Integrar en Ingenico ePayments DirectLink (de servidor a servidor)

Tabla de contenidos

8.2 Métodos de pago con solo mantenimiento a través de DirectLink

1. Introducción

Ingenico ePayments DirectLink le permite configurar una integración de servidor a servidor con nuestra plataforma. Mientras que con Ingenico ePayments e-Commerce el cliente era redireccionado a la página de pago seguro (alojada por Ingenico ePayments), con DirectLink el cliente permanece en una página propia que enviará de forma segura los datos de pago a nuestros servidores.

También puede usar DirectLink para las tareas de mantenimiento de transacciones, independientemente de que se hayan iniciado en DirectLink o en, por ejemplo, el modo e-Commerce.

Con DirectLink, no hay contacto entre nuestro sistema y el cliente del comerciante. Su sistema transmite toda la información necesaria para realizar directamente el pago en nuestro sistema en una solicitud HTTPS POST. Nuestro sistema solicita la transacción financiera (de forma sincrónica o asincrónica) a la entidad adquirente correspondiente y devuelve la respuesta a su servidor en formato XML. Su programa lee la respuesta y reanuda su procesamiento.

Será, por tanto, responsable de recopilar y almacenar los detalles de pago confidenciales del cliente y deberá garantizar la confidencialidad y seguridad de estos detalles mediante la seguridad del servidor y la comunicación web cifrada.

Para almacenar datos de tarjeta y personales, debe cumplir con las normas PCI

2. Configuración de seguridad y procedimientos generales

Los siguientes procedimientos generales y controles de seguridad son válidos para solicitudes de DirectLink: nuevas solicitudes de pedidos, solicitudes de mantenimiento y consultas directas.

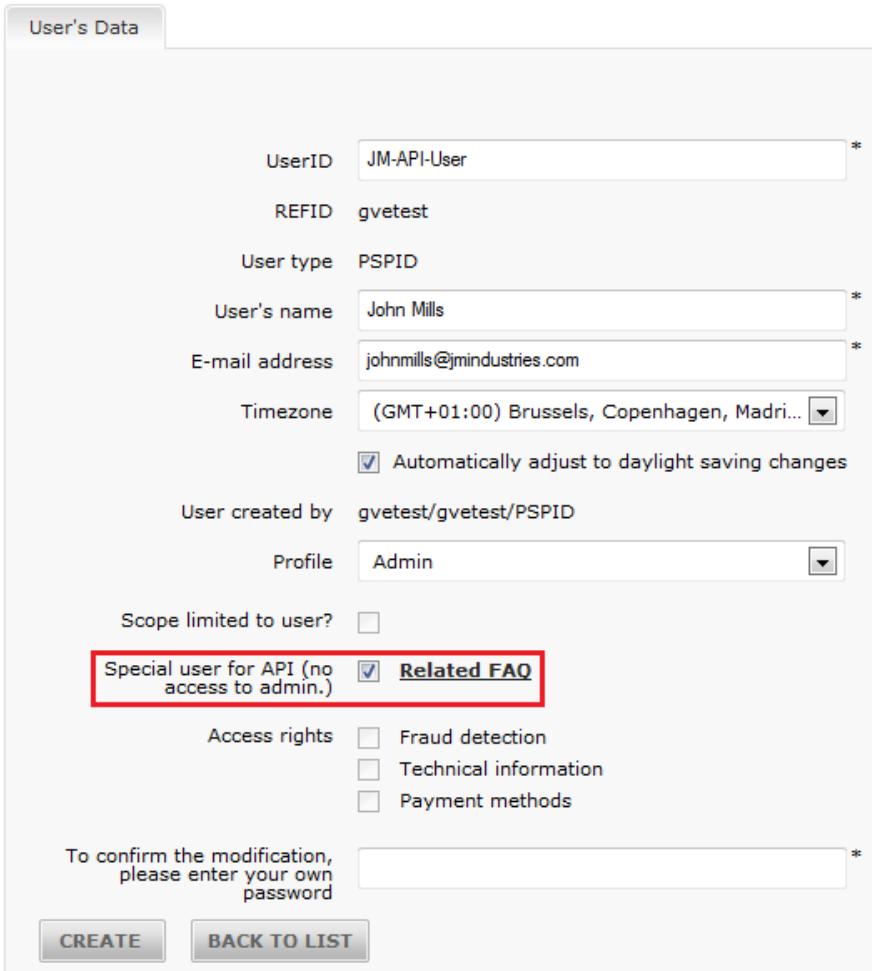
2.1 Usuario API

Para realizar solicitudes con DirectLink, se requiere un usuario de interfaz de programación de aplicaciones (API, Application Program Interface).

En general, se trata de un usuario diseñado de forma específica para que la aplicación lo utilice para realizar solicitudes automáticas a la plataforma de pago.

Puede crear un usuario API en su cuenta de Ingenico ePayments a través de "Configuración" > "Usuarios". Seleccione "Nuevo usuario" y complete los campos necesarios.

Para convertir al nuevo usuario en un usuario API, asegúrese de habilitar la casilla "Usuario Especial para el API (sin acceso a admin.)".



Aunque un usuario API disponga de diversos perfiles de usuario, recomendamos encarecidamente que configure este usuario con el perfil "Admin" (Administración).
Si desea limitar los derechos para el mantenimiento de transacciones (reembolsos, cancelaciones, etc.), puede seguir cambiando el perfil de usuario a, por ejemplo, "Codificador".

Si no está seguro, es recomendable que seleccione el perfil "Admin"; si no, vaya aPerfiles de usuario (Administrador de usuarios) para obtener más información.

La contraseña de un usuario API no tiene que cambiarse de forma regular. Es más cómodo cuando la contraseña debe modificarse en su aplicación. No obstante, recomendamos que cambie la contraseña de vez en cuando.

Si desea más información sobre tipos de usuario y cómo cambiar la contraseña del usuario API, vaya a Tipos de usuario (Administrador de usuarios).

2.2 Formulario de solicitud

Para nuevas solicitudes de pedido, solicitudes de mantenimiento y consultas directas, debe enviar las solicitudes con determinados parámetros a las URL específicas. Los parámetros de nuevo pedido/mantenimiento/consulta deben enviarse en una solicitud POST de la siguiente forma:

PSPID=value1&USERID=value2&PSWD=value3&...

El tipo/subtipo que indica el tipo de medio en el campo Content-Type entity-header de la solicitud POST debe ser "application/x-www-form-urlencoded".

DirectLink funciona en modo “una solicitud-una respuesta”. Cada pago se procesa de forma individual. Nuestro sistema gestiona las solicitudes de transacción individuales a través de DirectLink y puede funcionar de forma sincrónica. (donde está opción es compatible desde un punto de vista técnico). Por ejemplo, esperamos la respuesta del banco antes de devolver una respuesta XML para la solicitud.

2.3 Seguridad

Cuando recibimos una solicitud en nuestros servidores, comprobamos el nivel de cifrado y la dirección IP desde la que se envió la solicitud.

2.3.1 Cifrado

DirectLink se basa en un protocolo sólido de comunicación segura. DirectLink El API de lote es un conjunto de instrucciones enviadas con solicitudes HTTPS POST estándar.

En el extremo del servidor, usamos un certificado proporcionado por Verisign. El cifrado TLS garantiza que se comunica con nuestros servidores y que sus datos se transmiten de forma cifrada. No es necesario un certificado TLS de cliente.

Cuando recibimos una solicitud, comprobamos el nivel de cifrado. Permitimos a los comerciantes que se pongan en contacto con nosotros solo mediante el modo https seguro, usando protocolos TLS y recomendamos encarecidamente utilizar las versiones más recientes y seguras, que actualmente son TLS 1.1 y 1.2.

Nota: En este momento, seguimos siendo compatibles con SSL v3. No obstante, debido a determinadas vulnerabilidades, este protocolo se está quedando anticuado y con el tiempo dejará de ser compatible.

2.3.2 Dirección IP

Con cada solicitud, nuestro sistema comprueba la dirección IP en la que se originó la solicitud para garantizar que las solicitudes se están enviando desde el servidor del comerciante. En el campo Dirección IP de la sección "Comprobaciones de DirectLink" de la pestaña "Verificación de datos y origen" de la página Información técnica de la cuenta, debe especificar la dirección o las direcciones IP o el rango o

rangos IP de los servidores que envíen sus solicitudes.

Si la dirección IP de origen no se ha declarado en el campo de dirección IP correspondiente, recibirá el mensaje de error “pedido desconocido/1/i”. La dirección IP desde la que se envió la solicitud también aparecerá en el mensaje de error.

2.3.3 Firma SHA

La firma SHA se basa en el principio del servidor del comerciante que genera una cadena de caracteres única para cada pedido, generando un hash con algoritmos SHA-1, SHA-256 o SHA-512. El resultado de este hash se nos envía más adelante en su solicitud de pedido. Nuestro sistema reconstruye esta firma para comprobar la integridad de los datos del pedido que se nos han enviado en la solicitud.

Vaya a Firma SHA-IN (documentación de Ingenico ePayments e-Commerce). El principio es el mismo en modo e-Commerce y DirectLink.

Para DirectLink, la frase de contraseña SHA-IN debe configurarse en la sección "Comprobaciones de DirectLink" en la pestaña "Verificación de datos y origen" de su página Información técnica.

2.4 Análisis de respuesta

Devolveremos una respuesta XML a su solicitud. Asegúrese de que sus sistemas analizan esta respuesta XML con la mayor tolerancia posible para evitar problemas en el futuro. Por ejemplo, evitar nombres de atributos que distinguen mayúsculas de minúsculas, no formular un orden específico para los atributos devueltos en respuestas, garantizar que los nuevos atributos de la respuesta no causen problemas, etc.

3. Solicitud de nuevo pedido

3.1 URL de solicitud

- La URL de solicitud en el entorno de PRUEBA es https://ogone.test.v-psp.com/ncol/test/orderdirect.asp.
- La URL de solicitud en el entorno de PRODUCCIÓN es https://secure.ogone.com/ncol/prod/orderdirect.asp.

Cambiar "test" a "prod"

Sustituya “test” por “prod” en la URL de solicitud cuando cambie a la cuenta de producción. Si olvida cambiar la URL de solicitud una vez que inicia la producción con pedidos reales, las transacciones se enviarán al entorno de prueba y no serán procesadas por las entidades adquirientes/los bancos, por lo que no recibirá el pago.

3.2 Parámetros de solicitud

La siguiente tabla contiene los parámetros de solicitud para enviar una nueva solicitud de pedido:

Formato: AN= Alfanumérico/N=Numérico, cantidad máxima de caracteres permitida

Campo	Descripción	Formato	Obligatorio
PSPID	Su nombre de afiliación en nuestro sistema.	AN, 30	Sí
ORDERID	Su número de pedido único (referencia del comerciante).	AN, 40	Sí
USERID	Nombre de su usuario de aplicación (API). Consulte la documentación del Administrador de usuarios para obtener información sobre cómo crear un usuario API.	AN, 20 (mín. 2)	Sí
PSWD	Contraseña del usuario API (USERID).	AN	Sí
AMOUNT	Importe a pagar MULTIPLICADO POR 100, ya que el formato del importe no debe contener decimales u otros separadores.	N, 15	Sí
CURRENCY	Código de divisa de pedido alfa ISO, por ejemplo: EUR, USD, GBP, CHF, etc.	AN, 3	Sí
CARDNO	Número de tarjeta/cuenta.	AN, 21	Sí
ED	Fecha de caducidad.	MM/AA o MMAA	Sí
COM	Descripción del pedido.	AN, 100	No
CN	Nombre del cliente.	AN, 35	No
EMAIL	Dirección de correo electrónico del cliente.	AN, 50	No
SHASIGN	Firma (cadena con hash) para autenticar los datos (consulte Firma SHA-IN).	AN, 128	Sí

Campo	Descripción	Formato	Obligatorio
CVC	Código de verificación de la tarjeta. Dependiendo de la marca de la tarjeta, el código de verificación tendrá 3 o 4 dígitos en la parte delantera o posterior de la tarjeta, una fecha de inicio o una fecha de nacimiento.	N, 5	Sí
ECOM_PAYMENT_CARD_VERIFICATION	Alternativa a CVC: fecha de nacimiento/número de problema/etc. (dependiendo del país/banco)	N, 5	No
OWNERADDRESS	Número y nombre de la calle del cliente.	AN, 50	No
OWNERZIP	Código postal del cliente.	AN, 10	No
OWNERTOWN	Nombre de la localidad del cliente.	AN, 40	No
OWNERCTY	País del cliente, por ejemplo, BE, NL, FR, etc.	AN, 2	No
OWNERTELNO	Número de teléfono del cliente.	AN, 30	No
OPERATION	Define el tipo de transacción solicitado. Puede configurar una operación predeterminada (procedimiento de pago) en la pestaña "Parámetros de transacción globales", en la sección "Valor de ECI predeterminado" de la página Información técnica. Cuando envíe un valor de operación en la solicitud, este sobrescribirá el valor predeterminado. Valores posibles: • RES: solicitud de autorización • SAL: solicitud de venta directa • RFD: reembolso, no vinculado con un pago anterior. Por ejemplo, una operación de que no es de mantenimiento en una transacción existente (no se puede utilizar esta operación sin permiso específico de su entidad adquirente). Opcional: • PAU: Solicitud de preautorización: De acuerdo con la entidad adquiriente puede utilizar este código de operación para reservar fondos de forma temporal en la tarjeta de un cliente. Se trata de una práctica común en el sector de viajes y alquiler. En estos momentos, PAU/preautorización solo se puede utilizar en transacciones de MasterCard y es compatible con entidades adquirientes seleccionadas. Este código de operación no se puede definir como valor predeterminado en su cuenta de Ingenico ePayments. En el caso de que utilice PAU en transacciones a través de entidades adquirientes o con marcas de tarjetas que no admiten preautorización, estas transacciones no se bloquearán, sino que se procesarán como autorizaciones (RES) normales.	A, 3	Sí
WITHROOT	Añade un elemento raíz a nuestra respuesta XML. Valores posibles: 'Y' o vacío.	Y o <vacío.>	No

Campo	Descripción	Formato	Obligatorio
REMOTE_ADDR	Dirección IP del cliente (solo para el módulo de detección de fraude). Si no es necesario realizar una comprobación de país en la dirección IP, envíe "NONE".	AN	No
RTIMEOUT	Tiempo de espera de solicitud para la transacción (en segundos, valor entre 30 y 90) Importante: El valor definido aquí debe ser inferior al valor de tiempo de espera de su sistema (!)	N, 2	No
ECI	Indicador de comercio electrónico. Puede configurar un valor ECI predeterminado en la página Información técnica de su cuenta, pestaña "Parámetros de transacción globales", sección "Valor ECI predeterminado". Cuando envíe un valor ECI en la solicitud, este sobrescribirá el valor ECI predeterminado. Posibles valores (numéricos): 0 - Pasada por el lector 1 - Introducción manual (MOTO) (tarjeta no presente) 2 - Periódico (desde MOTO) 3 - Pagos a plazo 4 - Introducción manual, tarjeta presente 7 - Comercio electrónico con cifrado SSL 9 - Periódico (desde comercio electrónico)	N, 2	No

Los siguientes parámetros entran dentro del ámbito de aplicación de la directiva Credential-on-File (COF) de los esquemas de pago Visa / MasterCard. Se puede encontrar información detallada sobre su uso en el capítulo dedicado "Procesamiento de transacciones con credenciales guardadas".

COF_INITIATOR	Credential-on-file initiator Valores posibles: • CIT: Transacción iniciada por el titular de la tarjeta • MIT: Transacción iniciada por un comerciante	AN	No
COF_SCHEDULE	Credential-on-files programada (o no programada) Valores posibles: • SCHED: Transacción programada • UNSCHED: Transacción no programada	AN	No
COF_TRANSACTION	Credential-on-file transaction Valores posibles: • FIRST: Primera serie de transacciones	AN	No

	• SUBSEQ: Siguientes series de transacciones		
COF_RECURRING_EXPIRY	Fecha de fin: fecha del último pago programado de une serie	Fecha YYYYMMDD (por ejemplo: 20190914)	No
COF_RECURRING_FREQUENCY	Días entre pagos de una serie.	numérico entre 2 y 4 digitos (por ejemplo: 31, 031 o 0031)	No

La lista de posibles parámetros que enviar puede ser más larga para comerciantes que hayan activado determinadas funcionalidades/opciones en sus cuentas. Consulte la documentación de la opción correspondiente para obtener más información acerca de los parámetros adicionales vinculados a la opción.
Los siguientes parámetros de solicitud son obligatorios en los pedidos nuevos:

- PSPID y USERID
- PSWD
- ORDERID
- AMOUNT (x 100)
- CURRENCY
- CARDNO
- ED
- CVC
- OPERATION

3.3 Página de prueba

Nuestra página de prueba para enviar solicitudes de pedido en DirectLink está disponible aquí: https://ogone.test.v-psp.com/ncol/test/testodl.asp.

3.4 Excluding specific payment methods

If there are payment methods you don't want a customer to be able to pay with, you can use a parameter to do so.
This is particularly useful for sub-brands, when you want to accept a brand (e.g. MasterCard) but not one of its sub-brands (e.g. Maestro).

The parameter is the following:

Field	Usage
EXCLPMLIST	List of payment methods and/or credit card brands that should NOT be used, separated by a ";" (semicolon).

If a customer tries paying with a card linked to a payment method and/or (sub)brand you've excluded using the EXCLPMLIST parameter, the error message "Card number incorrect or incompatible" will be returned with the NCERRORPLUS return field.

3.5 Solicitud de pedido mediante 3-D Secure

Nuestro sistema admite el uso de 3-D Secure con DirectLink.

Importante

- Si desea utilizar 3-D Secure con DirectLink, es necesario que tenga la opción D3D activada en su cuenta.

- Algunos bancos adquirentes requieren el uso de 3-D Secure. Consulte con su entidad adquirente si este es su caso.

3.6 Dividir tarjetas de crédito/débito

La funcionalidad para dividir VISA y MasterCard en un método de pago de débito y de crédito le permite ofrecérselo a sus clientes como dos métodos de pago distintos (p. ej. VISA Débito y VISA Crédito) o puede decidir aceptar solo una de las dos marcas divididas.

Para utilizar la división de tarjetas de crédito y débito a través de DirectLink, tiene que incluir el parámetro CREDITDEBIT en los campos ocultos que envía a la página orderdirect.asp (y por tanto también se incluyen en el cálculo de SHA-IN).

Campo	Formato
CREDITDEBIT	"C": tarjeta de crédito "D": tarjeta de débito

Error relacionado: Cuando el comprador selecciona el método de tarjeta de crédito, pero introduce a continuación un número de tarjeta de crédito, se devuelve un código de error: ‘Se ha elegido una marca/método de pago incorrecto’.

Si el pago se ha procesado de forma correcta con el parámetro CREDITDEBIT, se devolverá el mismo parámetro en la respuesta XML o podrá solicitarse con una consulta directa. No obstante, mientras que los valores enviados sean C o D, los valores devueltos son "CREDIT" o "DEBIT".

También encontrará estos valores devueltos en la descripción general de la transacción a través de "Ver transacciones" e "Historial financiero", así como en informes que puede descargar más adelante.

Configuración en su cuenta

La funcionalidad de división también se puede activar y configurar según el método de pago en su cuenta de Ingenico ePayments. Acceda a Dividir tarjetas de crédito/débito para obtener más información.

3.7 Procesamiento de transacciones con credenciales guardadas

La transacción de credencial en archivo (COF) utiliza los detalles de la tarjeta que ya están almacenados por los comerciantes para procesar el pago. Antes de iniciar una transacción de credencial en archivo (COF), el titular de la tarjeta primero deberá autorizar al comerciante a almacenar los detalles de la tarjeta. La transacción de credencial en archivo (COF) se aplica principalmente a los pagos recurrentes y establece si es el titular de la tarjeta o el comerciante quien inicia el pago.

Hay dos tipos de transacciones de credenciales en archivo (COF): transacción iniciada por el titular de la tarjeta (CIT) o transacción iniciada por el comerciante (MIT). La transacción iniciada por el titular de la tarjeta (CIT) siempre deberá realizarse antes de la transacción iniciada por el comerciante (MIT).

Una transacción iniciada por el titular de la tarjeta (CIT) es una transacción en la que el titular de la tarjeta participa en la transacción y autentica personalmente la transacción mediante una firma, un dispositivo 3D-Secure o la presentación de documentos identificativos.

Ejemplo de una transacción iniciada por el titular de la tarjeta (CIT):

El titular de una tarjeta compra un billete de tren en línea y realiza un pago. Realiza el pago con su tarjeta de crédito y se le pide que

autentique y autorice el pago. Al mismo tiempo, se pregunta al titular de la tarjeta si desea guardar la información de la tarjeta de crédito relacionada con este pago. Si el titular de la tarjeta está de acuerdo, esta información se puede reutilizar en futuras transacciones iniciadas por el comerciante.

Una transacción iniciada por el comerciante (MIT) es una transacción iniciada por un comerciante que supervisa una transacción iniciada por el titular de la tarjeta (CIT) y por un pedido permanente previamente acordado de bienes y servicios comprados por el titular de la tarjeta. El titular de la tarjeta no tiene por qué estar involucrado en la transacción.

Ejemplo de una transacción iniciada por un comerciante (MIT):

Un comerciante puede iniciar automáticamente una transacción para cumplir con el pago del titular de la tarjeta en una suscripción mensual a una revista.

De acuerdo con las regulaciones establecidas por Visa y MasterCard para la transacción de credencial en archivo (COF), se deben enviar nuevos parámetros para determinar la transacción COF.

Esto le afecta si:

- Utiliza un alias
- Planea iniciar transacciones recurrentes (programadas o no) después de iniciar por primera vez una transacción iniciada por el titular de la tarjeta (CIT)

Acción necesaria:

De forma predeterminada, estos parámetros se utilizan en una transacción de DirectLink Server-to-Server:

Valores de parámetros COF_INITIATOR-COF_TRANSACTION-COF_SCHEDULE	Descripción
CIT-FIRST-UNSCHED	Se aplica cuando se utiliza o se crea un alias
CIT-FIRST-SCHED	Se aplica a un pago/suscripción programados
MIT-SUBSEQ-UNSCHED	Se aplica a pagos recurrentes
MIT-SUBSEQ-SCHED	Se aplica a pagos de cuotas

Los valores predeterminados se marcan si no se añade ningún parámetro. Sin embargo, si desea cambiarlos, puede sobrescribir estos valores predeterminados enviando los nuevos parámetros. No olvide recalcular también la firma SHA (**haga clic aquí** para obtener más información sobre la firma SHA.)

Parámetros	Valores	Descriptíon
COF_INITIATOR	CIT	Transacción iniciada por el titular de la tarjetar
	MIT	Transacción iniciada por un comerciante
COF_SCHEDULE	SCHED	Transacción programada
	UNSCHED	Transacción no programada

Parámetros	Valores	Descriptíon
COF_TRANSACTION	FIRST	Primera serie de transacciones
	SUBSEQ	Siguientes series de transacciones
COF_RECURRING_EXPIRY	Fecha YYYYMMDD (por ejemplo: 20190914)	Fecha de fin: fecha del último pago programado de une serie
COF_RECURRING_FREQUENCY	numérico entre 2 y 4 digitos (por ejemplo: 31, 031 o 0031)	Días entre pagos de una serie.

4. Respuesta de pedido

Nuestro servidor devuelve una respuesta XML a la solicitud:

Ejemplo de una respuesta XML a una solicitud de pedido

```
<?xml version=”1.0”?>
<ncresponse orderID=”99999” PAYID=”1111111” NCSTATUS=”0” NCERROR=”” NCERRORPLUS=”” ACCEPTANCE=”12345”
STATUS=”5” ECI=”7” amount="125" currency="EUR" PM="CreditCard" BRAND="VISA"/>
```

La siguiente tabla contiene una lista de los atributos de etiqueta ncresponse:

Campo	Descripción
ACCEPTANCE	Código de aceptación devuelto por la entidad adquiriente.
amount	Importe del pedido (sin multiplicar por 100).
BRAND	Marca de la tarjeta o información similar para otros métodos de pago.
currency	Divisa del pedido.
ECI	Indicador de comercio electrónico.
NCERROR	Código de error.
NCERRORPLUS	Explicación del código de error.
NCSTATUS	Primer dígito de NCERROR.
orderID	Su referencia de pedido.
PAYID	Referencia de pago en nuestro sistema.
PM	Método de pago.
STATUS	Estado de la transacción. (Posibles estados)

La lista de atributos puede ser más larga para comerciantes que tengan activadas determinadas opciones (por ejemplo, la Detección de fraude) en sus cuentas. Consulte la documentación de la opción correspondiente para obtener más información acerca de los atributos de respuesta adicionales vinculados a la opción.

4.1 Solicitud duplicada

Si su solicitud se procesa para un orderID ya existente (y correctamente procesado) nuestra respuesta XML contendrá el PAYID correspondiente al orderID existente, la aceptación (ACCEPTANCE) que le haya dado la entidad adquirente en el procesamiento anterior, STATUS “0” y NCERROR “50001113”.

5. Mantenimiento directo

Una solicitud de mantenimiento directa de su aplicación le permite:

- Realizar una captura de datos (pago) de un pedido autorizado de forma automática (en lugar de hacerlo manualmente en el área de administración);
- Cancelar una autorización sobre un pedido;
- Renovar una autorización de un pedido;
- Reembolsar un pedido pagado.

Las capturas de datos, las cancelaciones de autorización y las renovaciones de autorización son específicamente para comerciantes que hayan configurado su cuenta o sus solicitudes para realizar la autorización y la captura de datos en dos fases.

5.1 Solicitud de mantenimiento

5.1.1 URL de solicitud

- La URL de solicitud del entorno de PRUEBA es https://ogone.test.v-psp.com/ncol/test/maintenancedirect.asp.
- La URL de solicitud del entorno de PRODUCCIÓN es https://secure.ogone.com/ncol/prod/maintenancedirect.asp.

Cambiar "test" a "prod"

Sustituya “test” por “prod” en la URL de solicitud cuando cambie a la cuenta de producción. Si olvida cambiar la URL de solicitud una vez que empiece a trabajar con pedidos reales, las transacciones de mantenimiento se enviarán al entorno de prueba y no a las entidades adquirientes/los bancos.

5.1.2 Parámetros de solicitud

La siguiente tabla contiene los parámetros de solicitud obligatorios para realizar una operación de mantenimiento:

Campo	Descripción
AMOUNT	Importe del pedido multiplicado por 100. Sólo es necesario cuando el importe del mantenimiento difiere del importe de la autorización original. No obstante, recomendamos su uso en todos los casos. Nuestro sistema comprobará que el importe de la transacción de mantenimiento no sea más alto que el importe de autorización/pago.
OPERATION	Valores posibles: • REN: renovación de autorización, si la autorización original ya no es válida. • DEL: eliminar autorización, dejando la transacción abierta para más operaciones de mantenimiento potenciales. • DES: eliminar autorización, cerrando la transacción después de esta operación. • SAL: captura de datos parcial (pago), dejando la transacción abierta para otra captura de datos potencial. • SAS: captura (final) de datos parcial o completa (pago), cerrando la transacción (para capturas de datos adicionales) después de esta captura de datos. • RFD: reembolso parcial (de un pedido pagado), dejando la transacción abierta para otro reembolso potencial. • RFS: reembolso (final) parcial o completo (para un pedido pagado), cerrando la transacción después de este reembolso. Tenga en cuenta que, con DEL y DES, no todas las entidades adquirentes admiten la eliminación de una

Campo	Descripción
	autorización. Si la entidad adquirente no admite DEL/DES, simularemos en cualquier caso la eliminación de la autorización en el área de administración.
ORDERID	Puede enviar el PAYID o el orderID para identificar el pedido original. Recomendamos el uso del PAYID.
PAYID	
PSPID	El PSPID de su cuenta.
PSWD	Contraseña del usuario API
SHASIGN	Firma (cadena con hash) para autenticar los datos (consulte Firma SHA-IN).
USERID	Su usuario API

5.1.3 Página de prueba

Puede probar las solicitudes de mantenimiento directas aquí: https://ogone.test.v-psp.com/ncol/test/testdm.asp

5.2 Respuesta de mantenimiento

Nuestro servidor devuelve una respuesta XML a la solicitud:

Ejemplo de una respuesta XML a una solicitud de mantenimiento directa

```
<?xml version=”1.0”?>
<ncresponse orderID=”99999” PAYID=”1111111” PAYIDSUB=”3” NCSTATUS=”0” NCERROR=”” NCERRORPLUS=””
ACCEPTANCE=”12345” STATUS="91" amount="125" currency="EUR"/>
```

La siguiente tabla contiene una lista de los atributos de etiqueta ncresponse:

Campo	Descripción
ACCEPTANCE	Código de aceptación devuelto por la entidad adquiriente
AMOUNT	Importe del pedido (sin multiplicar por 100)
CURRENCY	Divisa del pedido
NCERROR	Código de error
NCERRORPLUS	Explicación del código de error
NCSTATUS	Primer dígito de NCERROR
ORDERID	Su referencia de pedido
PAYID	Referencia de pago en nuestro sistema
PAYIDSUB	El ID de nivel de historial de la operación de mantenimiento del PAYID

Campo	Descripción
STATUS	Estado de la transacción (Posibles estados)

Los atributos de etiqueta ncresponse estándar son los mismos que los de la respuesta XML a un nuevo pedido, salvo el atributo extra PAYIDSUB.

5.3 Solicitud duplicada

Si se solicita mantenimiento dos veces para el mismo pedido, el segundo se rechazará, en teoría, con un error “50001127” (este pedido no está autorizado), porque la transacción correcta inicial habrá cambiado el estado del pedido.

6. Consulta directa

Una solicitud de consulta directa de su aplicación le permite consultar el estado de un pedido de forma automática (a diferencia de manualmente en el área de administración). Solo puede consultar un pago a la vez y solo recibirá un importe limitado de información sobre el pedido.

Si necesita más detalles sobre el pedido, puede buscar la transacción en el área de administración o realizar una descarga de archivo manual o automática (consulte Consultar sus transacciones y Fichero de Lote).

6.1 Solicitud de consulta

6.1.1 URL de solicitud

- La URL de solicitud del entorno de PRUEBA es https://ogone.test.v-psp.com/ncol/test/querydirect.asp
- La URL de solicitud del entorno de PRODUCCIÓN es https://secure.ogone.com/ncol/prod/querydirect.asp

Cambiar "test" a "prod"

Sustituya “test” por “prod” en la URL de solicitud cuando cambie a la cuenta de producción.

6.1.2 Parámetros de solicitud

La siguiente tabla contiene los parámetros de solicitud obligatorios para realizar una consulta directa:

Campo	Descripción
ORDERID	Puede enviar el PAYID o el ORDERID para identificar el pedido original. Recomendamos el uso del PAYID.
PAYID	
PAYIDSUB	Puede indicar el ID de nivel de historial si utiliza el PAYID para identificar el pedido original (opcional).
PSPID	El PSPID de su cuenta.
PSWD	Contraseña del usuario API
USERID	Su usuario API

6.1.3 Página de prueba

Puede probar las solicitudes de consulta directa aquí: https://ogone.test.v-psp.com/ncol/test/testdq.asp.

6.2 Respuesta de consulta

Nuestro servidor devuelve una respuesta XML a la solicitud:

Ejemplo de una respuesta XML a una consulta directa

<?xml version=”1.0”?>
<ncresponse orderID=”99999” PAYID=”1111111” PAYIDSUB=”3” NCSTATUS=”0” NCERROR=”” NCERRORPLUS=””
ACCEPTANCE=”12345” STATUS="9" ECI=”7” amount="125" currency="EUR" PM="CreditCard" BRAND="VISA"

```
CARDNO="XXXXXXXXXXXX1111" IP="212.33.102.55"/>
```

La siguiente tabla contiene una lista de los atributos de etiqueta ncresponse:

Campo	Uso
ACCEPTANCE	Código de aceptación devuelto por la entidad adquiriente
amount	Importe del pedido (sin multiplicar por 100)
BRAND	Marca de la tarjeta o información similar para otros métodos de pago
CARDNO	El número de tarjeta de crédito enmascarado
currency	Divisa del pedido
ECI	Indicador de comercio electrónico
IP	La dirección IP del cliente, según la haya detectado nuestro sistema en una integración de nivel 3 o haya sido proporcionada por el comerciante en una integración de nivel 2
NCERROR	Código de error
NCERRORPLUS	Explicación del código de error
NCSTATUS	Primer dígito de NCERROR
orderID	Su referencia de pedido
PAYID	Referencia de pago en nuestro sistema
PAYIDSUB	El ID de nivel de historial de la operación de mantenimiento del PAYID
PM	Método de pago
STATUS	Estado de la transacción

Los atributos de etiqueta ncresponse estándar son idénticos a los de la respuesta XML a un nuevo pedido, salvo los atributos adicionales PAYIDSUB, CARDNO e IP.

La lista de atributos puede ser más larga para comerciantes que tengan activadas determinadas opciones (por ejemplo, la Detección de fraude) en sus cuentas. Consulte la documentación de la opción respectiva para obtener más información acerca de los atributos de respuesta adicionales vinculados a la opción.

6.2.1 Transacciones procesadas con e-Commerce

Si la transacción cuyo estado desea comprobar se ha procesado con e-Commerce, puede que también reciba los siguientes atributos adicionales (siempre que haya enviado estos campos con la transacción original de e-Commerce).

Campo	Descripción

Campo	Descripción
complus*	Un valor que deseaba que le devolviesen
(contenido de paramplus)*	Los parámetros y sus valores que deseaba que le devolviesen

*Consulte Parámetros de respuesta variables en la documentación de e-Commerce.

Ejemplo de una respuesta XML a una consulta directa para una transacción de e-Commerce

<ncresponse orderID=”99999” PAYID=”1111111” PAYIDSUB=”3” NCSTATUS=”0” NCERROR=”” NCERRORPLUS=”” ACCEPTANCE=”12345” STATUS="9" amount="125" currency="EUR" PM="CreditCard" BRAND="VISA" CARDNO="XXXXXXXXXXXX1111" IP="212.33.102.55" COMPLUS="12345678912345678912345678 9" SessionID="126548354" ShopperID="73541312"/>

6.3 Posibles estados de respuesta

El campo STATUS contendrá el estado de la transacción (consulte Posibles estados).

Solo el siguiente estado está relacionado de forma específica con la propia consulta:

Estado	NCERROR	NCSTATUS	Descripción
88			La consulta sobre querydirect.asp ha fallado

6.4 Consulta directa como último recurso

Los tiempos de respuesta de una solicitud de transacción de DirectLink suelen ser de unos pocos segundos. No obstante, algunas entidades adquirentes pueden tener tiempos de respuesta más largos.

Si no ha recibido una respuesta de nuestro sistema pasados 30 segundos, puede enviar una solicitud a querydirect.asp, pidiéndole el estado de su transacción más reciente enviada a orderdirect.asp. Si recibe una respuesta inmediata que contenga un estado no final para la transacción, puede que haya problemas por parte de la entidad adquirente.

Si no ha recibido una respuesta a esta solicitud de consulta directa pasados 10 segundos, puede que haya problemas de nuestro lado. Puede repetir esta solicitud a querydirect.asp cada 30 segundos hasta que vea que ha recibido una respuesta en 10 segundos.

Nota

- Este sistema de comprobación solo podrá detallar problemas por nuestra parte si también hay una comprobación por la suya para verificar que las solicitudes se han emitido correctamente desde los servidores.
- Un problema por nuestra parte no siempre estará necesariamente causado por el tiempo de inactividad, sino que también podría ser el resultado de tiempos de respuesta lentos debido a, por ejemplo, problemas en la base de datos.
- Utilice estas comprobaciones de manera juiciosa para evitar colapsar nuestros servidores de solicitudes. En caso contrario, podríamos restringirle el acceso a la página de querydirect.asp.

Importante

Para proteger nuestro sistema de sobrecargas innecesarias, prohibimos las comprobaciones de sistema activado que impliquen enviar

falsas transacciones o consultas sistemáticas, así como consultas sistemáticas para obtener respuesta de transacción para cada transacción.

7. Solicitud de aviso de privacidad de Controlador de datos

En función de los artículos 12, 13 y 14 del RGPD, un Controlador de datos tiene la obligación de informar a los clientes finales acerca del procesamiento futuro de sus datos personales. Dicha información debe realizarse de forma específica en función del tipo de datos personales que se introducen para una transacción concreta (p. ej., método de pago seleccionado, controlador/procesador, entidad adquiriente, fraude). El resultado debería estar disponible y visible en el momento de la recopilación de datos y al titular de tarjeta se le debe ofrecer una versión de los mismos que se pueda imprimir y descargar. Según la política del RGPD, tiene que mostrar la información al cliente antes de validar la transacción. Esta información debería mostrarse idealmente en la misma página donde el cliente rellena las credenciales de tarjeta/cuenta.
La solicitud de política de privacidad siguiente le permite recuperar toda la información que tiene que mostrar a sus clientes acerca de nuestros servicios para poder cumplir la normativa del RGPD.

7.1 URL de solicitud

7.1.1 Solicitud de consulta

• La URL de solicitud del entorno de PRUEBA es https://secure.ogone.com/ncol/test/privacy-policy.asp

• La URL de solicitud del entorno de PRODUCCIÓN es https://secure.ogone.com/ncol/prod/privacy-policy.asp

Cambiar "test" a "prod"

Sustituya "test" por "prod" en la URL de solicitud cuando cambie a la cuenta de producción.

7.1.2 Parámetros de solicitud

La tabla siguiente contiene los parámetros de solicitud obligatorios que enviar a su cliente en relación al uso de su información de privacidad:

Campo	Formato	Descripción
USERID	Cadena	Su usuario API
PSWD	Cadena	Su contraseña de usuario API
PSPID	Cadena	El PSPID de su cuenta
BRAND	Cadena (p. ej. Visa)	Opcional: Marca de método de pago Puede enviar este campo varias veces para obtener el resultado de varias marcas a la vez. • No enviar ninguna marca equivale a enviar todas las marcas activas. • Las marcas sin formato o con formato erróneo se ignoran.
LANGUAGE	ISO 639-1: Two-letter codes (e.g. FR)	Opcional: El idioma en el que desea recuperar el texto. Si no se facilita, el texto se devolverá en el idioma configurado por el comerciante.

7.1.3 Página de prueba

Puede probar las solicitudes de consulta directa aquí: https://secure.ogone.com/ncol/test/privacy-policy.asp

7.2 Respuesta de consulta

A continuación se muestra una lista de elementos XML y los ejemplos de respuestas XML devueltas para distintos resultados.

Nombre	Formato	Descripción
Response	Complejo	Nodo raíz, siempre presente
Response.Status	Cadena, valores posibles: Success, SuccessWithWarnings, Error	Siempre presente
Response.Body	Complejo	Presente solo cuando Response.Status = Success o SuccessWithWarnings
Response.Body.Html	Cadena / html	Vacío si Response.Status = SuccessWithWarnings y Response.Warnings.Warning.Code = NoContent
Response.Errors	Complejo	Presente solo cuando Response.Status = Error
Response.Errors.Error	Complejo	Puede ocurrir varias veces dentro de un nodo <Errors>
Response.Warnings	Complejo	Presente solo cuando Response.Status = SuccessWithWarnings o Error
Response.Warnings.Warning	Complex	Ocurre varias veces dentro de un nodo <Warnings>
Response.Errors.Error.Code Response.Warnings.Warning.Code	Cadena, valores posibles: • Dentro de un nodo <Error>: Unauthorized, InternalServerError • Dentro de un nodo <Warning>: NoContent	Siempre presente en un nodo <Error> o <Warning>
Response.Errors.Error.Message Response.Warnings.Warning.Message	Cadena	Opcional

Si se enfrenta a Response.Status=Error, consulte Response.Errors.Error para corregirlo.
Los siguientes son dos ejemplos de éxito:
1. Ejemplo de una respuesta XML para éxito con advertencias. Se devuelve si no se tiene que revelar al cliente información de privacidad.

```
<?xml version="1.0" encoding="utf-8"?>
 <Response>
    <Status>SuccessWithWarnings</Status>
    <Warnings>
        <Warning>
            <Code>NoContent</Code>
        </Warning>
    </Warnings>
    <Body>
        <Html/>
    </Body>
 </Response>
```

2. Ejemplo de una respuesta XML para éxito con contenido. El ejemplo muestra una visualización de dos secciones.

```
<?xml version="1.0" encoding="utf-8"?>
<Response>
    <Status>Success</Status>
    <Body>
        <Html><![CDATA[<ul><li><h2>Title 1</h2><p>Content 1</p></li><li>
<h2>Title 2 (VISA, American Express)</h2><p>Content 2</p></li></ul>]]></Html>
    </Body>
</Response>
```

8. Excepciones de método de pago

Para determinados métodos de pago, los valores de parámetro difieren de los de tarjeta de crédito estándar.

8.1 Direct Debits

8.1.1 Domiciliaciones AT

La siguiente tabla contiene los valores de parámetro específicos que permiten la transmisión de transacciones de Domiciliaciones AT a través de DirectLink.

Formato: AN= Alfanumérico/N=Numérico, cantidad máxima de caracteres permitida

Campo	Descripción	Formato/Valor
CARDNO	Número de cuenta bancaria	AN, 21 Formato: XXXXXXXXXXXBLZYYYYY XXXXXXXXXX: número de cuenta, numérico, 11 dígitos. YYYYY: Código de banco (Bankleitzahl), 5 dígitos.
CN	Nombre del titular de la cuenta bancaria	AN, 35
ED	Fecha de caducidad	„99/99“ o „9999“
OPERATION	Código de operación (acción que debe realizarse)	A, 3 Valores posibles: • RES: autorización • SAL/SAS: dinero de débito de la cuenta bancaria • RFD/RFS: reembolsar dinero (*)
OWNERADDRESS	Dirección del titular de la cuenta	AN, 50
OWNERTOWN	Ciudad/población del titular de la cuenta	AN, 40
OWNERZIP	Código postal del titular de la cuenta	AN, 10
PM	Método de pago	AN, 25 “Direct Debits AT”

(*Si la opción Reembolso está disponible y activa, y Reembolsos de DTAUS está disponible)

8.1.2 Domiciliaciones DE (ELV)

La siguiente tabla contiene los valores de parámetro específicos, que permiten la transmisión de transacciones de ELV a través de DirectLink. (no Wirecard/Billpay)

Formato: AN= Alfanumérico/N=Numérico, cantidad máxima de caracteres permitida

Campo	Descripción	Formato/Valor	Obligatorio
CARDNO	Número de cuenta bancaria	IBAN: 22 caracteres alfanuméricos O Número de cuenta bancaria + BLZ. Formato: XXXXXXXXXBLZYYYYYYYY XXXXXXXXXX: número de cuenta, numérico, de 1 a 10 dígitos. YYYYYYYY: Código de banco (Bankleitzahl), 8 dígitos.	Sí
CN	Nombre del titular de la cuenta bancaria	AN, 35	Sí
ED	Fecha de caducidad	„99/99“ o „9999“	Sí
MANDATEID	Referencia de autorización unívoca. Telego: Si no se proporciona, la plataforma usará el ORDERID o PAYID Nota: Si no se proporciona, Easycash generará un valor.	Telego: AN, 35/Conjunto de caracteres: “A-Z a-z 0-9 espacio /-?:().,'+”) Si no se proporciona, la plataforma tomará el ORDERID o PAYID Easycash: Formato: AN, 27/Conjunto de caracteres: “A-Z a-z 0-9 espacio /-?:().,'+”) Nota: Si no se proporciona, Easycash generará un valor.	No
OPERATION	Código de operación (acción que debe realizarse)	A, 3 Valores posibles: • RES: autorización • SAL/SAS: dinero de débito de la cuenta bancaria • RFD/RFS: reembolsar dinero (*)	No
OWNERADDRESS	Dirección postal y número del titular de la cuenta	AN, 50	Sí
OWNERTOWN	Ciudad/población del titular de la cuenta	AN, 40	Sí
OWNERZIP	Código postal del titular de la cuenta	AN, 10	Sí
PM	Método de pago	AN, 25 "Domiciliaciones DE”	Sí

Nota: Estos campos se pueden devolver en la respuesta XML de DirectLink y deben incluirse en el cálculo SHA-IN (opcionalmente, también en SHA-OUT).

(*Si la opción Reembolso está disponible y activa, y Reembolsos de DTAUS está disponible)

8.1.3 Domiciliaciones NL

La siguiente tabla contiene los valores de parámetro específicos que permiten la transmisión de transacciones de Domiciliaciones NL a través de DirectLink.

Formato: AN= Alfanumérico/N=Numérico, cantidad máxima de caracteres permitida

Campo	Descripción	Formato/Valor
CARDNO	Número de cuenta bancaria	Número de cuenta holandés normal: máx. 10 caracteres alfanuméricos (si es inferior, complete con ceros a la izquierda). O Número de cuenta IBAN: máx. 35 caracteres alfanuméricos (SEPA)
CN	Nombre del titular de la cuenta bancaria	AN, 35
ED	Fecha de caducidad	„99/99“ o „9999“
OPERATION	Código de operación (acción que debe realizarse)	A, 3 Valores posibles: • SAL o SAS: dinero de débito de la cuenta bancaria • RFD o RFS: dinero de crédito a la cuenta bancaria (reembolso)
OWNERTOWN	Ciudad del titular de la cuenta bancaria	AN, 40
PM	Método de pago	AN, 25 “Domiciliaciones NL”
Solo relevante para transacciones SEPA (*) :		
BIC	Código identificador de banco	AN, 11
MANDATEID	Referencia de autorización unívoca. Nota: Si no se proporciona, se usará el ORDERID.	AN, 35 No se permiten espacios; no puede empezar ni terminar con una barra inclinada "/" ni contener dos barras consecutivas.

Campo	Descripción	Formato/Valor
SEQUENCETYPE	El tipo de transacción de Domiciliaciones Nota: Si no se proporciona, las transacciones se considerarán de “una sola vez” y se usará el valor "OOFF".	Posibles valores para indicar el tipo de transacción de Domiciliaciones (AN, 4): • "FRST": Primer grupo de una serie de instrucciones de Domiciliaciones • "RCUR": Instrucciones de Domiciliaciones en las que se utiliza la autorización del deudor para transacciones normales de este tipo iniciadas por el acreedor • "FNAL": Grupo final de una serie de instrucciones de Domiciliaciones (posteriormente no se puede volver a utilizar el mismo MandateID) • "OOFF": orden de adeudo directo en la que se utiliza la autorización del deudor para iniciar una única transacción de domiciliación
SIGNDATE	Fecha en la que el comprador firmó la autorización. Nota: Si no se proporciona, se usará la fecha de la transacción.	AAAAMMDD

(*SEPA: Single Euro Payments Area o Zona Única de Pagos en Euros)

Nota: Estos campos se pueden devolver en la respuesta XML de DirectLink y deben incluirse en el cálculo SHA-IN (y, opcionalmente, SHA-OUT).

8.2 Métodos de pago con solo mantenimiento a través de DirectLink

Para determinados métodos de pago (tarjeta que no sea de crédito), no puede enviar nuevas transacciones a través de DirectLink, pero puede enviar determinadas operaciones de mantenimiento a través de DirectLink. Es el caso de la tarjeta PostFinance, PostFinance E-finance, compra mediante PayPal Express y TUNZ. Cuando se envían operaciones de mantenimiento, PM/BRAND/CARDNO/ED no son campos necesarios, así que, para estos métodos de pago, no deben enviarse valores específicos.