMPORTANTE: Esta clave debe ser almacenada en el servidor del comercio de la forma más segura posible para evitar un uso fraudulento de la misma. El comercio es responsable de la adecuada custodia y mantenimiento en secreto de dicha clave.

6.8.1.5 Firmar los datos de la petición

Una vez se ha generado el elemento con los datos de la petición de pago (<DATOSENTRADA>) y la clave específica del terminal se debe calcular la firma siguiendo los siguientes pasos:

1. Se genera una clave específica por operación. Para obtener la clave derivada a utilizar en una operación se debe realizar un cifrado 3DES entre la clave del comercio, la cual debe ser previamente decodificada en BASE 64, y el valor del número de pedido de la operación (DS_MERCHANT_ORDER).
2. Se calcula el HMAC SHA256 del elemento <DATOSENTRADA>.
3. El resultado obtenido se codifica en BASE 64, y el resultado de la codificación será el valor del elemento <**DS_SIGNATURE**>, tal y como se puede observar en el ejemplo de formulario mostrado al inicio del apartado 3.

6.8.2 Utilización de librerías de ayuda

En los apartados anteriores se ha descrito la forma de acceso al SIS utilizando conexión por Web Service y el sistema de firma basado en **HMAC SHA256**. En este apartado se explica cómo se utilizan las librerías disponibles en PHP y JAVA para facilitar los desarrollos y la generación de la firma.

6.8.2.1 Librería PHP

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería PHP proporcionada por Banco Sabadell:

1. Importar el fichero principal de la librería, tal y como se muestra a continuación:

   ```
   include ‘./apiRedsysWs.php’;
   ```

   El comercio debe decidir si la importación desea hacerla con la función “include” o “required”, según los desarrollos realizados.

   2. Definir un objeto de la clase principal de la librería, tal y como se muestra a continuación:

      ```
      $miObj = new RedsysAPIWs;
      ```

3. Calcular el elemento <**DS_SIGNATURE**>. Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería “createMerchantSignatureHostTo

Host()"con la clave de comercio facilitada y el elemento con los datos de la petición de pago (<DATOSENTRADA>), tal y como se muestra a continuación:

```
$datoEntrada='<DATOSENTRADA><DS_MERCHANT_
AMOUNT>'.$importe.'</DS_MERCHANT_AMOUNT><DS_
MERCHANT_ORDER>'.$num_pedido.'</DS_MERCHANT_
ORDER><DS_MERCHANT_MERCHANTCODE>'.$fuc.'</
DS_MERCHANT_MERCHANTCODE><DS_MER-
CHANT_CURRENCY>'.$moneda.'</DS_MER-
CHANT_CURRENCY><DS_MERCHANT_TRANS
ACTIONTYPE>'.$tipoTransaccion.'</DS_MER-
CHANT_TRANSACTIONTYPE><DS_MER-
CHANT_TERMINAL>'.$terminal.'</
DS_MERCHANT_TERMINAL><DS_MERCHANT_
MERCHANTURL>'.$mUrl.'</DS_MERCHANT_MERCHAN-
TURL></DATOSENTRADA>';
$clave = 'sq7HjrUOBfKmC576ILgskD5srU870gJ7';
$signature = $miObj->createMerchantSignatureHostToHo
st($clave, $datoEntrada);
```

Una vez obtenido el valor del elemento <**DS_SIGNATURE**>, ya es posible completar el mensaje de petición de pago y realizar la llamada Web Service.

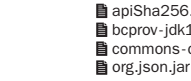
6.8.2.2 Librería JAVA

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería JAVA proporcionada por Banco Sabadell:

1. Importar la librería, tal y como se muestra a continuación:

   ```
   <%@page import="sis.redsys.api.ApiMacSha256"%>
   ```

   El comercio debe incluir en la vía de construcción del proyectotodas las librerías (JARs) que se proporcionan:

2. Definir un objeto de la clase principal de la librería, tal y como se muestra a continuación:

   ```
   ApiMacSha256 apiMacSha256 = new ApiMacSha256();
   ```

3. Calcular el elemento <**DS_SIGNATURE**>. Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería "createMerchantSignatureHostToHost()" con la clave de comercio facilitada y el elemento con los datos de la petición de pago (<DATOSENTRADA>), tal y como se muestra a continuación:

   ```
   String datosEntrada = "<DATOSENTRADA><DS_MERCHANT_
   AMOUNT>200</DS_ DS_MERCHANT_AMOUNT>..."
   String clave = "sq7HjrUOBfKmC576ILgskD5srU870gJ7";
   String firma = apiMacSha256.createMerchantSignatureH
   ostToHost(clave, datosEntrada);
   ```

   Una vez obtenido el valor del elemento <DS_SIGNATURE>, ya se puedo completar el mensaje de petición de pago y realizar la llamada Web Service.

6.8.2.3 Librería .NET

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería .NET proporcionada por Banco Sabadell:

1. Importar la librería, tal y como se muestra a continuación:

   ```
   Using RedsysAPIPrj;
   ```

2. Crear un objeto de la clase del Web Service de Redsys. Para poder realizar esto es necesario añadir una nueva referencia web con el fichero SerClsWSEntrada.wsdl.

   ```
   WebRedsysApi.WebRedsysWs.SercIsWSEntradaService
   s = new WebRedsysAPI.WebRedsysWs.SerClsWSEntra-
   daService();
   ```

   Nota: En el atributo location de la etiqueta <wsdlsoap:address> Del fichero SerClsWSEntrada.wsdl, indicar si se trata del entorno real o pruebas:

   ```
   https://sis-t.redsys.es:25443/sis/services/SerClsW-
   SEntrada (Pruebas)
   https://sis.redsys.es/sis/services/SerClsWSEntrada
   (Real)
   ```

3. Definir un objeto de la clase principal de la librería, tal y como se muestra a continuación:

   ```
   RedsysAPIWs r = new RedsysAPIWs();
   ```

Al realizar este paso se inicializan los atributos diccionario clave/valor m_keyvalues y cryp de la clase Cryptogra (Clase auxiliar para realizar las operaciones criptográficas necesarias)

4. Generar parámetros de **DATOSENTRADA** (Modalidad Petición de Pago con envío de datos de tarjeta) mediante la función:

```
string datoEntrada = r.GenerateDatoEntradaXML(importe
, merchantCode, moneda, numTarjeta, cvv2, transaction-
Type, terminal, expiryDate);
```

5. Calcular el elemento <**DS_SIGNATURE**>. Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería "createMerchantSignatureHostToHost()" con la clave obtenida del módulo de administración y el elemento con los datos de la petición de pago (<DATOSENTRADA>), tal y como se muestra a continuación:

```
string firma = r.createMerchantSignatureHostToHost(cla
ve, datoEntrada);
```

Una vez obtenido el valor del elemento <**DS_SIGNATURE**>, ya se puedo completar el mensaje de petición de pago y realizar la llamada Host to Host.

Se genera el string XML final de petición de pago con **DATOSENTRADA**, **DS_SIGNATUREVERSION** y **DS_SIGNATURE** calculado en punto 5.

```
string requestXML = r.GenerateRequestXML(datoEntra
da, firma);
```

Después se llama al método trataPeticion del Web Service de Redsys pasándole como parámetro el string XML final calculado con el método GenerateRequestXML.

```
string result = s.trataPeticion(requestXML);
```

6.8.3 Respuesta de petición Web Service

En el presente apartado se describen los datos que forman parte del mensaje de respuesta de una petición al TPV Virtual Web Service. Este mensaje se genera en formato XML y a continuación se muestra un ejemplo del mismo:

```
<RETORNOXML>
<CODIGO>0</CODIGO>
<OPERACION>
<Ds_Amount>145</Ds_Amount>
<Ds_Currency>978</Ds_Currency>
<Ds_Order>151029142229</Ds_Order>
<Ds_Signature>MRvyhuDEpg4BmzfTdgHKrI5qQ9U5UD2
Qe8eDadIZtyE=</Ds_Signature>
<Ds_MerchantCode>327234688</Ds_MerchantCode>
<Ds_Terminal>2</Ds_Terminal>
<Ds_Response>0000</Ds_Response>
<Ds_AuthorisationCode>185714</Ds_AuthorisationCo-
de>
<Ds_TransactionType>A</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>
```

Como se puede observar en el ejemplo anterior, la respuesta está formada por dos elementos principales:

- Código (<**CODIGO**>): 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 un código. (Ver códigos de error en apartado 6.5 de esta Guía)
- Datos de la operación (<**OPERACION**>): Recoge toda la información necesaria sobre la operación que se ha realizado. Mediante este elemento se determina si la operación ha sido autorizada o no.

NOTA: La relación de parámetros que forman parte de la respuesta se describe en el punto 6.5.

6.8.3.1 Firma del mensaje de respuesta

Una vez se ha obtenido el mensaje de respuesta y la clave específica del terminal, siempre y cuando la operación se autorice, se debe comprobar la firma de la respuesta siguiendo los siguientes pasos:

1. Se genera una clave específica por operación. Para obtener la clave derivada a utilizar en una operación se debe realizar un cifrado 3DES entre la clave del comercio, la cual debe ser previamente decodificada en BASE 64, y el valor del número de pedido de la operación (**DS_ORDER**).

2. Se calcula el **HMAC SHA256** de la cadena formada por la concatenación del valor de los siguientes campos:

   ```
   Cadena = Ds_Amount + Ds_Order + Ds_MerchantCode
   + Ds_Currency + Ds_Response + Ds_TransactionType +
   Ds_SecurePayment
   ```

   Si tomamos como ejemplo la respuesta que se presenta al inicio de este apartado la cadena resultante sería:

   ```
   Cadena = 145144491278999900888197800000
   ```

   Si el comercio tiene configurado envío de tarjeta asteriscada en la respuesta, se debe calcular el **HMAC SHA256** de la cadena formada por la concatenación del valor de los siguientes campos:

   ```
   Cadena = Ds_Amount + Ds_Order + Ds_MerchantCode
   + Ds_Currency + Ds_Response + Ds_CardNumber +
   Ds_TransactionType + Ds_SecurePayment
   ```

   Si tomamos como ejemplo la respuesta que se presenta al inicio de este apartado la cadena resultante sería:

   ```
   Cadena = 145144982154599900888197800004548
   81******000400
   ```

3. El resultado obtenido se codifica en BASE 64, y el resultado de la codificación debe ser el mismo que el valor del parámetro <**Ds_Signature**> obtenido en la respuesta.

6.8.3.2 Utilización de librerías de ayuda

En este apartado se explica cómo se utilizan las librerías disponibles en PHP y JAVA para facilitar los desarrollos y la generación de la firma de respuesta.

6.8.3.2.1 Librería PHP

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería PHP proporcionada por Banco Sabadell:

1. Importar el fichero principal de la librería, tal y como se muestra a continuación:

   ```
   Include './apiRedsysWs.php';
   ```

   El comercio debe decidir si la importación desea hacerla con la función "include" o "required", según los desarrollos realizados.

2. Definir un objeto de la clase principal de la librería, tal y como se muestra a continuación:

   ```
   $miObj = new RedsysAPIWs;
   ```

3. Calcular el parámetro <**Ds_Signature**>.Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería "createSignatureResponseHostToHost( )"con la clave de comercio facilitada, la cadena que se desea firmar(concatenación de campos descrita en el punto 2 del apartado 4.1 del presente documento) y el número de pedido.

   ```
   $cadenaConcatenada = "14515102914222932723468
   89780000A0";
   $numPedido = "151029142229";
   $clave = 'sq7HjrU0BfKmC576ILgskD5srU870gJ7';
   $firma = $miObj->createMerchantSignatureResponseHo
   stToHost($clave, $cadenaConcatenada, $numPedido);
   ```

   El resultado obtenido debe ser el mismo que el valor del parámetro <**Ds_Signature**> obtenido en la respuesta.

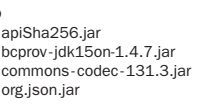
6.8.3.2.2 Librería JAVA

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería JAVA proporcionada por Banco Sabadell:

1. Importar la librería, tal y como se muestra a continuación:

```
<%@page import="sis.redsys.api.ApiWsMacSha256"%>
```

El comercio debe incluir en la vía de construcción del proyecto todas las librerías (JARs) que se proporcionan:



2. Calcular el parámetro <**Ds_Signature**>.Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería "createSignatureResponseHostToHost( )"con la clave de comercio facilitada, la cadena que se desea firmar(concatenación de campos descrita en el punto 2 del apartado 4.1 del presente documento) y el número de pedido.

```
String cadenaConcatenada = "145151029142229327
2346889780000A0";
String numPedido = "151029142229";
String clave = "sq7HjrU0BfKmC576ILgskD5srU870gJ7";
String firma = apiMacSha256.createMerchantSignat
ureResponseHostToHost(clave, cadenaConcatenada,
numPedido);
```

El resultado obtenido debe ser el mismo que el valor del parámetro <**Ds_Signature**> obtenido en la respuesta.

6.8.3.2.3 Librería .Net

A continuación se presentan los pasos que debe seguir un comercio para la utilización de la librería .NET proporcionada por Redsys:

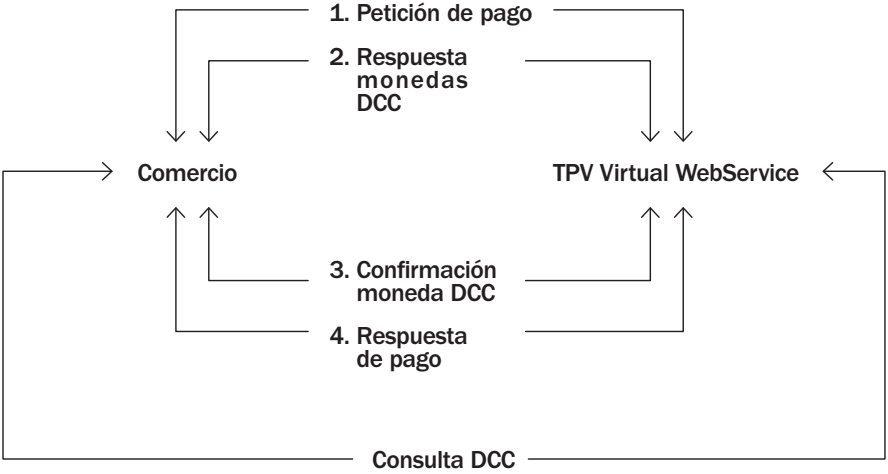
1. Convertir la cadena respuesta XML al atributo diccionario m_keyvalues de la clave RedsysAPIWs:

```
r.XMLToDiccionary(result);
```

2. Calcular el parámetro <**Ds_Signature**>.Para llevar a cabo el cálculo de este parámetro, se debe llamar a la función de la librería "cr eateSignatureResponseHostToHost()"con la clave obtenida del módulo de administración, la cadena que se desea firmar(concatenación de campos descrita en el punto 2 del apartado 5.1 del presente documento) y el número de pedido.

```
string cadena = r.GenerateCadena(result);
string numOrder = r.GetDictionary("Ds_Order");
string firmaCalculada = r.createSignatureResponseHostToHo
st(clave, cadena, numOrder);
```

El resultado obtenido debe ser el mismo que el valor del parámetro <**Ds_Signature**> obtenido en la respuesta.



6.8.4 Operativa DCC

A continuación se detallarán todas aquellas características adicionales de la operativa DCC que tengan los comercios que hayan contratado este servicio.

NOTA: Como se muestra en el gráfico la operativa **DCC** se basa en el envío de dos peticiones al WebService del TPV Virtual. Para garantizar el correcto funcionamiento del sistema, es necesario que el comercio mantenga la sesión entre la primera y la segunda llamada al WebService. El mantenimiento de la sesión dependerá del software utilizado para realizar la llamada al WebService. Por ejemplo si se utiliza el API de Axis, será suficiente con utilizar el mismo "Stub" para las dos peticiones y fijar la propiedad "setMaintainSession(true)" antes de realizar la primera llamada.

6.8.4.1 Métodos de acceso

El método de acceso "**trataPeticion**": permite la realización de operaciones a través del TPV Virtual WebService. Se usa el mismo método tanto para realizar los pagos tradicionales como para la operativa DCC y, en función de los campos que se remitan en el XML de petición, se realizará una u otra opción.

El método de acceso "**consultaDCC**": permite hacer consultas del DCC asociado a un importe y una moneda con anterioridad a ejecutar la transacción. Es meramente informativo.

6.8.4.2 Mensaje de petición inicial

El mensaje de petición inicial (1. Petición de pago) posee las mismas características que lo descrito anteriormente en el apartado 6.8.1 de la guía del TPV Virtual WebService.

6.8.4.2.1 Mensaje de respuesta DCC

A continuación se describen los datos necesarios y sus características, que se recibirán en los mensajes de respuesta DCC (2. Respuesta monedas DCC) del TPV Virtual en el formato XML descrito anteriormente para la operativa DCC y que sirven como ejemplo para la posterior confirmación DCC.

NOMBRE DEL 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.

6.8.4.2.2 Ejemplo de respuesta DCC

Este es el XML que se devolverá cuando se realice una operación con 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>vXYlxTsfkVJ6ZL82vJ48Lvm</
DS_MERCHANT_SESION>
</RETORNOXML>
```

6.8.4.2.3 Mensaje de confirmación DCC

A continuación se describen los datos necesarios y sus características para enviar una petición de confirmación DCC (3. Confirmación moneda DCC) al TPV Virtual Webservice en el formato y que sirven como ejemplo para confirmar el anterior mensaje de petición DCC.

```
<REQUEST>
<DATOSENTRADA>
<DS_MERCHANT_ORDER>0804620125</DS_MERCHANT_ORDER>
<DS_MERCHANT_MERCHANTCODE>327234688</DS_MERCHANT_MERCHANTCODE>
<DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
<SIS_DIVISA>826#1.03</SIS_DIVISA>
<DS_MERCHANT_SESION>vXYlxTsfkVJ6ZL82vJ48Lvm</DS_MERCHANT_SESION>
</DATOSENTRADA>
<DS_SIGNATUREVERSION>HMAC_SHA256_V1</DS_SIGNATUREVERSION>
<DS_SIGNATURE>iJ13pCEL09CmJ8hosYjyWWUF/KYdPb1vsSuWGI3k1zg=</DS_SIGNATURE>
</REQUEST>
```

NOMBRE DEL 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	- / A	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.

6.8.4.2.4 Mensaje de respuesta a confirmación de moneda DCC

El mensaje de respuesta (4. Respuesta de pago) posee las mismas características que lo descrito anteriormente en el apartado 6.8.3. de la guía del TPV Virtual WebService.

6.8.5 Operativa Flexipago

La operativa de "**Compra Fácil**" o **Flexipago** consiste en que el comercio envíe un código de aplazamiento que el TPV Virtual debe validar y enviar a la pasarela de pagos de Banco Sabadell.

Esta operativa sólo es válida para operaciones con tarjetas de crédito de Banco Sabadell.

El comercio podrá utilizar cualquiera de los tipos de conexión del TPV Virtual.

En principio todos los comercios de la entidad podrán utilizar esta operativa. El TPV Virtual

sólo validará que el código de aplazamientos esté permitido para el Banco Sabadell y que la tarjeta sea On-Us de crédito.

Se enviará un pago normal, pero añadiendo el parámetro opcional **Ds_Merchant_PartialPayment**. En este parámetro se enviará el código de aplazamiento que se desee aplicar en la operación.

El sistema realizará validaciones básicas del formato del campo **Ds_Merchant_PartialPayment** y validará que sea uno de los permitidos por Banco Sabadell.

La pasarela de pagos validará que la tarjeta utilizada para el pago sea de crédito de Banco Sabadell y en caso contrario rechazará la operación.

Si el comercio ha enviado código de fraccionamiento, no se tendrá en cuenta la posibilidad de Pago Aplazado Emisor (PAE), aunque en la operación fuese susceptible de aplicarse.

6.8.5.1 Códigos de fraccionamiento

CODIGO	SIGNIFICADO
00006	90 días Compra fácil
00005	180 días Compra Fácil
00020	365 días Compra Fácil
00021	540 días Compra Fácil
00022	730 días Compra Fácil
00000	El cliente no desea fraccionar. Si se envía este valor no se realizará fraccionamiento y tampoco se ofrecerá la posibilidad de PAE.

6.8.6 Campos de peticiones de pago Webservice

6.8.6.1 Peticiones de pago (con envío de datos de tarjeta)

En el siguiente apartado se describen los datos necesarios y sus características, para enviar una petición al Web Service. Así mismo se incluye un ejemplo de cómo utilizar esos datos en los mensajes de petición de pago.

DATO	NOMBRE DEL DATO	LONG/TIPO	COMENTARIOS
Identificación de comercio: código FUC	Ds_Merchant_ MerchantCode	Max. 9/N.	Obligatorio. Código FUC asignado al comercio.
Número de terminal	Ds_Merchant_ Terminal	3/N.	Obligatorio. Número de terminal que le asignará su banco. Tres se considera su longitud máxima
Tipo de transacción	Ds_Merchant_ TransactionType	1 / Núm.	Obligatorio. Para el comercio para indicar qué tipo de transacción es. Los posibles valores son: A – Autorización tradicional 1 – Preautorización 2 – Confirmación de preautorización 3 – Devolución Automática 5 – Transacción Recurrente 6 – Transacción Sucesiva 7 – Pre-autenticación 8 – Confirmación de pre-autenticación 9 – Anulación de Preautorización O – Autorización en diferido P – Confirmación de autorización en diferido Q – Anulación de autorización en diferido R – Cuota inicial diferido S– Cuota sucesiva diferido
Importe	Ds_Merchant_ Amount	12 / Núm.	Obligatorio. Para Euros las dos últimas posiciones se consideran decimales.
Moneda	Ds_Merchant_ Currency	4 / Núm.	Obligatorio. Se debe enviar el código numérico de la moneda según el ISO-4217, por ejemplo: 978 euros 840 dólares 826 libras 392 yenes 4 se considera su longitud máxima
Número de Pedido	Ds_Merchant_Order	12 / A-N.	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

URL del comercio para la notificación “on-line”	Ds_Merchant_ MerchantURL	250/A-N	Obligatorio si el comercio tiene notificación “on-line”. URL del comercio que recibirá un post con los datos de la transacción.
Importe total (cuota recurrente)	Ds_Merchant_ SumTotal	12/N.	Obligatorio. Representa la suma total de los importes de las cuotas. Las dos últimas posiciones se consideran decimales.
Datos del comercio	Ds_Merchant_ MerchantData	1024 /A-N	Opcional para el comercio para ser incluidos en los datos enviados por la respuesta “on-line” al comercio si se ha elegido esta opción.
Frecuencia	Ds_Merchant_ DateFrecuency	5/ N	Frecuencia en días para las transacciones recurrentes y recurrentes diferidas (obligatorio para recurrentes)
Fecha límite	Ds_Merchant_ ChargeExpiryDate	10/ A-N	Formato yyyy-MM-dd fecha límite para las transacciones Recurrentes (Obligatorio para recurrentes y recurrentes diferidas)
Código de Autorización	Ds_Merchant_ AuthorisationCode	6 / Num	Opcional. Representa el código de autorización necesario para identificar una transacción recurrente sucesiva en las devoluciones de operaciones recurrentes sucesivas. Obligatorio en devoluciones de operaciones recurrentes.
Fecha de la operación recurrente sucesiva	Ds_Merchant_ TransactionDate	10 / A-N	Opcional. Formato yyyy-mm-dd. Representa la fecha de la cuota sucesiva, necesaria para identificar la transacción en las devoluciones. Obligatorio en las devoluciones de cuotas sucesivas y de cuotas sucesivas diferidas.
Identificador	Ds_Merchant_ Identifier	Max. 40 / A-N	El valor “REQUIRED” 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.
Número de terminal	Ds_Merchant_ Terminal	3/N.	Obligatorio. Número de terminal que le asignará su banco. Tres se considera su longitud máxima
Grupo de comercios	Ds_Merchant_Group	Max. 9/N	Opcional. Permite asociar una referencia a un conjunto de comercios.
Pantallas adicionales	Ds_Merchant_ DirectPayment	-	Opcional. Este parámetro funciona como un flag que indica s hay que mostrar pantallas adicionales (DCC, Fraccionamiento, Autenticación, etc.)
Código de fraccionamiento de operativa Flexipago	Ds_Merchant_ PartialPayment	5 / N	Opcional. Este parámetro permite aplicar uno de los tipos de fraccionamiento existentes: 00006 - 90 días 00005 - 180 días 00020 - 365 días 00021 - 540 días 00022 - 730 días 00000 - El cliente no desea fraccionar. Si se envía este valor no se realizará fraccionamiento y tampoco se ofrecerá la posibilidad de PAE.

A continuación se muestra un ejemplo de un mensaje de petición de pago:

```
<REQUEST>
<DATOSENTRADA>
<DS_MERCHANT_AMOUNT>145</DS_MERCHANT_
AMOUNT>
<DS_MERCHANT_ORDER>151029142229</DS_MER-
CHANT_ORDER>
<DS_MERCHANT_MERCHANTCODE>327234688</
DS_MERCHANT_MERCHANTCODE>
<DS_MERCHANT_CURRENCY>978</DS_MERCHANT_
CURRENCY>
<DS_MERCHANT_PAN>4548812049400004</
DS_MERCHANT_PAN>
<DS_MERCHANT_EXPIRYDATE>1512</DS_MERCHANT_
EXPIRYDATE>
<DS_MERCHANT_CVV2>285</DS_MERCHANT_CVV2>
<DS_MERCHANT_TRANSACTIONTYPE>A</DS_MER-
CHANT_TRANSACTIONTYPE>
<DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TER-
MINAL>
</DATOSENTRADA>
<DS_SIGNATUREVERSION>HMAC_SHA256_V1</
DS_SIGNATUREVERSION>
<DS_SIGNATURE>2YW19YQ8rb/0LLav79Y5L24Yw045K
xN5hme27605WxY=</DS_SIGNATURE>
</REQUEST>
```

6.8.6.2 Peticiones de Confirmación/ Devolución

En el presente anexo se describen los datos necesarios y sus características, para enviar una petición al Web Service de Banco Sabadell en formato XML para realizar confirmaciones o devoluciones.

NOMBRE DEL DATO	LONG/TIPO	COMENTARIOS
DS_MERCHANT_AMOUNT	12 / N	Obligatorio. Las dos últimas posiciones se consideran decimales, salvo en el caso de los Yenes que no tienen.
DS_MERCHANT_ORDER	12 / A-N	Obligatorio. Número de pedido. Los 4 primeros dígitos deben ser numéricos. Cada pedido es único, no puede repetirse.
DS_MERCHANT_ MERCHANTCODE	9 / N	Obligatorio. Código FUC asignado al comercio.
DS_MERCHANT_ TERMINAL	3 / N	Obligatorio. Para Euros las dos últimas posiciones se consideran decimales.
DS_MERCHANT_ CURRENCY	4 / N	Obligatorio. Moneda del comercio. Tiene que ser la contratada para el Terminal. Valor 978 para Euros, 840 para Dólares, 826 para Libras esterlinas y 392 para Yenes.
DS_MERCHANT_ TRANSACTIONTYPE	1 / A-N	Obligatorio. Campo para el comercio para indicar qué tipo de transacción es. Los posibles valores son: 2 – Confirmación 3 – Devolución Automática 6 – Transacción Sucesiva 9 – Anulación de Preautorización P - Confirmación de autorización en diferido Q - Anulación de autorización en diferido S – Autorización recurrente sucesiva diferido
DS_MERCHANT_ AUTHORISATIONCODE	6 / Num	Opcional. Representa el código de autorización necesario para identificar una transacción recurrente sucesiva en las devoluciones de operaciones recurrentes sucesivas. Obligatorio en devoluciones de operaciones recurrentes.

A continuación se muestra un ejemplo de un mensaje de petición de pago recurrente:

```
<REQUEST>
<DATOSENTRADA>
<DS_MERCHANT_AMOUNT>145</DS_MERCHANT_AMOUNT>
<DS_MERCHANT_ORDER>151029150450</DS_MER-
CHANT_ORDER>
<DS_MERCHANT_MERCHANTCODE>327234688</DS_MER-
CHANT_MERCHANTCODE>
<DS_MERCHANT_CURRENCY>978</DS_MERCHANT_CU-
RRENCY>
<DS_MERCHANT_TRANSACTIONTYPE>3</DS_MERCHANT_
TRANSACTIONTYPE>
<DS_MERCHANT_TERMINAL>2</DS_MERCHANT_TERMINAL>
</DATOSENTRADA>
<DS_SIGNATUREVERSION>HMAC_SHA256_V1</DS_SIGNA-
TUREVERSION>
<DS_SIGNATURE>uegr2AawcuVR4pK1KN5KiOI7Kzj6Y+8z4Hg
HRFTYglw=</DS_SIGNATURE>
</REQUEST>
```

6.8.6.3 Respuesta Web Service

A continuación se presenta una tabla que recoge todos los parámetros que forman parte de la respuesta del Web Service.

NOMBRE DEL DATO	LONG/TIPO	COMENTARIOS
CODIGO		Obligatorio. 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 un código. (Ver códigos de error en apartado 5 de esta Guía)
Ds_Amount	12 / A-N	Obligatorio. Para Euros las dos últimas posiciones se consideran decimales, salvo en el caso de los Yenes que no tienen.
Ds_Currency	4 / N	Obligatorio. Moneda del comercio.
Ds_Order	12 /A- N	Obligatorio. Número de pedido.
Ds_Signature	40 / A-N	Obligatorio. Firma del comercio.
Ds_MerchantCode	9 / N	Obligatorio. Código FUC asociado al comercio.
Ds_Terminal	3 / N	Obligatorio. Número de Terminal del comercio.
Ds_Response	4 / N	Obligatorio. Valor que indica el resultado de la operación. Indicará si ha sido autorizada o no. Los posibles valores de este campo se describen en la siguiente tabla.
Ds_AuthorisationCode	6 / N	Optativo. Código de autorización en caso de existir para las operaciones autorizadas.
Ds_TransactionType	1 / A-N	Obligatorio. Indica qué tipo de transacción se ha realizado. Los posibles valores son: A – Autorización tradicional 1 – Preautorización 2 – Confirmación 3 – Devolución Automática 5 – Transacción Recurrente 6 – Transacción Sucesiva 9 – Anulación de Preautorización O – Autorización en diferido P - Confirmación de autorización en diferido Q - Anulación de autorización en diferido R – Autorización recurrente inicial diferido S – Autorización recurrente sucesiva diferido

Ds_SecurePayment		Obligatorio. Indica si el pago ha sido seguro o no: • 0: seguro (no se aplica) • 1: no seguro.
Ds_Card_Number	15-19/A-N	Opcional: El valor de esta variable será el número de tarjeta asteriscado. Esta variable por defecto no se encuentra activada.
Ds_Merchant_Identifier	40/A-N	Referencia generada en la petición de pago por referencia. Esta variable solo se enviará si se ha activado la operativa de pago por referencia
Ds_ExpiryDate	4 / N	Fecha de caducidad de la tarjeta. Esta variable solo se enviará si se ha activado la operativa de pago por referencia

6.9 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 "Webservice": https://sis-t.redsys.es:25443/sis/services/SerClsWSEntrada

2. Número de comercio (Ds_Merchant_MerchantCode): 327234688
3. Clave secreta (Ds_Merchant_MerchantSignature): sq7HjrU0BfKmC576ILgskD5srU870gJ7
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 y Webservice (pagos considerados NO seguros)

5. Tarjeta aceptada:

- 4548 8120 4940 0004, caducidad 12/20, código CVV2: 533
- 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/bsabadell
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

6.9.1 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 del procesador de pagos de Banco Sabadell y por lo tanto el comercio evitará tener que cumplir los requerimientos de seguridad PCI-DSS.

- **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**', 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 entrada 'realizarPago'**: se devolverá la referencia y la fecha de caducidad en la notificación On-Line y en la URL OK.

  ii. **Para la entrada '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', 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.

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 ne- cesario 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 gene- rar 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 ente 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
- Nº 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; 7490da44 6dee0a...25b6bd52e086c3181
999008881;1;130211123739;
2013-02-1112.37.40.429;d5ac083cb97d183...548f168c32c7bb5ab7d

6.9.2 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

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).

Anexos

Anexo I. Códigos ISO países

Anexo II. Códigos ISO divisas

Anexo I. Códigos ISO países

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

Anexo I. Códigos ISO países

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

Anexo II. Códigos ISO divisas

Lek	ALL	8
Algerian Dinar	DZD	12
Angola Kwanza	AON	24
Argentine Peso	ARS	32
Australian Dollar	AUD	36
Bahamian Dollar	BSD	44
Bahraini Dinar	BHD	48
Taka	BDT	50
Armenian Dram	AMD	51
Barbados Dollar	BBD	52
Bermudian Dollar	BMD	60
Ngultrum	BTN	64
Boliviano	BOB	68
Dinar	BAM	70
Pula	BWP	72
Cruzeiro	BRC	76
Belize Dollar	BZD	84
Solomon Islands Dollar	SBD	90
Brunei Dollar	BND	96
Kyat	MMK	104
Burundi Franc	BIF	108
Bellarusian Ruble	BYB	112
Riel	KHR	116
Canadian Dollar	CAD	124
Cape Verde Escudo	CVE	132
Cayman Islands Dollar	KYD	136
Sri Lanka Rupee	LKR	144
Chilean Peso	CLP	152
Yuan Renminbi	CNY	156
Chinese Renmimbi	CNH	157
Chinese Renmimbi	CNX	158
Colombian Peso	COP	170
Comoro Franc	KMF	174
Costa Rican Colon	CRC	188
Croatian Kuna	HRK	191
Cuban Peso	CUP	192
Cyprus Pound	CYP	196
Koruna	CSK	200
Czech Koruna	CZK	203
Danish Krone	DKK	208
Dominican Peso	DOP	214
El Salvador Colon	SVC	222
Ethiopian Birr	ETB	230
Nakfa	ERN	232
Kroon	EEK	233
Falkland Islands Pound	FKP	238
Fiji Dollar	FJD	242
Djibouti Franc	DJF	262
Dalasi	GMD	270
Ghana Cedi	GHC	288
Gibraltar Pound	GIP	292
Quetzal	GTQ	320
Guinea Franc	GNF	324
Guyana Dollar	GYD	328
Gourde	HTG	332
Lempira	HNL	340
Hong Kong Dollar	HKD	344
Forint	HUF	348
Iceland Krona	ISK	352
Indian Rupee	INR	356
Rupiah	IDR	360
Iraqi Dinar	IQD	368
New Israeli Sheqel	ILS	376
Jamaican Dollar	JMD	388
Yen	JPY	392
Tenge	KZT	398
Jordanian Dinar	JOD	400
Kenyan Shilling	KES	404
Won	KRW	410
Kuwaiti Dinar	KWD	414
Som	KGS	417
Kip	LAK	418
Lebanese Pound	LBP	422
Loti	LSL	426
Latvian Lats	LVL	428
Liberian Dollar	LRD	430
Libyan Dinar	LYD	434
Lithuanian Litas	LTL	440
Pataca	MOP	446
Malagassy Franc	MGF	450
Kwacha	MWK	454
Malaysian Ringgit	MYR	458
Rufiyaa	MVR	462
Mali	MLF	466
Maltese Lira	MTL	470
Ouguiya	MRO	478
Mauritius Rupee	MUR	480
Mexican Peso	MXN	484
Tugrik	MNT	496
Moldovan Leu	MDL	498
Moroccan Dirham	MAD	504
Rial Omani	OMR	512

Anexo II. Códigos ISO divisas

Namibia Dollar	NAD	516
Nepalese Rupee	NPR	524
Netherlands Antillian Guilder	ANG	532
Aruban Guilder	AWG	533
Yugoslavian New Dian	NTZ	536
Vatu	VUV	548
New Zealand Dollar	NZD	554
Naira	566	556
Cordoba Oro	NIO	558
Naira	NGN	566
Norwegian Krone	NOK	578
Pacific Island	PCI	582
Pakistan Rupee	PKR	586
Balboa	PAB	590
Kina	PGK	598
Guarani	PYG	600
Nuevo Sol	PEN	604
Philippine Peso	PHP	608
Guinea-Bissau Peso	GWP	624
Timor Escudo	TPE	626
Qatari Rial	QAR	634
Russian Ruble	RUB	643
Rowanda Franc	RWF	646
Saint Helena Pound	SHP	654
Dobra	STD	678
Saudi Riyal	SAR	682
Seychelles Rupee	SCR	690
Leone	SLL	694
Singapore Dollar	SGD	702
Dong	VND	704
Slovenian Tolar	SIT	705
Somali Shilling	SOS	706
Rand	ZAR	710
Zimbabwe Dollar	ZWD	716
Yemeni Dinar	YDD	720
Sudanese Pound	SDP	736
Sudan Airlines	SDA	737
Lilangeni	SZL	748
Swedish Krona	SEK	752
Swiss Franc	CHF	756
Syrian Pound	SYP	760
Tajik Ruble	TJR	762
Baht	THB	764
Pa'anga	TOP	776
Trinidad and Tobago Dollar	TTD	780
UAE Dirham	AED	784
Tunisian Dinar	TND	788
Turkish Lira	PTL	793
Manat	TMM	795
Uganda Shilling	UGX	800
Karbovanet	UAK	804
Denar	MKD	807
Egyptian Pound	EGP	818
Pound Sterling	GBP	826
Tanzanian Shilling	TZS	834
US Dollar	USD	840
Peso Uruguayo	UYU	858
Uzbekistan Sum	UZS	860
Tala	WST	882
Yemeni Rial	YER	886
Serbian Dinar	CSD	891
Zambian Kwacha	ZMK	894
New Taiwan Dollar	TWD	901
Manat	TMT	934
Cedi	GHS	936
Bolivar Fuerte	VEF	937
Serbian Dinar	RSD	941
Metical	MZN	943
Azerbaijanian Manat	AZN	944
New Leu	RON	946
Turkish Lira	TRY	949
CFA Franc BEAC	XAF	950
East Caribbean Dollar	XCD	951
CFA Franc BCEAO	XOF	952
CFP Franc	XPF	953
European Currency UN	XEU	954
Kwacha	ZMW	967
Surinam Dollar	SRD	968
Malagasy Ariary	MGA	969
Afghani	AFN	971
Somoni	TJS	972
Kwanza	AOA	973
Belarussian Ruble	BYN	974
Bulgarian Lev	BGN	975
Congolese Franc	CDF	976
Convertible Marks	BAM	977
Euro	EUR	978
Hryvnia	UAH	980
Lari	GEL	981
Zloty	PLN	985
Brazilian Real	BRL	986
Peseta Convertible	ESB	995

01-2018