



COLLECTOR DE PAGOS

Pago por token y suscripciones

Guía de implementación

Versión del documento 3.15

Contenido

1. HISTORIAL DEL DOCUMENTO.....	4
2. PRESENTACIÓN DEL SERVICIO.....	7
2.1. Unicidad de los medios de pago registrados.....	8
3. MEDIOS DE PAGO COMPATIBLES.....	10
4. COMPARTIR EL TOKEN.....	13
5. ENCADENAMIENTO DE LAS TRANSACCIONES CIT/MIT.....	14
6. CASOS DE USO.....	15
6.1. Creación del token sin pago.....	16
6.2. Cambio de información asociada al token.....	18
6.3. Creación del token durante un pago.....	20
6.4. Creación del token al suscribirse a una recurrencia.....	22
6.5. Creación del token al suscribir a una recurrencia acompañada de un pago.....	25
6.6. Pago por Token.....	28
6.7. Uso de un token para suscribirse a una recurrencia.....	30
6.8. Pago con propuesta al titular para crear un token.....	32
7. CICLO DE VIDA DE UN PAGO RECURRENTE.....	34
8. CICLO DE VIDA DE UN PAGO RECURRENTE CON AUTORIZACIÓN ANTICIPADA.....	35
8.1. Lista de códigos de retorno de la solicitud de autorización.....	37
8.2. Notificación por e-mail en caso de rechazo de una cuota.....	39
9. OFRECER INTENTOS DE PAGO ADICIONALES.....	40
10. ESTABLECER DIÁLOGO CON LA PLATAFORMA DE PAGO.....	41
10.1. Similitudes con el pago unitario.....	41
11. CONFIGURAR NOTIFICACIONES.....	42
11.1. Configurar la notificación al final del pago.....	43
11.2. Configurar la notificación en caso de abandono/cancelación.....	44
11.3. Configurar la notificación de una operación proveniente del Back Office.....	45
11.4. Configurar la notificación al crear una recurrencia.....	46
11.5. Configurar la notificación al autorizar por batch.....	47
11.6. Reejecutar automáticamente en caso de fallo.....	48
11.7. Configurar correos electrónicos enviados al comprador.....	50
12. GENERAR UN FORMULARIO DE PAGO.....	51
12.1. Crear un formulario 'Creación del token sin pago'.....	53
12.2. Crear un formulario 'Cambio de información asociada al token'.....	53
12.3. Crear un formulario 'Creación del token durante un pago'.....	55
12.4. Crear un formulario 'Creación del token al suscribirse a una recurrencia'.....	56
12.5. Crear un formulario 'Creación del token al suscribir a una recurrencia acompañada de un pago'.....	58
12.6. Crear un formulario 'Pago por token'.....	60
12.7. Crear un formulario 'Usar un token para suscribirse a una recurrencia'.....	61
12.8. Crear un formulario 'Pago con propuesta al titular para crear un token'.....	63
13. USAR FUNCIONES ADICIONALES.....	65
13.1. Definir un monto diferente para las primeras n cuotas.....	66
13.2. Definir la moneda para crear o actualizar un token.....	66

14. CALCULAR LA FIRMA.....	68
15. ENVÍO DE LA SOLICITUD DE PAGO.....	70
15.1. Redirección del comprador hacia la página de pago.....	70
15.2. Gestión de errores.....	70
15.3. Administrar tiempos de espera.....	73
16. IMPLEMENTAR LA IPN.....	74
16.1. Preparar su entorno.....	75
16.2. Recuperar los datos devueltos en la respuesta.....	76
16.3. Calcular la firma de la IPN.....	77
16.4. Comparar firmas.....	78
16.5. Analizar la naturaleza de la notificación.....	79
16.6. Tratamiento de los datos de la respuesta.....	80
16.6.1. Creación de un token sin pago.....	80
16.6.2. Cambio de información asociada al token.....	84
16.6.3. Creación del token durante un pago.....	87
16.6.4. Creación del token al suscribirse a una recurrencia.....	91
16.6.5. Creación del token al suscribir a una recurrencia acompañada de un pago.....	95
16.6.6. Pago por Token.....	99
16.6.7. Suscripción a una recurrencia.....	102
16.6.8. Pago con propuesta al titular para crear un token.....	104
16.6.9. Pago de un vencimiento de una recurrencia.....	107
16.7. Test y troubleshooting.....	111
17. OBTENER AYUDA.....	114
18. APÉNDICES.....	115
18.1. Crear automáticamente una recurrencia por Web Services.....	115
18.2. Dar de baja automáticamente una recurrencia por Web Services.....	115
18.3. Tarjetas de test.....	115

1. HISTORIAL DEL DOCUMENTO

Versión	Autor	Fecha	Comentario
3.15	Lyra Collect	19/05/23	<ul style="list-style-type: none"> Actualización del capítulo <i>Presentación del servicio</i>.
3.14.2	Lyra Collect	20/09/22	<ul style="list-style-type: none"> Actualización del capítulo <i>Presentación del servicio</i> Actualización de la descripción de los valores del campo vads_risk_assessment_result en el capítulo <i>Tratamiento de los datos de la respuesta</i>.
3.14.1	Lyra Collect	25/05/2022	<ul style="list-style-type: none"> Precisión sobre el monto de la autenticación y los diferentes tipos de uso.
3.14	Lyra Collect	26/04/22	<ul style="list-style-type: none"> Adición del capítulo <i>Proponer intentos de pago suplementarios</i>. Adición del capítulo <i>Encadenamiento de las transacciones CIT/MIT</i> Adición de la moneda en los parámetros para transmitir durante la creación de un token sin pago. Actualización de los tipos de uso para mostrar el encadenamiento de las transacciones. Actualización del capítulo <i>Medios de pago compatibles</i>. Adición del campo vads_initial_issuer_transaction_identifier en el capítulo <i>Procesar los datos de la respuesta</i>.
3.13	Lyra Collect	10/02/22	<ul style="list-style-type: none"> Actualización del capítulo <i>Medios de pago compatibles</i>. Actualización de capítulos <i>Creación del token sin pago</i>, <i>Creación del token durante un pago</i>, <i>Creación del token al suscribirse a una recurrencia</i> y <i>Creación del token al suscribirse a una recurrencia acompañada de un pago</i>. Actualización de capítulo <i>Ciclo de vida de un pago recurrente</i>.
3.12	Lyra Collect	12/10/21	<ul style="list-style-type: none"> Actualización de la definición del campo vads_sub_effect_date.
3.11	Lyra Collect	01/03/2021	<ul style="list-style-type: none"> Adición del campo vads_occurrence_type en el capítulo <i>Ciclo de vida de un pago recurrente</i>. Adición de un campo que describe la recurrencia en los capítulos relativos a la notificación de una creación de recurrencia. Adición del capítulo <i>Pago de un vencimiento de una recurrencia</i>. Actualización del capítulo <i>Pago por token</i>: la se requieren la entrada del CVV y una autenticación del portador. Actualización de los capítulos relativos a la creación de un token: el portador se debe someter a una autenticación fuerte.
3.10	Lyra Collect	18/01/2021	<ul style="list-style-type: none"> Actualización del capítulo <i>Presentación del servicio</i>. Adición del capítulo <i>Unicidad de los medios de pago registrados</i>. Precisión sobre las recurrencias diarias añadidas en los capítulos relativos a la recurrencia de una recurrencia. Actualización del capítulo <i>Medios de pago compatibles</i>.

Versión	Autor	Fecha	Comentario
			<ul style="list-style-type: none"> Actualización del capítulo <i>Dar de baja automáticamente una recurrencia por Web Services</i>. Adición del capítulo <i>Tarjetas de test</i> en anexos.
3.9	Lyra Collect	05/05/20	<ul style="list-style-type: none"> Aclaración sobre el fin de los intentos realizados por la plataforma de pago en caso de activación de las autorizaciones anticipadas. Aclaraciones sobre la creación de los pagos en caso de vencimiento del medio de pago o de purga de los datos del medio de pago. Actualización de la configuración de las reglas de notificación.
3.8	Lyra Collect	21/10/19	<ul style="list-style-type: none"> Actualización de los medios de pago aceptados. Adición de un capítulo sobre la garantía de pago durante un pago por token. Actualización de la definición del campo vads_sub_desc en el capítulo <i>Generar un formulario de pago</i>.
3.7	Lyra Collect	05/08/19	<ul style="list-style-type: none"> Ahora el algoritmo hash está disponible en el menú Configuración > Tienda, pestaña Claves. Adición del campo vads_identifier como parámetro de entrada para la creación de un token. Adición de la categoría Información sobre el análisis de riesgos en el Diccionario de datos. vads_threeds_auth_type: el campo siempre está presente en la respuesta y puede estar vacío. Ahora el algoritmo hash está disponible en el menú Configuración > Tienda, pestaña Claves. Aclaraciones proporcionadas sobre el cálculo de firma de IPN. Aclaraciones proporcionadas sobre el formato de los campos vads_trans_date y vads_presentation_date. Aclaración proporcionada sobre el formato de los campos vads_product_label, vads_cust_zip, vads_order_id, vads_cust_first_name, vads_cust_last_name, vads_cust_phone, vads_cust_cell_phone, vads_cust_id, vads_cust_city, vads_cust_address vads_auth_result: corrección del formato del campo (an..11) vads_contracts: Posibilidad de forzar la que se utilizará.
3.6	Lyra Collect	22/05/19	<p>Detalles sobre los métodos de creación y de baja de la recurrencia a través de los Terminal ID web services</p> <p>Diccionario de datos: actualización de vads_trans_date</p>
3.5	Lyra Collect	26/03/19	<ul style="list-style-type: none"> Adición de un detalle sobre la eliminación de datos en el capítulo Gestionar los pagos por token. Adición de las horas de creación de los pagos recurrentes en el capítulo Gestionar los pagos por token. Actualización de las capturas en los capítulos Crear un token en modo Test y Crear un token en modo Production Actualización de las capturas en Crear una recurrencia desde el Back Office Expert Adición del capítulo Definir la moneda para crear o actualizar un token.

Versión	Autor	Fecha	Comentario
			<ul style="list-style-type: none"> • Actualización de la tabla de parámetros en el capítulo Crear un formulario "Pago con propuesta al titular para crear un token" • Diccionario de datos: <ul style="list-style-type: none"> • Adición de un detalle sobre el formato del campo vads_product_qty • Adición del campo vads_presentation_date en la sección Información sobre la transacción • Adición de un detalle sobre el formato del campo vads_identifier • Adición de un detalle sobre el formato del campo vads_subscription • Eliminación de los campos vads_ext_info_donation, vads_ext_info_donation_recipient, vads_ext_info_donation_recipient_name, vads_ext_info_donation_merchant, vads_ext_info_donation_contribution y vads_risk_primary_warranty.
3.4	Lyra Collect	04/03/19	Versión inicial

Este documento y su contenido son estrictamente confidenciales. No es contractual. Cualquier reproducción y/o distribución total o parcial de este documento o de su contenido a una entidad tercera está estrictamente prohibido o sujeta a una autorización escrita previa de Lyra Collect. Todos los derechos reservados.

2. PRESENTACIÓN DEL SERVICIO

Gestión de pagos por token

El servicio de gestión de pagos por token permite que los vendedores ofrezcan a sus compradores la posibilidad de asociar un token a un medio de pago para facilitar los pagos posteriores en el sitio web (sin necesidad de volver a ingresar su número de tarjeta bancaria o su IBAN).

Los token permiten:

- pagos rápidos y seguros.

El comprador ya no tiene que ingresar sus datos bancarios al hacer pagos posteriores (pago con 1 solo clic).

Los datos bancarios son almacenados en la plataforma en un entorno de alta seguridad de conformidad con la norma PCI-DSS. Solo el token pasa durante los intercambios.

- efectuar pagos recurrentes (recurrencias).



Los token pueden ser utilizados por todas las tiendas de una misma empresa.

El servicio también permite:

- Identificar las tarjetas próximas a vencer, a fin de poner en alerta al vendedor enviándole un archivo con los tokens cuya tarjeta está por vencer.
- Actualizar los datos bancarios asociados a un token, desde la página de pago o manualmente desde el Back Office Expert.
- Detectar automáticamente si el medio de pago ha expirado y proponer la actualización durante un pago por medio de token.
- entonces detectar la creación de un token si el medio de pago ya se ha registrado precedentemente,
- Gestionar el cambio de los otros datos correspondientes al comprador.



Conforme a las reglas de seguridad y de protección de los datos bancarios exigidas por PCI DSS, los datos del medio de pago serán eliminados si transcurrieron 15 meses sin utilizar el token asociado.

El token siempre podrá verse en el Back Office Expert y podrá actualizarse con nuevos datos.

Gestión de pagos recurrentes (recurrencia)

El servicio de gestión de pagos recurrentes permite a los vendedores crear suscripciones **con montos y vencimientos fijos**, también llamados “pagos recurrentes” con o sin fecha de fin, dentro del límite de validez de la tarjeta.

Al crear un pago recurrente, el vendedor define la fecha de inicio, el monto de los vencimientos y la regla de recurrencia a aplicar.

Un vez alcanzada la fecha de inicio (también llamada "fecha de efecto"), la plataforma de pago procede automáticamente a tratar los vencimientos.

Entonces el vendedor ya no tiene la posibilidad de modificar el monto de los vencimientos.

Para ser notificado del resultado de un plazo, la regla **URL de notificación al crear una recurrencia** debe estar activada y configurada desde el Back Office Expert (menú **Configuración > Reglas de notificaciones**).

En el modo PRUEBA, la transacción correspondiente al primer vencimiento se crea a más tardar 1 hora después de la suscripción, según el calendario determinado por la regla de suscripción.

En modo PRODUCTION, las transacciones se crean una vez al día entre medianoche y las 5:00 h, en la zona horaria Europa/París.

2.1. Unicidad de los medios de pago registrados

Por defecto, la plataforma autoriza al comprador registrar varias veces su medio de pago en un mismo sitio de comerciante.

Sin embargo, si el comerciante lo desea, puede activar una opción desde su Back Office Expert que permitirá detectar, al crear un token, si el medio de pago ya se ha registrado.



Se desaconseja activar el control de unicidad de los medios de pago registrados si no domina los impactos en su implementación.

- [Principio de funcionamiento](#)
- [¿Qué hacer en caso de detectar un doble medio de pago?](#)
- [Activación de la detección de la unicidad de los medios de pago](#)

Principio de funcionamiento

Una vez activada la opción, la plataforma verifica cada vez que se crea un token, la validez del medio de pago con el emisor y luego procede a verificar la unicidad del medio de pago.

Si nunca se ha registrado un medio de pago, entonces se crea un nuevo token asociado a este medio de pago y se devuelve su identificador al sitio del comerciante al notificar el fin de pago.

Si ya se ha registrado el medio de pago (mismo número y misma fecha de validez), entonces se utiliza el token existente y se devuelve su identificador al sitio del comerciante al notificar el fin de pago.

Los datos del comprador enviados son los transmitidos por el comerciante, no los del token precedentemente registrado.

El campo **vads_identifier_status** se valoriza en **CREATED** incluso si, en este caso, no se ha creado un token.

Entonces la notificación contiene un campo suplementario valorizado en **true**:

- **vads_identifier_previously_registered** para notificar en el formato Formulario API,
- **paymentMethodTokenPreviouslyRegistered** para notificar en formato API REST.



- No hay detección de unicidad del medio de pago al actualizar un token.
- Si el medio de pago está asociado a varios token, la notificación de fin de pago contiene el identificador del token más reciente.
- Se rechaza la creación de un token desde Back Office Expert si el medio de pago está asociado a otro token.
- El campo **vads_identifier_previously_registered** no se devuelve al regresar a la tienda.
- El campo **vads_identifier_previously_registered** nunca se devuelve al notificar el fin de pago si no se detecta un duplicado. Por lo tanto, el valor **false** nunca es enviado al sitio del vendedor.

¿Qué hacer en caso de detectar un doble medio de pago?

Todo depende de sus necesidades de oficio.

- Usted puede decidir no hacer nada y brindar el servicio o suministrar el bien al comprador.
- Puede verificar si el código cliente asociado al token existente corresponde al código cliente del comprador. Si no es el caso, puede buscar si el vínculo primario entre los dos clientes explica el por qué el mismo medio de pago lo utilizan dos clientes diferentes.
- Puede verificar si la persona que solicita el registro del medio de pago es la misma que ya ha registrado este medio de pago (por ejemplo, verificando los datos de contacto, la dirección electrónica, el país, etc...).
- Si fracasan todos los controles realizados, es posible que se trate de un fraude y entonces usted puede decidir cancelar el pago.

Activación de la detección de la unicidad de los medios de pago

1. Desde el Back Office Expert, abra el menú **Configuración > Empresa** y haga clic en la pestaña **Configuración de suscripción y alias**.

Configuración de la compañía: [...]

← Registro de actividad Tiendas Configuración de suscripción y alias Opciones de pago →

Parámetros Recurrencia

Número máximo de vencimientos visibles en el calendario de pagos *: 12

Plazo de alerta para las suscripciones están cerca de un vencimiento. *: 5 día(s)

Plazo de alerta para los medios de pago próximos de la fecha de vencimiento *: 2 mes(es)

Parametro tokens

Comprobar la unicidad de un token: En el caso de solicitud de creación de token en un medio de pago ya registrado, la plataforma reutilizará el token anterior.

Guardar

2. En el marco **Parametro tokens**, marque la casilla **Comprobar la unicidad de un token**.
3. Haga clic en el botón **Guardar** para registrar sus cambios.

3. MEDIOS DE PAGO COMPATIBLES

Lista de los medios de pago compatibles con el servicio de Gestión de pagos por token:

Código Red	Medio de pago	Tipo de tarjetas (vads_payment_cards)	Acepta el pago por token
ACCORD	Tarjeta regalo Illicado	ILLICADO	✗
ACCORD	Tarjeta marca Accord	ACCORD_STORE	✗
ACCORD_SANDBOX	Tarjeta regalo Illicado - Modo sandbox	ILLICADO_SB	✗
AMEXGLOBAL	American Express	AMEX	✓
APPLE PAY	Pago por Wallet Apple Pay	APPLE_PAY	✗
AURORE	Tarjeta Cpay	AURORE-MULTI	✗
CB	Tarjeta bancaria CB	CB	✓
CB	Maestro	MAESTRO	✗
CB	Mastercard	MASTERCARD	✓
CB	Tarjeta Titre-Restaurant Apetiz	APETIZ	✓
CB	Tarjeta Titre-Restaurant Chèque Déjeuner	CHQ_DEJ	✓
CB	Tarjeta Ticket Restaurant Mastercard 1.ª generación	EDENRED	✓
CB	Tarjeta Titre-Restaurant Sodexo	SODEXO	✓
CB	Tarjeta virtual e-Carte Bleue	TARJETA DÉBITO ELECTRÓNICA	✓
CB	Visa	VISA	✓
CB	Visa Electron	VISA_ELECTRON	✓
CB	Visa Vpay	VPAY	✓
CONECs	Tarjeta Titre-Restaurant Apetiz	APETIZ	✓
CONECs	Tarjeta Titre-Restaurant Chèque Déjeuner	CHQ_DEJ	✓
CONECs	Tarjeta Titre-Restaurant Conecs	CONECs	✓
CONECs	Tarjeta Titre-Restaurant Sodexo	SODEXO	✓
CVCONNECT	Chèque-Vacances Connect	CVCO	✗
DINERS	Diners Club	DINERS	✓
DINERS	Discover	DISCOVER	✓
EDENRED	Ticket Eco Cheque Edenred	EDENRED_EC	✓
EDENRED	Ticket Sport & Culture Edenred	EDENRED_SC	✓
EDENRED	Ticket Compliment Edenred	EDENRED_TC	✓
EDENRED	Ticket Restaurant Edenred	EDENRED_TR	✓
FRANFINANCE	Pago en 3 vencimientos Franfinance	FRANFINANCE_3X	✗
FRANFINANCE	Pago en 4 vencimientos Franfinance	FRANFINANCE_4X	✗
FRANFINANCE_SB	Pago en 3 vencimientos Franfinance - Modo sandbox	FRANFINANCE_3X	✗
FRANFINANCE_SB	Pago en 4 vencimientos Franfinance - Modo sandbox	FRANFINANCE_4X	✗
FULLCB	Pago en 3x sin recargo por BNPP PF	FULLCB3X	✗

Código Red	Medio de pago	Tipo de tarjetas (vads_payment_cards)	Acepta el pago por token
FULLCB	Pago en 4x sin recargo por BNPP PF	FULLCB4X	✗
GATECONEX	Bancontact	BANCONTACT	✗
GATECONEX	Diners Club	DINERS	✓
GATECONEX	Discover	DISCOVER	✓
GATECONEX	Tarjeta virtual e-Carte Bleue	TARJETA DÉBITO ELECTRÓNICA	✓
GATECONEX	Maestro	MAESTRO	✗
GATECONEX	Mastercard	MASTERCARD	✓
GATECONEX	Visa	VISA	✓
GATECONEX	Visa Electron	VISA_ELECTRON	✗
GATECONEX	Visa Vpay	VPAY	✗
GICC	Bancontact	BANCONTACT	✗
GICC	Maestro	MAESTRO	✗
GICC	Mastercard	MASTERCARD	✓
GICC	Visa	VISA	✓
GICC	Visa Electron	VISA_ELECTRON	✗
GICC_DINERS	Diners Club	DINERS	✓
GICC_DINERS	Discover	DISCOVER	✓
GICC_MAESTRO	Bancontact	BANCONTACT	✗
GICC_MAESTRO	Maestro	MAESTRO	✗
GICC_MASTERCARD	Mastercard	MASTERCARD	✓
GICC_VISA	Visa	VISA	✓
GICC_VISA	Visa	VPAY	✗
GICC_VISA	Visa Electron	VISA_ELECTRON	✗
GOOGLEPAY	Pago por Wallet Google Pay	GOOGLEPAY	✗
JCB	JCB	JCB	✓
LYRA_COLLECT_PPRO	Pago con wallet Alipay	ALIPAY	✗
LYRA_COLLECT_PPRO	Bancontact	BANCONTACT	✗
LYRA_COLLECT_PPRO	Transferencia bancaria GIROPAY	GIROPAY	✗
LYRA_COLLECT_PPRO	Transferencia bancaria iDEAL	IDEAL	✗
LYRA_COLLECT_PPRO	Pago con cupón en la red MultiBanco:	MULTIBANCO	✗
LYRA_COLLECT_PPRO	Transferencia bancaria MyBank	MYBANK	✗
LYRA_COLLECT_PPRO	Transferencia bancaria Przelewy24	PRZELEWY24	✗
LYRA_COLLECT_PPRO	Transferencia bancaria Sofort	SOFORT_BANKING	✗
LYRA_COLLECT_PPRO	Tarjeta UnionPay	UNION_PAY	✗
LYRA_COLLECT_PPRO	Pago con wallet We Chat Pay	WECHAT	✗
ONEY	Pago en 3 o 4 cuotas con tarjeta bancaria FacilyPay	ONEY	✗
ONEY_API	Pago 3x 4x Oney	ONEY_3X_4X	✗
ONEY_API	Pago 10x 12x Oney	ONEY_10X_12X	✗
ONEY_API	Pago Oney Pay Later	ONEY_PAYLATER	✗
ONEY_API	Tarjetas de marcas asociadas de Oney.	ONEY_ENSEIGNE	✗
ONEY_API_SANDBOX	Pago 3x 4x Oney en modo sandbox	ONEY_3X_4X	✗

Código Red	Medio de pago	Tipo de tarjetas (vads_payment_cards)	Acepta el pago por token
ONEY_API_SANDBOX	Pago 10x 12x Oney en modo sandbox	ONEY_10X_12X	✘
ONEY_API_SANDBOX	Pago Oney Pay Later en modo sandbox	ONEY_PAYLATER	✘
ONEY_API_SANDBOX	Tarjetas de marcas asociadas de Oney en modo sandbox.	ONEY_ENSEIGNE	✘
ONEY_API_SB	Pago en 3 o 4 vencimientos Oney - Modo sandbox	ONEY_3X_4X	✘
ONEY_SANDBOX	Pago en 3 o 4 cuotas con tarjeta bancaria FacilyPay - Modo sandbox	ONEY_SANDBOX	✘
PAYDIREKT_V2	Transferencia bancaria paydirekt	PAYDIREKT	✘
PAYPAL	Pago con PayPal	PAYPAL	✔
PAYPAL_SB	Pago con PayPal - Modo sandbox	PAYPAL_SB	✔
PLANET_DCC	Mastercard	MASTERCARD	✔
PLANET_DCC	Visa	VISA	✔
POSTFINANCEV2	Pago con tarjeta PostFinance Card	POSTFINANCE	✘
POSTFINANCEV2	Transferencia bancaria PostFinance Efinance	POSTFINANCE_EFIN	✘
PRESTO	Solución de crédito en línea Presto de Cetelem.	PRESTO	✘
SEPA	Extracción Bancaria SEPA DIRECT DEBIT	SDD	✔

4. COMPARTIR EL TOKEN

Es posible compartir el token entre varias entidades jurídicas.

Los tokens compartidos entre varias entidades jurídicas deben ser únicos y deben ser generados obligatoriamente por la plataforma de pago.

Sin embargo, esta funcionalidad está sujeta a condiciones particulares. Por favor, contacte al interlocutor de su plataforma de pago para conocerlas.

5. ENCADENAMIENTO DE LAS TRANSACCIONES CIT/MIT

La segunda directiva sobre los servicios de pago (DSP2) hizo necesaria la autenticación del titular de la tarjeta desde para cualquier transacción de e-commerce.

Es indispensable entonces distinguir si la solicitud de pago ha sido iniciada:

- por el comprador:

CIT (Customer Initiated Transaction): Transacción iniciada por el comprador con interacción de este.

Ej.: pago (o registro de una tarjeta) que requiere el ingreso de los datos de la tarjeta o la autenticación del titular.

- o por el vendedor:

MIT (Merchant Initiated Transaction): Transacción iniciada por el vendedor, sin presencia del comprador, relacionada con una transacción inicial **CIT**.

Ej.: X cuota de un pago en cuotas o de un pago recurrente.

Se introduce un nuevo principio para el seguimiento de las autenticación de las transacciones: **el encadenamiento de las operaciones**.

Para una transacción **CIT**, la reglamentación exige la autenticación del titular de la tarjeta. Como respuesta a la solicitud de autorización o de verificación de tarjeta, el emisor devuelve un identificador único de transacción, llamado "referencia de encadenamiento". Conocida como "referencia de encadenamiento", se utiliza en las transacciones de **MIT** para indicar al emisor que la transacción forma parte de una serie de pagos para los que el portador se autenticó en el momento del primer pago.

Sin esta información, el emisor puede rechazar una transacción **MIT** por falta de autenticación (soft decline).

6. CASOS DE USO

El formulario de pago permite realizar las siguientes operaciones clasificadas por caso.

Cada uno de estos casos corresponde a una valorización diferente del campo **vads_page_action**.

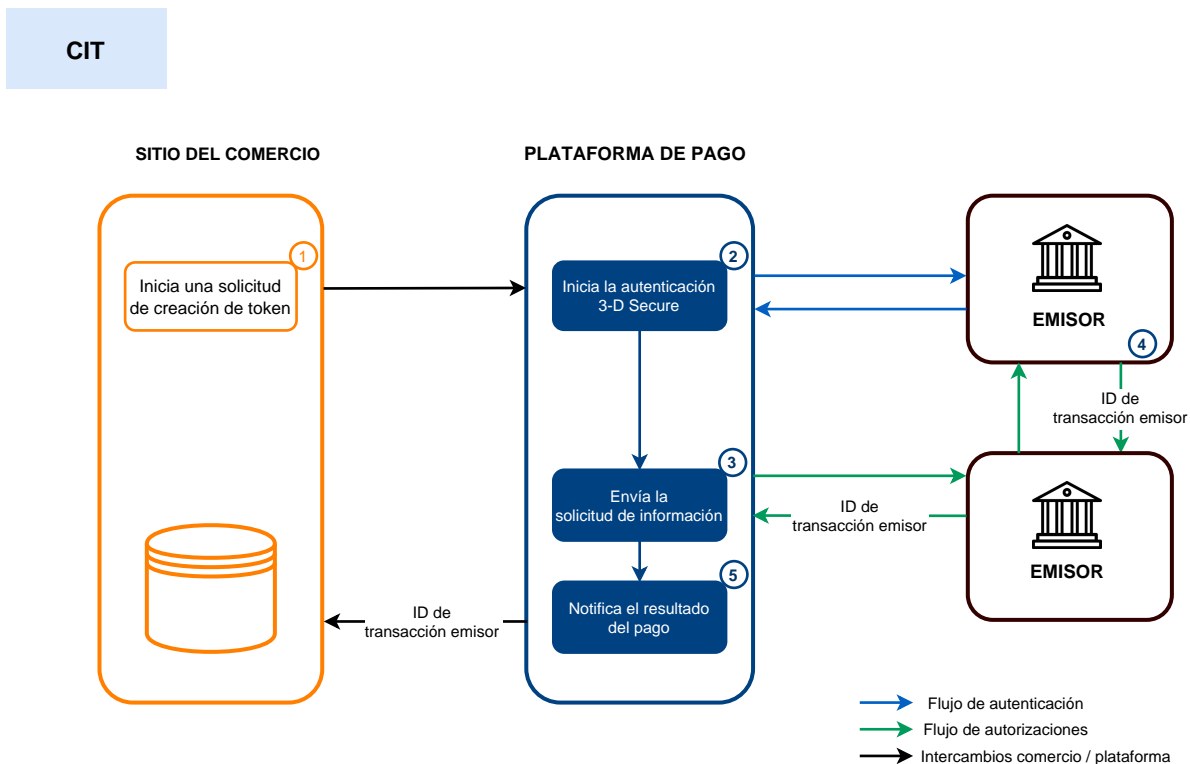
Casos de uso	Valorización del campo vads_page_action
Creación del token sin pago	REGISTER
Actualización de la información asociada al token.	REGISTER_UPDATE
Creación del token durante un pago	REGISTER_PAY
Creación del token al suscribirse a una recurrencia	REGISTER_SUBSCRIBE
Creación del token al suscribir a una recurrencia acompañada de un pago	REGISTER_PAY_SUBSCRIBE
Pago por Token	PAYMENT
Uso de un token para suscribirse a una recurrencia	SUBSCRIBE
Pago con propuesta al titular para crear un token	ASK_REGISTER_PAY

Según el tipo de uso (valorización del campo **vads_page_action**), las interacciones entre el comprador y la página de pago diferirán.

6.1. Creación del token sin pago

Este caso corresponde a la simple creación de un token.

Esquema simplificado



1. El sitio web vendedor una *solicitud de creación de token*.

Nota para las tiendas con la opción "Conversión de moneda":

La moneda es obligatorio durante la creación de un token.

Sólo se seleccionarán los contratos que admitan la moneda introducida como parámetro. No se tiene en cuenta la conversión de monedas.

Ejemplo: Para una solicitud de creación de un alias en moneda USD, en una tienda asociada a un contrato AMEX y a un contrato CB:

si el contrato AMEX sólo admite la moneda USD y el contrato CB sólo admite la moneda EUR, entonces sólo se aceptarán las tarjetas AMEX para la creación del alias.

El comprador elige el método de pago que se debe registrar, entrega los datos de este y luego valida.

2. La plataforma de pago inicia el proceso de autenticación del portador con el emisor.

En este caso, la reglamentación exige una autenticación fuerte.

La autenticación se realiza por un monto 0 EUR.

3. Una vez que la autenticación ha terminado, la plataforma realiza la solicitud de información con los datos de autenticación del titular.
4. El emisor genera un identificador único de transacción y lo transmite en la respuesta de la verificación de tarjeta.

5. La plataforma de pago notifica al sitio web vendedor el *resultado*.

En particular, la respuesta contiene:

- el código único de transacción generado por el emisor, para su información,
- el token creado recientemente.

Esta operación, se da lugar a la creación de una transacción de tipo VERIFICATION, que aparece en el Back Office Expert y posee las siguientes características:



- su monto es de 1.00 EUR o 0 EUR si el adquirente lo soporta,
- su estado es, o bien "Aceptado" o bien "Rechazado",
- nunca se envía al banco y permanece en la pestaña "Transacciones en curso".



El token no se creará si la solicitud de autorización o de información es rechazada.

La plataforma muestra el ticket al comprador. En particular, contiene:

- el token creado recientemente,
- Los datos del comprador.

Si ha configurado las reglas de notificación correspondientes, el comprador recibirá un correo electrónico:

- la confirmación del registro de sus datos bancarios en la plataforma de pago de la tienda,
- su token que podrá utilizar posteriormente para efectuar otra operación bancaria.



La plataforma de pago registra el identificador de transacción emisor a nivel del token.

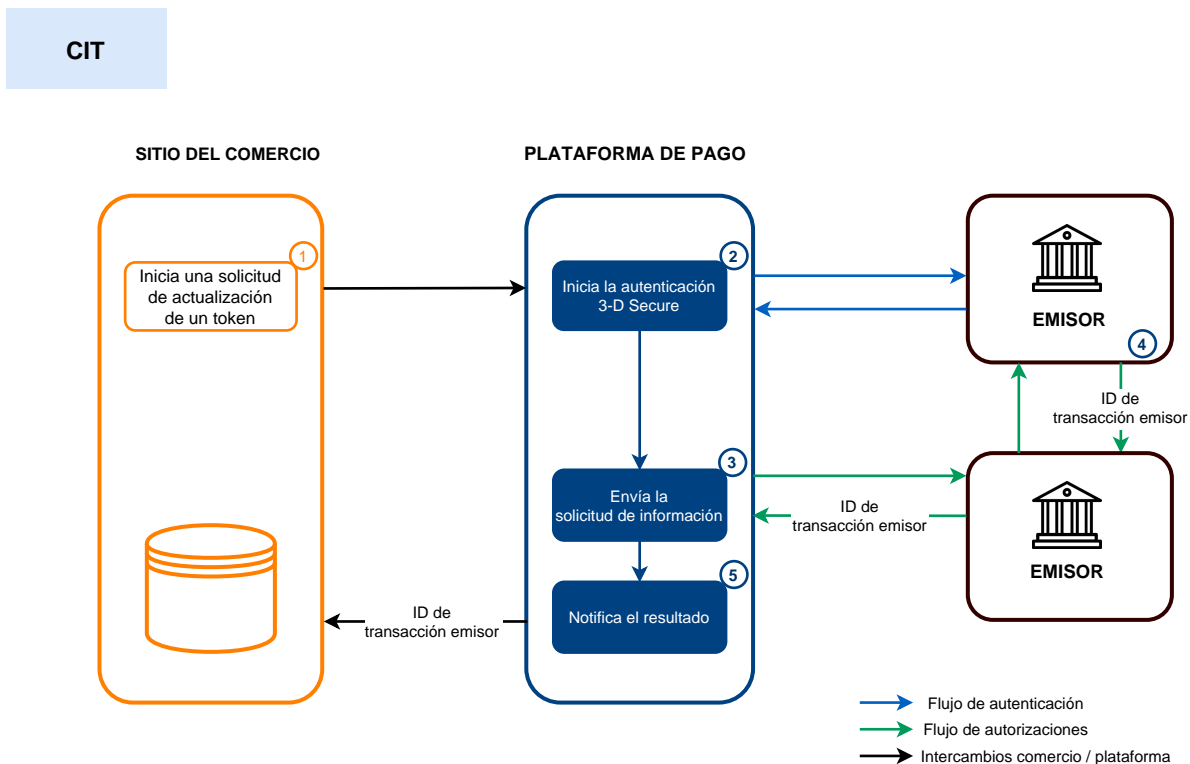
En función del uso que se hará del token (pago en 1 clic, pago sin clics, suscripción, etc.), la plataforma utilizará por defecto el identificador de transacción emisor como referencia de encadenamiento si fuera necesario.

En este caso, la gestión de la referencia de encadenamiento es transparente para el vendedor.

6.2. Cambio de información asociada al token

Por iniciativa del comprador, este caso corresponde a la actualización de los datos relacionados con su medio de pago y/o sus datos personales.

Esquema simplificado



1. El sitio web vendedor una *solicitud de actualización de un token*.

El comprador elige el método de pago que se debe registrar, entrega los datos de este y luego valida.

2. La plataforma de pago inicia el proceso de autenticación del portador con el emisor.



La reglamentación exige una autenticación fuerte cada vez que se registra una tarjeta.
La autenticación se realiza por un monto 0 EUR.

3. Una vez que la autenticación ha terminado, la plataforma realiza la solicitud de información con los datos de autenticación del titular.
4. El emisor genera un identificador único de transacción y lo transmite en la respuesta de la verificación de tarjeta.
5. La plataforma de pago notifica al sitio web vendedor el *resultado*.

En particular, la respuesta contiene:

- el código único de transacción generado por el emisor, para su información,
- el token actualizado.



Esta operación, se da lugar a la creación de una transacción de tipo VERIFICATION, que aparece en el Back Office Expert y posee las siguientes características:

- su monto es de 1.00 EUR o 0 EUR si el adquirente lo soporta,
- su estado es, o bien "Aceptado" o bien "Rechazado",

- nunca se envía al banco y permanece en la pestaña "Transacciones en curso".



El token no se actualizará si la solicitud de autorización o de información es rechazada.

La plataforma muestra el ticket al comprador. En particular, contiene:

- el token,
- Los datos del comprador.

Si ha configurado las reglas de notificación correspondientes, el comprador recibirá un correo electrónico:

- la confirmación del registro de sus datos bancarios en la plataforma de pago de la tienda,
- su token que podrá utilizar posteriormente para efectuar otra operación bancaria.



El código de la transacción emisor guardado en el token es reemplazado por el código generado por el emisor al actualizar el token.

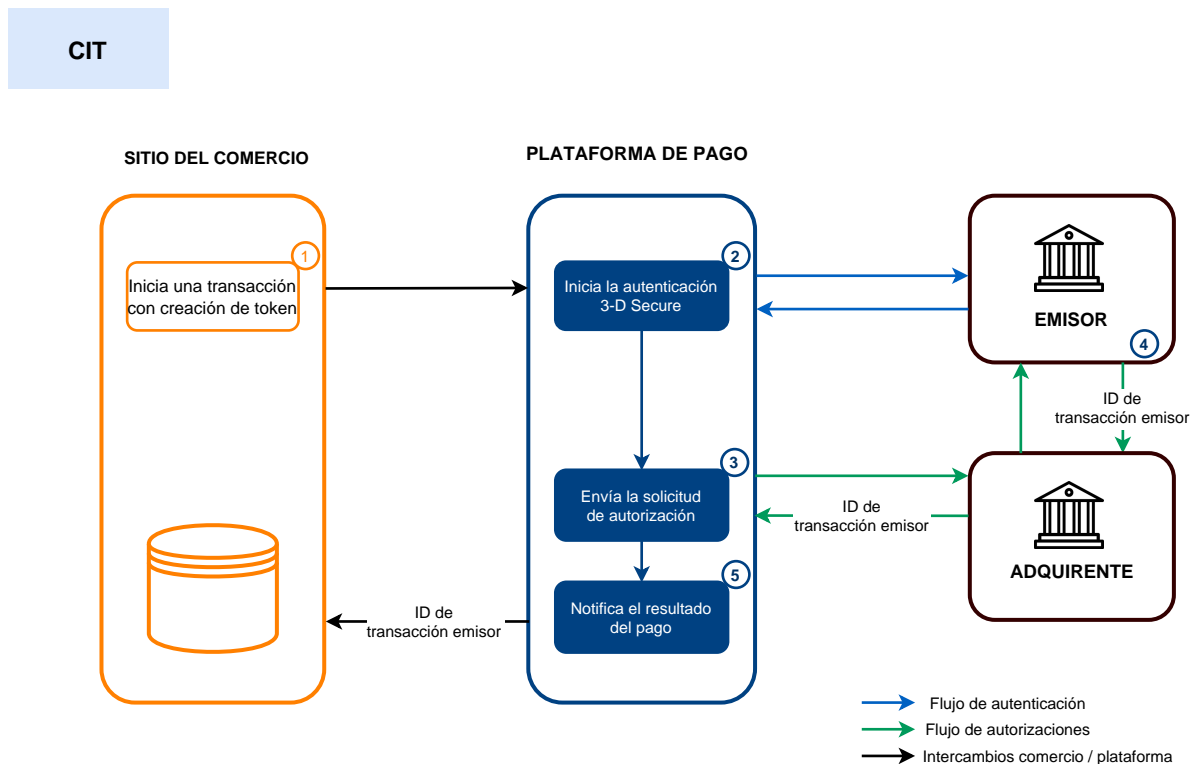
En función del uso que se hará del token (pago en 1 clic, pago sin clics, suscripción, etc.), se utilizará el identificador de transacción emisor como referencia de encadenamiento si fuera necesario.

En cuanto a la creación de un token, la gestión de la referencia de encadenamiento es transparente para el vendedor.

6.3. Creación del token durante un pago

En este caso, los parámetros necesarios para la inscripción se completan con los parámetros que se requieren para una solicitud de pago.

Esquema simplificado



1. El sitio web vendedor emite una *solicitud de pago con creación de token*.

Nota para las tiendas con la opción "Conversión de moneda"



Una vez realizado el pago en el momento del pedido, se permite la conversión de monedas. Por lo tanto, se admite la conversión de monedas para esta operación, a diferencia de la creación de un token con o sin suscripción.

El comprador elige el método de pago que se debe registrar, entrega los datos de este y luego valida.

2. La plataforma de pago inicia el proceso de autenticación del portador con el emisor.



En este caso, la reglamentación exige una autenticación fuerte. La Autenticación se realiza en el monto del pago.

3. Una vez que la autenticación ha terminado, la plataforma realiza la solicitud de autorización con los datos de autenticación del titular.
4. El emisor genera un identificador único de transacción y lo transmite en la respuesta de la solicitud de autorización.
5. La plataforma de pago notifica al sitio web vendedor el *resultado*.

En particular, la respuesta contiene:

- el resultado del pago,
- el código único de transacción generado por el emisor, para su información,

- el token creado recientemente.



El token no se creará si la solicitud de autorización o de información es rechazada.

La plataforma muestra el ticket al comprador. En particular, contiene:

- el resultado del pago,
- el token creado recientemente.

Si ha configurado las reglas de notificación correspondientes, el comprador recibirá un correo electrónico:

- el ticket de pago
- la confirmación del registro de sus datos bancarios en la plataforma de pago de la tienda,
- su token que podrá utilizar posteriormente para efectuar otra operación bancaria.



La plataforma de pago registra el identificador de transacción emisor a nivel del token y de la transacción.

En función del uso que se hará del token (pago en 1 clic, pago sin clics, suscripción, etc.), la plataforma utilizará por defecto el identificador de transacción emisor como referencia de encadenamiento si fuera necesario.

En caso de que el vendedor duplique (*MIT*) la transacción creada el día del pedido, la plataforma utilizará automáticamente este identificador como referencia de encadenamiento.

En este caso, la gestión de la referencia de encadenamiento es transparente para el vendedor.

6.4. Creación del token al suscribirse a una recurrencia

Además de la información utilizada en el caso de la **Creación del token sin pago**, este caso de uso también debe mostrar la información relacionada con la recurrencia, tal como:

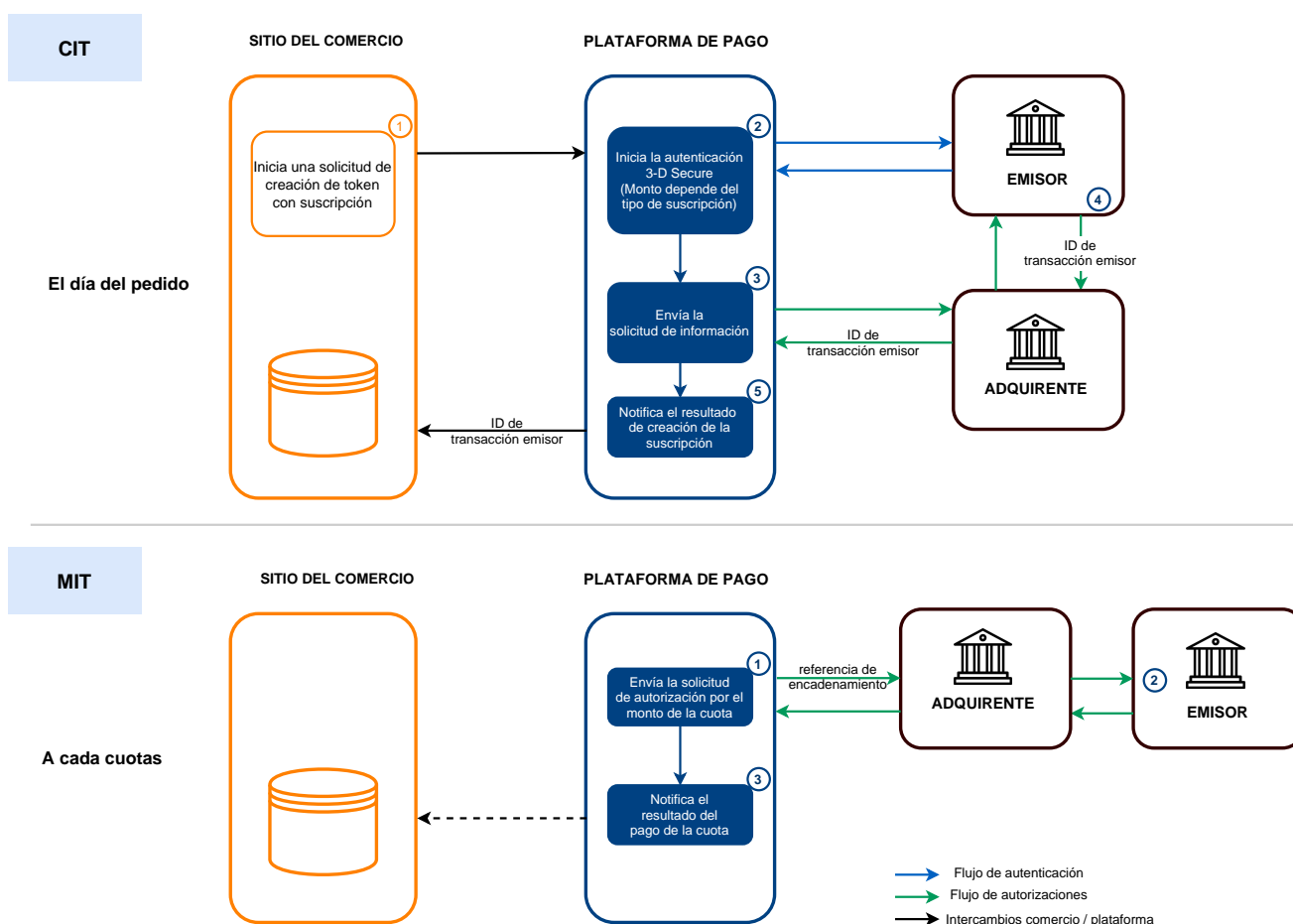
- el monto inicial de la recurrencia (monto utilizado durante el/los primer/os vencimientos) si este es diferente (opcional),
- el monto de la recurrencia (monto de los vencimientos, o bien el utilizado en los siguientes vencimientos cuando el primer es diferente).



No se realizará ningún pago al momento de la recurrencia. Solamente se realizará una solicitud de información para confirmar los datos del medio de pago.

El primer pago se realizará en la fecha efectiva, entre las 00:00 y las 05:00 h.

Esquema simplificado



El día del pedido:

1. El sitio web vendedor una *solicitud de creación de token y inscripción a una suscripción*.



Nota para las tiendas con la opción "Conversión de moneda":

La moneda es obligatorio durante la creación de un token.

Sólo se seleccionarán los contratos que admitan la moneda introducida como parámetro. No se tiene en cuenta la conversión de monedas.

Ejemplo: Para una solicitud de creación de un alias en moneda USD, en una tienda asociada a un contrato AMEX y a un contrato CB:

si el contrato AMEX sólo admite la moneda USD y el contrato CB sólo admite la moneda EUR, entonces sólo se aceptarán las tarjetas AMEX para la creación del alias.

El comprador elige el método de pago que desea registrar, entrega los datos de este y luego valida.

2. La plataforma de pago inicia el proceso de autenticación del portador con el emisor.



- En este caso, la reglamentación exige una autenticación fuerte.
- La autenticación se realiza por el monto de la primera cuota.

3. Una vez que la autenticación ha terminado, la plataforma realiza la solicitud de información con los datos de autenticación del titular.

4. El emisor genera un identificador único de transacción y lo transmite en la respuesta de la verificación de tarjeta.

5. La plataforma de pago notifica al sitio web vendedor el *resultado*.

En particular, la respuesta contiene:

- el código único de transacción generado por el emisor, para su información,
- el token creado recientemente,
- el detalle de la recurrencia.



Esta operación, se da lugar a la creación de una transacción de tipo VERIFICATION, que aparece en el Back Office Expert y posee las siguientes características:

- su monto es de 1.00 EUR o 0 EUR si el adquirente lo soporta,
- su estado es, o bien "Aceptado" o bien "Rechazado",
- nunca se envía al banco y permanece en la pestaña "Transacciones en curso".



El token no se creará si la solicitud de autorización o de información es rechazada.

La plataforma muestra el ticket al comprador. En particular, contiene:

- el token creado recientemente,
- Los montos de la recurrencia.

Si ha configurado las reglas de notificación correspondientes, el comprador recibirá un correo electrónico:

- la confirmación del registro de sus datos bancarios en la plataforma de pago de la tienda,
- la confirmación del registro de la recurrencia.



La plataforma de pago registra el identificador de transacción emisor a nivel del token.

En función del uso que se hará del token (pago en 1 clic, pago sin clics, suscripción, etc.), la plataforma utilizará por defecto el identificador de transacción emisor como referencia de encadenamiento si fuera necesario.

A cada cuotas :

1. La plataforma de pago realiza una solicitud de autorización por el monto de la cuota entregando un identificador de transacción inicial (CIT) como referencia de encadenamiento.
2. El emisor categoriza la transacción como una **MIT** dentro de una serie de pagos para la que el titular se autenticó previamente y realiza la solicitud de autorización.

La transacción no será rechazada por error de autenticación (soft decline).

3. Si el comercio ha activado la regla de notificación **URL de notificación al crear una recurrencia**, la plataforma de pago notifica al sitio web vendedor el *resultado del pago*.



En este caso, la gestión de la referencia de encadenamiento es transparente para el vendedor.

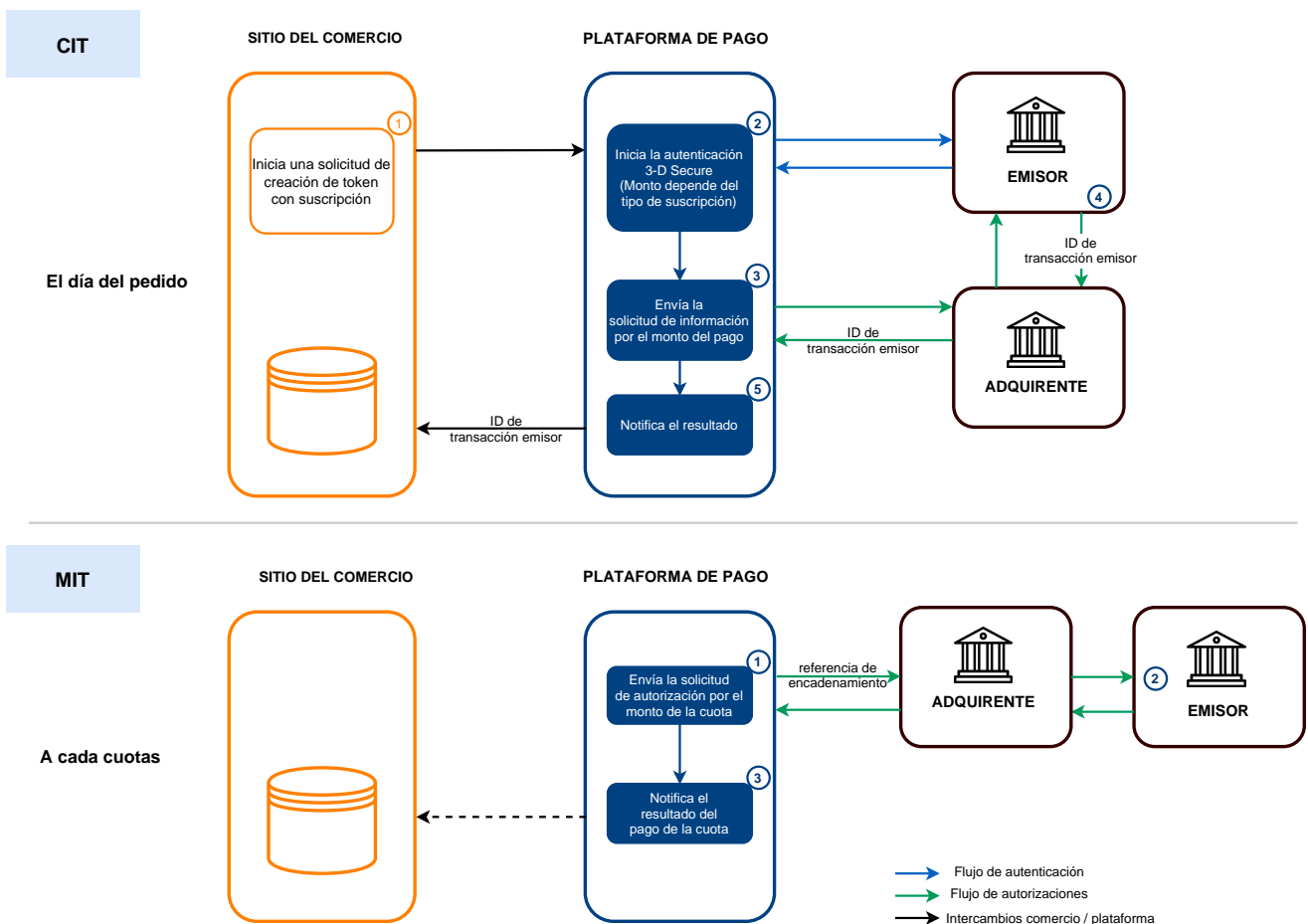
6.5. Creación del token al suscribir a una recurrencia acompañada de un pago

Este caso de uso debe mostrar información tal como:

- la información sobre el comprador,
- el identificador de la transacción,
- la información sobre la recurrencia (montos).

Ejemplo de uso: una recurrencia de un monto de X EUR/ N meses con gastos de puesta en servicio para pagar al tomar el pedido.

Esquema simplificado



El día del pedido:

1. El sitio web vendedor emite una *solicitud de creación de token y de suscripción con pago inmediato*.

Nota para las tiendas con la opción "Conversión de moneda"



Una vez realizado el pago en el momento del pedido, se permite la conversión de monedas. Por lo tanto, se admite la conversión de monedas para esta operación, a diferencia de la creación de un token con o sin suscripción.

El comprador elige el método de pago que se debe registrar, entrega los datos de este y luego valida.

2. La plataforma de pago inicia el proceso de autenticación del portador con el emisor.



- En este caso, la reglamentación exige una autenticación fuerte.
- La autenticación se realiza por el monto de la primera cuota.

3. Una vez que la autenticación ha terminado, la plataforma realiza la solicitud de autorización con los datos de autenticación del titular.
4. El emisor genera un identificador único de transacción y lo transmite en la respuesta de la solicitud de autorización.
5. La plataforma de pago notifica al sitio web vendedor el *resultado*.

En particular, la respuesta contiene:

- el resultado del pago,
- el detalle de la recurrencia,
- el código único de transacción generado por el emisor, para su información,
- el token creado recientemente.



El token y la suscripción no se crearán si la solicitud de autorización es rechazada.

La plataforma muestra el ticket al comprador. En particular, contiene:

- el resultado del pago,
- Los montos de la recurrencia,
- el token creado recientemente.

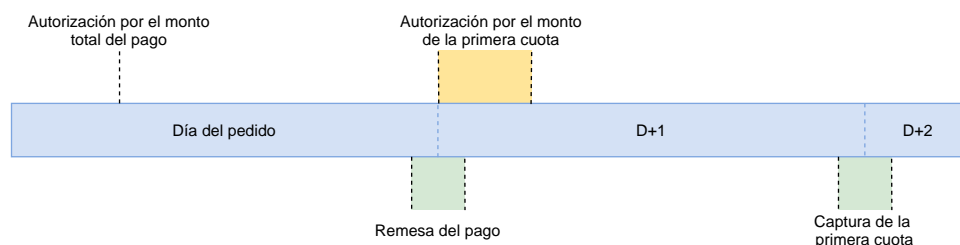
Si ha configurado las reglas de notificación correspondientes, el comprador recibirá un correo electrónico:

- el ticket de pago,
- la confirmación del registro de sus datos bancarios en la plataforma de pago de la tienda,
- la confirmación del registro de la recurrencia,
- su token que podrá utilizar posteriormente para efectuar otra operación bancaria.

El monto del pago se cobrará al comprador el día del pedido (o al día siguiente del pedido según el adquirente).

El cobro de la primera cuota de la suscripción se realizará en la fecha efectiva, entre las 00:00 y las 05:00 de la mañana.

Si la fecha efectiva se fija al día del pedido, se cobrará al comprador dos días seguidos (el día del pago y al día siguiente, la primera cuota)



Si desea que el pago realizado el día del pedido corresponda a la primera cuota de la suscripción, debe adaptar la fecha efectiva. Por ejemplo, para una suscripción mensual, la fecha efectiva debe fijarse a +30 días al hacer la solicitud de creación de la suscripción.

A cada cuotas :

1. La plataforma de pago realiza una solicitud de autorización por el monto de la cuota entregando un identificador de transacción inicial (CIT) como referencia de encadenamiento.
2. El emisor categoriza la transacción como una **MIT** dentro de una serie de pagos para la que el titular se autenticó previamente y realiza la solicitud de autorización.

La transacción no será rechazada por error de autenticación (soft decline).

3. Si el comercio ha activado la regla de notificación **URL de notificación al crear una recurrencia**, la plataforma de pago notifica al sitio web vendedor el *resultado del pago*.

La plataforma de pago registra el identificador de transacción emisor a nivel del token y de la transacción.

En función del uso que se hará del token (pago en 1 clic, pago sin clics, suscripción, etc.), la plataforma utilizará por defecto el identificador de transacción emisor como referencia de encadenamiento si fuera necesario.

En caso de que el vendedor duplique (**MIT**) la transacción creada el día del pedido, la plataforma utilizará automáticamente este identificador como referencia de encadenamiento.

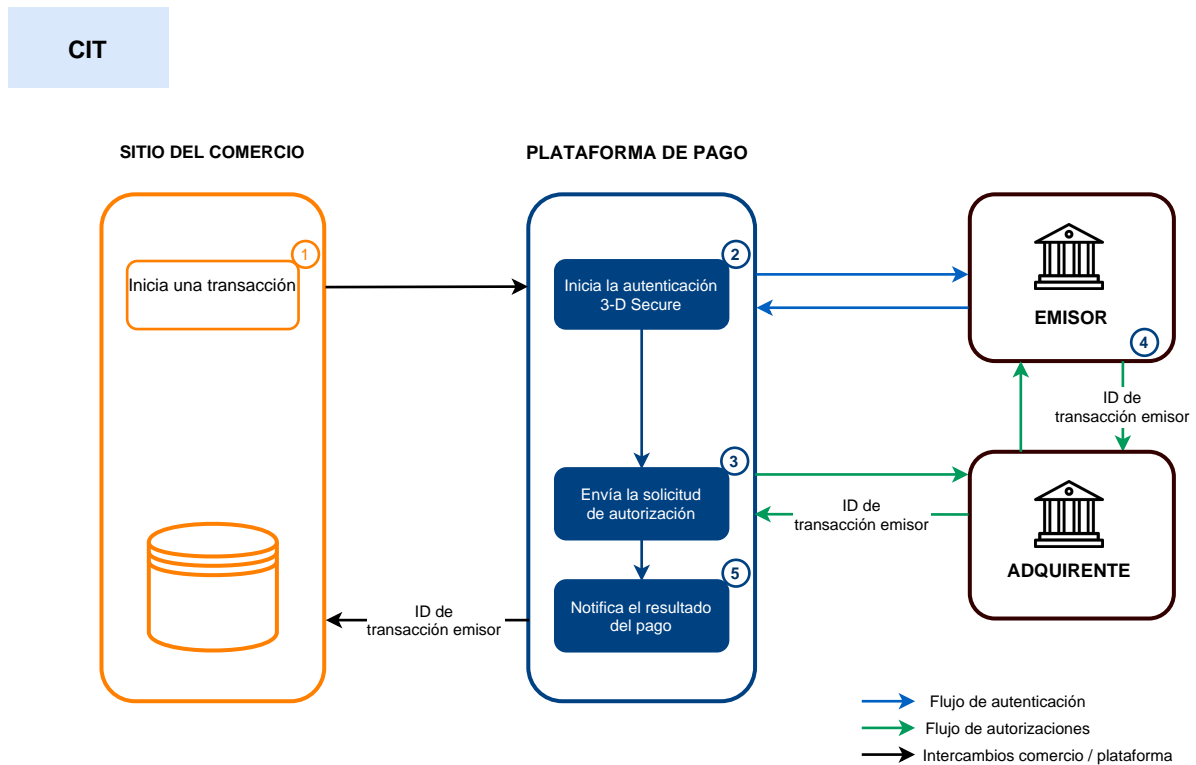
En este caso, la gestión de la referencia de encadenamiento es transparente para el vendedor.

6.6. Pago por Token

El pago por token permite, si ya se ha registrado un token previamente, realizar pagos unitarios o múltiples sin tener que seleccionar un medio de pago ni ingresar datos bancarios.

En dicho caso, se presenta una simple etapa de confirmación con un resumen de la transacción (número y monto).

Esquema simplificado



1. El sitio web vendedor emite una *solicitud de pago con reutilización de un token*.

El comprador verifica la información que muestra la página de pago, introduce el CVV de su tarjeta y la valida.



Si el token está asociado a un medio de pago expirado, la plataforma de pago propondrá automáticamente al comprador ingresar nuevos datos bancarios a fin de realizar el pago y actualizar el token asociado a este.

2. La plataforma de pago inicia el proceso de autenticación del portador con el emisor.



En este caso, la reglamentación exige el requisito del CVV y una autenticación del portador. La Autenticación se realiza en el monto del pago.

3. Una vez que la autenticación (challenge o frictionless) ha terminado, la plataforma realiza la solicitud de autorización con los datos de autenticación del titular.
4. El emisor genera un identificador único de transacción y lo transmite en la respuesta de la solicitud de autorización.
5. La plataforma de pago notifica al sitio web vendedor el *resultado*.

La plataforma muestra el ticket al comprador.

Si ha configurado las reglas de notificación correspondientes, el comprador recibirá la confirmación del pago por correo electrónico.



La plataforma de pago registra el identificador de transacción emisor.

En caso de que el vendedor duplique (**MIT**) la transacción, la plataforma utilizará automáticamente este identificador como referencia de encadenamiento.

En este caso, la gestión de la referencia de encadenamiento es transparente para el vendedor.

6.7. Uso de un token para suscribirse a una recurrencia

Una vez creado el token, es posible agregar una o varias recurrencia/s adicional/es que utilizará/n este token.

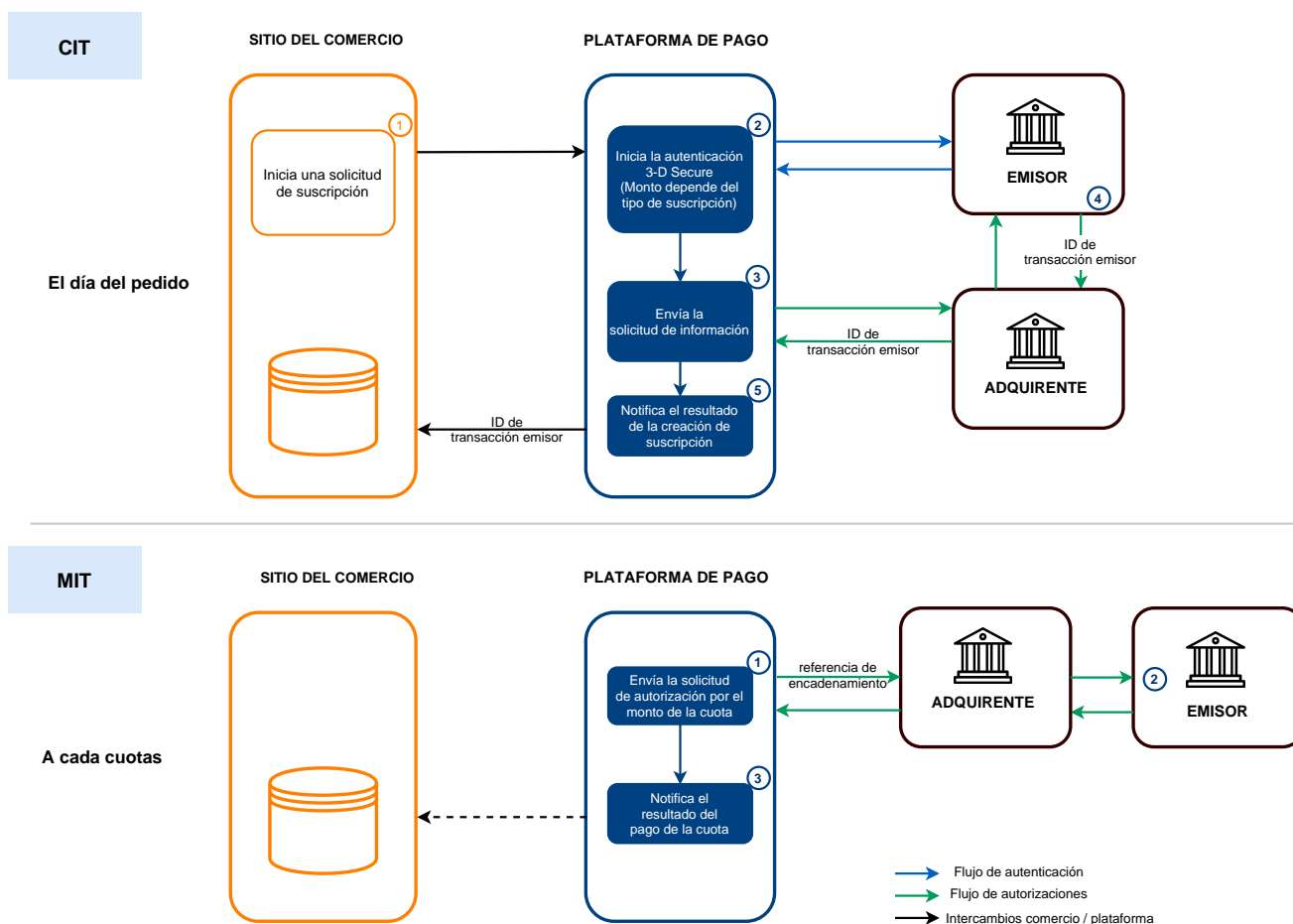
Al suscribirse a una nueva recurrencia, no se solicitará ingresar ningún dato bancario. Solo se requerirá una confirmación por parte del comprador.



No se realizará ningún pago al momento de la recurrencia. Solamente se realiza una solicitud de información para confirmar los datos del medio de pago.

El primer pago se realizará en la fecha efectiva, entre las 00:00 y las 05:00 h.

Esquema simplificado



El día del pedido:

1. El sitio web vendedor emite una *solicitud de suscripción a partir de un token existente*.

El comprador verifica los datos de la suscripción y valida.

2. La plataforma de pago notifica al sitio web vendedor el *resultado*.

La plataforma muestra el ticket al comprador. Contiene los montos de la suscripción.

Si ha configurado las reglas de notificación correspondientes, el comprador recibirá un correo electrónico de confirmación del registro de la recurrencia.

A cada cuotas :

1. La plataforma de pago realiza una solicitud de autorización por el monto de la cuota entregando un identificador de transacción inicial (CIT) como referencia de encadenamiento.
2. El emisor categoriza la transacción como una **MIT** dentro de una serie de pagos para la que el titular se autenticó previamente y realiza la solicitud de autorización.
La transacción no será rechazada por error de autenticación (soft decline).
3. Si el comercio ha activado la regla de notificación **URL de notificación al crear una recurrencia**, la plataforma de pago notifica al sitio web vendedor el *resultado del pago*.

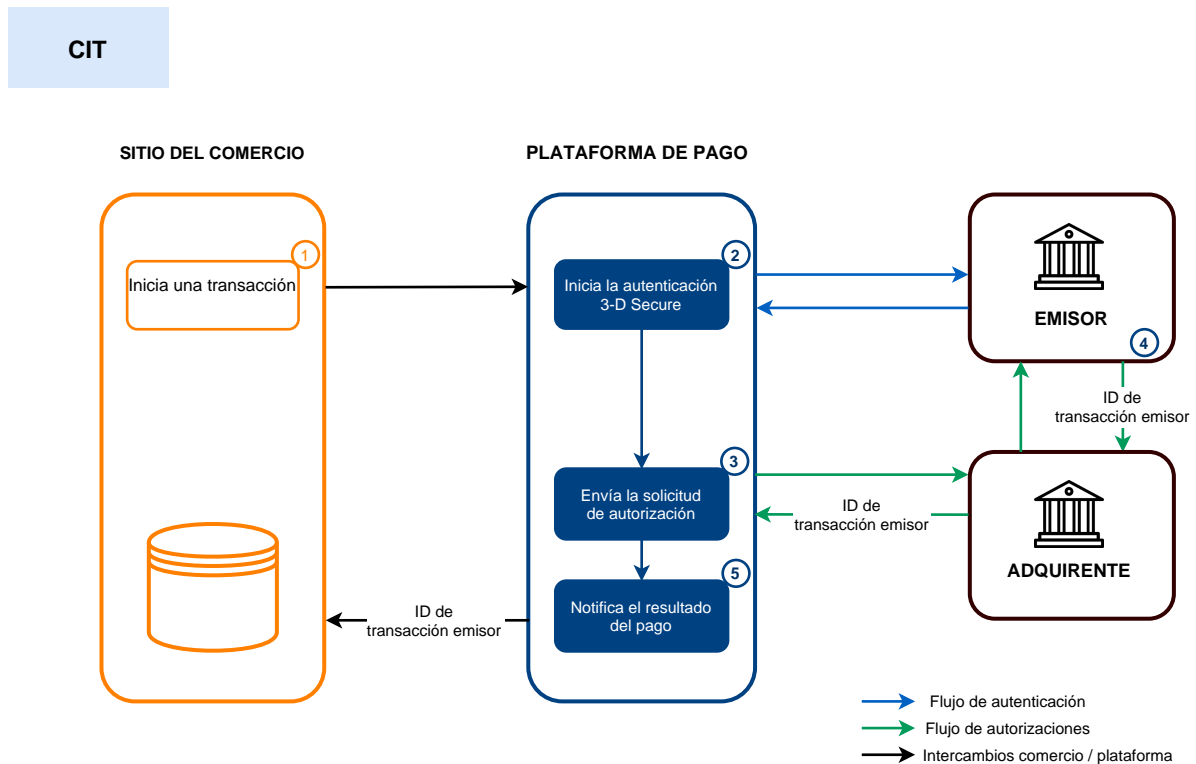


En este caso, la gestión de la referencia de encadenamiento es transparente para el vendedor.

6.8. Pago con propuesta al titular para crear un token

En el momento del pago, el comprador tiene la posibilidad de memorizar sus datos bancarios marcando la casilla correspondiente. Esta operación, totalmente segura, permite al comprador facilitar sus futuras compras.

Esquema simplificado



1. El sitio web vendedor una *solicitud de pago*.

El comprador elige el método de pago que se debe registrar y entrega los datos de este.

El comprador puede aceptar que la plataforma de pago registre su método de pago marcando una casilla a ese efecto. Por defecto, esta casilla no está marcada.

2. La plataforma de pago inicia el proceso de autenticación del portador con el emisor.



Si el comprador ha marcado la casilla, se ha creado un token del método de pago. Una autenticación fuerte es impuesta por regulaciones.

En caso contrario, el comprador debe autenticarse con o sin interacción.

Sea cual sea la elección del comprador, la Autenticación se realiza en el monto del pago.

3. Una vez que la autenticación ha terminado, la plataforma realiza la solicitud de autorización con los datos de autenticación del titular.

4. El emisor genera un identificador único de transacción y lo transmite en la respuesta de la solicitud de autorización.

5. La plataforma de pago notifica al sitio web vendedor el *resultado*.



El token no se creará si la solicitud de autorización o de información es rechazada.

La plataforma muestra el ticket al comprador. En particular, contiene:

- el resultado del pago,
- el token creado eventualmente.

Si ha configurado las reglas de notificación correspondientes, el comprador recibirá un correo electrónico:

- el ticket de pago
- la confirmación del registro de sus datos bancarios en la plataforma de pago de la tienda,
- su token que podrá utilizar posteriormente para efectuar otra operación bancaria.



La plataforma de pago registra el identificador de transacción emisor a nivel del token y de la transacción.

En función del uso que se hará del token (pago en 1 clic, pago sin clics, suscripción, etc.), la plataforma utilizará por defecto el identificador de transacción emisor como referencia de encadenamiento si fuera necesario.

En caso de que el vendedor duplique (**MIT**) la transacción creada el día del pedido, la plataforma utilizará automáticamente este identificador como referencia de encadenamiento.

En este caso, la gestión de la referencia de encadenamiento es transparente para el vendedor.

7. CICLO DE VIDA DE UN PAGO RECURRENTE

La recurrencia se inicia en su fecha efectiva.

La plataforma de pago creará entonces los pagos conforme al registro de vencimientos definido por la regla de recurrencia enviada en el formulario de creación de la recurrencia (campo `vads_sub_desc`).

En el contexto de la aplicación de la DSP2, la plataforma de pago transmite una referencia de encadenamiento en la solicitud de autorización, con el fin de evitar rechazos por falta de autenticación (soft decline).

Por cada vencimiento de una recurrencia, si la regla **URL de notificación al crear una recurrencia** se activa y configura correctamente, el sitio del vendedor recibirá el resultado del pago en su URL de notificación (IPN).

En particular, la notificación contiene:

- el campo `vads_subscription`, que indica la referencia de la recurrencia,
- el campo `vads_recurrence_number`, que indica el número del vencimiento,
- el campo `vads_occurrence_type`, que indica de qué vencimiento se trata (primero, enésimo o último vencimiento),
- el campo `vads_trans_status`, que indica el estado del pago (aceptado o rechazado).

En caso de pago denegado:

- el vendedor no será notificado por correo electrónico,
- el pago no volverá a solicitarse automáticamente.

Si el medio de pago alcanza su fecha de vencimiento, se crea una transacción rechazada sin llamada al banco emisor. El detalle del error (`vads_payment_error`) se establece en 8 - La fecha de vencimiento de la tarjeta no permite esta acción.

Si los datos del medio de pago fueron purgados tras un periodo de inactividad de 15 meses, se crea una transacción rechazada sin llamada al banco emisor. El detalle del error (`vads_payment_error`) se establece en 107 - El medio de pago asociado al token ya no es válido.

Caso particular de las recurrencias con frecuencia diaria

Si solicita la creación de una recurrencia para debitar el portador a diario (`RRULE:FREQ=DAILY;INTERVAL=1`) y que la fecha de efecto solicitada (`vads_sub_effect_date`) corresponde a la fecha de creación de la recurrencia, entonces la plataforma de pago tratará esta recurrencia al día siguiente (entre medianoche y las 5:00), se crearán 2 pagos:

- el de la víspera (que corresponde a la fecha de efecto),
- y el del día.

Para evitarlo, se aconseja transmitir una fecha de efecto al día siguiente del día en que se creó la recurrencia.

8. CICLO DE VIDA DE UN PAGO RECURRENTE CON AUTORIZACIÓN ANTICIPADA

Gracias a esta opción, cuando se rechaza un pago por un motivo no fraudulento (ver capítulo [Lista de códigos de retorno de la solicitud de autorización](#)) la plataforma de pago puede realizar automáticamente una nueva solicitud de autorización, todos los días y hasta dos días antes de la fecha prevista de captura.

En cuanto se activa la opción en la tienda, los pagos recurrentes se crean 6 días antes de la fecha prevista por la regla de recurrencia.

Es indispensable activar la regla **URL de notificación al autorizar por batch** desde su Back Office Expert (ver capítulo [Configurar la notificación al autorizar por batch](#)).

D-6 : creación del pago recurrente

- La solicitud de autorización es aceptada.
 - El pago permanecerá **En espera de captura** hasta la fecha prevista inicialmente.
 - Si la regla **URL de notificación al crear una recurrencia** se activa, se generará un llamado a la URL de notificación. La solicitud constará de los siguientes valores:

Nombre del campo	Valor
vads_url_check_src	REC
vads_trans_status	AUTHORISED

- La solicitud de autorización es rechazada por un motivo fraudulento.
 - El pago es **Rechazado** definitivamente.
 - Si la regla **URL de notificación al crear una recurrencia** se activa, se generará un llamado a la URL de notificación. La solicitud constará de los siguientes valores:

Nombre del campo	Valor
vads_url_check_src	REC
vads_trans_status	REFUSED

- La solicitud de autorización es rechazada por un motivo no fraudulento.
 - El pago permanecerá **En espera de autorización**.
 - Si la regla **URL de notificación al crear una recurrencia** se activa, se generará un llamado a la URL de notificación. La solicitud constará de los siguientes valores:

Nombre del campo	Valor
vads_url_check_src	REC
vads_trans_status	WAITING_AUTHORISATION

D-5, D-4, D-3: Nueva solicitud de autorización iniciada automáticamente

- La solicitud de autorización es aceptada.
 - El pago permanecerá **En espera de captura** hasta la fecha prevista inicialmente.
 - Si la regla **URL de notificación al autorizar por batch** se activa, se generará un llamado a la URL de notificación. En este caso, la solicitud constará de los siguientes valores:

Nombre del campo	Valor
vads_url_check_src	BATCH_AUTO
vads_trans_status	AUTHORISED

- La solicitud de autorización es rechazada por un motivo fraudulento.
 - El pago es **Rechazado** definitivamente.
 - Si la regla **URL de notificación al autorizar por batch** se activa, se generará un llamado a la URL de notificación. En este caso, la solicitud constará de los siguientes valores:

Nombre del campo	Valor
vads_url_check_src	BATCH_AUTO
vads_trans_status	REFUSED

- La solicitud de autorización es rechazada por un motivo no fraudulento.
 - El pago permanecerá **En espera de captura** hasta la fecha prevista.
 - Si la regla **URL de notificación al autorizar por batch** se activa, se generará un llamado a la URL de notificación. En este caso, la solicitud constará de los siguientes valores:

Nombre del campo	Valor
vads_url_check_src	BATCH_AUTO
vads_trans_status	WAITING_AUTHORISATION

D-2: Última solicitud de autorización iniciada automáticamente

- La solicitud de autorización es aceptada.
 - El pago permanecerá **En espera de captura** hasta la fecha prevista inicialmente.
 - Si la regla **URL de notificación al autorizar por batch** se activa, se generará un llamado a la URL de notificación. En este caso, la solicitud constará de los siguientes valores:

Nombre del campo	Valor
vads_url_check_src	BATCH_AUTO
vads_trans_status	AUTHORISED

- La solicitud de autorización es rechazada (por cualquier motivo)
 - El pago es **Rechazado** definitivamente.
 - Si la regla **URL de notificación al autorizar por batch** se activa, se generará un llamado a la URL de notificación. En este caso, la solicitud constará de los siguientes valores:

Nombre del campo	Valor
vads_url_check_src	BATCH_AUTO
vads_trans_status	REFUSED

D-2: Captura de la transacción

El pago es capturado automáticamente.

No se generará ningún llamado a la URL de notificación.

Notas

- *Rechazo de un pago entre D-6 y D-2*

Cuando el pago se rechaza definitivamente, usted deberá asegurarse de que el acceso al servicio en el que se suscribió a la recurrencia sea dado de baja en la fecha prevista y no el día en que se recibió el pago rechazado.

- *Baja de una recurrencia*

Cuando el comprador da de baja su recurrencia, es responsabilidad del vendedor dar de baja los pagos que han sido creados de forma anticipada.

8.1. Lista de códigos de retorno de la solicitud de autorización

Los códigos de retorno de la solicitud de autorización son devueltos por el banco emisor, si está disponible.

Valor	Descripción	Repetición autorizada.
00	Transacción aprobada o procesada con éxito	
02	Póngase en contacto con el emisor de la tarjeta.	
03	Aceptador invalido	SI
04	Conservar la tarjeta	SI
05	No honrar	SI
07	Conservar la tarjeta, condiciones especiales	SI
08	Aprobar después de la identificación	
12	Transacción inválida	SI
13	Monto inválido	SI
14	Número de tarjetahabiente inválido	SI
15	Emisor de tarjeta desconocido	SI
17	Cancelación del comprador	
19	Repetir la transacción más tarde	
20	Respuesta incorrecta (error en el dominio del servidor)	
24	Actualización de archivo no compatible	
25	No se puede localizar el registro en el archivo	
26	Registro duplicado, registro antiguo reemplazado	
27	Error en "editar" en el campo de lista de archivos	
28	No hay acceso al archivo	
29	No se puede actualizar	
30	Error de formato	
31	Identificador del organismo adquirente desconocido	SI
33	La fecha de vencimiento de la tarjeta a caducado	SI
34	Sospecha de fraude	SI
38	La fecha de vencimiento de la tarjeta a caducado	
41	Tarjeta perdida	SI
43	Tarjeta robada	SI
46	Cuenta de cliente cerrada	
51	Saldo insuficiente o crédito rebasado	
54	La fecha de vencimiento de la tarjeta a caducado	SI
55	PIN incorrecto	
56	Tarjeta ausente del archivo	SI
57	Transacción no permitida a este portador	SI
58	Transacción no permitida a este portador	
59	Sospecha de fraude	SI
60	El aceptador de la tarjeta debe contactar al adquirente	
61	Monto del retiro de fondos supera el límite	
63	Reglas de seguridad no respetadas	SI
65	Número de retiros excedidos	
68	Respuesta no alcanzada o recibida demasiado tarde	
75	Número de intentos de PIN superado	
76	El titular ya está en oposición, antiguo registro mantenido	SI
78	Transacción bloqueada, primera transacción con una tarjeta no desbloqueada correctamente	
80	El emisor no acepta los pagos contactless	
81	El emisor no acepta pagos sin autenticación Safekey	
82	CVV, dCVV, iCVV incorrectos	
83	Revocación todos los pagos recurrentes para la tarjeta	

Valor	Descripción	Repetición autorizada.
84	R1: Revocación de pago recurrente para la tarjeta en el comercio o para el código MCC y la tarjeta	
86	6P - La verificación de datos del emisor falló	
90	Interrupción momentánea del sistema	
91	Emisor de tarjeta inaccesible	
94	Transacción duplicada	
96	Mal funcionamiento del sistema	
97	El time-out de supervisión global ha expirado	
98	Servidor no disponible. Intento de conexión solicitado nuevamente	
99	Problema de conexión con el adquirente	

8.2. Notificación por e-mail en caso de rechazo de una cuota

Caso de la opción Autorización anticipada

Cuando el pago es rechazado, se envía un e-mail de advertencia al vendedor.

9. OFRECER INTENTOS DE PAGO ADICIONALES

Cuando se rechaza un pago, puede ofrecer al comprador la posibilidad de intentar con otro medio de pago.

La cantidad de intentos suplementarios se puede parametrizar desde el Back Office Expert:

1. Abra el menú **Configuración > Tienda** y haga clic en el nombre de la tienda cuya configuración desea modificar.
2. Seleccione la pestaña **Configuración**.
3. Indique el número de intentos adicionales autorizados en caso de rechazo de un pago.

Si usted configura 2 intentos suplementarios, entonces el comprador podrá realizar en total 3 intentos de pago.

4. Si lo desea, puede activar el envío de una notificación al final del pago (IPN) para cada intento rechazado marcando la casilla **URL de notificación sobre tentativa rechazada**.
5. Haga clic en el botón **Guardar**.



No se podrán ofrecer intentos adicionales:

- si el vendedor solicitó un retorno automático a la tienda en el campo **vads_redirect_error_timeout**,
- si se trata de un pago en varios vencimientos.



Intentos de pago suplementarios y pago por alias (1 clic).

Si el pago en 1 clic es rechazado, el comprador deberá elegir otro método de pago e ingresar los datos de su tarjeta.

Si el pago es aceptado:

- la transacción no se asociará al token transmitido en la solicitud,
- el token no será actualizado.

10. ESTABLECER DIÁLOGO CON LA PLATAFORMA DE PAGO

El diálogo entre el sitio web vendedor y la plataforma de pago se realiza mediante un intercambio de datos.

Para crear un pago, estos datos se envían a través de un formulario HTML por el navegador del comprador.

Al final del pago, el resultado se transmite al sitio web vendedor de dos maneras:

- automáticamente mediante notificaciones denominadas URL de notificación instantánea (también conocidas como IPN, del inglés Instant Payment Notification), consulte el capítulo **Configurar notificaciones**.
- en el navegador cuando el comprador hace clic en el botón para volver al sitio web vendedor, consulte el capítulo **Gestionar el diálogo al sitio web vendedor**.

Para garantizar la seguridad de los intercambios, los datos se firmarán mediante una clave conocida solamente por el comerciante y la plataforma de pago.

10.1. Similitudes con el pago unitario

Todas las funcionalidades disponibles para el pago unitario lo están también para los pagos por token y por recurrencias.

Para más información, consulte el *Guía de implementación Formulario API*

A continuación, encontrará una lista no exhaustiva:

- Pago unitario: se realiza en una vez o en forma fraccionada.
- Gestión de varias monedas.
- Gestión de varios medios de pago y de afiliaciones de vendedores asociados.
- Personalización de las páginas de pago.
- Visualización en un iframe.

11. CONFIGURAR NOTIFICACIONES

Varios tipos de notificaciones están a disposición en el Back Office Expert.

- Llamada URL de notificación
- E-mail enviado al vendedor
- E-mail enviado al comprador
- SMS enviado al vendedor
- SMS enviado al comprador

Permiten gestionar los eventos (pago aceptado, abandono por parte del comprador, cancelación por parte del vendedor...) que generarán el envío de una notificación al sitio web vendedor, al vendedor o al comprador.



Las notificaciones de tipo Llamada URL de notificación son las más importantes, pues representan el único medio confiable para que el sitio del comerciante pueda obtener el resultado de un pago.

Si la plataforma no logra conectarse a la URL de su página, se enviará un correo electrónico a la dirección especificada.

Este contiene:

- El código HTTP del error encontrado
- Elementos de análisis en función del error
- Sus consecuencias
- El procedimiento a seguir desde el Back Office Expert para enviar la solicitud a la URL definida.

Para acceder a la gestión de las reglas de notificación:

1. Conéctese a su Back Office Vendedor disponible en la siguiente URL:
<https://secure.lyra.com/portal/>
2. Haga clic en el botón **Otras acciones** para acceder a su Back Office Expert.
3. Vaya al menú **Configuración > Reglas de notificaciones**.

Reglas de notificación de la tienda: ...	
Activada	Etiqueta
	URL de notificación sobre anulación
	URL de notificación sobre una operación proveniente del Back Office
	URL de notificación al final del pago
	URL de notificación sobre modificación por batch
	URL de notificación durante la creación de una suscripción

11.1. Configurar la notificación al final del pago

Esta regla permite notificar al sitio del comerciante en los siguientes casos:

- Pago aceptado
- Pago rechazado
- Creación o actualización de un token
- Registro de una recurrencia



Esta notificación es indispensable para comunicar el resultado de una solicitud de pago, de una creación de token o de una creación de suscripción.

Esta informará el resultado al sitio del vendedor si el cliente no ha hecho clic en el botón Volver a la tienda.

1. Haga clic derecho en la línea **URL de notificación al final del pago**.
2. Seleccione **Gestionar la Regla**.
3. En la sección **Configuración general**, ingrese el campo **Dirección(es) e-mail(s) a notificar en caso de falla**.
Para especificar varias direcciones de e-mail, sepárelas con un punto y coma.
4. Marque la casilla **Reenvío automático en caso de falla** si desea autorizar a la plataforma a reenviar automáticamente la notificación hasta 4 veces en caso de falla.
Para más información, consulte el capítulo [Reejecutar automáticamente en caso de fallo](#) en la página 48.
5. En la sección **URL de notificación de la API formulario V1, V2**, ingrese la URL de su página en los campos **URL a llamar en modo PRUEBA** y **URL a llamar en modo PRODUCCIÓN** si desea recibir las notificaciones en el formato Formulario API.
6. Guarde sus cambios.

11.2. Configurar la notificación en caso de abandono/cancelación

Esta regla permite notificar al sitio del comerciante en los siguientes casos:

- En caso de abandono o cancelación por parte del comprador, a través del botón **Cancelar y regresar a la tienda**.
- Cuando el comprador no ha terminado su pago antes de la expiración de su sesión de pago.
La duración máxima de una sesión de pago es de 10 minutos.

Esta configuración es **obligatoria** si utiliza el medio de pago **FacilyPay Oney**.

Esta regla está **desactivada por defecto**.

1. Haga clic derecho en la línea **URL de notificación al abandonar (comprador)**.
2. Seleccione **Gestionar la Regla**.
3. En la sección **Configuración general**, ingrese el campo **Dirección(es) e-mail(s) a notificar en caso de falla**.
Para especificar varias direcciones de e-mail, sepárelas con un punto y coma.
4. Marque la casilla **Reenvío automático en caso de falla** si desea autorizar a la plataforma a reenviar automáticamente la notificación hasta 4 veces en caso de falla.
Para más información, consulte el capítulo [Reejecutar automáticamente en caso de fallo](#) en la página 48.
5. En la sección **URL de notificación de la API formulario V1, V2**, ingrese la URL de su página en los campos **URL a llamar en modo PRUEBA** y **URL a llamar en modo PRODUCCIÓN** si desea recibir las notificaciones en el formato Formulario API.
6. En la sección **URL de notificación de la API REST**, ingrese la URL de su página en los campos **URL de la IPN a llamar en modo prueba** y **URL de la IPN a llamar en modo producción** si utiliza el cliente JavaScript.
7. Guarde sus cambios.
8. Active la regla con un clic derecho en **URL de notificación al abandonar (comprador)** y seleccione **Activar la regla**.

11.3. Configurar la notificación de una operación proveniente del Back Office

Esta regla permite notificar al sitio del comerciante cada vez que se realiza una operación en el Back Office Expert:

- Creación de un pago manual (aceptado o rechazado)
 - Modificación de una transacción
 - Duplicación de una transacción
 - Reembolso de una transacción
 - Cancelación de una transacción
 - Validación de una transacción
 - Creación de un token
 - Actualización de un token
1. Haga clic derecho en la línea **URL de notificación al modificar una transacción en el Back Office (vendedor)**.
 2. Seleccione **Gestionar la Regla**.
 3. En la sección **Configuración general**, ingrese el campo **Dirección(es) e-mail(s) a notificar en caso de falla**.
Para especificar varias direcciones de e-mail, sepárelas con un punto y coma.
 4. Marque la casilla **Reenvío automático en caso de falla** si desea autorizar a la plataforma a reenviar automáticamente la notificación hasta 4 veces en caso de falla.
Para más información, consulte el capítulo [Reejecutar automáticamente en caso de fallo](#) en la página 48.
 5. En la sección **URL de notificación de la API formulario V1, V2**, ingrese la URL de su página en los campos **URL a llamar en modo PRUEBA** y **URL a llamar en modo PRODUCCIÓN** si desea recibir las notificaciones en el formato Formulario API.
 6. En la sección **URL de notificación de la API REST**, ingrese la URL de su página en los campos **URL de la IPN a llamar en modo prueba** y **URL de la IPN a llamar en modo producción** si utiliza el cliente JavaScript.
 7. Guarde sus cambios.
 8. Active la regla con un clic derecho en **URL de notificación al modificar una transacción en el Back Office (vendedor)** y seleccione **Activar la regla**.

11.4. Configurar la notificación al crear una recurrencia

Esta regla permite notificar al sitio del comerciante en los siguientes casos:

- Cuando la plataforma de pago crea un nuevo vencimiento de un pago recurrente.
- En cada nuevo intento de pago, después de que un vencimiento de un pago recurrente fue rechazado. Necesita la activación de la opción de autorización anticipada.

Esta regla está **desactivada por defecto**.

1. Haga clic derecho en la línea **URL de notificación al crear una recurrencia**.
2. Seleccione **Gestionar la Regla**.
3. En la sección **Configuración general**, ingrese el campo **Dirección(es) e-mail(s) a notificar en caso de falla**.
Para especificar varias direcciones de e-mail, sepárelas con un punto y coma.
4. Marque la casilla **Reenvío automático en caso de falla** si desea autorizar a la plataforma a reenviar automáticamente la notificación hasta 4 veces en caso de falla.
Para más información, consulte el capítulo [Reejecutar automáticamente en caso de fallo](#) en la página 48.
5. En la sección **URL de notificación de la API formulario V1, V2**, ingrese la URL de su página en los campos **URL a llamar en modo PRUEBA** y **URL a llamar en modo PRODUCCIÓN** si desea recibir las notificaciones en el formato Formulario API.
6. En la sección **URL de notificación de la API REST**, ingrese la URL de su página en los campos **URL de la IPN a llamar en modo prueba** y **URL de la IPN a llamar en modo producción** si utiliza el cliente JavaScript.
7. Guarde sus cambios.
8. Active la regla con un clic derecho en **URL de notificación al crear una recurrencia** y seleccione **Activar la regla**.

11.5. Configurar la notificación al autorizar por batch

Si la tienda cuenta con la opción **Autorización anticipada**, deberá activarse la regla **URL de notificación al autorizar por batch** a fin de recibir el resultado final del pago.

Esta regla está **desactivada por defecto**.

1. Haga clic derecho en la línea **URL de notificación al autorizar por batch**.
2. Seleccione **Gestionar la Regla**.
3. En la sección **Configuración general**, ingrese el campo **Dirección(es) e-mail(s) a notificar en caso de falla**.
Para especificar varias direcciones de e-mail, sepárelas con un punto y coma.
4. Marque la casilla **Reenvío automático en caso de falla** si desea autorizar a la plataforma a reenviar automáticamente la notificación hasta 4 veces en caso de falla.
Para más información, consulte el capítulo [Reejecutar automáticamente en caso de fallo](#) en la página 48.
5. En la sección **URL de notificación de la API formulario V1, V2**, ingrese la URL de su página en los campos **URL a llamar en modo PRUEBA** y **URL a llamar en modo PRODUCCIÓN** si desea recibir las notificaciones en el formato Formulario API.
6. En la sección **URL de notificación de la API REST**, ingrese la URL de su página en los campos **URL de la IPN a llamar en modo prueba** y **URL de la IPN a llamar en modo producción** si utiliza el cliente JavaScript.
7. Guarde sus cambios.
8. Active la regla con un clic derecho en **URL de notificación al autorizar por batch** y seleccione **Activar la regla**.

11.6. Reejecutar automáticamente en caso de fallo

El reenvío automático no se aplica a las notificaciones activadas manualmente desde el Back Office Expert.

El vendedor puede activar un mecanismo que permita a la plataforma de pago reenviar automáticamente las notificaciones cuando el sitio del comerciante es realmente inalcanzable **hasta 4 veces**.

Una notificación se considerará infructuosa si el código de retorno HTTP devuelto por el sitio del comerciante no se encuentra en la siguiente lista: **200, 201, 202, 203, 204, 205, 206, 301, 302, 303, 307, 308**.

Los intentos de llamada se programan a horas fijas cada 15 minutos (00, 15, 30, 45).

Tras cada tentativa infructuosa, se enviará un e-mail de alerta a la dirección especificada en la configuración de la regla de notificación correspondiente.

El asunto del e-mail de alerta contiene el número del intento de enviar la notificación. Se presenta en la forma **attempt #** seguida del número de intento.

- Ejemplo de asunto de un correo electrónico de alerta recibido después de la primera notificación fallida al final de un pago:

```
[MODE TEST] Mi Tienda - Tr. Ref. 067925 / FALLO al invocar a su URL de notificación  
[unsuccessful attempt #1]
```

- Ejemplo de asunto de e-mail recibido en el segundo error:

```
[MODE TEST] Mi Tienda - Tr. Ref. 067925 / FALLO al invocar a su URL de notificación  
[unsuccessful attempt #2]
```

- Ejemplo de asunto de e-mail recibido en el tercer error:

```
[MODE TEST] Mi Tienda - Tr. Ref. 067925 / FALLO al invocar a su URL de notificación  
[unsuccessful attempt #3]
```

- Ejemplo de asunto de e-mail recibido en el último intento:

```
[MODE TEST] Mi Tienda - Tr. Ref. 067925 / FALLO al invocar a su URL de notificación  
[unsuccessful attempt #last]
```

Para notificar al sitio del comerciante el fallo del último intento de notificación, el asunto del e-mail incluirá **attempt #last**.

Cuando hay reenvío automático, parte de la información no se guarda en la base de datos o se modifica.

Ejemplos de campos no disponibles / no registrados en la base de datos:

Nombre del campo	Descripción
vads_page_action	Operación realizada
vads_payment_config	Tipo de pago (al contado o en vencimientos)
vads_action_mode	Modo de adquisición de la información del medio de pago

Ejemplos de campos enviados con diferentes valores:

Nombre del campo	Nuevo valor
vads_url_check_src	Se asignará el valor RETRY en el caso de un reenvío automático.
vads_trans_status	El estado de la transacción puede variar entre la llamada inicial y el reenvío automático (cancelación del vendedor, remesa al banco de la transacción, etc.).
vads_hash	El valor de este campo se regenera en cada llamada.
firma	El valor de la firma depende de los diferentes estados que pueden variar entre la llamada inicial y el reenvío automático.

Estos e-mails detallan:

- el problema encontrado
- los elementos de análisis en función del error
- sus consecuencias
- el procedimiento a seguir desde el Back Office Expert para activar la notificación de forma manual.



Después del cuarto intento, todavía es posible reenviar la URL de notificación **manualmente** desde su Back Office Expert.



Atención, durante el período de reenvío automático, cualquier llamada manual a la URL de notificación afectará el número de reintentos automáticos:

- una llamada manual exitosa detendrá el reenvío automático
- una llamada manual fallida no tendrá ningún impacto en el reenvío automático actual.

11.7. Configurar correos electrónicos enviados al comprador

En la pestaña **E-mail enviado al comprador**:

1. Haga clic derecho en la regla por modificar y seleccione **Activar la regla**.
2. Haga otro clic derecho en la regla y seleccione **Gestionar la Regla**.
Aparece el asistente de gestión de una regla de notificación.
3. En la sección Configuración general, puede personalizar la descripción de la regla.
4. Para personalizar el contenido del correo electrónico:
 - a. Haga clic en **Configuración e-mail comprador**.
 - b. Seleccione el modelo de e-mail que aplicará.
 - c. Seleccione el idioma en el cual desea realizar modificaciones.
 - d. Haga clic en el enlace **Personalizar valores de texto predeterminados** si desea modificar el asunto y el contenido del e-mail "por defecto".
 - e. Haga clic en **Campos a incluir** para mostrar la lista de campos disponibles para personalizar el correo electrónico.
 - f. Seleccione los campos que desea incluir. Se agregará un resumen detallado del procesamiento de la solicitud al contenido del correo electrónico.



Para obtener una vista previa de los cambios realizados, haga clic en **Vista previa del correo electrónico** en la parte inferior del cuadro de diálogo.

5. Para modificar los eventos que activan la notificación:
 - a. Haga clic en la pestaña **Condiciones de la regla**
Una condición consiste en una variable, un operador de comparación y un valor de referencia.
Ejemplo: "mode = TEST", "monto superior a 1000". Al ejecutar una regla, el valor de la variable se recupera y se compara con el valor de referencia.
 - b. Haga doble clic en una condición existente para modificarla.
 - c. Haga clic en **Agregar** para crear una nueva condición.
Todas las condiciones deben ser validadas para que se ejecute la regla.
6. Haga clic en **Guardar**.

12. GENERAR UN FORMULARIO DE PAGO

Para generar una solicitud de pago, debe crear un formulario HTML de la siguiente forma:

```
<form method="POST" action="https://secure.lyra.com/vads-payment/">
  <input type="hidden" name="parametre1" value="valeur1" />
  <input type="hidden" name="parametre2" value="valeur2" />
  <input type="hidden" name="parametre3" value="valeur3" />
  <input type="hidden" name="signature" value="signature"/>
  <input type="submit" name="pagar" value="Pagar"/>
</form>
```

Este contiene:

- Los siguientes elementos técnicos:
 - Las etiquetas `<form>` y `</form>` que permiten crear un formulario HTML.
 - El atributo `method="POST"` que especifica el método utilizado para enviar los datos.
 - El atributo `action="https://secure.lyra.com/vads-payment/"` que especifica a dónde enviar los datos del formulario.
- Los datos del formulario:
 - El identificador de la tienda.
 - Las características del pago en función del caso de utilización.
 - Información adicional según sus necesidades.
 - La fecha que asegura la integridad del formulario.

Estos datos son agregados al formulario utilizando la etiqueta `<input>`:

```
<input type="hidden" name="parametre1" value="valeur1" />
```

Para asignar un valor a los atributos `name` y `value`, consulte el **Diccionario de datos** disponible también en el sitio de documentación.

Todos los datos del formulario deben estar codificados en **UTF-8**.

De esta forma, los caracteres especiales (acentos, puntuación, etc.) serán interpretados correctamente por la plataforma de pago. En el caso contrario, el cálculo de la firma será erróneo y el formulario será rechazado.

- El botón **Pagar** para enviar los datos:

```
<input type="submit" name="pagar" value="Pagar"/>
```

En los capítulos siguientes se presentan casos de utilización. Estos le permitirán construir su formulario de pago en función de sus necesidades.

La siguiente tabla proporciona indicaciones sobre los diferentes formatos que puede encontrar durante la construcción de su formulario.

Notación	Descripción
a	Caracteres alfabéticos (de 'A' a 'Z' y de 'a' a 'z')
n	Caracteres numéricos
s	Caracteres especiales
an	Caracteres alfanuméricos
ans	Caracteres alfanuméricos y especiales (excepto "<" y ">")
3	Longitud fija de 3 caracteres
..12	Longitud variable hasta 12 caracteres
json	<p>JavaScript Object Notation.</p> <p>Un objeto que contiene pares clave/valor separados por comas.</p> <p>Comienza con un refuerzo izquierdo " {" y termina con un refuerzo derecho " }".</p> <p>Cada par de clave/valor contiene el nombre de la clave entre comillas dobles seguidas de ":", seguido de un valor.</p> <p>El nombre de la clave debe ser alfanumérico.</p> <p>El valor puede ser:</p> <ul style="list-style-type: none"> • una cadena de caracteres (en este caso debe estar encuadrada entre comillas dobles) • un número • un objeto • un tablero • un booleano • vacío <p>Ejemplo: {"name1":45,"name2":"value2", "name3":false}</p>
bool	Booleano. Puede tomar el valor true o false .
enum	<p>Caracteriza un campo con un número finito de valores.</p> <p>La lista de valores posibles se da en la definición del campo.</p>
lista de enum	<p>Lista de valores separados por un ";".</p> <p>La lista de valores posibles se da en la definición del campo.</p> <p>Ejemplo: vads_available_languages=fr;en</p>
map	<p>Lista de pares clave/valores separados por un ";".</p> <p>Cada par de clave / valor contiene el nombre de la clave seguido de "=".</p> <p>El valor puede ser:</p> <ul style="list-style-type: none"> • una cadena de caracteres • un booleano • un objeto json • un objeto xml <p>La lista de valores posibles para cada par de clave / valor se proporciona en la definición del campo.</p> <p>Ejemplo: vads_theme_config=SIMPLIFIED_DISPLAY=true;RESPONSIVE_MODEL=Model_1</p>

12.1. Crear un formulario 'Creación del token sin pago'

Caso de uso: creación de un token para efectuar rápidamente pagos posteriores.



Dentro del marco de la aplicación de la DSP2, se requiere una autenticación fuerte al registrar una tarjeta. El campo `vads_threeds_mpi` es ignorado y el valor `CHALLENGE_MANDATE` se aplica automáticamente.

1. Utilice todos los campos que se encuentran en el cuadro a continuación para crear su formulario.

Nombre del campo	Descripción	Formato	Valor
<code>vads_page_action</code>	Acción a realizar	enum	REGISTER
<code>vads_action_mode</code>	Modo de adquisición de la información del medio de pago	enum	INTERACTIVE
<code>vads_currency</code>	Código numérico de la moneda que se utilizará para el pago, según la norma ISO 4217 (código numérico)	n3	Ejemplo: 978 para el euro (EUR)
<code>vads_ctx_mode</code>	Adquisición de los datos en la plataforma de pago	enum	TEST o PRODUCTION
<code>vads_cust_email</code>	Dirección de correo electrónico del comprador	ans..150	Ej.: abc@example.com
<code>vads_site_id</code>	Identificador de la tienda	n8	Ejemplo: 12345678
<code>vads_trans_date</code>	Fecha y hora del formulario de pago en el huso horario UTC	n14	Respete el formato AAAAMMDDHHMMSS Ejemplo: 20200101130025
<code>vads_version</code>	Versión del protocolo de intercambio con la plataforma de pago	enum	V2
<code>signature</code>	Firma que garantiza la integridad de las solicitudes intercambiadas entre el sitio web vendedor y la plataforma de pago.	ans..44	Calcule el valor del campo signature utilizando todos los campos de su formulario, cuyo nombre comienza con <code>vads_</code> (véase capítulo Calcular la firma).

2. Utilice el campo `vads_identifier` si desea generar el identificador del token asociado al medio de pago.

El formato del token no debe ser `ans..32`. Este formato está reservado para los tokens generados por la plataforma de pago.

Si ha activado la detección de la unidad de los tokens, el valor del campo `vads_identifier` transmitido en el formulario puede ser diferente al presente en la notificación si el medio de pago ya está asociado a otro token.

3. Agregue los campos opcionales en función de sus necesidades (véase capítulo [Utilizar funciones complementarias](#)).

La lista de los campos devueltos en la notificación se describen en el capítulo [Creación de un token sin pago](#) en la página 80.

12.2. Crear un formulario 'Cambio de información asociada al token'

Caso de uso: actualización de los datos bancarios asociados a un token.



Dentro del marco de la aplicación de la DSP2, se requiere una autenticación fuerte al registrar una tarjeta. El campo `vads_threeds_mpi` es ignorado y el valor `CHALLENGE_MANDATE` se aplica automáticamente.

1. Utilice todos los campos que se encuentran en el cuadro a continuación para crear su formulario.

Nombre del campo	Descripción	Formato	Valor
<code>vads_page_action</code>	Acción a realizar.	enum	REGISTER_UPDATE
<code>vads_ctx_mode</code>	Adquisición de los datos en la plataforma de pago	enum	TEST o PRODUCTION
<code>vads_cust_email</code>	Dirección de correo electrónico del comprador	ans..150	Ej.: abc@example.com
<code>vads_action_mode</code>	Modo de adquisición de la información del medio de pago	enum	INTERACTIVE
<code>vads_identifier</code>	Token (único) asociado a un medio de pago.	ans..50	Ejemplo: MiToken Nota: dos formatos posibles: <ul style="list-style-type: none">• an32: cuando el identificador es generado por la plataforma• ans..50: cuando el identificador es generado por el vendedor
<code>vads_site_id</code>	Identificador de la tienda	n8	Ejemplo: 12345678
<code>vads_trans_date</code>	Fecha y hora del formulario de pago en el huso horario UTC	n14	Respete el formato AAAAMMDDHHMMSS Ejemplo: 20200101130025
<code>vads_version</code>	Versión del protocolo de intercambio con la plataforma de pago	enum	V2
<code>signature</code>	Firma que garantiza la integridad de las solicitudes intercambiadas entre el sitio web vendedor y la plataforma de pago.	ans..44	Calcule el valor del campo signature utilizando todos los campos de su formulario, cuyo nombre comienza con vads_ (véase capítulo Calcular la firma).

2. Agregue los campos opcionales en función de sus necesidades (véase capítulo [Utilizar funciones complementarias](#)).

La lista de los campos devueltos en la notificación se describen en el capítulo [Cambio de información asociada al token](#) en la página 84.

12.3. Crear un formulario 'Creación del token durante un pago'

Caso de uso: pago con creación de un token.



Dentro del marco de la aplicación de la DSP2, se requiere una autenticación fuerte al registrar una tarjeta. El campo `vads_threeds_mpi` es ignorado y el valor `CHALLENGE_MANDATE` se aplica automáticamente.

1. Utilice todos los campos que se encuentran en el cuadro a continuación para crear su formulario.

Nombre del campo	Descripción	Formato	Valor
<code>vads_page_action</code>	Acción a realizar	enum	REGISTER_PAY
<code>vads_amount</code>	Monto del pago en su unidad monetaria más pequeña (el centavo para el euro)	n..12	Ejemplo: 4525 para 45,25 EUR
<code>vads_ctx_mode</code>	Adquisición de los datos en la plataforma de pago	enum	TEST o PRODUCTION
<code>vads_currency</code>	Código numérico de la moneda que se utilizará para el pago, según la norma ISO 4217 (código numérico)	n3	Ejemplo: 978 para el euro (EUR)
<code>vads_cust_email</code>	Dirección de correo electrónico del comprador	ans..150	Ej.: abc@example.com
<code>vads_action_mode</code>	Modo de adquisición de la información del medio de pago	enum	INTERACTIVE
<code>vads_payment_config</code>	Tipo de pago	enum	SINGLE
<code>vads_site_id</code>	Identificador de la tienda	n8	Ejemplo: 12345678
<code>vads_trans_date</code>	Fecha y hora del formulario de pago en el huso horario UTC	n14	Respete el formato AAAAMMDDHHMMSS Ejemplo: 20200101130025
<code>vads_trans_id</code>	Número de la transacción. Debe ser único en un mismo día (de 00:00:00 a 23:59:59 UTC). Atención: Este campo no distingue entre mayúsculas y minúsculas.	an6	Ejemplo: xrT15p
<code>vads_version</code>	Versión del protocolo de intercambio con la plataforma de pago	enum	V2
<code>signature</code>	Firma que garantiza la integridad de las solicitudes intercambiadas entre el sitio web vendedor y la plataforma de pago.	ans..44	Calcule el valor del campo signature utilizando todos los campos de su formulario, cuyo nombre comienza con <code>vads_</code> (véase capítulo Calcular la firma).

2. Utilice el campo `vads_identifier` si desea generar el identificador del token asociado al medio de pago.

El formato del token no debe ser `an..32`. Este formato está reservado para los tokens generados por la plataforma de pago.

Si ha activado la detección de la unidad de los tokens, el valor del campo `vads_identifier` transmitido en el formulario puede ser diferente al presente en la notificación si el medio de pago ya está asociado a otro token.

3. Agregue los campos opcionales en función de sus necesidades (véase capítulo [Utilizar funciones complementarias](#)).

La lista de los campos devueltos en la notificación se describen en el capítulo [Creación del token durante un pago](#) en la página 87.

12.4. Crear un formulario 'Creación del token al suscribirse a una recurrencia'

Caso de uso: recurrencia de una recurrencia con creación de un token.



Dentro del marco de la aplicación de la DSP2, se requiere una autenticación fuerte al registrar una tarjeta. El campo `vads_threeds_mpi` es ignorado y el valor `CHALLENGE_MANDATE` se aplica automáticamente.



No se realizará ningún pago al momento de la recurrencia. Solamente se realizará una solicitud de verificación para confirmar los datos del medio de pago.

El primer pago se realizará en la fecha efectiva, entre las 00:00 y las 05:00 h.

Si desea que el comprador pague el primer vencimiento al momento de la recurrencia, consulte el capítulo: ['Crear un formulario 'Creación del token al suscribir a una recurrencia acompañada de un pago'](#) en la página 58.

1. Utilice todos los campos que se encuentran en el cuadro a continuación para crear su formulario.

Nombre del campo	Descripción	Formato	Valor
<code>vads_page_action</code>	Acción a realizar	enum	REGISTER_SUBSCRIBE
<code>vads_ctx_mode</code>	Adquisición de los datos en la plataforma de pago	enum	TEST o PRODUCTION
<code>vads_cust_email</code>	Dirección de correo electrónico del comprador	ans..150	Ej.: abc@example.com
<code>vads_action_mode</code>	Modo de adquisición de la información del medio de pago	enum	INTERACTIVE
<code>vads_site_id</code>	Identificador de la tienda	n8	Ejemplo: 12345678
<code>vads_sub_amount</code>	Monto de los vencimientos de la recurrencia (en su unidad monetaria más pequeña). El monto de los vencimientos no se puede valorar en 0.	n..12	Ejemplo: 4525 para 45,25 EUR
<code>vads_sub_effect_date</code>	Fecha de inicio de la recurrencia (o fecha efectiva) el en huso UTC, en formato AAAAMMDD.	n8	Ejemplo: 20210601
<code>vads_sub_currency</code>	Código de la moneda utilizada para la recurrencia.	n3	Ejemplo: 978 para el euro (EUR)
<code>vads_sub_desc</code>	Regla de recurrencia para aplicar de acuerdo con la especificación iCalendar RFC5545. Si solicita la creación de una recurrencia para debitar el portador a diario (RRULE:FREQ=DAILY;INTERVAL y que la fecha de efecto solicitada (<code>vads_sub_effect_date</code>) corresponde a la fecha de creación de la recurrencia, entonces la plataforma de pago tratará esta recurrencia al día siguiente (entre medianoche y las 5:00), se crearán 2 pagos:	string	La frecuencia de la recurrencia puede ser diaria, semanal o mensual. Puede especificar el número del día o del mes (por ejemplo "el día 10 del mes" o "cada 3 meses"). <i>Nota: la cadena no debe tener espacios.</i> Ejemplos: <ul style="list-style-type: none"> Para definir una recurrencia semanal: <pre>RRULE:FREQ=WEEKLY</pre> Para definir una recurrencia cada dos semanas, hoy y cada 7 días. <pre>RRULE:FREQ=WEEKLY;INTERVAL=2</pre>

Nombre del campo	Descripción	Formato	Valor
	<ul style="list-style-type: none"> el de la víspera (que corresponde a la fecha de efecto), y el del día. <p>Para evitarlo, se aconseja transmitir una fecha de efecto al día siguiente del día en que se creó la recurrencia.</p>		<ul style="list-style-type: none"> Para definir los vencimientos de pago que tienen lugar el último día de cada mes, durante 12 meses: <pre>RRULE:FREQ=MONTHLY; BYMONTHDAY=28,29,30,31; BYSETPOS=-1;COUNT=12</pre> Para definir los vencimientos de pago que tienen lugar el día 10 de cada mes, durante 12 meses: <pre>RRULE:FREQ=MONTHLY; COUNT=12;BYMONTHDAY=10</pre>
vads_trans_date	Fecha y hora del formulario de pago en el huso horario UTC	n14	Respete el formato AAAAMMDDHHMMSS Ejemplo: 20200101130025
vads_version	Versión del protocolo de intercambio con la plataforma de pago	enum	V2
signature	Firma que garantiza la integridad de las solicitudes intercambiadas entre el sitio web vendedor y la plataforma de pago.	ans..44	Calcule el valor del campo signature utilizando todos los campos de su formulario, cuyo nombre comienza con vads_ (véase capítulo Calcular la firma).



El valor de **vads_sub_effect_date** no debe estar en el pasado.

- Utilice el campo **vads_identifier** si desea generar el identificador del token asociado al medio de pago.

El formato del token no debe ser an..32. Este formato está reservado para los tokens generados por la plataforma de pago.

Si ha activado la detección de la unidad de los tokens, el valor del campo **vads_identifier** transmitido en el formulario puede ser diferente al presente en la notificación si el medio de pago ya está asociado a otro token.

- Agregue los campos opcionales en función de sus necesidades (véase capítulo [Utilizar funciones complementarias](#)).

La lista de los campos devueltos en la notificación se describen en el capítulo [Creación del token al suscribirse a una recurrencia](#) en la página 91.

12.5. Crear un formulario 'Creación del token al suscribir a una recurrencia acompañada de un pago'

Caso de uso: pago y una recurrencia de una recurrencia con creación de un token.



Dentro del marco de la aplicación de la DSP2, se requiere una autenticación fuerte al registrar una tarjeta. El campo `vads_threeds_mpi` es ignorado y el valor `CHALLENGE_MANDATE` se aplica automáticamente.

1. Utilice todos los campos que se encuentran en el cuadro a continuación para crear su formulario.

Nombre del campo	Descripción	Formato	Valor
<code>vads_page_action</code>	Acción a realizar	enum	REGISTER_PAY_SUBSCRIBE
<code>vads_amount</code>	Monto del pago en su unidad monetaria más pequeña (el centavo para el euro)	n..12	Ejemplo: 4525 para 45,25 EUR
<code>vads_ctx_mode</code>	Adquisición de los datos en la plataforma de pago	enum	TEST o PRODUCTION
<code>vads_currency</code>	Código numérico de la moneda que se utilizará para el pago, según la norma ISO 4217 (código numérico)	n3	Ejemplo: 978 para el euro (EUR)
<code>vads_cust_email</code>	Dirección de correo electrónico del comprador	ans..150	Ej.: abc@example.com
<code>vads_action_mode</code>	Modo de adquisición de la información del medio de pago	enum	INTERACTIVE
<code>vads_payment_config</code>	Tipo de pago	enum	SINGLE
<code>vads_site_id</code>	Identificador de la tienda	n8	Ejemplo: 12345678
<code>vads_sub_amount</code>	Monto de los vencimientos de la recurrencia (en su unidad monetaria más pequeña). El monto de los vencimientos no se puede valorar en 0.	n..12	Ejemplo: 4525 para 45,25 EUR
<code>vads_sub_currency</code>	Código de la moneda utilizada para la recurrencia.	n3	Ejemplo: 978 para el euro (EUR)
<code>vads_sub_desc</code>	Regla de recurrencia para aplicar de acuerdo con la especificación iCalendar RFC5545. Si solicita la creación de una recurrencia para debitar el portador a diario (RRULE:FREQ=DAILY;INTERVAL y que la fecha de efecto solicitada (<code>vads_sub_effect_date</code>) corresponde a la fecha de creación de la recurrencia, entonces la plataforma de pago tratará esta recurrencia al día siguiente (entre medianoche y las 5:00), se crearán 2 pagos: <ul style="list-style-type: none"> el de la víspera (que corresponde a la fecha de efecto), 	string	La frecuencia de la recurrencia puede ser diaria, semanal o mensual. Puede especificar el número del día o del mes (por ejemplo "el día 10 del mes" o "cada 3 meses"). <i>Nota: la cadena no debe tener espacios.</i> Ejemplos: <ul style="list-style-type: none"> Para definir una recurrencia semanal: <pre>RRULE:FREQ=WEEKLY</pre> Para definir una recurrencia cada dos semanas, hoy y cada 7 días. <pre>RRULE:FREQ=WEEKLY;INTERVAL=2</pre> Para definir los vencimientos de pago que tienen lugar el último día de cada mes, durante 12 meses: <pre>RRULE:FREQ=MONTHLY;</pre>

Nombre del campo	Descripción	Formato	Valor
	<ul style="list-style-type: none"> y el del día. Para evitarlo, se aconseja transmitir una fecha de efecto al día siguiente del día en que se creó la recurrencia.		<pre>BYMONTHDAY=28, 29, 30, 31;</pre> <pre>BYSETPOS=-1;COUNT=12</pre> <ul style="list-style-type: none"> Para definir los vencimientos de pago que tienen lugar el día 10 de cada mes, durante 12 meses: <pre>RRULE:FREQ=MONTHLY;</pre> <pre>COUNT=12;BYMONTHDAY=10</pre>
vads_sub_effect_date	Fecha de inicio de la recurrencia (o fecha efectiva) en el huso UTC, en formato AAAAMMDD.	n8	Ejemplo: 20210601
vads_trans_date	Fecha y hora del formulario de pago en el huso horario UTC	n14	Respete el formato AAAAMMDDHHMMSS Ejemplo: 20200101130025
vads_trans_id	Número de la transacción. Debe ser único en un mismo día (de 00:00:00 a 23:59:59 UTC). Atención: Este campo no distingue entre mayúsculas y minúsculas.	an6	Ejemplo: xrT15p
vads_version	Versión del protocolo de intercambio con la plataforma de pago	enum	V2
signature	Firma que garantiza la integridad de las solicitudes intercambiadas entre el sitio web vendedor y la plataforma de pago.	ans..44	Calcule el valor del campo signature utilizando todos los campos de su formulario, cuyo nombre comienza con vads_ (véase capítulo Calcular la firma).



El valor de **vads_sub_effect_date** no debe estar en el pasado.

- Utilice el campo **vads_identifier** si desea generar el identificador del token asociado al medio de pago.

El formato del token no debe ser an..32. Este formato está reservado para los tokens generados por la plataforma de pago.

Si ha activado la detección de la unidad de los tokens, el valor del campo **vads_identifier** transmitido en el formulario puede ser diferente al presente en la notificación si el medio de pago ya está asociado a otro token.

- Agregue los campos opcionales en función de sus necesidades (véase capítulo [Utilizar funciones complementarias](#)).

La lista de los campos devueltos en la notificación se describen en el capítulo [Creación del token al suscribir a una recurrencia acompañada de un pago](#) en la página 95.

12.6. Crear un formulario 'Pago por token'

Caso de uso: pago con un clic (uso de un token existente y válido).



Dentro del marco de la aplicación de la DSP2, se requieren la entrada del CVV, así como una autenticación del portador al pagar por token a partir del momento en que el comprador está presente. El `vads_threads_mpi` se toma en cuenta para permitir una eventual autenticación sin interacción.

1. Utilice todos los campos que se encuentran en el cuadro a continuación para crear su formulario.

Nombre del campo	Descripción	Formato	Valor
<code>vads_page_action</code>	Acción a realizar	enum	PAYMENT
<code>vads_amount</code>	Monto del pago en su unidad monetaria más pequeña (el centavo para el euro)	n..12	Ejemplo: 4525 para 45,25 EUR
<code>vads_ctx_mode</code>	Adquisición de los datos en la plataforma de pago	enum	TEST o PRODUCTION
<code>vads_currency</code>	Código numérico de la moneda que se utilizará para el pago, según la norma ISO 4217 (código numérico)	n3	Ejemplo: 978 para el euro (EUR)
<code>vads_action_mode</code>	Modo de adquisición de la información del medio de pago	enum	INTERACTIVE
<code>vads_identifier</code>	Token (único) asociado a un medio de pago.	ans..50	Ejemplo: MiToken Nota: dos formatos posibles: <ul style="list-style-type: none">• an32: cuando el identificador es generado por la plataforma• ans..50: cuando el identificador es generado por el vendedor
<code>vads_payment_config</code>	Tipo de pago	enum	SINGLE
<code>vads_site_id</code>	Identificador de la tienda	n8	Ejemplo: 12345678
<code>vads_trans_date</code>	Fecha y hora del formulario de pago en el huso horario UTC	n14	Respete el formato AAAAMMDDHHMMSS Ejemplo: 20200101130025
<code>vads_trans_id</code>	Número de la transacción. Debe ser único en un mismo día (de 00:00:00 a 23:59:59 UTC). Atención: Este campo no distingue entre mayúsculas y minúsculas.	an6	Ejemplo: xrT15p
<code>vads_version</code>	Versión del protocolo de intercambio con la plataforma de pago	enum	V2
<code>signature</code>	Firma que garantiza la integridad de las solicitudes intercambiadas entre el sitio web vendedor y la plataforma de pago.	ans..44	Calcule el valor del campo signature utilizando todos los campos de su formulario, cuyo nombre comienza con vads_ (véase capítulo Calcular la firma).

2. Agregue los campos opcionales en función de sus necesidades (véase capítulo [Utilizar funciones complementarias](#)).

La lista de los campos devueltos en la notificación se describen en el capítulo [Pago por Token](#) en la página 99.

12.7. Crear un formulario 'Usar un token para suscribirse a una recurrencia'

Caso de uso: uso de un token existente y válido para suscribirse a una recurrencia.



No se realizará ningún pago al momento de la recurrencia.

El primer pago se realizará en la fecha efectiva, entre las 00:00 y las 05:00 h.

1. Utilice todos los campos que se encuentran en el cuadro a continuación para crear su formulario.

Nombre del campo	Descripción	Formato	Valor
vads_page_action	Acción a realizar.	enum	SUBSCRIBE
vads_ctx_mode	Adquisición de los datos en la plataforma de pago	enum	TEST o PRODUCTION
vads_action_mode	Modo de adquisición de la información del medio de pago	enum	INTERACTIVE
vads_identifier	Token (único) asociado a un medio de pago.	ans..50	Ejemplo: MiToken Nota: dos formatos posibles: <ul style="list-style-type: none">• an32: cuando el identificador es generado por la plataforma• ans..50: cuando el identificador es generado por el vendedor
vads_site_id	Identificador de la tienda	n8	Ejemplo: 12345678
vads_sub_amount	Monto de los vencimientos de la recurrencia (en su unidad monetaria más pequeña). El monto de los vencimientos no se puede valorar en 0.	n..12	Ejemplo: 4525 para 45,25 EUR
vads_sub_effect_date	Fecha de inicio de la recurrencia (o fecha efectiva) el en huso UTC, en formato AAAAMMDD.	n8	Ejemplo: 20210601
vads_sub_currency	Código de la moneda utilizada para la recurrencia.	n3	Ejemplo: 978 para el euro (EUR)
vads_sub_desc	Regla de recurrencia para aplicar de acuerdo con la especificación iCalendar RFC5545. Si solicita la creación de una recurrencia para debitar el portador a diario (RRULE:FREQ=DAILY;INTERVAL y que la fecha de efecto solicitada (vads_sub_effect_date) corresponde a la fecha de creación de la recurrencia, entonces la plataforma de pago tratará esta recurrencia al día siguiente (entre medianoche y las 5:00), se crearán 2 pagos: <ul style="list-style-type: none">• el de la víspera (que corresponde a la fecha de efecto),	string	La frecuencia de la recurrencia puede ser diaria, semanal o mensual. Puede especificar el número del día o del mes (por ejemplo "el día 10 del mes" o "cada 3 meses"). Nota: la cadena no debe tener espacios. Ejemplos: <ul style="list-style-type: none">• Para definir una recurrencia semanal: <code>RRULE:FREQ=WEEKLY</code>• Para definir una recurrencia cada dos semanas, hoy y cada 7 días. <code>RRULE:FREQ=WEEKLY;INTERVAL=2</code>• Para definir los vencimientos de pago que tienen lugar el último día de cada mes, durante 12 meses: <code>RRULE:FREQ=MONTHLY;</code>

Nombre del campo	Descripción	Formato	Valor
	<ul style="list-style-type: none"> y el día. <p>Para evitarlo, se aconseja transmitir una fecha de efecto al día siguiente del día en que se creó la recurrencia.</p>		<pre>BYMONTHDAY=28, 29, 30, 31;</pre> <pre>BYSETPOS=-1; COUNT=12</pre> <ul style="list-style-type: none"> Para definir los vencimientos de pago que tienen lugar el día 10 de cada mes, durante 12 meses: <pre>RRULE:FREQ=MONTHLY;</pre> <pre>COUNT=12; BYMONTHDAY=10</pre>
vads_trans_date	Fecha y hora del formulario de pago en el huso horario UTC	n14	Respete el formato AAAAMMDDHHMMSS Ejemplo: 20200101130025
vads_version	Versión del protocolo de intercambio con la plataforma de pago	enum	V2
signature	Firma que garantiza la integridad de las solicitudes intercambiadas entre el sitio web vendedor y la plataforma de pago.	ans..44	Calcule el valor del campo signature utilizando todos los campos de su formulario, cuyo nombre comienza con vads_ (véase capítulo Calcular la firma).



El valor de **vads_sub_effect_date** no debe estar en el pasado.

- Agregue los campos opcionales en función de sus necesidades (véase capítulo [Utilizar funciones complementarias](#)).

La lista de los campos devueltos en la notificación se describen en el capítulo [Suscripción a una recurrencia](#) en la página 102.

12.8. Crear un formulario 'Pago con propuesta al titular para crear un token'

Caso de uso: proponer la creación de un token durante un pago.



Dentro del marco de la aplicación de la DSP2, se requiere una autenticación fuerte al registrar una tarjeta. El campo `vads_threeds_mpi` es ignorado y el valor `CHALLENGE_MANDATE` se aplica automáticamente.

1. Utilice todos los campos que se encuentran en el cuadro a continuación para crear su formulario.

Nombre del campo	Descripción	Formato	Valor
<code>vads_page_action</code>	Acción a realizar	enum	ASK_REGISTER_PAY
<code>vads_amount</code>	Monto del pago en su unidad monetaria más pequeña (el centavo para el euro)	n..12	Ejemplo: 4525 para 45,25 EUR
<code>vads_ctx_mode</code>	Adquisición de los datos en la plataforma de pago	enum	TEST o PRODUCTION
<code>vads_currency</code>	Código numérico de la moneda que se utilizará para el pago, según la norma ISO 4217 (código numérico)	n3	Ejemplo: 978 para el euro (EUR)
<code>vads_cust_email</code>	Dirección de correo electrónico del comprador	ans..150	Ej.: abc@example.com
<code>vads_action_mode</code>	Modo de adquisición de la información del medio de pago	enum	INTERACTIVE
<code>vads_payment_config</code>	Tipo de pago	enum	SINGLE
<code>vads_site_id</code>	Identificador de la tienda	n8	Ejemplo: 12345678
<code>vads_trans_date</code>	Fecha y hora del formulario de pago en el huso horario UTC	n14	Respete el formato AAAAMMDHMMSS Ejemplo: 20200101130025
<code>vads_trans_id</code>	Número de la transacción. Debe ser único en un mismo día (de 00:00:00 a 23:59:59 UTC). Atención: Este campo no distingue entre mayúsculas y minúsculas.	an6	Ejemplo: xrT15p
<code>vads_version</code>	Versión del protocolo de intercambio con la plataforma de pago	enum	V2
<code>signature</code>	Firma que garantiza la integridad de las solicitudes intercambiadas entre el sitio web vendedor y la plataforma de pago.	ans..44	Calcule el valor del campo signature utilizando todos los campos de su formulario, cuyo nombre comienza con vads_ (véase capítulo Calcular la firma).

2. Utilice el campo `vads_identifier` si desea generar el identificador del token asociado al medio de pago.

El formato del token no debe ser an..32. Este formato está reservado para los tokens generados por la plataforma de pago.

Si ha activado la detección de la unidad de los tokens, el valor del campo `vads_identifier` transmitido en el formulario puede ser diferente al presente en la notificación si el medio de pago ya está asociado a otro token.

3. Agregue los campos opcionales en función de sus necesidades (véase capítulo [Utilizar funciones complementarias](#)).

La lista de los campos devueltos en la notificación se describen en el capítulo [Pago con propuesta al titular para crear un token](#) en la página 104.

13. USAR FUNCIONES ADICIONALES

13.1. Definir un monto diferente para las primeras n cuotas

Desea definir una recurrencia a cuyo/s primer/os vencimiento/s se le asigna/n un valor diferente al/a los asignado/s por el campo **vads_sub_amount**.

Ejemplo: definir una recurrencia cuyos 3 primeros vencimientos son a 45,25 EUR , y las demás a 75,90 EUR.

Para ello:

1. Utilice todos los campos necesarios para su caso de uso (recurrencia fija) para crear su formulario de pago.
2. Utilice los siguientes campos:

Nombre del campo	Descripción	Valor
vads_sub_init_amount_number	Número de vencimientos a los que aplicar el monto definido por vads_sub_init_amount	3
vads_sub_init_amount	Monto de los primeros vencimientos. El número de los primeros vencimientos lo define vads_sub_init_amount_number .	2500
vads_sub_amount	Monto de los vencimientos de la recurrencia, excepto las posiblemente definidas por vads_sub_init_amount_number .	3000
vads_sub_currency	Moneda utilizada en todos los vencimientos de la recurrencia	Ejemplo: 978 para el euro (EUR)



Los campos **vads_sub_init_amount** y **vads_sub_amount** no pueden tener asignado el valor 0.



Para definir una recurrencia cuyos 3 primeros meses son gratuitos, basta con escalonar la fecha efectiva (**vads_sub_effect_date**) hasta 3 meses.

Ejemplo de formulario :

```
<form method="POST" action="https://secure.lyra.com/vads-payment/">
<input type="hidden" name="vads_action_mode" value="INTERACTIVE" />
<input type="hidden" name="vads_capture_delay" value="0" />
<input type="hidden" name="vads_ctx_mode" value="TEST" />
<input type="hidden" name="vads_currency" value="978" />
<input type="hidden" name="vads_cust_country" value="FR" />
<input type="hidden" name="vads_cust_email" value="exemple@gmail.com" />
<input type="hidden" name="vads_cust_first_name" value="Paul" />
<input type="hidden" name="vads_cust_last_name" value="Juve" />
<input type="hidden" name="vads_cust_title" value="M." />
<input type="hidden" name="vads_page_action" value="REGISTER SUBSCRIBE" />
<input type="hidden" name="vads_payment_config" value="SINGLE" />
<input type="hidden" name="vads_site_id" value="91335531" />
<input type="hidden" name="vads_trans_date" value="20190716080441" />
<input type="hidden" name="vads_trans_id" value="362812" />
<input type="hidden" name="vads_validation_mode" value="0" />
<input type="hidden" name="vads_sub_currency" value="978" />
<input type="hidden" name="vads_sub_init_amount_number" value="3" />
<input type="hidden" name="vads_sub_init_amount" value="2500" />
<input type="hidden" name="vads_sub_amount" value="3000" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="G6oZchxNT+ySm7YQ/zvQvfgxmOmubvZ01PwFKKVUSyI=" />
<input type="submit" name="payer" value="Payer"/>
</form>
```

13.2. Definir la moneda para crear o actualizar un token

En caso de que:

- posea una afiliación que acepta varias monedas,
 - posea varias tiendas,
 - sus tiendas estén asociadas a la misma afiliación,
 - cada tienda genere pagos en una moneda diferente,
- (Ejemplo: US dólar para la primera tienda, Euro para la segunda tienda)

es posible que la moneda utilizada al crear o actualizar un token no sea compatible con la tienda.

Efectivamente, la plataforma de pago seleccionará por defecto la primera moneda que encuentre en orden alfabético para efectuar las verificaciones necesarias con el emisor del medio de pago.

Para evitar errores de procesamiento de IPN, tiene la posibilidad de enviar la moneda que utilizará en el formulario.



Para efectuar pagos con cualquier moneda aceptada por la afiliación, siempre podrá utilizar el token.

Nombre del campo	Descripción	Formato	Valor
vads_currency	Código numérico de la moneda que se utilizará para el pago, según la norma ISO 4217 (código numérico)	n3	Ejemplo: 978 para el euro (EUR)

14. CALCULAR LA FIRMA

Para poder calcular la firma debe disponer:

- de los campos cuyos nombres comienzan **convads_**
- del tipo de algoritmo elegido en la configuración de la tienda;
- de la **clave**.

El valor de la clave está disponible en el Back Office Expert en el menú **Configuración > Tienda > pestaña Claves**.

El tipo de algoritmo se define en su Back Office Expert en el menú **Configuración > Tienda > pestaña Configuración**.



Para máxima seguridad, se recomienda utilizar el algoritmo HMAC-SHA-256 además de una clave alfanumérica.

El algoritmo SHA-1 está en desuso, pero se mantiene por razones de compatibilidad.

Para calcular la firma:

1. Ordena los campos cuyos nombres comienzan **convads_** por orden alfabético.
2. Asegúrese de que todos los campos estén codificados en UTF-8.
3. Concatene los valores de estos campos separándolos con el carácter "+".
4. Concatene el resultado con la clave de prueba o de producción separándolos con el carácter "+".
5. De acuerdo con el algoritmo de firma definido en la configuración de su tienda:
 - a. si su tienda está configurada para usar "SHA-1", aplique la función de hash **SHA-1** en el string obtenido en el paso anterior. **Depreciado**.
 - b. si su tienda está configurada para usar "HMAC-SHA-256", calcule y codifique en formato Base64 la firma del mensaje usando el algoritmo **HMAC-SHA-256** con los siguientes parámetros:
 - la función hash SHA-256,
 - la clave de prueba o de producción (según el valor del campo **vads_ctx_mode**) como clave compartida,
 - el resultado del paso anterior como mensaje a autenticar.
6. Guarde el resultado del paso anterior en el campo **signature**.

Ejemplo de parámetros enviados a la plataforma de pago:

```
<form method="POST" action="https://secure.lyra.com/vads-payment/">
<input type="hidden" name="vads_action_mode" value="INTERACTIVE" />
<input type="hidden" name="vads_amount" value="5124" />
<input type="hidden" name="vads_ctx_mode" value="TEST" />
<input type="hidden" name="vads_currency" value="978" />
<input type="hidden" name="vads_page_action" value="PAYMENT" />
<input type="hidden" name="vads_payment_config" value="SINGLE" />
<input type="hidden" name="vads_site_id" value="12345678" />
<input type="hidden" name="vads_trans_date" value="20170129130025" />
<input type="hidden" name="vads_trans_id" value="123456" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="ycA5Do5tNvsnKdc/eP1bj2xa19z9q3iWPy9/rpesfS0=" />

<input type="submit" name="pagar" value="Pagar" />
</form>
```

Este ejemplo de formulario se desglosa de la siguiente manera:

1. Se organizan en orden **alfabética** los campos cuyo nombre comienzavads_ :

- vads_action_mode
- vads_amount
- vads_ctx_mode
- vads_currency
- vads_page_action
- vads_payment_config
- vads_site_id
- vads_trans_date
- vads_trans_id
- vads_version

2. Se concatena el valor de estos campos con el carácter "+" :

```
INTERACTIVE+5124+TEST+978+PAYMENT+SINGLE+12345678+20170129130025+123456+V2
```

3. Se agrega el valor de la clave de prueba al final del string, separado por el carácter "+". En este ejemplo, la clave de prueba es**1122334455667788**

```
INTERACTIVE+5124+TEST+978+PAYMENT+SINGLE+12345678+20170129130025+123456+V2+1122334455667788
```

4. Si usa el algoritmo SHA-1, aplíquelo al string resultante.

El resultado a transmitir en el campo firma es:**59c96b34c74b9375c332b0b6a32e6deec87de2b**

5. Si su tienda está configurada para usar "HMAC-SHA-256", calcule y codifique en formato Base64 la firma del mensaje usando el algoritmo **HMAC-SHA-256** con los siguientes parámetros:

- la función hash SHA-256,
- la clave de prueba o de producción (según el valor del campovads_ctx_mode) como clave compartida,
- el resultado del paso anterior como mensaje a autenticar.

El resultado a transmitir en el campo firma es:

ycA5Do5tNvsnKdc/eP1bj2xa19z9q3iWPy9/rpesfS0=

15. ENVÍO DE LA SOLICITUD DE PAGO

En cada transacción, se debe redirigir al comprador a la página de pago para finalizar su compra. Su navegador debe transmitir los datos del formulario de pago.

15.1. Redirección del comprador hacia la página de pago

La URL de la plataforma de pago es la siguiente:

<https://secure.lyra.com/vads-payment/>

Ejemplo de parámetros enviados a la plataforma de pago:

```
<form method="POST" action="https://secure.lyra.com/vads-payment/">
<input type="hidden" name="vads_action_mode" value="INTERACTIVE" />
<input type="hidden" name="vads_amount" value="2990" />
<input type="hidden" name="vads_ctx_mode" value="TEST" />
<input type="hidden" name="vads_currency" value="978" />
<input type="hidden" name="vads_cust_country" value="" />
<input type="hidden" name="vads_cust_email" value="me@example.com" />
<input type="hidden" name="vads_order_id" value="CMD012859" />
<input type="hidden" name="vads_page_action" value="REGISTER_PAY" />
<input type="hidden" name="vads_payment_config" value="SINGLE" />
<input type="hidden" name="vads_site_id" value="12345678" />
<input type="hidden" name="vads_trans_date" value="20200426101407" />
<input type="hidden" name="vads_trans_id" value="x6Z41p" />
<input type="hidden" name="vads_version" value="V2" />
<input type="hidden" name="signature" value="NM25DPLKEbtGEHCDHn8MBT4ki6aJI/ODaWhCzCnAfVY=" />
<input type="submit" name="payer" value="Payer"/>
</form>
```

15.2. Gestión de errores

Si la plataforma detecta una anomalía durante la recepción del formulario, se mostrará un mensaje de error y el comprador no podrá proceder con el pago.

En modo TEST

El mensaje indica el origen del error y muestra un vínculo hacia la descripción del código del error para ayudarle a identificar las posibles causas.

En modo PRODUCTION

El mensaje simplemente indica al comprador que ocurrió un problema técnico.

En los dos casos, el vendedor recibe un e-mail de advertencia.

Este contiene:

- el origen del error,
- un vínculo hacia las posibles causas para este código de error para facilitar el diagnóstico,
- todos los campos contenidos en el formulario.

El e-mail se envía al contacto administrador de la marca.

Si desea modificar esta dirección o añadir una dirección adicional, póngase en contacto con adv@lyra-collect.com.

También tiene la posibilidad de crear una regla de notificación personalizada para recibir ese e-mail en otra dirección.

Para esto:

1. Conéctese a su Back Office Expert.
<https://secure.lyra.com/portal/>
2. Abra el menú **Configuración > Reglas de notificaciones**.
3. Seleccione **Notificación avanzada**.
4. Seleccione el tipo de notificación **E-mail enviado al vendedor**.
5. Haga clic en **Siguiente**.
6. Seleccione el evento desencadenante **Formulario de pago inválido**.
7. En la sección **Configuración general**, ingrese los campos:
 - **Etiqueta de la regla**
 - **Dirección e-mail a notificar**
8. Haga clic en el botón **Crear**.

Una descripción de los códigos de error con sus posibles causas está disponible en nuestro sitio de Internet.

<https://docs.lyra.com/fr/collect/error-code/error-00.html>

Otros mensajes pueden surgir durante el pago.

A continuación hay una lista de los mensajes más comunes:

Mensaje	Descripción
Su solicitud de pago ha sido denegada por su banco.	<ul style="list-style-type: none">• El banco del comprador rechazó la solicitud de autorización o de información.• Las reglas de gestión de riesgos provocaron el rechazo de la transacción.
Su solicitud de inscripción fue rechazada por su establecimiento financiero.	<ul style="list-style-type: none">• El banco del comprador rechazó la solicitud de autorización o de información.• Las reglas de gestión de riesgos provocaron el rechazo de la transacción.
Esta solicitud de pago expiró. Establezca contacto con su tienda.	El comprador hizo clic en el enlace de pago después de la fecha final de validez de la solicitud.
Esta solicitud de pago ya ha sido pagada	El comprador hizo clic de nuevo en el enlace de pago después de haber realizado el pago previamente.
Ocurrió una fallo durante la solicitud de pago; el sitio del comerciante fue informado sobre la posibilidad de finalizar la transacción.	El formulario de pago fue rechazado. El responsable de la tienda recibió un e-mail que detalla el origen del error.
La transacción ya fue realizada.	El sitio web vendedor envía un identificador de transacción ya utilizado para otra transacción (aceptada o rechazada). El identificador de transacción debe ser único en un día (00:00:00 a 23:59:59 UTC).
Lo sentimos, se ha superado el tiempo máximo de inactividad, ha sido desconectado por motivos de seguridad.	<ul style="list-style-type: none">• El comprador trata de validar su número de tarjeta cuando su sesión de pago expiró. La duración de la sesión es de 10 minutos.• El sitio del comerciante envía un identificador de transacción ya utilizado pero que no dio lugar a una transacción (por ejemplo, pago abandonado). El

Mensaje	Descripción
	identificador de transacción debe ser único en un día (00:00:00 a 23:59:59 UTC).
Su navegador bloqueó las cookies. Autorícelas antes de reiniciar la operación.	El comprador desactivó el uso de cookies en su navegador. Las cookies son indispensables para el correcto desarrollo del pago.

15.3. Administrar tiempos de espera

Concepto de sesión de pago

Una "sesión de pago" es el tiempo que pasa un comprador en la página de pago.

La sesión de pago comienza al recibir el formulario por la plataforma de pago.

La duración de la sesión es de 10 minutos (a excepción de ciertos medios de pago).

Dicha duración es:

- **suficiente** para permitir a cada comprador hacer su pago
- **fijo**: no se restablece a todas las acciones del usuario.
- **no modificable**: es fijado por la plataforma de pago para cumplir con las limitaciones técnicas.

Después de este tiempo, la sesión se agota y los datos de la sesión se borran.

Caducidad de la sesión de pago.

Es posible que en algunos casos la sesión de pago caduque mientras el comprador no haya completado el pago.

Casos más frecuentes:

1. Una vez redirigido a la página de pago, el comprador se da cuenta de que es hora de ir a almorzar, por ejemplo.

Una hora más tarde, decide continuar con su pago y hace clic en el logotipo correspondiente a sus medios de pago.

Su sesión de pago ha caducado, la plataforma de pago muestra un mensaje de error que indica que se desconectó debido a una inactividad demasiado larga.

Luego, el comprador tiene la oportunidad de hacer clic en un botón para volver al sitio web vendedor.

El retorno a la tienda es a la URL especificada por el vendedor:

- en el campo `vads_url_return` enviado en el formulario de pago,
 - en el campo "URL de la tienda" Back Office Expert, si la URL no se especifica en el campo `vads_url_return` del formulario de pago.
2. Una vez redirigido a la página de pago, el comprador cierra su navegador (por error o porque ya no quiere hacer el pago).

Notificación en caso de expiración de la sesión

El sitio web vendedor tiene la posibilidad de ser notificado en caso de expiración de la sesión.

Para ello, el vendedor debe configurar y activar la regla **URL de notificación al abandonar (comprador)** (consultar capítulo [Configurar la notificación en caso de abandono/cancelación](#) en la página 44).

16. IMPLEMENTAR LA IPN

El script debe incluir al menos los siguientes pasos:

- Recuperar la lista de campos presentes en la respuesta enviada en POST
- Calcular la firma tomando en cuenta los datos recibidos
- Comparar la firma calculada con la recibida.
- Analizar la naturaleza de la notificación
- Recuperar el resultado del pago

El script puede, por ejemplo, probar el estado del pedido (o la información de su elección) para verificar que no se haya actualizado.

Una vez que se han completado estos pasos, el script puede actualizar la base de datos (nuevo estado del pedido, actualización del stock, registro de la información de pago, etc.).

A fin de facilitar el soporte y el diagnóstico por el vendedor en caso de error durante una notificación, se recomienda escribir mensajes que permitan conocer en qué etapa del procesamiento se produjo el error.

La plataforma lee y guarda los primeros 256 bytes del cuerpo de la respuesta HTTP.

Usted puede escribir mensajes durante todo el procesamiento. Aquí tiene un ejemplo de mensaje que puede utilizar:

Mensaje	Casos de uso
Data received	Mensaje que se mostrará durante la recuperación de los datos. Permite confirmar que el sitio del comerciante ha recibido correctamente la notificación.
POST is empty	Mensaje que se mostrará durante la recuperación de los datos. Permite indicar una eventual redirección que ha perdido los parámetros publicados por la plataforma de pago.
An error occurred while computing the signature.	Mensaje que se mostrará cuando haya fracasado la verificación de la firma.
Order successfully updated.	Mensaje que se mostrará al final del archivo una vez que sus procesamientos se hayan terminado con éxito.
An error occurred while updating the order.	Mensaje que se mostrará al final del archivo si se produjo un error durante sus procesamientos.

16.1. Preparar su entorno



Las notificaciones de tipo Llamada URL de notificación son las más importantes, pues representan el único medio confiable para que el sitio del comerciante pueda obtener el resultado de un pago.

Por lo tanto, es fundamental controlar que las notificaciones funcionen correctamente.

A continuación le presentamos algunas recomendaciones:

- Para que el diálogo entre la plataforma de pago y su sitio comerciante funcione, usted debe comprobar con sus equipos técnicos que el rango de la dirección IP **194.50.38.0/24** esté autorizada en los diferentes dispositivos de su arquitectura (firewalls, servidor apache, servidor proxy, etc.)

Las notificaciones se envían desde una dirección IP dentro del rango 194.50.38.0/24 **en modo TEST y en modo PRODUCTION.**

- Los redireccionamientos dan como resultado la pérdida de datos en POST.

Este caso se da si existe una configuración en sus dispositivos o en su proveedor que redirige las URL de tipo "http://www.example.com" vers "http://example.com" o "http://example.com" hacia "https://example.com".

- La página no debe tener una vista HTML. El acceso a recursos como imágenes o hojas de estilo ralentizan los intercambios entre la plataforma de pago y el sitio web vendedor.

- Evite las tareas que consumen tanto tiempo como generar facturas PDF o enviar e-mails en su script.

El tiempo de procesamiento tiene un efecto directo en el plazo de la visualización de la página de resumen de pago.

Cuanto mayor sea el procesamiento de la notificación, más se demora la visualización. Si el tiempo de procesamiento supera los 35 segundos, la plataforma considera que la llamada ha fallado (timeout).

- Si a su página solo se puede acceder por https, pruebe su URL en el sitio deQualys SSL Labs (<https://www.ssllabs.com/ssltest/>) y modifique su configuración, si fuera necesario, a fin de obtener un grado A. Su certificado SSL debe firmarlo una autoridad de certificación conocida y reconocida en el mercado.
- Asegúrese de utilizar las últimas versiones del protocolo TLS a fin de mantener un alto nivel de seguridad.

16.2. Recuperar los datos devueltos en la respuesta

Los datos devueltos en la respuesta dependen de los parámetros enviados en la solicitud de pago, el tipo de pago realizado y las opciones de su tienda y del formato de la notificación.

Los datos siempre son enviados en **POST** por la plataforma de pago.

Por lo tanto, el primer paso es recuperar el contenido recibido en el modo POST.

Ejemplos:

- En PHP, los datos se almacenarán en la variable superglobal **\$_POST**.
- En ASP.NET (C #), debe usar la propiedad **Form** de la clase **HttpRequest**.
- En java, debe usar el método **getParameter** de la clase **HttpServletRequest**.

La respuesta constituye una lista de campos. Cada campo contiene un valor de respuesta. La lista de campos puede cambiar.

El script tendrá que hacer un bucle para recuperar todos los campos transmitidos.

Se recomienda probar la presencia del campo **vads_hash**, presente solo durante una notificación.

```
if (empty ($_POST)){
    echo 'POST is empty';

}

}else{
    echo 'Data Received ';
    if (isset($_POST['vads_hash'])){

        echo 'Form API notification detected';
        //Signature computation
        //Signature verification
        //Order Update
    }
}
```

16.3. Calcular la firma de la IPN

La firma se calcula de acuerdo con la misma lógica utilizada al solicitar el pago.



Los datos transmitidos por la plataforma de pago están codificados en UTF-8. Cualquier alteración de los datos recibidos dará lugar a un cálculo de firma errónea.

Debe calcular la firma con los campos recibidos en la notificación y no con los que transmitió en la solicitud de pago.

1. Considere todos los campos cuyos nombres comienzan con **vads_**.
2. Ordene estos campos alfabéticamente.
3. Concatene los valores de estos campos separándolos con el carácter "+".
4. Concatene el resultado con la clave de prueba o de producción separándolos con el carácter "+".
5. De acuerdo con el algoritmo de firma definido en la configuración de su tienda:
 - a. si su tienda está configurada para usar "SHA-1", aplique la función de hash **SHA-1** en el string obtenido en el paso anterior. **Depreciado**.
 - b. si su tienda está configurada para usar "HMAC-SHA-256", calcule y codifique en formato Base64 la firma del mensaje usando el algoritmo **HMAC-SHA-256** con los siguientes parámetros:
 - la función hash SHA-256,
 - la clave de prueba o de producción (según el valor del campo **vads_ctx_mode**) como clave compartida,
 - el resultado del paso anterior como mensaje a autenticar.

Ejemplos en PHP:

```
función getSignature ($params,$key)
{
    /**
     * Función que calcula la firma.
     * $ params: matriz que contiene los campos que se enviarán en la IPN.
     * $key : clave de TEST o PRODUCTION
     */
    //Inicialización de la variable que contendrá el string a cifrar
    $contenu_signature = "";

    //Ordenar los campos alfabéticamente
    ksort($params);
    foreach($params as $nom=>$valeur){

        //Recuperación de los campos vads_
        if (substr($nom,0,5)=='vads_'){

            //Concatenación con el separador "+"
            $contenu_signature .= $valeur."+";

        }

    }
    //Añadir la clave al final del string
    $contenu_signature .= $key;

    //Codificación base64 del string cifrada con el algoritmo HMAC-SHA-256
    $sign = base64_encode(hash_hmac('sha256',$contenu_signature, $key, true));
    return $sign;
}
```

16.4. Comparar firmas

Para garantizar la integridad de la respuesta, debe comparar el valor de la firma contenida en la IPN con el valor calculado en el paso anterior.



No se debe comparar la firma de la IPN con la firma que transmitió en su solicitud de pago.

Si las firmas coinciden,

- luego puede considerar la respuesta como segura y proceder como resultado del análisis.
- de lo contrario, el script lanzará una excepción y advertirá al vendedor de la anomalía.

Ejemplo PHP:

```
if ($_POST['signature'] == $sign){
    //Processing data
}else{
    throw new Exception('An error occurred while computing the signature');
}
```

Las firmas no coinciden en el caso:

- error de implementación (error en su cálculo, problema de codificación UTF-8, etc.),
- un error en el valor de la clave utilizada o en el campo **vads_ctx_mode** (un problema frecuente al entrar en producción),
- intento de corromper los datos.

16.5. Analizar la naturaleza de la notificación

El campo **vads_url_check_src** permite diferenciar las notificaciones según su evento desencadenante:

- creación de un token (con o sin recurrencia a una recurrencia).
- pago de un vencimiento de una recurrencia.
- Referencia de la notificación en el Back Office Expert por el vendedor.

Especifica la regla de notificación aplicada:

Valor	Regla aplicada
PAY	El valor PAY se envía en los siguientes casos: <ul style="list-style-type: none">• solicitud de creación de una orden o de un token (REGISTER)• solicitud de creación de una orden o de un token al registrar una suscripción (REGISTER_SUBSCRIBE)• pago inmediato (pago al contado o primer vencimiento de un pago en vencimientos)• pago abandonado o cancelado por el comprador. solo si el vendedor ha configurado la regla URL de notificación al abandonar (comprador).
BO	Ejecución de la notificación desde el Back Office Expert (haga clic con el botón derecho en una transacción > Ejecutar la URL de notificación). Compruebe la presencia del campo vads_recurrence_number: <ul style="list-style-type: none">• si está presente, la notificación corresponde al resultado de un pago recurrente (repetición de una notificación de tipo REC),• si está ausente, la notificación corresponde a una notificación de fin de pago.
BATCH	El valor BATCH se envía al actualizar el estado de una transacción tras la sincronización con el adquirente. Este es el caso de los pagos redirigidos al adquirente. Solo si el vendedor ha configurado la regla URL de notificación al modificar por batch .
BATCH_AUTO	El valor BATCH_AUTO se envía en los siguientes casos: <ul style="list-style-type: none">• pago diferido a más de 7 días• vencimientos para un pago en vencimientos (excepto el primero). solo si el vendedor ha configurado la regla URL de notificación al autorizar por batch. La notificación se enviará cuando se solicite autorización para un pago con el estado "autorización pendiente".
REC	El valor REC solo se enviará para los pagos por suscripción si el vendedor ha establecido la regla URL de notificación para crear un pago recurrente . Consulte el capítulo Pago de un vencimiento de una recurrencia en la página 107 para el detalle de las informaciones enviadas.
MERCH_BO	El valor MERCH_BO se enviará: <ul style="list-style-type: none">• durante una operación realizada desde el Back Office Expert (cancelación, reembolso, modificación, validación, duplicación, creación o actualización de token), si el vendedor ha configurado la regla de notificación: URL de notificación al modificar una transacción en el Back Office (vendedor)
RETRY	Repetición automática de la URL de notificación. Compruebe la presencia del campo vads_recurrence_number: <ul style="list-style-type: none">• si está presente, la notificación corresponde al resultado de un pago recurrente (repetición de una notificación de tipo REC),• si está ausente, la notificación corresponde a una notificación de fin de pago.

Tabla 1: Valores asociados al campo vads_url_check_src

Al probar su valor, el script puede realizar un procesamiento diferente según la naturaleza de la notificación.

Por ejemplo:

Si **vads_url_check_src** tiene asignado el valor **PAY** o **BATCH_AUTO** entonces el script actualizará el estado del pedido, ...

Si **vads_url_check_src** tiene asignado el valor **REC** entonces el script recuperará la referencia de recurrencia e incrementará el número de vencimientos vencidas en caso de pago aceptado...

En el marco de un débito recurrente (procedente de un REGISTER_SUBSCRIBE), la plataforma de pago notifica al acreedor (vendedor) cada vez que se crea una transacción.


16.6. Tratamiento de los datos de la respuesta

- [Creación de un token sin pago](#) en la página 80
- [Cambio de información asociada al token](#) en la página 84
- [Creación del token durante un pago](#) en la página 87
- [Creación del token al suscribirse a una recurrencia](#) en la página 91
- [Creación del token al suscribir a una recurrencia acompañada de un pago](#) en la página 95
- [Pago por Token](#) en la página 99
- [Suscripción a una recurrencia](#) en la página 102
- [Pago con propuesta al titular para crear un token](#) en la página 104
- [Pago de un vencimiento de una recurrencia](#) en la página 107

16.6.1. Creación de un token sin pago

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es REGISTER .
vads_identifier_status	Estado de la creación de token. Los valores posibles son: <ul style="list-style-type: none">• CREATED: la solicitud de autorización o de información si el adquirente lo soporta es aceptada. El token se crea correctamente y se ve en el Back Office Expert.• NOT_CREATED: la solicitud de autorización o de información es rechazada. El token no se crea.• ABANDONED: acción abandonada por el comprador. El token no se crea.
vads_identifier	Identificador del token. El valor devuelto es: <ul style="list-style-type: none">• igual al valor enviado en la solicitud, cualquiera sea el resultado de la creación del token, incluso en caso de abandono,• o el valor generado por la plataforma, si el campo no es enviado en la solicitud y si el token se crea correctamente (vads_identifier_status=CREATED). <p>Nota</p> <p>Si ha activado la verificación de la unicidad de los token y que el medio de pago ya está registrado con otro token, entonces es otro token el que se devolverá.</p> <p>El campo vads_identifier no se devolverá:</p> <ul style="list-style-type: none">• si no es enviado en la solicitud y si el comprador abandona (vads_identifier_status=ABANDONED),

Nombre del campo	Descripción
	<ul style="list-style-type: none"> si no es enviado en la solicitud y si el token no se crea (vads_identifier_status=NOT_CREATED).
vads_identifier_previously_registered	<p>únicamente presente si las dos condiciones son verdaderas:</p> <ul style="list-style-type: none"> usted ha activado la verificación de la unidad de los token, el medio de pago utilizado ya está registrado con otro token.
vads_initial_issuer_transaction_identifier	<p>Identificador de transacción único generado por el emisor.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> La plataforma de pago registra el identificador de transacción emisor a nivel del token. En función del uso que se hará del token (pago en 1 clic, pago sin clics, suscripción, etc.), se utilizará el identificador de transacción emisor como referencia de encadenamiento si fuera necesario.</p> </div>
vads_cust_email	Dirección de correo electrónico del comprador enviada en la solicitud.
vads_site_id	<p>Identificación de la tienda.</p> <p>El valor devuelto es igual al enviado en la solicitud.</p>
vads_ctx_mode	<p>Modo de funcionamiento.</p> <p>El valor devuelto (TEST o PRODUCTION) es igual al enviado en la solicitud.</p>

Una solicitud de “creación de token sin pago” permite crear una transacción de tipo VERIFICATION, que se ve en el Back Office Expert.



La función de esta transacción es ayudar al vendedor a entender, desde su Back-Office, las razones de rechazo de la creación del token.

A continuación, encontrará sus características:

Nombre del campo	Descripción
vads_operation_type	Tipo de transacción. Su valor es VERIFICATION .
vads_trans_status	<p>Estado de la transacción.</p> <p>Los valores posibles son:</p> <ul style="list-style-type: none"> ACCEPTED La solicitud de autorización o de información ha sido aceptada. El token se crea y aparece en el Back Office Expert. REFUSED La solicitud de autorización o de información ha sido denegada. El token no se crea.
vads_occurrence_type	Tipo de ocurrencia de la transacción. Su valor es UNITAIRE .
vads_amount	
vads_trans_id	Identificador de la transacción. La plataforma de pago genera el valor.
vads_trans_uuid	Identificador único de la transacción. La plataforma de pago genera el valor.
vads_auth_mode	Tipo de solicitud realizada en los servidores de autorización. Su valor es MARK .
vads_auth_number	Número de autorización devuelto por el servidor bancario. Vacío si la autorización falló.
vads_auth_result	Código de retorno de la solicitud de autorización devuelta por el banco emisor. Ver capítulo Gestionar los códigos de retorno de la solicitud de autorización . Vacío si aparece un error antes de la autorización.
vads_risk_assessment_result	Lista de acciones efectuadas sobre la transacción, tras el desencadenamiento de las reglas de gestión de riesgo avanzada.

Nombre del campo	Descripción
	<p>Las reglas relativas al monto o cuya acción es “Validar manualmente” no se aplican en el caso de una transacción de tipo VERIFICATION.</p> <p>Los valores posibles son:</p> <ul style="list-style-type: none"> • ENABLE_3DS: 3D Secure activado. • DISABLE_3DS: 3D Secure desactivado. • CHALLENGE_REQUESTED: <ul style="list-style-type: none"> • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge). • CHALLENGE_MANDATE: <ul style="list-style-type: none"> • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge por razones reglamentarias) por motivos normativos. • REFUSE: El token es rechazado. • RUN_RISK_ANALYSIS: Resultado del analizador de riesgos externo. Consulte la descripción del campo vads_risk_analysis_result para más detalles. • INFORM: Se levanta una alerta. El vendedor recibe una alerta porque se ha identificado un riesgo a través de una o varias reglas del centro de notificación.

Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo Medios de pago compatibles para obtener la lista de valores posibles.
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto. o IBAN y BIC (si están completos) utilizados para el pago, separados por una '_' en el caso de un débito puntual. Como el BIC es opcional, puede que no aparezca .
vads_expiry_month	Mes de caducidad de la tarjeta utilizada.  Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.
vads_expiry_year	Año de caducidad de la tarjeta utilizada.  Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.


Detalles de la autenticación del portador:

Nombre del campo	Nota
vads_threeds_auth_type	Tipo de autenticación del titular. Es obligatoria una autenticación fuerte del portador al registrar una tarjeta. Por lo tanto, el campo siempre se valorizará en CHALLENGE .
vads_threeds_enrolled	Estado de la inscripción del titular al programa 3D Secure. Los valores posibles son: <ul style="list-style-type: none"> • Y: Autenticación disponible. • N: Autenticación no disponible • U: Estado de la inscripción al programa 3DS desconocido • vacío: Proceso 3DS no realizado (3DS desactivado en la solicitud, vendedor no afiliado al medio de pago no elegible para 3DS).
vads_threeds_status	Resultado de la autenticación 3D Secure. Los valores posibles son: <ul style="list-style-type: none"> • Y: Portador autenticado correctamente. • N: Error de autenticación del portador. • U: Autenticación imposible • A: Tentativa de autenticación, pero no se realizó la autenticación. • vacío: Autenticación 3DS no realizada (3DS desactivado en la solicitud, titular no afiliado al medio de pago no elegible para 3DS).

Los campos opcionales enviados en la solicitud son devueltos en la respuesta sin cambios en sus valores.

16.6.2. Cambio de información asociada al token

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es REGISTER_UPDATE .
vads_identifier_status	Estado de la actualización del token. Los valores posibles son: <ul style="list-style-type: none"> • UPDATED: el token se actualizó correctamente. • NOT_UPDATED: el token no se ha actualizado. • ABANDONED: acción abandonada por el comprador. El token no se crea, por lo tanto, no se ve en el Back Office Expert.
vads_identifier	Identificador del token para actualizar. El valor devuelto es igual al enviado en la solicitud.
vads_initial_issuer_transaction_identifier	Identificador de transacción único generado por el emisor. <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;">  La plataforma de pago registra el identificador de transacción emisor a nivel del token. En función del uso que se hará del token (pago en 1 clic, pago sin clics, suscripción, etc.), se utilizará el identificador de transacción emisor como referencia de encadenamiento si fuera necesario. </div>
vads_cust_email	Dirección de correo electrónico del comprador enviada en la solicitud.
vads_site_id	Identificación de la tienda. El valor devuelto es igual al enviado en la solicitud.
vads_ctx_mode	Modo de funcionamiento. El valor devuelto (TEST o PRODUCTION) es igual al enviado en la solicitud.

Una solicitud de “actualización de token” permite crear una transacción de tipo **VERIFICATION**, que se ve en el Back Office Expert.


La función de esta transacción es ayudar al vendedor a entender, desde su Back-Office, las razones de rechazo de la creación del token.


A continuación, encontrará sus características:

Nombre del campo	Descripción
vads_operation_type	Tipo de transacción. Su valor es VERIFICATION .
vads_trans_status	Estado de la transacción. Los valores posibles son: <ul style="list-style-type: none"> • ACCEPTED La solicitud de autorización o de información ha sido aceptada. El token se crea y aparece en el Back Office Expert. • REFUSED La solicitud de autorización o de información ha sido denegada. El token no se crea.
vads_occurrence_type	Tipo de ocurrencia de la transacción. Su valor es UNITAIRE .
vads_amount	
vads_trans_id	Identificador de la transacción. La plataforma de pago genera el valor.
vads_trans_uuid	Identificador único de la transacción. La plataforma de pago genera el valor.
vads_auth_mode	Tipo de solicitud realizada en los servidores de autorización. Su valor es MARK .

Nombre del campo	Descripción
vads_auth_number	Número de autorización devuelto por el servidor bancario. Vacío si la autorización falló.
vads_auth_result	Código de retorno de la solicitud de autorización devuelta por el banco emisor. Ver capítulo Gestionar los códigos de retorno de la solicitud de autorización . Vacío si aparece un error antes de la autorización.
vads_risk_assessment_result	Lista de acciones efectuadas sobre la transacción, tras el desencadenamiento de las reglas de gestión de riesgo avanzada. Las reglas relativas al monto o cuya acción es “Validar manualmente” no se aplican en el caso de una transacción de tipo VERIFICATION. Los valores posibles son: <ul style="list-style-type: none"> • ENABLE_3DS: 3D Secure activado. • DISABLE_3DS: 3D Secure desactivado. • CHALLENGE_REQUESTED: <ul style="list-style-type: none"> • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge). • CHALLENGE_MANDATE: <ul style="list-style-type: none"> • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge por razones reglamentarias) por motivos normativos. • REFUSE: El token es rechazado. • RUN_RISK_ANALYSIS: Resultado del analizador de riesgos externo. Consulte la descripción del campo vads_risk_analysis_result para más detalles. • INFORM: Se levanta una alerta. El vendedor recibe una alerta porque se ha identificado un riesgo a través de una o varias reglas del centro de notificación.

Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo Medios de pago compatibles para obtener la lista de valores posibles.
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto. o IBAN y BIC (si están completos) utilizados para el pago, separados por una '_' en el caso de un débito puntual. Como el BIC es opcional, puede que no aparezca .
vads_expiry_month	Mes de caducidad de la tarjeta utilizada.  Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.
vads_expiry_year	Año de caducidad de la tarjeta utilizada.

Nombre del campo	Nota
	 Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.

Detalles de la autenticación del portador:

Nombre del campo	Nota
vads_threeds_auth_type	Tipo de autenticación del titular. Es obligatoria una autenticación fuerte del portador al registrar una tarjeta. Por lo tanto, el campo siempre se valorizará en CHALLENGE .
vads_threeds_enrolled	Estado de la inscripción del titular al programa 3D Secure. Los valores posibles son: <ul style="list-style-type: none"> • Y: Autenticación disponible. • N: Autenticación no disponible • U: Estado de la inscripción al programa 3DS desconocido • vacío: Proceso 3DS no realizado (3DS desactivado en la solicitud, vendedor no afiliado al medio de pago no elegible para 3DS).
vads_threeds_status	Resultado de la autenticación 3D Secure. Los valores posibles son: <ul style="list-style-type: none"> • Y: Portador autenticado correctamente. • N: Error de autenticación del portador. • U: Autenticación imposible • A: Tentativa de autenticación, pero no se realizó la autenticación. • vacío: Autenticación 3DS no realizada (3DS desactivado en la solicitud, titular no afiliado al medio de pago no elegible para 3DS).

Los campos opcionales enviados en la solicitud son devueltos en la respuesta sin cambios en sus valores.

16.6.3. Creación del token durante un pago

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es REGISTER_PAY .
vads_identifier_status	Estado de la creación de token. Los valores posibles son: <ul style="list-style-type: none"> • CREATED: la solicitud de autorización o de información si el adquirente lo soporta es aceptada. El token se crea con éxito. • NOT_CREATED: la solicitud de autorización o de información es rechazada. El token no se crea, por lo tanto, no se ve en el Back Office Expert. • ABANDONED: acción abandonada por el comprador. El token no se crea, por lo tanto, no se ve en el Back Office Expert.
vads_trans_status	Estado de la transacción. Los valores posibles son: <ul style="list-style-type: none"> • AUTHORISED La solicitud de autorización o de información ha sido aceptada. El token se crea y aparece en el Back Office Expert. • AUTHORISED_TO_VALIDATE La solicitud de autorización o de información ha sido aceptada. El vendedor debe validar la transacción de forma manual. El token se crea y aparece en el Back Office Expert. • CAPTURED La solicitud de autorización o de información ha sido aceptada. El pago aparece en la pestaña "Transacciones capturadas" del Back-Office. El token se crea y aparece en el Back Office Expert. • WAITING_AUTHORISATION El plazo de captura al banco es superior a la duración de validez de la autorización. La solicitud de autorización por el monto total aún no se ha creado. El token se crea y aparece en el Back Office Expert. • WAITING_AUTHORISATION_TO_VALIDATE Para validar y autorizar El plazo de captura al banco es superior a la duración de validez de la autorización. Se aceptó una autorización 1 EUR (o solicitud de información en la red de CB si el adquirente lo admite). El vendedor debe validar manualmente la transacción para que se realice la solicitud de autorización y la captura. • REFUSED La solicitud de autorización o de información ha sido denegada. El token no se crea. • ABANDONED Operación abandonada por el comprador. La transacción no aparece en el Back Office Expert. El token no se crea.
vads_identifier	Identificador del token. El valor devuelto es: <ul style="list-style-type: none"> • igual al valor enviado en la solicitud, cualquiera sea el resultado de la creación del token, incluso en caso de abandono, • o el valor generado por la plataforma, si el campo no es enviado en la solicitud y si el token se crea correctamente (vads_identifier_status=CREATED). Nota

Nombre del campo	Descripción
	Si ha activado la verificación de la unicidad de los token y que el medio de pago ya está registrado con otro token, entonces es otro token el que se devolverá. El campo vads_identifier no se devolverá: <ul style="list-style-type: none"> si no es enviado en la solicitud y si el comprador abandona (vads_identifier_status=ABANDONED), si no es enviado en la solicitud y si el token no se crea (vads_identifier_status=NOT_CREATED).
vads_identifier_previously_registered	únicamente presente si las dos condiciones son verdaderas: <ul style="list-style-type: none"> usted ha activado la verificación de la unidad de los token, el medio de pago utilizado ya está registrado con otro token.
vads_initial_issuer_transaction_identifier	Identificador de transacción único generado por el emisor. <div style="border: 1px solid #add8e6; padding: 10px; margin-top: 10px;"> <ul style="list-style-type: none"> La plataforma de pago registra el identificador de transacción emisor a nivel del token y de la transacción. En función del uso que se hará del token (pago en 1 clic, pago sin clics, suscripción, etc.), se utilizará el identificador de transacción emisor como referencia de encadenamiento si fuera necesario. En caso de que el vendedor duplique (MIT) la transacción, la plataforma utilizará automáticamente este identificador como referencia de encadenamiento. </div>
vads_cust_email	Dirección de correo electrónico del comprador enviada en la solicitud.
vads_site_id	Identificación de la tienda. El valor devuelto es igual al enviado en la solicitud.
vads_ctx_mode	Modo de funcionamiento. El valor devuelto (TEST o PRODUCTION) es igual al enviado en la solicitud.


Para conocer el detalle del pago, consulte los siguientes parámetros:


Información sobre la transacción:

Nombre del campo	Descripción
vads_operation_type	Tipo de transacción. Su valor es DEBIT .
vads_occurrence_type	Tipo de ocurrencia de la transacción. Su valor es UNITAIRE .
vads_amount	Monto de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_currency	Código de la moneda utilizada para el pago.
vads_trans_id	Identificador de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_trans_uuid	Identificador único de la transacción. La plataforma de pago genera el valor.
vads_contract_used	Número de la afiliación asociada a la transacción.
vads_auth_mode	Tipo de solicitud realizada en los servidores de autorización: <ul style="list-style-type: none"> MARK: corresponde a una autorización de 1 EUR (o solicitud de información en la red de CB si el adquirente lo admite). Valor utilizado también si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente posterior al período de validez de la autorización. FULL: corresponde a una autorización del monto total de la transacción. Valor utilizado si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente anterior al período de validez de la autorización.
vads_auth_number	Número de autorización devuelto por el servidor bancario. Vacío si la autorización falló.
vads_auth_result	Código de retorno de la solicitud de autorización devuelta por el banco emisor.

Nombre del campo	Descripción
	Ver capítulo Gestionar los códigos de retorno de la solicitud de autorización . Vacío si aparece un error antes de la autorización.
vads_risk_control	Resultado de los controles de riesgo. Cuando, al menos, un control devuelve el valor ERROR , la transacción es rechazada. Consulte la descripción del campo vads_risk_analysis_result para más detalles.
vads_risk_assessment_result	Lista de acciones efectuadas sobre la transacción, tras el desencadenamiento de las reglas de gestión de riesgo avanzada. Los valores posibles son: <ul style="list-style-type: none"> • ENABLE_3DS: 3D Secure activado. • DISABLE_3DS: 3D Secure desactivado. • CHALLENGE_REQUESTED: <ul style="list-style-type: none"> • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge). • CHALLENGE_MANDATE: <ul style="list-style-type: none"> • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge por razones reglamentarias) por motivos normativos. • MANUAL_VALIDATION: La transacción se crea con validación manual. La remesa del pago se bloquea temporalmente para permitir que el vendedor realice todas las verificaciones deseadas. • REFUSE: La transacción se ha rechazado. • RUN_RISK_ANALYSIS: Resultado del analizador de riesgos externo. Consulte la descripción del campo vads_risk_analysis_result para más detalles. • INFORM: Se levanta una alerta. El vendedor recibe una alerta porque se ha identificado un riesgo a través de una o varias reglas del centro de notificación.

Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo Medios de pago compatibles para obtener la lista de valores posibles.
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto. o IBAN y BIC (si están completos) utilizados para el pago, separados por una '_' en el caso de un débito puntual. Como el BIC es opcional, puede que no aparezca .
vads_expiry_month	Mes de caducidad de la tarjeta utilizada. <div style="border: 1px solid #add8e6; padding: 5px; display: inline-block;">  Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token. </div>
vads_expiry_year	Año de caducidad de la tarjeta utilizada.

Nombre del campo	Nota
	 Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.


Detalles de la autenticación del portador:

Nombre del campo	Nota
vads_threeds_auth_type	Tipo de autenticación del titular. Es obligatoria una autenticación fuerte del portador al registrar una tarjeta. Por lo tanto, el campo siempre se valorizará en CHALLENGE .
vads_threeds_enrolled	Estado de la inscripción del titular al programa 3D Secure. Los valores posibles son: <ul style="list-style-type: none"> • Y: Autenticación disponible. • N: Autenticación no disponible • U: Estado de la inscripción al programa 3DS desconocido • vacío: Proceso 3DS no realizado (3DS desactivado en la solicitud, vendedor no afiliado al medio de pago no elegible para 3DS).
vads_threeds_status	Resultado de la autenticación 3D Secure. Los valores posibles son: <ul style="list-style-type: none"> • Y: Portador autenticado correctamente. • N: Error de autenticación del portador. • U: Autenticación imposible • A: Tentativa de autenticación, pero no se realizó la autenticación. • vacío: Autenticación 3DS no realizada (3DS desactivado en la solicitud, titular no afiliado al medio de pago no elegible para 3DS).

Los campos opcionales enviados en la solicitud son devueltos en la respuesta sin cambios en sus valores.

16.6.4. Creación del token al suscribirse a una recurrencia

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es REGISTER_SUBSCRIBE .
vads_identifier_status	Estado de la creación de token. Los valores posibles son: <ul style="list-style-type: none"> • CREATED: la solicitud de autorización o de información si el adquirente lo soporta es aceptada. El token se crea con éxito. Consulte el valor del campo vads_recurrence_status para determinar si se ha creado la recurrencia. • NOT_CREATED: la solicitud de autorización o de información es rechazada. El token no se crea, por lo tanto, no se ve en el Back Office Expert. La recurrencia no se crea. • ABANDONED: acción abandonada por el comprador. El token no se crea, por lo tanto, no aparece en el Back Office Expert. La recurrencia no se crea.
vads_recurrence_status	Estado de la creación de la recurrencia. Los valores posibles son: <ul style="list-style-type: none"> • CREATED: La afiliación fue creada con éxito. • NOT_CREATED: La recurrencia no se crea. • ABANDONED: acción abandonada por el comprador. La recurrencia no se crea.
vads_identifier	Identificador del token. El valor devuelto es: <ul style="list-style-type: none"> • igual al valor enviado en la solicitud, cualquiera sea el resultado de la creación del token, incluso en caso de abandono, • o el valor generado por la plataforma, si el campo no es enviado en la solicitud y si el token se crea correctamente (vads_identifier_status=CREATED). <p>Nota</p> <p>Si ha activado la verificación de la unicidad de los token y que el medio de pago ya está registrado con otro token, entonces es otro token el que se devolverá.</p> <p>El campo vads_identifier no se devolverá:</p> <ul style="list-style-type: none"> • si no es enviado en la solicitud y si el comprador abandona (vads_identifier_status=ABANDONED), • si no es enviado en la solicitud y si el token no se crea (vads_identifier_status=NOT_CREATED).
vads_identifier_previously_registered	únicamente presente si las dos condiciones son verdaderas: <ul style="list-style-type: none"> • usted ha activado la verificación de la unidad de los token, • el medio de pago utilizado ya está registrado con otro token.
vads_initial_issuer_transaction_identifier	Identificador de transacción único generado por el emisor. <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;">  <p>La plataforma de pago registra el identificador de transacción emisor a nivel del token. En función del uso que se hará del token (pago en 1 clic, pago sin clics, suscripción, etc.), se utilizará el identificador de transacción emisor como referencia de encadenamiento si fuera necesario.</p> </div>
vads_cust_email	Dirección de correo electrónico del comprador enviada en la solicitud.
vads_site_id	Identificación de la tienda. El valor devuelto es igual al enviado en la solicitud.
vads_ctx_mode	Modo de funcionamiento.

Nombre del campo	Descripción
	El valor devuelto (TEST o PRODUCTION) es igual al enviado en la solicitud.

Para conocer el detalle de la recurrencia consulte los siguientes parámetros:

Nombre del campo	Nota
vads_subscription	Identificador de la recurrencia. El valor devuelto es: <ul style="list-style-type: none"> el valor enviado en la solicitud, cualquiera sea el resultado de la creación de la recurrencia; o el valor generado por la plataforma de pago, si el campo no es enviado en la solicitud y si la recurrencia se crea correctamente (vads_recurrence_status=CREATED). El campo vads_subscription no se devolverá: <ul style="list-style-type: none"> si no es enviado en la solicitud y si el comprador abandona (vads_recurrence_status=ABANDONED), si no es enviado en la solicitud y si la recurrencia no se crea (vads_recurrence_status=NOT_CREATED).
vads_sub_amount	Monto de los vencimientos de la recurrencia (en su unidad monetaria más pequeña).
vads_sub_currency	Código de la moneda utilizada para la recurrencia. Ejemplo: 978 para el euro (EUR)
vads_sub_desc	Regla de recurrencia para aplicar de acuerdo con la especificación iCalendar RFC5545. Ejemplo: RRULE:FREQ=MONTHLY
vads_sub_effect_date	Fecha de inicio de la recurrencia (o fecha efectiva) el en huso UTC, en formato AAAAMMDD. Ejemplo: 20210601
vads_sub_init_amount	Monto de los primeros vencimientos. El número de los primeros vencimientos lo define vads_sub_init_amount_number . Ejemplo: 1000
vads_sub_init_amount_number	Número de vencimientos a los que aplicar el monto definido por vads_sub_init_amount . Ejemplo: 3

Una solicitud de “creación de token al suscribir una recurrencia” permite crear una transacción de tipo **VERIFICATION**, que se ve en el Back Office Expert.

La función de esta transacción es ayudar al vendedor a entender, desde su Back-Office, las razones de rechazo de la creación del token.



A continuación, encontrará sus características:

Nombre del campo	Descripción
vads_operation_type	Tipo de transacción. Su valor es VERIFICATION .
vads_trans_status	Estado de la transacción. Los valores posibles son: <ul style="list-style-type: none"> ACCEPTED La solicitud de autorización o de información ha sido aceptada. El token se crea y aparece en el Back Office Expert. REFUSED La solicitud de autorización o de información ha sido denegada. El token no se crea.
vads_occurrence_type	Tipo de ocurrencia de la transacción. Su valor es UNITAIRE .
vads_amount	

Nombre del campo	Descripción
vads_trans_id	Identificador de la transacción. La plataforma de pago genera el valor.
vads_trans_uuid	Identificador único de la transacción. La plataforma de pago genera el valor.
vads_auth_mode	Tipo de solicitud realizada en los servidores de autorización. Su valor es MARK .
vads_auth_number	Número de autorización devuelto por el servidor bancario. Vacío si la autorización falló.
vads_auth_result	Código de retorno de la solicitud de autorización devuelta por el banco emisor. Ver capítulo Gestionar los códigos de retorno de la solicitud de autorización . Vacío si aparece un error antes de la autorización.
vads_risk_assessment_result	Lista de acciones efectuadas sobre la transacción, tras el desencadenamiento de las reglas de gestión de riesgo avanzada. Las reglas relativas al monto o cuya acción es "Validar manualmente" no se aplican en el caso de una transacción de tipo VERIFICATION. Los valores posibles son: <ul style="list-style-type: none"> • ENABLE_3DS: 3D Secure activado. • DISABLE_3DS: 3D Secure desactivado. • CHALLENGE_REQUESTED: <ul style="list-style-type: none"> • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge). • CHALLENGE_MANDATE: <ul style="list-style-type: none"> • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge por razones reglamentarias) por motivos normativos. • REFUSE: El token es rechazado. • RUN_RISK_ANALYSIS: Resultado del analizador de riesgos externo. Consulte la descripción del campo vads_risk_analysis_result para más detalles. • INFORM: Se levanta una alerta. El vendedor recibe una alerta porque se ha identificado un riesgo a través de una o varias reglas del centro de notificación.

Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo Medios de pago compatibles para obtener la lista de valores posibles.
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto. o IBAN y BIC (si están completos) utilizados para el pago, separados por una '_' en el caso de un débito puntual. Como el BIC es opcional, puede que no aparezca .

Nombre del campo	Nota
vads_expiry_month	Mes de caducidad de la tarjeta utilizada.  Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.
vads_expiry_year	Año de caducidad de la tarjeta utilizada.  Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.

Detalles de la autenticación del portador:


Nombre del campo	Nota
vads_threeds_auth_type	Tipo de autenticación del titular. Es obligatoria una autenticación fuerte del portador al registrar una tarjeta. Por lo tanto, el campo siempre se valorizará en CHALLENGE .
vads_threeds_enrolled	Estado de la inscripción del titular al programa 3D Secure. Los valores posibles son: <ul style="list-style-type: none"> • Y: Autenticación disponible. • N: Autenticación no disponible • U: Estado de la inscripción al programa 3DS desconocido • vacío: Proceso 3DS no realizado (3DS desactivado en la solicitud, vendedor no afiliado al medio de pago no elegible para 3DS).
vads_threeds_status	Resultado de la autenticación 3D Secure. Los valores posibles son: <ul style="list-style-type: none"> • Y: Portador autenticado correctamente. • N: Error de autenticación del portador. • U: Autenticación imposible • A: Tentativa de autenticación, pero no se realizó la autenticación. • vacío: Autenticación 3DS no realizada (3DS desactivado en la solicitud, titular no afiliado al medio de pago no elegible para 3DS).

Los campos opcionales enviados en la solicitud son devueltos en la respuesta sin cambios en sus valores.

16.6.5. Creación del token al suscribir a una recurrencia acompañada de un pago

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es REGISTER_PAY_SUBSCRIBE .
vads_identifier_status	Estado de la creación de token. Los valores posibles son: <ul style="list-style-type: none">• CREATED: la solicitud de autorización o de información si el adquirente lo soporta es aceptada. El token se crea con éxito. Consulte el valor del campo vads_recurrence_status para determinar si se ha creado la recurrencia.• NOT_CREATED: la solicitud de autorización o de información es rechazada. El token no se crea, por lo tanto, no se ve en el Back Office Expert. La recurrencia no se crea.• ABANDONED: acción abandonada por el comprador. El token no se crea, por lo tanto, no aparece en el Back Office Expert. La recurrencia no se crea.
vads_trans_status	Estado de la transacción. Los valores posibles son: <ul style="list-style-type: none">• AUTHORISED La solicitud de autorización o de información ha sido aceptada. El token se crea y aparece en el Back Office Expert.• AUTHORISED_TO_VALIDATE La solicitud de autorización o de información ha sido aceptada. El vendedor debe validar la transacción de forma manual. El token se crea y aparece en el Back Office Expert.• CAPTURED La solicitud de autorización o de información ha sido aceptada. El pago aparece en la pestaña “Transacciones capturadas” del Back-Office. El token se crea y aparece en el Back Office Expert.• WAITING_AUTHORISATION El plazo de captura al banco es superior a la duración de validez de la autorización. La solicitud de autorización por el monto total aún no se ha creado. El token se crea y aparece en el Back Office Expert.• WAITING_AUTHORISATION_TO_VALIDATE Para validar y autorizar El plazo de captura al banco es superior a la duración de validez de la autorización. Se aceptó una autorización 1 EUR (o solicitud de información en la red de CB si el adquirente lo admite). El vendedor debe validar manualmente la transacción para que se realice la solicitud de autorización y la captura.• REFUSED La solicitud de autorización o de información ha sido denegada. El token no se crea.• ABANDONED Operación abandonada por el comprador. La transacción no aparece en el Back Office Expert. El token no se crea.
vads_recurrence_status	Estado de la creación de la recurrencia. Los valores posibles son: <ul style="list-style-type: none">• CREATED: La afiliación fue creada con éxito.

Nombre del campo	Descripción
	<ul style="list-style-type: none"> • NOT_CREATED: La recurrencia no se crea. • ABANDONED: acción abandonada por el comprador. La recurrencia no se crea.
vads_identifier	<p>Identificador del token. El valor devuelto es:</p> <ul style="list-style-type: none"> • igual al valor enviado en la solicitud, cualquiera sea el resultado de la creación del token, incluso en caso de abandono, • o el valor generado por la plataforma, si el campo no es enviado en la solicitud y si el token se crea correctamente (vads_identifier_status=CREATED). <p>Nota Si ha activado la verificación de la unicidad de los token y que el medio de pago ya está registrado con otro token, entonces es otro token el que se devolverá. El campo vads_identifier no se devolverá:</p> <ul style="list-style-type: none"> • si no es enviado en la solicitud y si el comprador abandona (vads_identifier_status=ABANDONED), • si no es enviado en la solicitud y si el token no se crea (vads_identifier_status=NOT_CREATED).
vads_identifier_previously_registered	<p>únicamente presente si las dos condiciones son verdaderas:</p> <ul style="list-style-type: none"> • usted ha activado la verificación de la unidad de los token, • el medio de pago utilizado ya está registrado con otro token.
vads_initial_issuer_transaction_identifier	<p>Identificador de transacción único generado por el emisor.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> La plataforma de pago registra el identificador de transacción emisor a nivel del token y de la transacción. En función del uso que se hará del token (pago en 1 clic, pago sin clics, suscripción, etc.), se utilizará el identificador de transacción emisor como referencia de encadenamiento si fuera necesario.</p> </div>
vads_cust_email	Dirección de correo electrónico del comprador enviada en la solicitud.
vads_site_id	Identificación de la tienda. El valor devuelto es igual al enviado en la solicitud.
vads_ctx_mode	Modo de funcionamiento. El valor devuelto (TEST o PRODUCTION) es igual al enviado en la solicitud.

Para conocer el detalle de la recurrencia consulte los siguientes parámetros:

Nombre del campo	Nota
vads_subscription	<p>Identificador de la recurrencia. El valor devuelto es:</p> <ul style="list-style-type: none"> • el valor enviado en la solicitud, cualquiera sea el resultado de la creación de la recurrencia; • o el valor generado por la plataforma de pago, si el campo no es enviado en la solicitud y si la recurrencia se crea correctamente (vads_recurrence_status=CREATED). <p>El campo vads_subscription no se devolverá:</p> <ul style="list-style-type: none"> • si no es enviado en la solicitud y si el comprador abandona (vads_recurrence_status=ABANDONED), • si no es enviado en la solicitud y si la recurrencia no se crea (vads_recurrence_status=NOT_CREATED).
vads_sub_amount	Monto de los vencimientos de la recurrencia (en su unidad monetaria más pequeña).
vads_sub_currency	Código de la moneda utilizada para la recurrencia. Ejemplo: 978 para el euro (EUR)

Nombre del campo	Nota
vads_sub_desc	Regla de recurrencia para aplicar de acuerdo con la especificación iCalendar RFC5545. Ejemplo: RRULE:FREQ=MONTHLY
vads_sub_effect_date	Fecha de inicio de la recurrencia (o fecha efectiva) el en huso UTC, en formato AAAAMMDD. Ejemplo: 20210601
vads_sub_init_amount	Monto de los primeros vencimientos. El número de los primeros vencimientos lo define vads_sub_init_amount_number . Ejemplo: 1000
vads_sub_init_amount_number	Número de vencimientos a los que aplicar el monto definido por vads_sub_init_amount . Ejemplo: 3



Para conocer el detalle del pago, consulte los siguientes parámetros:

Información sobre la transacción:

Nombre del campo	Descripción
vads_operation_type	Tipo de transacción. Su valor es DEBIT .
vads_occurrence_type	Tipo de ocurrencia de la transacción. Su valor es UNITAIRE .
vads_amount	Monto de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_currency	Código de la moneda utilizada para el pago.
vads_trans_id	Identificador de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_trans_uuid	Identificador único de la transacción. La plataforma de pago genera el valor.
vads_contract_used	Número de la afiliación asociada a la transacción.
vads_auth_mode	Tipo de solicitud realizada en los servidores de autorización: <ul style="list-style-type: none"> MARK: corresponde a una autorización de 1 EUR (o solicitud de información en la red de CB si el adquirente lo admite). Valor utilizado también si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente posterior al período de validez de la autorización. FULL: corresponde a una autorización del monto total de la transacción. Valor utilizado si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente anterior al período de validez de la autorización.
vads_auth_number	Número de autorización devuelto por el servidor bancario. Vacío si la autorización falló.
vads_auth_result	Código de retorno de la solicitud de autorización devuelta por el banco emisor. Vacío si aparece un error antes de la autorización.
vads_risk_control	Resultado de los controles de riesgo. Cuando, al menos, un control devuelve el valor ERROR , la transacción es rechazada. Consulte la descripción del campo vads_risk_analysis_result para más detalles.
vads_risk_assessment_result	Lista de acciones efectuadas sobre la transacción, tras el desencadenamiento de las reglas de gestión de riesgo avanzada. Los valores posibles son: <ul style="list-style-type: none"> ENABLE_3DS: 3D Secure activado. DISABLE_3DS: 3D Secure desactivado. CHALLENGE_REQUESTED: <ul style="list-style-type: none"> Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge).

Nombre del campo	Descripción
	<ul style="list-style-type: none"> • CHALLENGE_MANDATE: <ul style="list-style-type: none"> • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge por razones reglamentarias) por motivos normativos. • MANUAL_VALIDATION: La transacción se crea con validación manual. La remesa del pago se bloquea temporalmente para permitir que el vendedor realice todas las verificaciones deseadas. • REFUSE: La transacción se ha rechazado. • RUN_RISK_ANALYSIS: Resultado del analizador de riesgos externo. Consulte la descripción del campo vads_risk_analysis_result para más detalles. • INFORM: Se levanta una alerta. El vendedor recibe una alerta porque se ha identificado un riesgo a través de una o varias reglas del centro de notificación.

Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo Medios de pago compatibles para obtener la lista de valores posibles.
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto. o IBAN y BIC (si están completos) utilizados para el pago, separados por una '_' en el caso de un débito puntual. Como el BIC es opcional, puede que no aparezca .
vads_expiry_month	Mes de caducidad de la tarjeta utilizada.  Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.
vads_expiry_year	Año de caducidad de la tarjeta utilizada.  Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.

Detalles de la autenticación del portador:

Nombre del campo	Nota
vads_threeds_auth_type	Tipo de autenticación del titular. Es obligatoria una autenticación fuerte del portador al registrar una tarjeta. Por lo tanto, el campo siempre se valorizará en CHALLENGE .
vads_threeds_enrolled	Estado de la inscripción del titular al programa 3D Secure. Los valores posibles son: <ul style="list-style-type: none"> • Y: Autenticación disponible. • N: Autenticación no disponible • U: Estado de la inscripción al programa 3DS desconocido

Nombre del campo	Nota
	<ul style="list-style-type: none"> vacío: Proceso 3DS no realizado (3DS desactivado en la solicitud, vendedor no afiliado al medio de pago no elegible para 3DS).
vads_threeds_status	<p>Resultado de la autenticación 3D Secure. Los valores posibles son:</p> <ul style="list-style-type: none"> Y: Portador autenticado correctamente. N: Error de autenticación del portador. U: Autenticación imposible A: Tentativa de autenticación, pero no se realizó la autenticación. vacío: Autenticación 3DS no realizada (3DS desactivado en la solicitud, titular no afiliado al medio de pago no elegible para 3DS).

Los campos opcionales enviados en la solicitud son devueltos en la respuesta sin cambios en sus valores.

16.6.6. Pago por Token

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es PAYMENT .
vads_trans_status	<p>Estado de la transacción. Los valores posibles son:</p> <ul style="list-style-type: none"> AUTHORISED La solicitud de autorización fue aceptada. AUTHORISED_TO_VALIDATE La solicitud de autorización fue aceptada. El vendedor debe validar la transacción de forma manual. CAPTURED La solicitud de autorización fue aceptada. El pago aparece en la pestaña "Transacciones capturadas" del Back-Office. WAITING_AUTHORISATION El plazo de captura al banco es superior a la duración de validez de la autorización. La solicitud de autorización por el monto total aún no se ha creado. WAITING_AUTHORISATION_TO_VALIDATE Para validar y autorizar El plazo de captura al banco es superior a la duración de validez de la autorización. Se aceptó una autorización 1 EUR (o solicitud de información en la red de CB si el adquirente lo admite). El vendedor debe validar manualmente la transacción para que se realice la solicitud de autorización y la captura. REFUSED La solicitud de autorización fue denegada. ABANDONED Operación abandonada por el comprador. La transacción no aparece en el Back Office Expert.
vads_identifier	Identificador del token para debitar. El valor devuelto es igual al enviado en la solicitud.
vads_cust_email	Dirección de correo electrónico del comprador asociado al token.
vads_site_id	Identificación de la tienda. El valor devuelto es igual al enviado en la solicitud.

Nombre del campo	Descripción
vads_ctx_mode	Modo de funcionamiento. El valor devuelto (TEST o PRODUCTION) es igual al enviado en la solicitud.



Para conocer el detalle del pago, consulte los siguientes parámetros:

Información sobre la transacción:

Nombre del campo	Descripción
vads_operation_type	Tipo de transacción. Su valor es DEBIT .
vads_occurrence_type	Tipo de ocurrencia de la transacción. Su valor es RECURRENT_INTERMEDIAIRE .
vads_amount	Monto de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_currency	Código de la moneda utilizada para el pago.
vads_trans_id	Identificador de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_trans_uuid	Identificador único de la transacción. La plataforma de pago genera el valor.
vads_initial_issuer_transaction_identifier	Identificador de transacción único generado por el emisor.
vads_contract_used	Número de la afiliación asociada a la transacción.
vads_auth_mode	Tipo de solicitud realizada en los servidores de autorización: <ul style="list-style-type: none"> MARK: corresponde a una autorización de 1 EUR (o solicitud de información en la red de CB si el adquirente lo admite). Valor utilizado también si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente posterior al período de validez de la autorización. FULL: corresponde a una autorización del monto total de la transacción. Valor utilizado si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente anterior al período de validez de la autorización.
vads_auth_number	Número de autorización devuelto por el servidor bancario. Vacío si la autorización falló.
vads_auth_result	Código de retorno de la solicitud de autorización devuelta por el banco emisor. Ver capítulo Gestionar los códigos de retorno de la solicitud de autorización . Vacío si aparece un error antes de la autorización.
vads_risk_control	Resultado de los controles de riesgo. Cuando, al menos, un control devuelve el valor ERROR , la transacción es rechazada. Consulte la descripción del campo vads_risk_analysis_result para más detalles.
vads_risk_assessment_result	Lista de acciones efectuadas sobre la transacción, tras el desencadenamiento de las reglas de gestión de riesgo avanzada. Los valores posibles son: <ul style="list-style-type: none"> ENABLE_3DS: 3D Secure activado. DISABLE_3DS: 3D Secure desactivado. CHALLENGE_REQUESTED: <ul style="list-style-type: none"> Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge). CHALLENGE_MANDATE: <ul style="list-style-type: none"> Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge por razones reglamentarias) por motivos normativos. MANUAL_VALIDATION: La transacción se crea con validación manual.

Nombre del campo	Descripción
	<p>La remesa del pago se bloquea temporalmente para permitir que el vendedor realice todas las verificaciones deseadas.</p> <ul style="list-style-type: none"> • REFUSE: La transacción se ha rechazado. • RUN_RISK_ANALYSIS: Resultado del analizador de riesgos externo. Consulte la descripción del campo vads_risk_analysis_result para más detalles. • INFORM: Se levanta una alerta. El vendedor recibe una alerta porque se ha identificado un riesgo a través de una o varias reglas del centro de notificación.

Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo Medios de pago compatibles para obtener la lista de valores posibles.
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto. o IBAN y BIC (si están completos) utilizados para el pago, separados por una '_' en el caso de un débito puntual. Como el BIC es opcional, puede que no aparezca .
vads_expiry_month	Mes de caducidad de la tarjeta utilizada.  Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.
vads_expiry_year	Año de caducidad de la tarjeta utilizada.  Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.

Detalles de la autenticación fuerte:

Nombre del campo	Nota
vads_threeds_auth_type	Tipo de autenticación del titular. Los valores posibles son: <ul style="list-style-type: none"> • “Vacío” si el comprador no se autenticó correctamente, • FRICITIONLESS: autenticación del titular sin interacción con el servidor de autenticación. Valor devuelto únicamente con 3DS v2, • CHALLENGE: autenticación interactiva del titular (ingreso de una contraseña de uso único o respuesta a una serie de preguntas). Valor devuelto con 3DS v1 y 3DS v2.
vads_threeds_enrolled	Estado de la inscripción del titular al programa 3D Secure. Los valores posibles son: <ul style="list-style-type: none"> • Y: Autenticación disponible. • N: Autenticación no disponible • U: Estado de la inscripción al programa 3DS desconocido

Nombre del campo	Nota
	<ul style="list-style-type: none"> vacío: Proceso 3DS no realizado (3DS desactivado en la solicitud, vendedor no afiliado al medio de pago no elegible para 3DS).
vads_threeds_status	<p>Resultado de la autenticación 3D Secure. Los valores posibles son:</p> <ul style="list-style-type: none"> Y: Portador autenticado correctamente. N: Error de autenticación del portador. U: Autenticación imposible A: Tentativa de autenticación, pero no se realizó la autenticación. vacío: Autenticación 3DS no realizada (3DS desactivado en la solicitud, titular no afiliado al medio de pago no elegible para 3DS).

Los campos opcionales enviados en la solicitud son devueltos en la respuesta sin cambios en sus valores.

16.6.7. Suscripción a una recurrencia

Para entender el resultado, analice los siguientes campos:



Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es SUBSCRIBE .
vads_recurrence_status	Estado de la creación de la recurrencia. Los valores posibles son: <ul style="list-style-type: none"> CREATED: La afiliación fue creada con éxito. NOT_CREATED: La recurrencia no se crea. ABANDONED: acción abandonada por el comprador. La recurrencia no se crea.
vads_identifier	Identificador del token para debitar. El valor devuelto es igual al enviado en la solicitud.
vads_cust_email	Dirección de e-mail del comprador asociada al token.
vads_site_id	Identificación de la tienda. El valor devuelto es igual al enviado en la solicitud.
vads_ctx_mode	Modo de funcionamiento. El valor devuelto (TEST o PRODUCTION) es igual al enviado en la solicitud.

Para conocer el detalle de la recurrencia consulte los siguientes parámetros:

Nombre del campo	Nota
vads_subscription	<p>Identificador de la recurrencia. El valor devuelto es:</p> <ul style="list-style-type: none"> el valor enviado en la solicitud, cualquiera sea el resultado de la creación de la recurrencia; o el valor generado por la plataforma de pago, si el campo no es enviado en la solicitud y si la recurrencia se crea correctamente (vads_recurrence_status=CREATED). <p>El campo vads_subscription no se devolverá:</p> <ul style="list-style-type: none"> si no es enviado en la solicitud y si el comprador abandona (vads_recurrence_status=ABANDONED), si no es enviado en la solicitud y si la recurrencia no se crea (vads_recurrence_status=NOT_CREATED).

Nombre del campo	Nota
vads_sub_amount	Monto de los vencimientos de la recurrencia (en su unidad monetaria más pequeña).
vads_sub_currency	Código de la moneda utilizada para la recurrencia. Ejemplo: 978 para el euro (EUR)
vads_sub_desc	Regla de recurrencia para aplicar de acuerdo con la especificación iCalendar RFC5545. Ejemplo: RRULE:FREQ=MONTHLY
vads_sub_effect_date	Fecha de inicio de la recurrencia (o fecha efectiva) el en huso UTC, en formato AAAAMMDD. Ejemplo: 20210601
vads_sub_init_amount	Monto de los primeros vencimientos. El número de los primeros vencimientos lo define vads_sub_init_amount_number . Ejemplo: 1000
vads_sub_init_amount_number	Número de vencimientos a los que aplicar el monto definido por vads_sub_init_amount . Ejemplo: 3

Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo Medios de pago compatibles para obtener la lista de valores posibles.
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto. o IBAN y BIC (si están completos) utilizados para el pago, separados por una '_' en el caso de un débito puntual. Como el BIC es opcional, puede que no aparezca .
vads_expiry_month	Mes de caducidad de la tarjeta utilizada.  Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.
vads_expiry_year	Año de caducidad de la tarjeta utilizada.  Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.

Detalles de la autenticación fuerte realizada al crear el token:

Nombre del campo	Nota
vads_threeds_auth_type	Tipo de autenticación del titular. Es obligatoria una autenticación fuerte del portador al registrar una tarjeta. Por lo tanto, el campo siempre se valorizará en CHALLENGE .
vads_threeds_enrolled	Estado de la inscripción del titular al programa 3D Secure. Los valores posibles son: <ul style="list-style-type: none"> • Y: Autenticación disponible. • N: Autenticación no disponible • U: Estado de la inscripción al programa 3DS desconocido

Nombre del campo	Nota
	<ul style="list-style-type: none"> • vacío: Proceso 3DS no realizado (3DS desactivado en la solicitud, vendedor no afiliado al medio de pago no elegible para 3DS).
vads_threeds_status	<p>Resultado de la autenticación 3D Secure. Los valores posibles son:</p> <ul style="list-style-type: none"> • Y: Portador autenticado correctamente. • N: Error de autenticación del portador. • U: Autenticación imposible • A: Tentativa de autenticación, pero no se realizó la autenticación. • vacío: Autenticación 3DS no realizada (3DS desactivado en la solicitud, titular no afiliado al medio de pago no elegible para 3DS).

Los campos opcionales enviados en la solicitud son devueltos en la respuesta sin cambios en sus valores.

16.6.8. Pago con propuesta al titular para crear un token

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	<p>Acción realizada. El valor devuelto es ASK_REGISTER_PAY.</p>
vads_identifier_status	<p>Estado de la creación de token. El campo no se enviará si el comprador no tiene su consentimiento para registrar los datos de su tarjeta. Los valores posibles son:</p> <ul style="list-style-type: none"> • CREATED: la solicitud de autorización o de información si el adquirente lo soporta es aceptada. El token se crea con éxito. • NOT_CREATED: la solicitud de autorización o de información es rechazada. El token no se crea, por lo tanto, no se ve en el Back Office Expert. • ABANDONED: acción abandonada por el comprador. El token no se crea, por lo tanto, no se ve en el Back Office Expert.
vads_trans_status	<p>Estado de la transacción. Los valores posibles son:</p> <ul style="list-style-type: none"> • AUTHORISED La solicitud de autorización o de información ha sido aceptada. El token se crea y aparece en el Back Office Expert. • AUTHORISED_TO_VALIDATE La solicitud de autorización o de información ha sido aceptada. El vendedor debe validar la transacción de forma manual. El token se crea y aparece en el Back Office Expert. • CAPTURED La solicitud de autorización o de información ha sido aceptada. El pago aparece en la pestaña "Transacciones capturadas" del Back-Office. El token se crea y aparece en el Back Office Expert. • WAITING_AUTHORISATION El plazo de captura al banco es superior a la duración de validez de la autorización. La solicitud de autorización por el monto total aún no se ha creado. El token se crea y aparece en el Back Office Expert. • WAITING_AUTHORISATION_TO_VALIDATE Para validar y autorizar

Nombre del campo	Descripción
	<p>El plazo de captura al banco es superior a la duración de validez de la autorización.</p> <p>Se aceptó una autorización 1 EUR (o solicitud de información en la red de CB si el adquirente lo admite).</p> <p>El vendedor debe validar manualmente la transacción para que se realice la solicitud de autorización y la captura.</p> <ul style="list-style-type: none"> • REFUSED La solicitud de autorización o de información ha sido denegada. El token no se crea. • ABANDONED Operación abandonada por el comprador. La transacción no aparece en el Back Office Expert. El token no se crea.
vads_identifier	<p>Identificador del token.</p> <p>El campo no se enviará si el comprador no tiene su consentimiento para registrar los datos de su tarjeta.</p> <p>El valor devuelto es:</p> <ul style="list-style-type: none"> • igual al valor enviado en la solicitud, cualquiera sea el resultado de la creación del token, incluso en caso de abandono, • o el valor generado por la plataforma, si el campo no es enviado en la solicitud y si el token se crea correctamente (vads_identifier_status=CREATED). <p>Nota</p> <p>Si ha activado la verificación de la unicidad de los token y que el medio de pago ya está registrado con otro token, entonces es otro token el que se devolverá.</p> <p>El campo vads_identifier no se devolverá:</p> <ul style="list-style-type: none"> • si no es enviado en la solicitud y si el comprador abandona (vads_identifier_status=ABANDONED), • si no es enviado en la solicitud y si el token no se crea (vads_identifier_status=NOT_CREATED).
vads_cust_email	Dirección de correo electrónico del comprador enviada en la solicitud.
vads_site_id	Identificación de la tienda. El valor devuelto es igual al enviado en la solicitud.
vads_ctx_mode	Modo de funcionamiento. El valor devuelto (TEST o PRODUCTION) es igual al enviado en la solicitud.

Para conocer el detalle del pago, consulte los siguientes parámetros:



Información sobre la transacción:

Nombre del campo	Descripción
vads_operation_type	Tipo de transacción. Su valor es DEBIT .
vads_amount	Monto de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_currency	Código de la moneda utilizada para el pago.
vads_trans_id	Identificador de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_trans_uuid	Identificador único de la transacción. La plataforma de pago genera el valor.
vads_initial_issuer_transaction_identifier	Identificador de transacción único generado por el emisor.
vads_contract_used	Número de la afiliación asociada a la transacción.
vads_auth_mode	Tipo de solicitud realizada en los servidores de autorización:

Nombre del campo	Descripción
	<ul style="list-style-type: none"> • MARK: corresponde a una autorización de 1 EUR (o solicitud de información en la red de CB si el adquirente lo admite). Valor utilizado también si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente posterior al período de validez de la autorización. • FULL: corresponde a una autorización del monto total de la transacción. Valor utilizado si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente anterior al período de validez de la autorización.
vads_auth_number	Número de autorización devuelto por el servidor bancario. Vacío si la autorización falló.
vads_auth_result	Código de retorno de la solicitud de autorización devuelta por el banco emisor. Ver capítulo Gestionar los códigos de retorno de la solicitud de autorización . Vacío si aparece un error antes de la autorización.
vads_risk_control	Resultado de los controles de riesgo. Cuando, al menos, un control devuelve el valor ERROR , la transacción es rechazada. Consulte la descripción del campo vads_risk_analysis_result para más detalles.
vads_risk_assessment_result	Lista de acciones efectuadas sobre la transacción, tras el desencadenamiento de las reglas de gestión de riesgo avanzada. Los valores posibles son: <ul style="list-style-type: none"> • ENABLE_3DS: 3D Secure activado. • DISABLE_3DS: 3D Secure desactivado. • CHALLENGE_REQUESTED: <ul style="list-style-type: none"> • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge). • CHALLENGE_MANDATE: <ul style="list-style-type: none"> • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge por razones reglamentarias) por motivos normativos. • MANUAL_VALIDATION: La transacción se crea con validación manual. La remesa del pago se bloquea temporalmente para permitir que el vendedor realice todas las verificaciones deseadas. • REFUSE: La transacción se ha rechazado. • RUN_RISK_ANALYSIS: Resultado del analizador de riesgos externo. Consulte la descripción del campo vads_risk_analysis_result para más detalles. • INFORM: Se levanta una alerta. El vendedor recibe una alerta porque se ha identificado un riesgo a través de una o varias reglas del centro de notificación.

Información sobre el medio de pago utilizado:

Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo Medios de pago compatibles para obtener la lista de valores posibles.

Nombre del campo	Nota
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto. o IBAN y BIC (si están completos) utilizados para el pago, separados por una '_' en el caso de un débito puntual. Como el BIC es opcional, puede que no aparezca .
vads_expiry_month	Mes de caducidad de la tarjeta utilizada. <div style="border: 1px solid #0056b3; padding: 5px; background-color: #e6f2ff;">  Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token. </div>
vads_expiry_year	Año de caducidad de la tarjeta utilizada. <div style="border: 1px solid #0056b3; padding: 5px; background-color: #e6f2ff;">  Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token. </div>

Detalles de la autenticación del portador:

Nombre del campo	Nota
vads_threeds_auth_type	Tipo de autenticación del titular. Es obligatoria una autenticación fuerte del portador al registrar una tarjeta. Por lo tanto, el campo siempre se valorizará en CHALLENGE .
vads_threeds_enrolled	Estado de la inscripción del titular al programa 3D Secure. Los valores posibles son: <ul style="list-style-type: none"> • Y: Autenticación disponible. • N: Autenticación no disponible • U: Estado de la inscripción al programa 3DS desconocido • vacío: Proceso 3DS no realizado (3DS desactivado en la solicitud, vendedor no afiliado al medio de pago no elegible para 3DS).
vads_threeds_status	Resultado de la autenticación 3D Secure. Los valores posibles son: <ul style="list-style-type: none"> • Y: Portador autenticado correctamente. • N: Error de autenticación del portador. • U: Autenticación imposible • A: Tentativa de autenticación, pero no se realizó la autenticación. • vacío: Autenticación 3DS no realizada (3DS desactivado en la solicitud, titular no afiliado al medio de pago no elegible para 3DS).

Los campos opcionales enviados en la solicitud son devueltos en la respuesta sin cambios en sus valores.

16.6.9. Pago de un vencimiento de una recurrencia

Para entender el resultado, analice los siguientes campos:

Nombre del campo	Descripción
vads_page_action	Acción realizada. El valor devuelto es PAYMENT .
vads_trans_status	Estado de la transacción. Los valores posibles son: <ul style="list-style-type: none"> • AUTHORISED La solicitud de autorización fue aceptada.

Nombre del campo	Descripción
	<ul style="list-style-type: none"> • AUTHORISED_TO_VALIDATE La solicitud de autorización fue aceptada. El vendedor debe validar la transacción de forma manual. • CAPTURED La solicitud de autorización fue aceptada. El pago aparece en la pestaña “Transacciones capturadas” del Back-Office. • REFUSED La solicitud de autorización fue denegada.
vads_identifier	Identificador del token.
vads_cust_email	Correo electrónico del comprador.
vads_site_id	Identificación de la tienda.
vads_ctx_mode	Modo de funcionamiento.

Para conocer el detalle de la recurrencia consulte los siguientes parámetros:

Nombre del campo	Nota
vads_subscription	Identificador de la recurrencia.
vads_recurrence_number	Número de vencimiento de la recurrencia.


Para conocer el detalle del pago, consulte los siguientes parámetros:


Información sobre la transacción:

Nombre del campo	Descripción
vads_operation_type	Tipo de transacción. Su valor es DEBIT .
vads_occurrence_type	Tipo de ocurrencia de la transacción. Valores posibles: <ul style="list-style-type: none"> • RECURRENT_INITIAL: Primer vencimiento. • RECURRENT_INTERMEDIAIRE: Enésimo vencimiento. Consulte el campo vads_recurrence_number para conocer el número del vencimiento. • RECURRENT_FINAL: último vencimiento.
vads_amount	Monto de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_currency	Código de la moneda utilizada para el pago.
vads_trans_id	Identificador de la transacción. El valor devuelto es igual al enviado en la solicitud.
vads_trans_uuid	Identificador único de la transacción. La plataforma de pago genera el valor.
vads_contract_used	Número de la afiliación asociada a la transacción.
vads_auth_mode	Tipo de solicitud realizada en los servidores de autorización: <ul style="list-style-type: none"> • MARK: corresponde a una autorización de 1 EUR (o solicitud de información en la red de CB si el adquirente lo admite). Valor utilizado también si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente posterior al período de validez de la autorización. • FULL: corresponde a una autorización del monto total de la transacción. Valor utilizado si la duración entre la fecha de remesa solicitada y la fecha actual es estrictamente anterior al período de validez de la autorización.
vads_auth_number	Número de autorización devuelto por el servidor bancario. Vacío si la autorización falló.
vads_auth_result	Código de retorno de la solicitud de autorización devuelta por el banco emisor. Ver capítulo Gestionar los códigos de retorno de la solicitud de autorización . Vacío si aparece un error antes de la autorización.

Nombre del campo	Descripción
vads_risk_control	Resultado de los controles de riesgo. Cuando, al menos, un control devuelve el valor ERROR , la transacción es rechazada. Consulte la descripción del campo vads_risk_analysis_result para más detalles.
vads_risk_assessment_result	Lista de acciones efectuadas sobre la transacción, tras el desencadenamiento de las reglas de gestión de riesgo avanzada. Los valores posibles son: <ul style="list-style-type: none"> • ENABLE_3DS: 3D Secure activado. • DISABLE_3DS: 3D Secure desactivado. • CHALLENGE_REQUESTED: <ul style="list-style-type: none"> • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge). • CHALLENGE_MANDATE: <ul style="list-style-type: none"> • Tarjeta 3DS1: El módulo de riesgo ha solicitado una autenticación 3DS. • Tarjeta 3DS2: El módulo de riesgo ha solicitado una autenticación con interacción del portador (challenge por razones reglamentarias) por motivos normativos. • MANUAL_VALIDATION: La transacción se crea con validación manual. La remesa del pago se bloquea temporalmente para permitir que el vendedor realice todas las verificaciones deseadas. • REFUSE: La transacción se ha rechazado. • RUN_RISK_ANALYSIS: Resultado del analizador de riesgos externo. Consulte la descripción del campo vads_risk_analysis_result para más detalles. • INFORM: Se levanta una alerta. El vendedor recibe una alerta porque se ha identificado un riesgo a través de una o varias reglas del centro de notificación.

Información sobre el medio de pago utilizado:


Nombre del campo	Nota
vads_acquirer_network	Código de la red del adquirente.
vads_bank_code	Código del banco emisor
vads_bank_label	Código del banco emisor de la tarjeta utilizada.
vads_bank_product	Código de producto de la tarjeta utilizada.
vads_card_brand	Medio de pago utilizado. Consulte el capítulo Medios de pago compatibles para obtener la lista de valores posibles.
vads_card_country	Código país de la tarjeta utilizada según la norma ISO 3166.
vads_card_number	Número de tarjeta truncado/oculto. o IBAN y BIC (si están completos) utilizados para el pago, separados por una '_' en el caso de un débito puntual. Como el BIC es opcional, puede que no aparezca .
vads_expiry_month	Mes de caducidad de la tarjeta utilizada. <div style="border: 1px solid #add8e6; padding: 5px; display: inline-block;">  Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token. </div>
vads_expiry_year	Año de caducidad de la tarjeta utilizada.

Nombre del campo	Nota
	 Es aconsejable utilizar estos datos para comprobar la fecha de caducidad del token.

16.7. Test y troubleshooting

Para probar las notificaciones, siga las siguientes etapas:

1. Realice un pago (en modo TEST o en modo PRODUCTION).
2. Una vez finalizado el pago, busque la transacción en su Back Office (Menú **Gestión > Transacciones o Transacciones de TEST** si realizó el pago en modo TEST).
3. Haga doble clic en la transacción para ver el **detalle de la transacción**.
4. En el detalle de la transacción, busque la sección **Datos técnicos**.
5. Compruebe el estado de la URL de notificación:

Datos técnicos	
Estado de la URL de notificación :	Enviado (Mostrar las informaciones)
Certificado :	

La lista de los estados posibles se presenta a continuación:

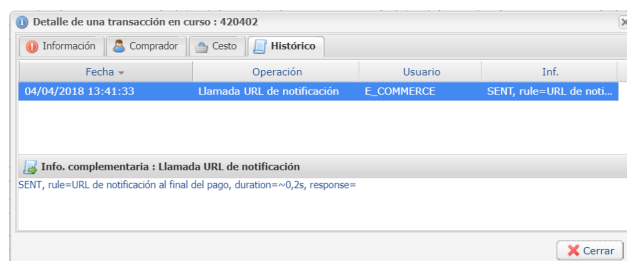
Estado	Descripción
N/A	La transacción no dio lugar a una notificación o no se activó ninguna regla de notificación.
URL no definido	Un evento activó la regla de notificación de fin de pago, pero la URL no está configurada.
Llamada en curso	La notificación está en curso Este estado es temporal.
Enviado	La notificación se ha enviado correctamente y un equipo distante respondió con un código HTTP 200, 201, 202, 203, 204, 205 ou 206.
Enviado (redirección permanente)	El sitio del comerciante ha devuelto un código HTTP 301 o 308 con una nueva URL para contactar. Una nueva llamada en modo POST se realiza hacia la nueva URL.
Enviado (redirección temporal)	El sitio del comerciante ha devuelto un código HTTP 302 o 307 con una nueva URL para contactar. Una nueva llamada en modo POST se realiza hacia la nueva URL.
Enviado (redirección a otra página)	El sitio del comerciante ha devuelto un código HTTP 301 con una nueva URL para contactar. Una nueva llamada en modo GET se realiza hacia la nueva URL.
Fallido	Error genérico diferente de los códigos descritos a continuación.
Servidor inalcanzable	La notificación duró más de 35 s.
Error con SSL handshake	La configuración de su servidor no es correcta. Realice un diagnóstico en el sitio de Qualys (https://www.ssllabs.com/ssltest/) y corrija los errores.
Conexión interrumpida	Error de comunicación.
Conexión rechazada	Error de comunicación.
Error servidor 300	Caso de redirección no aceptado por la plataforma.
Error servidor 304	Caso de redirección no aceptado por la plataforma.
Error servidor 305	Caso de redirección no aceptado por la plataforma.
Error servidor 400	El sitio del vendedor ha devuelto un código HTTP 400 Bad Request.
Error servidor 401	El sitio del vendedor ha devuelto un código HTTP 401 Unauthorized. Asegúrese de que el recurso no esté protegido por un archivo .htaccess.
Error servidor 402	El sitio del vendedor ha devuelto un código HTTP 402 Payment Required.
Error servidor 403	El sitio del vendedor ha devuelto un código HTTP 403 Forbidden. Asegúrese de que el recurso no esté protegido por un archivo .htaccess.
Error servidor 404	El sitio del vendedor ha devuelto un código HTTP 404 Not Found. Verifique que el ingreso de la URL esté correcto en la configuración de la regla. También verifique que el archivo esté presente en su servidor.
Error servidor 405	El sitio del vendedor ha devuelto un código HTTP 405 Method Not allowed.
Error servidor 406	El sitio del vendedor ha devuelto un código HTTP 406 Not Acceptable.
Error servidor 407	El sitio del vendedor ha devuelto un código HTTP 407 Proxy Authentication Required.
Error servidor 408	El sitio del vendedor ha devuelto un código HTTP 408 Request Time-out.

Estado	Descripción
Error servidor 409	El sitio del vendedor ha devuelto un código HTTP 409 Conflict.
Error servidor 410	El sitio del vendedor ha devuelto un código HTTP 410 Gone.
Error servidor 411	El sitio del vendedor ha devuelto un código HTTP 411 Length Required.
Error servidor 412	El sitio del vendedor ha devuelto un código HTTP 412 Precondition Failed.
Error servidor 413	El sitio del vendedor ha devuelto un código HTTP 413 Request Entity Too Large.
Error servidor 414	El sitio del vendedor ha devuelto un código HTTP 414 Request-URI Too long.
Error servidor 415	El sitio del vendedor ha devuelto un código HTTP 415 Unsupported Media Type.
Error servidor 416	El sitio del vendedor ha devuelto un código HTTP 416 Requested range unsatisfiable.
Error servidor 417	El sitio del vendedor ha devuelto un código HTTP 417 Expectation failed.
Error servidor 419	El sitio del vendedor ha devuelto un código HTTP 419 Authentication Timeout.
Error servidor 421	El sitio del vendedor ha devuelto un código HTTP 421 Misdirected Request.
Error servidor 422	El sitio del vendedor ha devuelto un código HTTP 422 Unprocessable Entity.
Error servidor 423	El sitio del vendedor ha devuelto un código HTTP 423 Locked.
Error servidor 424	El sitio del vendedor ha devuelto un código HTTP 424 Failed Dependency.
Error servidor 425	El sitio del vendedor ha devuelto un código HTTP 425 Too Early.
Error servidor 426	El sitio del vendedor ha devuelto un código HTTP 426 Upgrade Required.
Error servidor 429	El sitio del vendedor ha devuelto un código HTTP 431 Request Header Fields Too Large.
Error servidor 431	El sitio del vendedor ha devuelto un código HTTP 415 Unsupported Media Type.
Error servidor 451	El sitio del vendedor ha devuelto un código HTTP 451 Unavailable For Legal Reasons.
Error servidor 500	El sitio del vendedor ha devuelto un código HTTP 500 Internal Server Error. Se ha producido un error aplicativo en el servidor de su tienda. Consulte los registros de su servidor HTTP (generalmente apache). El problema solo puede corregirse al intervenir en su servidor.
Error servidor 501	El sitio del vendedor ha devuelto un código HTTP 501 Not Implemented.
Error servidor 502	El sitio del vendedor ha devuelto un código HTTP 502 Bad Gateway / Proxy Error.
Error servidor 503	El sitio del vendedor ha devuelto un código HTTP 503 Service Unavailable.
Error servidor 504	El sitio del vendedor ha devuelto un código HTTP 504 Gateway Time-out. El servidor del vendedor no ha aceptado la llamada dentro del tiempo de espera establecido de 10 s.
Error servidor 505	El sitio del vendedor ha devuelto un código HTTP 505 HTTP Version not supported.

Para obtener más información sobre una notificación, haga clic en el enlace **Mostrar la información** o haga clic en la pestaña **Historial** y busque la línea **Llamada URL de notificación**.

Para ayudar al vendedor a identificar el origen del error, la plataforma analiza sistemáticamente los primeros 512 caracteres que devuelve el sitio del comerciante y los muestra en la columna **Información**.

- Ejemplo de notificación procesada con éxito:



- Ejemplo de notificación incorrecta

The screenshot shows a window titled "Detalle de una transacción en curso". It contains a table with the following data:

Fecha	Operación	Usuario	Inf.
22/06/2016 12:04...	E-mail de confirmación ven...	BATCH	to: [icon]
22/06/2016 12:04...	E-mail de confirmación co...	BATCH	to: [icon]
22/06/2016 12:04...	Llamada URL de notificación	E_COMMERCE	FAILED_FILE_NOT_FOUND, rule=URL de

Si la plataforma no logra conectarse a la URL de su página, se enviará un e-mail de alerta a la dirección especificada.

Este contiene:

- El código HTTP del error encontrado
- Elementos de análisis en función del error
- Sus consecuencias
- El procedimiento a seguir desde el Back Office Expert para reenviar la solicitud a la URL definida en la configuración de la regla.

17. OBTENER AYUDA

¿Necesita ayuda? Consulte las preguntas frecuentes en nuestro sitio web

<https://docs.lyra.com/es/collect/faq/sitemap.html>

Para cualquier pregunta técnica o solicitud de asistencia, contacte [el soporte técnico](#).

Para facilitar el procesamiento de sus solicitudes, se le pedirá que informe su código cliente (ejemplo: **CLXXXXX**, **MKXXXXX** o **AGXXXXX**).

Esta información está disponible en el Back Office Vendedor (en la parte superior del menú).

18. APÉNDICES

18.1. Crear automáticamente una recurrencia por Web Services

Utilice el método **Charge/CreateSubscription** para realizar pagos recurrentes (recurrencias) con un token existente y válido.

Para más informaciones, consultar la descripción del método [Charge/CreateSubscription](#).

18.2. Dar de baja automáticamente una recurrencia por Web Services

Utilice el método **Subscription/Cancel** para dar de baja una recurrencia.

Para más informaciones, consultar la descripción del método [Subscription/Cancel](#).

18.3. Tarjetas de test

Las tarjetas de test están disponibles en la página de pago.

En función del escenario de test asociado a la tarjeta, permiten:

- crear un token y / o un pago recurrente únicamente si el resultado del test es "Pago aceptado".
- no crear token si el resultado de test es "Pago rechazado".

Para probar el comportamiento cuando se rechaza un vencimiento, debe utilizar la siguiente tarjeta de test:

Número de tarjeta	Caso de prueba verificado
4970101000001002	Creación de token OK - Pago rechazado debido al límite excedido si el monto del vencimiento es superior a 0.

Nota

Esta tarjeta no se propone en la página de pago al crear un token.