



Payment by token and recurring payment

Implementation Guide

Document version 3.15

Contents

1. HISTORY OF THE DOCUMENT.....	4
2. PRESENTATION OF THE SERVICE.....	8
2.1. Uniqueness of registered payment methods.....	9
3. COMPATIBLE PAYMENT METHODS.....	11
4. TOKEN SHARING.....	13
5. CHAINING OF CIT/MIT TRANSACTIONS.....	14
6. USE CASE.....	15
6.1. Creating a token without payment.....	16
6.2. Updating token details.....	18
6.3. Creating a token during a payment.....	20
6.4. Creating a token during a recurring payment.....	22
6.5. Creating a token upon the creation of a subscription with payment.....	25
6.6. Payment by token.....	28
6.7. Using a token to create a recurring payment.....	30
6.8. Payment with the token creation option for the cardholder.....	32
7. LIFECYCLE OF A RECURRING PAYMENT.....	34
8. LIFECYCLE OF A RECURRING PAYMENT WITH ANTICIPATED AUTHORIZATION.....	35
8.1. List of authorization request return codes.....	37
8.2. E-mail notification in case of installment rejection.....	39
9. OFFERING ADDITIONAL PAYMENT ATTEMPTS.....	40
10. ESTABLISHING INTERACTION WITH THE PAYMENT GATEWAY.....	41
10.1. Similarities with single payment.....	41
11. SETTING UP NOTIFICATIONS.....	42
11.1. Setting up the Instant Payment Notification.....	43
11.2. Setting up notifications in case of abandoned or canceled payments.....	44
11.3. Instant Payment Notification URL on an operation coming from the Back Office.....	45
11.4. Setting up a notification upon creating a recurring payment.....	46
11.5. Setting up a notification on batch authorization.....	47
11.6. Automatic retry in case of failure.....	48
11.7. Configuring e-mails sent to the buyer.....	50
12. GENERATING A PAYMENT FORM.....	51
12.1. Creating a 'Create a token without payment' form.....	53
12.2. Creating an 'Edit information associated with the token' form.....	53
12.3. Creating a 'Create a token during a payment' form.....	55
12.4. Creating a 'Create a token when making a recurring payment' form.....	56
12.5. 'Create of a token when creating a subscription with payment' form.....	58
12.6. Creating a 'Payment by token' form.....	60
12.7. Creating a 'Use a token to create a recurring payment' form.....	61
12.8. Creating a 'Payment with option for the cardholder to create a token' form.....	63
13. USING ADDITIONAL FEATURES.....	64
13.1. Defining a different amount for the first n installments.....	65
13.2. Defining the currency for creating or updating a token.....	65

14. COMPUTING THE SIGNATURE.....	67
15. SENDING THE PAYMENT REQUEST.....	69
15.1. Redirecting the buyer to the payment page.....	69
15.2. Processing errors.....	69
15.3. Managing timeouts.....	72
16. IMPLEMENTING THE IPN.....	73
16.1. Preparing your environment.....	74
16.2. Retrieving data returned in the response.....	75
16.3. Computing the IPN signature.....	76
16.4. Comparing signatures.....	77
16.5. Analyzing the nature of the notification.....	78
16.6. Processing the response data.....	79
16.6.1. Creating a token without payment.....	79
16.6.2. Updating token details.....	83
16.6.3. Creating a token during a payment.....	86
16.6.4. Creating a token during a recurring payment.....	90
16.6.5. Creating a token upon the creation of a subscription with payment.....	94
16.6.6. Payment by token.....	98
16.6.7. Creating a recurring payment.....	101
16.6.8. Payment with the token creation option for the cardholder.....	103
16.6.9. Installment payment.....	106
16.7. Running tests and troubleshooting.....	109
17. OBTAINING HELP.....	112
18. APPENDIX.....	113
18.1. Automatically creating a recurring payment via Web services.....	113
18.2. Automatically canceling a recurring payment via Web services.....	113
18.3. Test cards.....	113

1. HISTORY OF THE DOCUMENT

Version	Author	Date	Comment
3.15	BPCE Payment Services	5/19/2023	<ul style="list-style-type: none"> Update of the <i>Presentation of the service</i> chapter.
3.14.2	BPCE Payment Services	9/20/2022	<ul style="list-style-type: none"> Update of the <i>Presentation of the service</i> chapter Update the description of the vads_risk_assessment_result field values in the <i>Processing the response data</i> chapter.
3.14.1	BPCE Payment Services	5/25/2022	<ul style="list-style-type: none"> Added clarification on the amount of authentication in the different use cases.
3.14	BPCE Payment Services	4/26/2022	<ul style="list-style-type: none"> Added chapter <i>Suggesting additional payment attempts</i>. Added chapter <i>Chaining of CIT/MIT transactions</i>. Added the currency in the parameters to be transmitted when creating a token without payment. Updated use cases for displaying transaction chaining. Update of the chapter <i>Compatible payment methods</i>. Addition of vads_initial_issuer_transaction_identifier fields in the <i>Processing the response data</i> chapter.
3.13	BPCE Payment Services	2/10/2022	<ul style="list-style-type: none"> Update of the chapter <i>Compatible payment methods</i>. Update of chapters <i>Creating a token without payment</i>, <i>Creating a token during a payment</i>, <i>Creating a token during a recurring payment</i> and <i>Creating a token upon the creation of a subscription with payment</i>. Update of <i>Lifecycle of a recurring payment</i> chapter.
3.12	BPCE Payment Services	10/12/2021	<ul style="list-style-type: none"> Update of the vads_sub_effect_date field description.
3.11	BPCE Payment Services	3/1/2021	<ul style="list-style-type: none"> Addition of the vads_occurrence_type field in the <i>Lifecycle of a recurring payment</i> chapter. Addition of fields describing the recurrence in the chapters related to the notification upon the creation of a recurring payment. Addition of the <i>Installment payment</i> chapter. Update of the <i>Payment by token</i> chapter: the CVV entry and cardholder authentication are required. Update of the chapters related to token creation: the cardholder must undergo strong authentication.
3.10	BPCE Payment Services	1/18/2021	<ul style="list-style-type: none"> Update of the <i>Presentation of the service</i> chapter. Addition of the <i>Uniqueness of registered payment methods</i> chapter. Clarification on daily recurrences added to chapters related to recurring payment creation. Update of the chapter <i>Compatible payment methods</i>. Update of the chapter <i>Automatically canceling a recurring payment via Web Services</i>. Addition of the <i>Test cards</i> chapter in the appendix.
3.9	BPCE Payment Services	5/5/2020	<ul style="list-style-type: none"> Additional information on the attempts made by the payment gateway in case of activation of anticipated authorizations.

Version	Author	Date	Comment
			<ul style="list-style-type: none"> Additional details on payment creation in case of an expired payment method or purged payment data. Update of notification rule configuration.
3.8	BPCE Payment Services	10/21/2019	<ul style="list-style-type: none"> Update of compatible payment methods. Addition of a chapter on the payment guarantee during a payment by token. Update of the description of the vads_sub_desc field in the Generating a payment form chapter.
3.7	BPCE Payment Services	8/5/2019	<ul style="list-style-type: none"> The hash algorithm is now available via Settings > Shop, Keys tab. Addition of the vads_identifier field as an input parameter when creating a token. Addition of the Risk analysis details category in the Data dictionary. vads_threeds_auth_type: the field is always present in the response and can be empty. The hash algorithm is now available via Settings > Shop, Keys tab. Additional information provided on the computation of the IPN signature. Additional information provided on the format of the vads_trans_date and vads_presentation_date fields. Additional information provided on the format of the fields: 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: correction of field format (an..11) vads_contracts: Possibility to force the to be used.
3.6	BPCE Payment Services	5/22/2019	Clarifications provided on the methods of creation and termination of recurring payments via web services Terminal ID Data dictionary: update of vads_trans_date .
3.5	BPCE Payment Services	3/26/2019	<ul style="list-style-type: none"> Addition of a note on token creation via the Merchant Back Office Addition of a clarification on data deletion in the chapter Managing payments by identifier. Addition of the time of recurring payment creation in the chapter Managing payments by identifier. Update of screenshots in chapters Creating a token in Test mode and Creating a token in Production mode. Update of screenshots in Creating a recurring payment via the Merchant Back Office Addition of the chapter Defining the currency for creating or updating a token. Update of the table of parameters in the chapter Creating a "Payment with the token creation option for the cardholder" form. Data dictionary: <ul style="list-style-type: none"> Clarification added about the format of the vads_product_qty field.

Version	Author	Date	Comment
			<ul style="list-style-type: none"> • Addition of the vads_presentation_date field in the Transaction details section. • Clarification added about the format of the vads_identifier field. • Clarification added about the format of the vads_subscription field. • Removal of the fields 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 and vads_risk_primary_warranty.
3.4.1	BPCE Payment Services	3/19/2019	<ul style="list-style-type: none"> • Creation of a "Verification" transaction when requesting an update or creating tokens without payment via the Merchant Back Office. • New value for the vads_trans_status : ACCEPTED field. • New value for the vads_operation_type field: VERIFICATION
3.4	BPCE Payment Services	1/14/2019	<p>Addition of chapters:</p> <ul style="list-style-type: none"> • Creating a token in Test mode via the Merchant Back Office • Creating a token via the Merchant Back Office • Payment with the token creation option for the cardholder • Creating a 'Payment with option for the cardholder to create a token' form • Redraft of chapter Analyzing the payment result. • Data dictionary: <ul style="list-style-type: none"> • Addition of the vads_bank_label field. • Addition of the vads_tax_rate field. • Addition of the vads_pretax_amount field. • Addition of the vads_totalamount_vat field. • Addition of the vads_wallet field. • Update of the vads_ship_to_legal_name field description. • Update of the vads_payment_src field description. • Update of the values in the vads_bank_product field. • Update of the vads_tax_amount field description.

This document and its contents are confidential. It is not legally binding. Any reproduction and / or distribution of all or part of this document or its content to a third party is strictly prohibited or subject to prior written authorization from BPCE Payment Services. All rights reserved.

2. PRESENTATION OF THE SERVICE

Management of payments by token

The payment by token management service allows merchants to offer their buyer the possibility to associate a token with a payment method, which will facilitate their subsequent payments on the website (no more need to re-enter the credit card number).

Tokens allow you to:

- Make fast and secure payments.

The buyer no longer has to fill in bank details when making subsequent payments (1-click payment).

The gateway stores the bank details in a highly secure environment, in accordance with the PCI-DSS requirements. Only the token is transferred during the exchange.

- Make recurring payments (subscriptions).



Token are usable by all the shops of the same company.

The service also allows you to:

- Identify cards that are due to expire, in order to notify the Merchant via a file containing the token of the expiring card.
- Update the bank details associated with a token via the payment page, or manually via the Merchant Back Office.
- Automatically detect if the payment method has expired and offer an update in case of payment by token.
- When creating a token, detect if the payment method has been previously registered.
- Manage other buyer detail updates.



In compliance with the banking data security and protection rules implemented by PCI DSS, the payment method details are destroyed after the associated token has not been used for 15 months.

The token will remain visible in the Merchant Back Office and can be updated with new details.

Recurring payment (subscription) management

The recurring payment management service allows merchants to create subscriptions with **fixed amounts and payment schedule**, also known as “recurring payments”, with or without an expiry date, within the limits of the card validity period.

When creating a recurring payment, the merchant defines the start date, the amount of the installments and the recurrence rule to apply.

Once the start date (also known as the “effective date”) has been reached, the payment gateway automatically processes the installments.

After that, the merchant can no longer edit the amount of the installment payments.

To be notified of the result of a deadline, the **Instant Payment Notification URL when creating a recurring payment** rule must be activated and configured from the Merchant Back Office (menu **Settings > Notification rules**).

In TEST mode, the transaction corresponding to the first installment is created no later than 1 hour after the subscription, according to the schedule determined by the subscription rule.

In PRODUCTION mode, transactions are created once a day between midnight and 5:00 am, in the Europe/Paris time zone.

2.1. Uniqueness of registered payment methods

By default, the gateway authorizes the buyer to register their payment method several times on the merchant website.

However, if the merchant wants to, they can enable an option via their Merchant Back Office that will allow them to detect when a token is created, if the payment method has been previously registered.



It is not recommended to enable the uniqueness check of the registered payment method if you do not control its impact on your implementation.

- [Operating principle](#)
- [What should I do if a duplicate payment method is detected?](#)
- [Activation of the payment method uniqueness detection](#)

Operating principle

Once the option is activated, the gateway verifies the validity of the payment method with the issuer each time a token is created, and then proceeds to verify the uniqueness of the payment method.

If the payment method has never been registered, then a new token associated with this payment method is created and its identifier is returned to the merchant website upon the end of payment notification.

If the payment method has already been registered (same number and expiration date), then an existing token is used and its identifier is returned to the merchant website upon the end of payment notification.

The returned buyer's data is the same as the data transmitted by the merchant, and not the same as the details of the previously registered token.

The field **vads_identifier_status** is set to **CREATED**, even if in this case no token is created.

The notification then contains an additional field set to **true**:

- **vads_identifier_previously_registered** for the notification in the Hosted Payment Form format.
- **paymentMethodTokenPreviouslyRegistered** for the notification in the REST API format.



- There is no detection of payment method uniqueness during the token update.
- If the payment method is already associated with several tokens, the end of payment notification contains the identifier of the most recent token.
- The creation of a token via Merchant Back Office is refused if the payment method is already associated with another token.
- The **vads_identifier_previously_registered** field is not returned upon return to shop.
- The **vads_identifier_previously_registered** field is never returned in the end of payment notification if no duplicate payment methods are detected. Therefore, the **false** value is never sent to the merchant website.

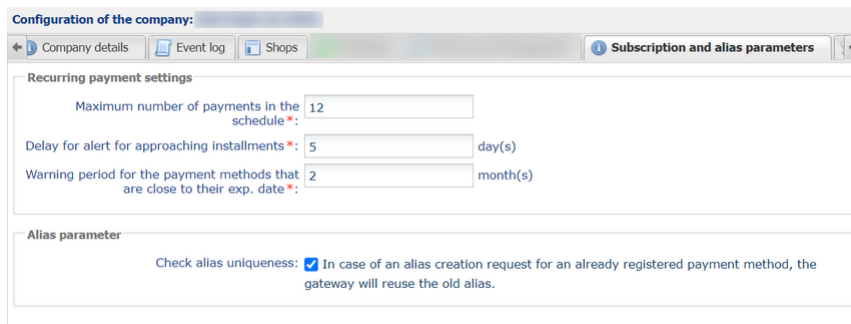
What should I do if a duplicate payment method is detected?

It depends on your business requirements.

- You can decide to do nothing and provide the service or deliver the goods to the buyer.
- You can check whether the customer code associated with the existing token matches the buyer's customer code. If this is not the case, you can search if a family tie between the two customers explains why the same payment method is used by two different customers.
- You can check if the person requesting the registration of the payment method is the same person who has already registered this payment method (e.g. by checking their contact details, e-mail address, country etc.).
- If all the controls put in place fail, that means that you might be a victim of fraud and can then decide to cancel the payment.

Activation of the payment method uniqueness detection

1. Via the Merchant Back Office, go to **Settings > Company**, then click on the **Subscription and alias parameters** tab.



The screenshot shows the 'Configuration of the company' window with the 'Subscription and alias parameters' tab selected. It contains two main sections: 'Recurring payment settings' and 'Alias parameter'.

Recurring payment settings:

- Maximum number of payments in the schedule *: 12
- Delay for alert for approaching installments *: 5 day(s)
- Warning period for the payment methods that are close to their exp. date *: 2 month(s)

Alias parameter:

Check alias uniqueness: ☒ In case of an alias creation request for an already registered payment method, the gateway will reuse the old alias.

2. In the **Alias parameter** section, check the **Check alias uniqueness** box.
3. Click the **Save** button to save the changes.

3. COMPATIBLE PAYMENT METHODS

List of payment methods compatible with Payment by token Management Service:

Network code	Payment method	Card types (vads_payment_cards)	Supports payment by token
ACCORD	Illicado Gift Card	ILICADO	✗
ACCORD	Jouéclub gift card	JOUECLUB_CDX	✗
ACCORD	Accord brand card	ACCORD_STORE	✗
ACCORD_SANDBOX	JouéClub gift card - Sandbox mode	ILICADO_SB	✗
ACCORD_SANDBOX	JouéClub gift card - Sandbox mode	JOUECLUB_CDX_SB	✗
AMEX	American Express	AMEX	✓
AMEXGLOBAL	American Express	AMEX	✓
AUORE	Cpay card	AUORE-MULTI	✗
CB	CB bank card	CB	✓
CB	CADO gift card	CA_DO_CARTE	✗
CB	Maestro	MAESTRO	✗
CB	Mastercard	MASTERCARD	✓
CB	Apetiz Meal Voucher card	APETIZ	✓
CB	Chèque Déjeuner Meal Voucher card	CHQ_DEJ	✓
CB	1st generation Mastercard Meal Voucher card	EDENRED	✓
CB	Sodexo Meal Voucher card	SODEXO	✓
CB	e-Carte Bleue virtual card	E-CARTEBLEUE	✓
CB	Visa	VISA	✓
CB	Visa Electron	VISA_ELECTRON	✓
CB	Visa Vpay	VPAY	✓
COFINOGA	BeSmart Cofinoga card	COFINOGA	✗
CONECS	Apetiz Meal Voucher card	APETIZ	✓
CONECS	Chèque Déjeuner Meal Voucher card	CHQ_DEJ	✓
CONECS	Conecs Meal Voucher card	CONECS	✓
CONECS	Sodexo Meal Voucher card	SODEXO	✓
CVCONNECT	Chèque-Vacances Connect	CVCO	✗
GATECONEX	Bancontact	BANCONTACT	✗
GATECONEX	Diners Club	DINERS	✓
GATECONEX	Discover	DISCOVER	✓
GATECONEX	e-Carte Bleue virtual card	E-CARTEBLEUE	✓
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	✓

Network code	Payment method	Card types (vads_payment_cards)	Supports payment by token
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	✗
GIROPAY	GIROPAY wire transfer	GIROPAY	✗
GOOGLEPAY	Google Pay wallet payment	GOOGLEPAY	✗
IDEAL	iDEAL wire transfer	IDEAL	✗
JCB	JCB	JCB	✓
MASTERPASS	Payment by Masterpass wallet	MASTERPASS	✗
ONEY_API	Oney 3x 4x payment	ONEY_3X_4X	✗
ONEY_API	Payment 10x 12x Oney	ONEY_10X_12X	✗
ONEY_API	Payment Oney Pay Later	ONEY_PAYLATER	✗
ONEY_API	Oney partner brand cards	ONEY_ENSEIGNE	✗
ONEY_API_SANDBOX	Oney 3x 4x payment (Sandbox mode)	ONEY_3X_4X	✗
ONEY_API_SANDBOX	Oney 10x 12x payment (Sandbox mode)	ONEY_10X_12X	✗
ONEY_API_SANDBOX	Payment Oney Pay Later (Sandbox mode)	ONEY_PAYLATER	✗
ONEY_API_SANDBOX	Oney partner brand cards in Sandbox mode	ONEY_ENSEIGNE	✗
ONEY_API_SB	Oney payment in 3 or 4 installments - Sandbox mode	ONEY_3X_4X	✗
PAYPAL	Payment by PayPal	PAYPAL	✓
PAYPAL_SB	Payment by PayPal - Sandbox mode	PAYPAL_SB	✓
PLANET_DCC	Mastercard	MASTERCARD	✓
PLANET_DCC	Visa	VISA	✓
POSTFINANCEV2	Payment by PostFinance Card	POSTFINANCE	✗
POSTFINANCEV2	Efinance PostFinance wire transfer	POSTFINANCE_EFIN	✗
SOFORT	Sofort wire transfer	SOFORT_BANKING	✗

* Subject to availability via your financial institution

4. TOKEN SHARING

It is possible to share tokens between several legal entities.

Tokens shared between several legal entities have to be unique and must be generated by the payment gateway.

However, this feature is subject to conditions. Please contact the customer service of your payment gateway to know the details.

5. CHAINING OF CIT/MIT TRANSACTIONS

The second Payment Services Directive (PSD2) introduced the need to authenticate the cardholder when initiating an e-commerce transaction.

It then becomes essential to identify whether the payment request is initiated:

- by the buyer:

CIT (Customer Initiated Transaction): buyer-initiated transaction with buyer interaction.

E.g.: payment (or card registration) that requires card data entry or cardholder authentication.

- or by the merchant:

MIT (Merchant Initiated Transaction): transaction initiated by the merchant, without the presence of the buyer, linked to an initial **CIT** transaction.

E.g.: umpteenth installment of a payment in installments or of a recurrent payment.

A new principle appears for the following transaction authentications: **operation chaining**.

In the context of a **CIT** transaction, regulations require a cardholder authentication. In response to the request for authorization or information, the issuer returns a unique transaction identifier, hereafter referred to as the “chaining reference”. This chaining reference is then used in the **MIT** transactions to indicate to the issuer that the transaction is part of a series of payments, for which the cardholder authenticated him or herself in the first payment.

Without this information, the issuer can refuse an **MIT** transaction for lack of authentication (soft decline).

6. USE CASE

The payment form allows to make the following operations classified according to different cases.

Each of these cases corresponds to a different value of the **vads_page_action** field.

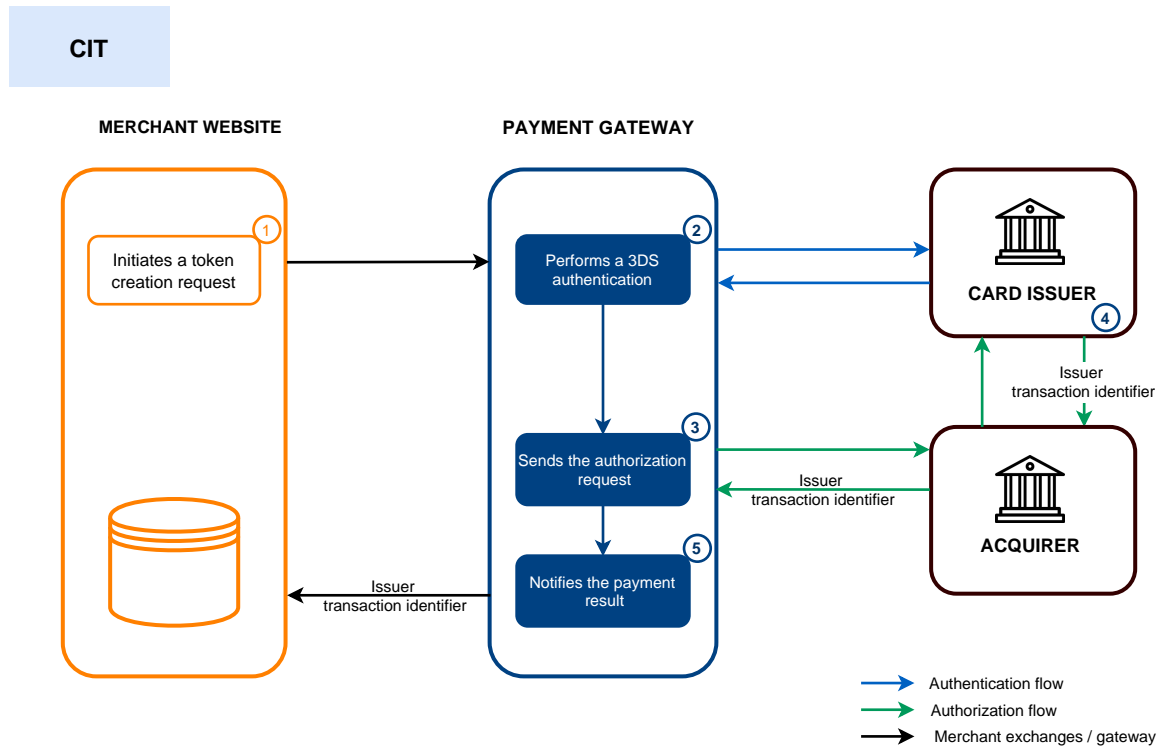
Use case	Value of the vads_page_action field
Creating a token without payment	REGISTER
Updating information associated with the token	REGISTER_UPDATE
Creating a token during a payment	REGISTER_PAY
Creating a token during a recurring payment	REGISTER_SUBSCRIBE
Creating a token upon the creation of a subscription with payment	REGISTER_PAY_SUBSCRIBE
Payment by token	PAYMENT
Using a token to create a recurring payment	SUBSCRIBE
Payment with the token creation option for the cardholder	ASK_REGISTER_PAY

Depending on the use case (valuation of the **vads_page_action** field), the interactions between the buyer and the payment page will be different.

6.1. Creating a token without payment

This case corresponds to a simple token creation.

Simplified diagram



1. The merchant site submits a *alias creation request*.

Note for stores with the "Currency Conversion" option:

The currency is mandatory when creating an alias.

Only contracts that support the currency passed in parameter will be selected. Currency conversion is therefore not taken into account.

E.g.: For an alias creation request in USD currency, on a shop associated with an AMEX contract and a CB contract:

if the AMEX contract only supports USD and the CB contract only supports EUR, then only AMEX cards will be accepted for the alias creation.

The buyer selects the payment method to be registered, enters their payment method details and confirms the entry.

2. The payment gateway initiates the cardholder's authentication process with the issuer.

Regulations require strong authentication for this use case.

Authentication is performed for an amount of EURO.

3. Once the authentication is completed, the gateway proceeds with the registration request by providing the cardholder's authentication details.
4. The issuer generates a unique transaction identifier and transmits it in the response to the registration request.

5. The payment gateway notifies the merchant website about the *result*.

The response contains:

- the unique transaction identifier generated by the issuer, for information purposes,
- the newly created token.



This operation results in the creation of a VERIFICATION type transaction, visible in the Merchant Back Office and possessing the following characteristics:

- its amount is 1.00 EUR or 0 EUR if supported by the acquirer,
- its status is either "Accepted" or "Refused",
- it is never captured and remains in the "Transactions in progress" tab.



The token will not be created if the authorization or information request is rejected.

The gateway displays the receipt to the buyer. It contains:

- the newly created token,
- the buyer details.

If you have configured the corresponding notification rules, the buyer will receive an e-mail with:

- the banking details registration confirmation on the payment gateway of the shop,
- the buyer's token that they can later use for another financial operation.



The issuer transaction identifier is stored by the payment gateway at the level of the alias.

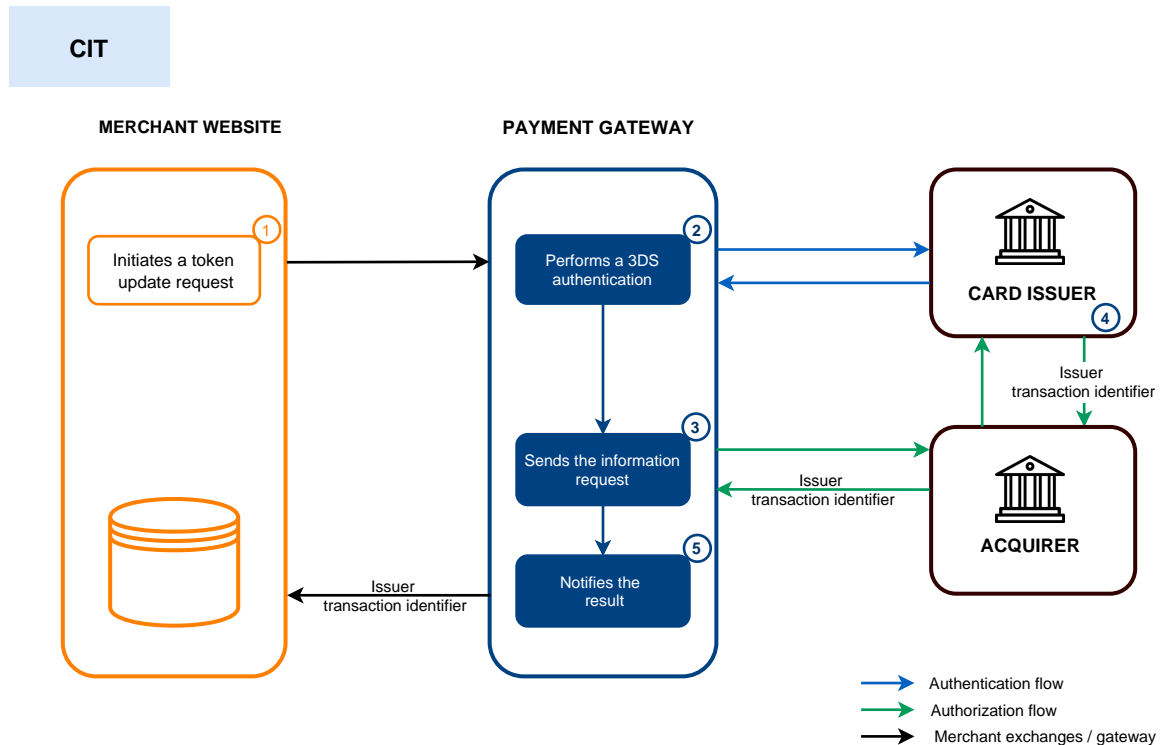
Depending on how you use the alias (1-click payment, 0-click payment, recurring payment, etc.) the gateway will use the issuer transaction ID as the default chaining reference if necessary.

In this use case, the way the chaining reference is handled is transparent to the merchant.

6.2. Updating token details

This case corresponds to updating, at the initiative of the buyer, the information related to his or her payment method and/or his or her personal information.

Simplified diagram



1. The merchant site submits a *alias update request*.

The buyer selects the payment method to be registered, enters their payment method details and confirms the entry.

2. The payment gateway initiates the cardholder's authentication process with the issuer.



Regulations require strong authentication for each card registration.
Authentication is performed for an amount of EURO.

3. Once the authentication is completed, the gateway proceeds with the registration request by providing the cardholder's authentication details.
4. The issuer generates a unique transaction identifier and transmits it in the response to the registration request.
5. The payment gateway notifies the merchant website about the *result*.

The response contains:

- the unique transaction identifier generated by the issuer, for information purposes,
- the updated alias.



This operation results in the creation of a VERIFICATION type transaction, visible in the Merchant Back Office and possessing the following characteristics:

- its amount is 1.00 EUR or 0 EUR if supported by the acquirer,
- its status is either "Accepted" or "Refused",

- it is never captured and remains in the "Transactions is progress" tab.



The token will not be updated if the authorization or information request is rejected.

The gateway displays the receipt to the buyer. It contains:

- token,
- the buyer details.

If you have configured the corresponding notification rules, the buyer will receive an e-mail with:

- the banking details registration confirmation on the payment gateway of the shop,
- the buyer's token that they can later use for another financial operation.



The issuer transaction identifier stored at the level of the alias is replaced by the identifier that is generated by the issuer upon the alias update.

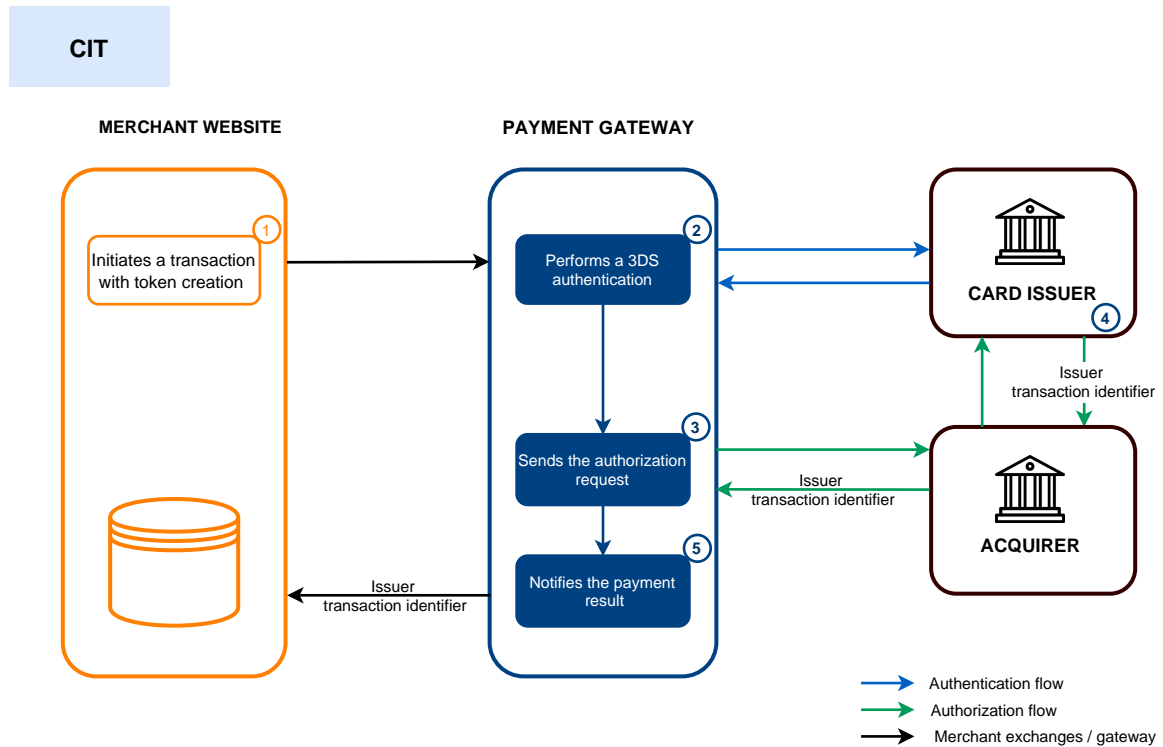
Depending on how you use the alias (1-click payment, 0-click payment, recurring payment, etc.) the issuer transaction ID will be used as a chaining reference if necessary.

Similarly to the alias creation, the way the chaining reference is handled is transparent to the merchant.

6.3. Creating a token during a payment

In this case, the parameters necessary for registration are completed by the parameters required for a payment request.

Simplified diagram



1. The merchant site submits a *payment request with alias creation*.

Note for stores with the "Currency Conversion" option



As soon as a payment is made at the time of the order, the currency conversion is authorized. Currency conversion is therefore supported for this operation, unlike the creation of an alias with or without subscription.

The buyer selects the payment method to be registered, enters their payment method details and confirms the entry.

2. The payment gateway initiates the cardholder's authentication process with the issuer.



Regulations require strong authentication for this use case. Authentication is performed for the payment amount.

3. Once the authentication is completed, the gateway proceeds with the authorization request by providing the cardholder's authentication details.
4. The issuer generates a unique transaction identifier and transmits it in the response to the authorization request.
5. The payment gateway notifies the merchant website about the *result*.

The response contains:

- the payment result,

- the unique transaction identifier generated by the issuer, for information purposes,
- the newly created token.



The token will not be created if the authorization or information request is rejected.

The gateway displays the receipt to the buyer. It contains:

- the payment result,
- the newly created token.

If you have configured the corresponding notification rules, the buyer will receive an e-mail with:

- the payment receipt,
- the banking details registration confirmation on the payment gateway of the shop,
- the buyer's token that they can later use for another financial operation.



The issuer transaction identifier is stored by the payment gateway at the level of the alias and the transaction.

Depending on how you use the alias (1-click payment, 0-click payment, recurring payment, etc.) the gateway will use the issuer transaction ID as the default chaining reference if necessary.

In case the merchant duplicates (**MIT**) the transaction created on the day of the order, the gateway automatically uses this identifier as a chaining reference.

In this use case, the way the chaining reference is handled is transparent to the merchant.

6.4. Creating a token during a recurring payment

In addition to the information used in the case of **Creating a token without making a payment**, this use case must also include information related to the recurring payment, such as:

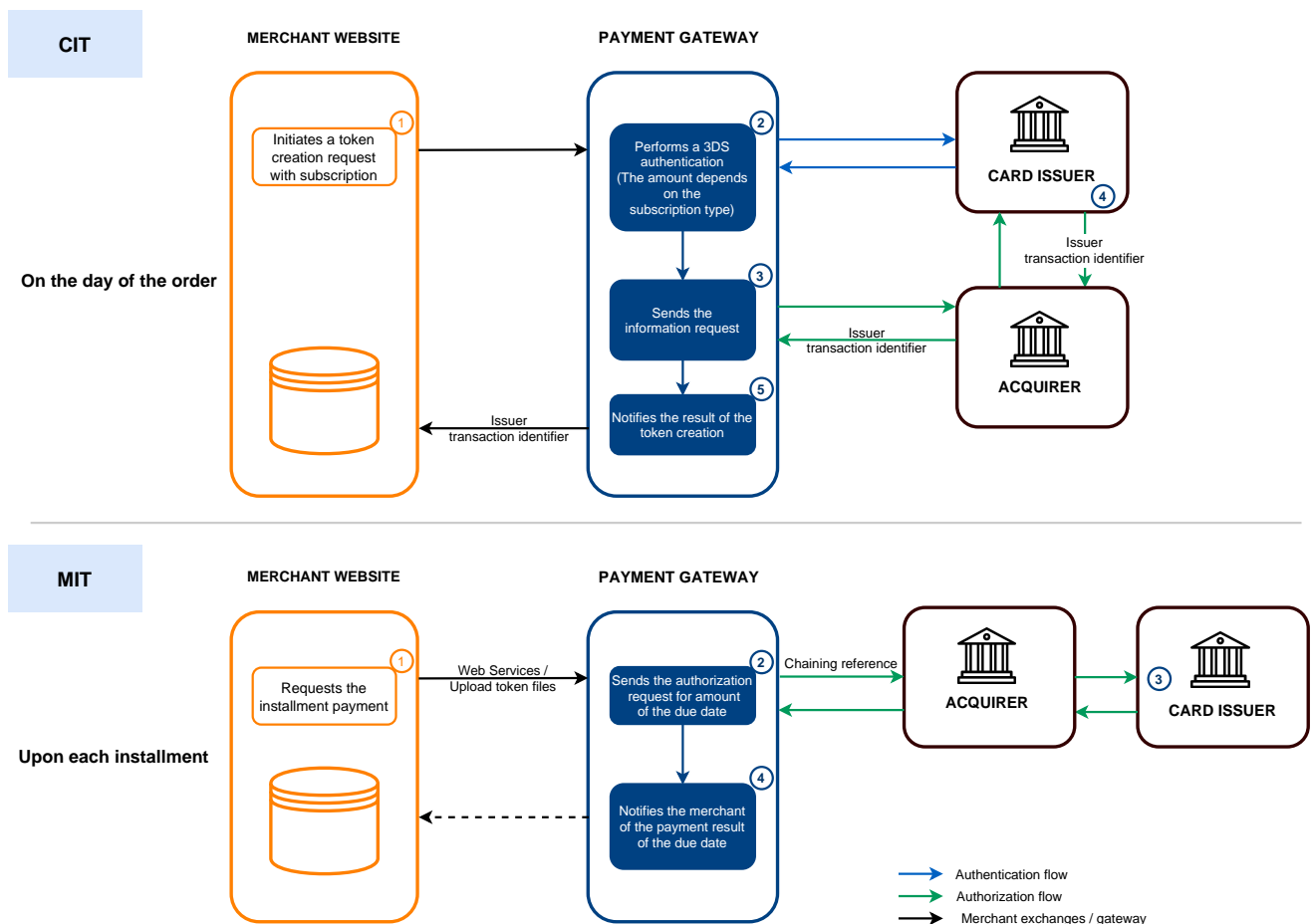
- the initial amount of the recurring payment (amount used for the first installment/s) if it is different (optional),
- the amount of the recurring payment (amount of installments or the amount used for the following installments when the first one is different).



No payments will be made during the subscription. Only an information request will be made in order to validate the payment method details.

The first payment will be made once the due date is reached, between 12 a.m. and 5 a.m.

Simplified diagram



On the day of the order:

1. The merchant site submits a *request to create an alias and subscribe to a recurring payment*.

Note for stores with the "Currency Conversion" option:



The currency is mandatory when creating an alias.

Only contracts that support the currency passed in parameter will be selected. Currency conversion is therefore not taken into account.

E.g.: For an alias creation request in USD currency, on a shop associated with an AMEX contract and a CB contract:

if the AMEX contract only supports USD and the CB contract only supports EUR, then only AMEX cards will be accepted for the alias creation.

The buyer selects the payment method that they would like to register, enters their payment method details and confirms the entry.

2. The payment gateway initiates the cardholder's authentication process with the issuer.



- Regulations require strong authentication for this use case.
- Authentication is performed for the amount of the first installment.

3. Once the authentication is completed, the gateway proceeds with the registration request by providing the cardholder's authentication details.
4. The issuer generates a unique transaction identifier and transmits it in the response to the registration request.
5. The payment gateway notifies the merchant website about the *result*.

The response contains:

- the unique transaction identifier generated by the issuer, for information purposes,
- the newly created token,
- the recurring payment details.



This operation results in the creation of a VERIFICATION type transaction, visible in the Merchant Back Office and possessing the following characteristics:

- its amount is 1.00 EUR or 0 EUR if supported by the acquirer,
- its status is either "Accepted" or "Refused",
- it is never captured and remains in the "Transactions in progress" tab.



The token will not be created if the authorization or information request is rejected.

The gateway displays the receipt to the buyer. It contains:

- the newly created token,
- the amounts of the recurring payment.

If you have configured the corresponding notification rules, the buyer will receive an e-mail with:

- the banking details registration confirmation on the payment gateway of the shop,
- the confirmation of the recurring payment registration.



The issuer transaction identifier is stored by the payment gateway at the level of the alias.

Depending on how you use the alias (1-click payment, 0-click payment, recurring payment, etc.) the gateway will use the issuer transaction ID as the default chaining reference if necessary.

Upon each installment:

1. The payment gateway performs an authorization request for the installment amount, providing the initial transaction identifier (ITC) as a chaining reference.
2. The issuer recognizes the transaction as a **MIT** that is part of a series of payments for which the cardholder has previously authenticated themselves and proceeds with the authorization request.

The transaction will not be rejected for lack of authentication (soft decline).

3. If the merchant has enabled the notification rule **Instant Payment Notification URL when creating recurring payments**, the payment gateway notifies the merchant site of the [payment result](#).



In this use case, the way the chaining reference is handled is transparent to the merchant.

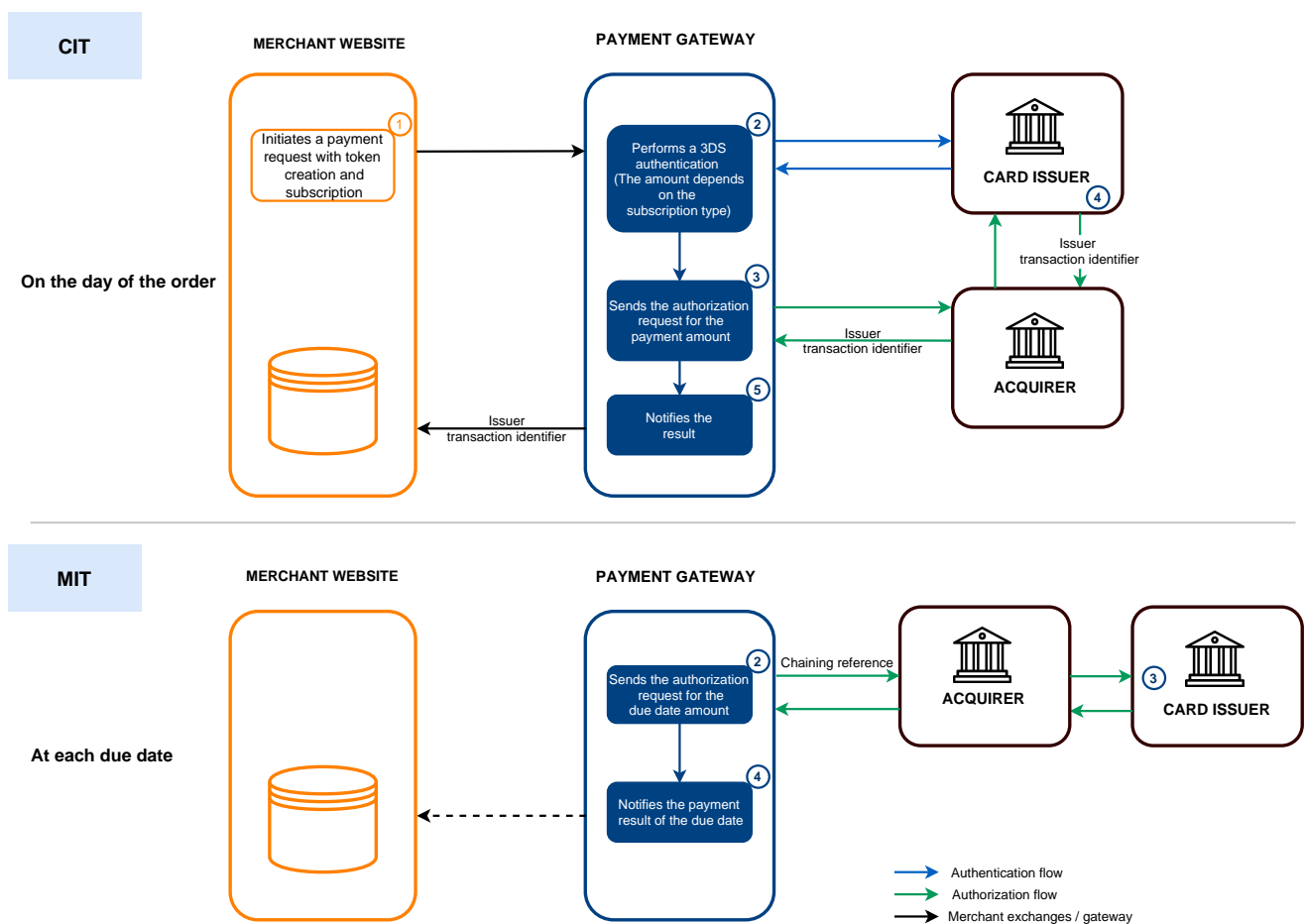
6.5. Creating a token upon the creation of a subscription with payment

In this use case, the following information must be visible:

- the buyer details,
- the transaction identifier,
- the recurring payment details (amounts).

Example: a recurring payment of X EUR/ over N months with commission fees to be paid upon taking the order.

Simplified diagram



On the day of the order:

1. The merchant site submits a *request to create an alias and subscribe to a recurring payment with immediate payment*.



Note for stores with the "Currency Conversion" option

As soon as a payment is made at the time of the order, the currency conversion is authorized.

Currency conversion is therefore supported for this operation, unlike the creation of an alias with or without subscription.

The buyer selects the payment method to be registered, enters their payment method details and confirms the entry.

2. The payment gateway initiates the cardholder's authentication process with the issuer.



- Regulations require strong authentication for this use case.
- Authentication is performed for the amount of the first installment.

3. Once the authentication is completed, the gateway proceeds with the authorization request by providing the cardholder's authentication details.
4. The issuer generates a unique transaction identifier and transmits it in the response to the authorization request.
5. The payment gateway notifies the merchant website about the *result*.

The response contains:

- the payment result,
- the recurring payment details,
- the unique transaction identifier generated by the issuer, for information purposes,
- the newly created token.



The alias (token) and subscription will not be created if the authorization request is refused.

The gateway displays the ticket to the buyer. It contains:

- the payment result,
- the recurring payment amounts,
- the newly created token.

If you have configured the corresponding notification rules, the buyer will receive an e-mail with:

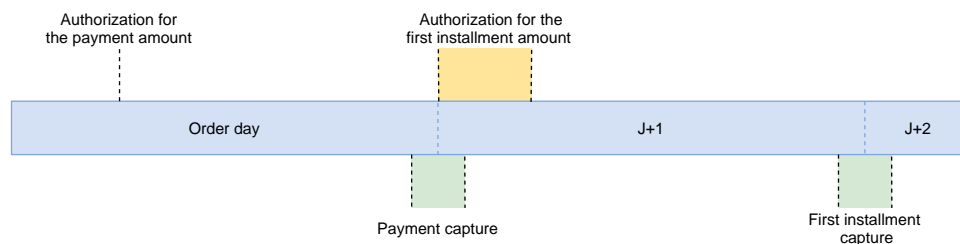
- the payment receipt,
- the banking details registration confirmation on the payment gateway of the shop,
- the confirmation of the recurring payment registration.
- the buyer's token that they can later use for another financial operation.



The buyer will be debited with the payment amount on the day of the order (or the day after, depending on the buyer).

The first installment of the subscription will be debited once the effective date is reached, between 00:00 and 05:00.

If the effective date is scheduled on the day of the order, the buyer will be debited 2 days in a row (on D for the payment and on D+1 for the first installment).



If you want the payment made on the day of the order to correspond to the first installment of the recurring payment, you must change the effective date. For example, for a monthly subscription, set the effective date to D+30 when requesting the creation of a recurring payment.

Upon each installment:

1. The payment gateway performs an authorization request for the installment amount, providing the initial transaction identifier (ITC) as a chaining reference.
2. The issuer recognizes the transaction as a **MIT** that is part of a series of payments for which the cardholder has previously authenticated themselves and proceeds with the authorization request.
The transaction will not be rejected for lack of authentication (soft decline).
3. If the merchant has enabled the notification rule **Instant Payment Notification URL when creating recurring payments**, the payment gateway notifies the merchant site of the [payment result](#).



The issuer transaction identifier is stored by the payment gateway at the level of the alias and the transaction.

Depending on how you use the alias (1-click payment, 0-click payment, recurring payment, etc.) the gateway will use the issuer transaction ID as the default chaining reference if necessary.

In case the merchant duplicates (**MIT**) the transaction created on the day of the order, the gateway automatically uses this identifier as a chaining reference.

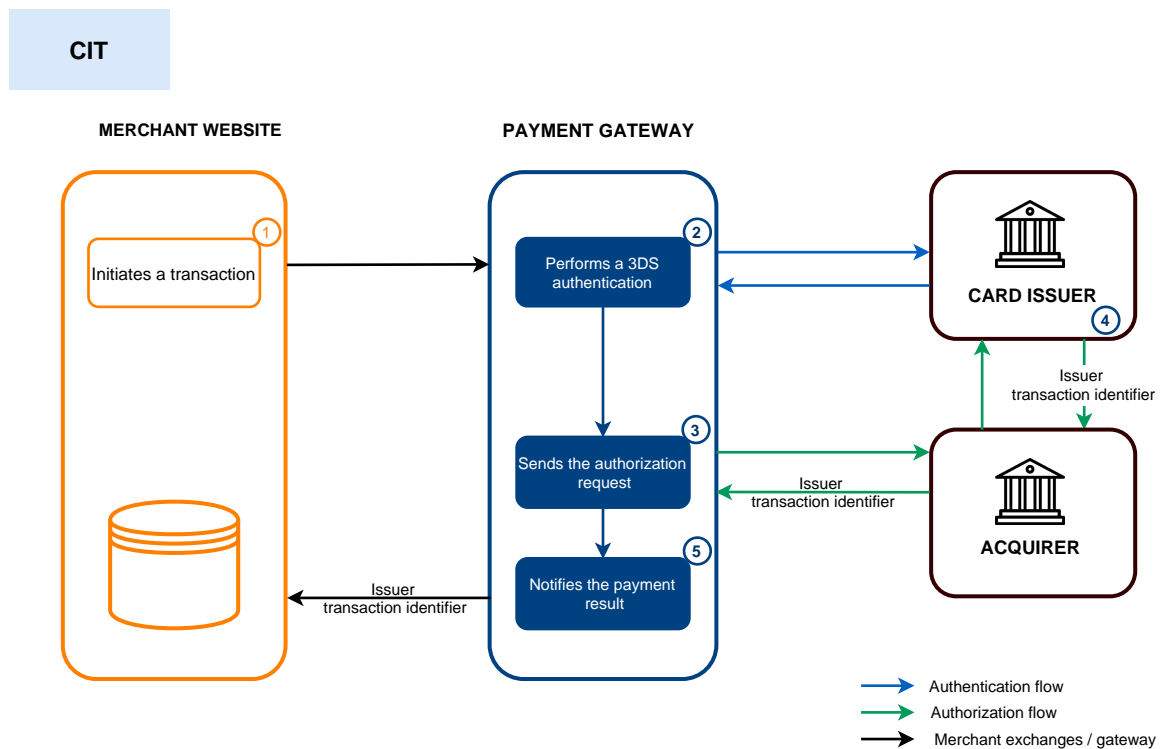
In this use case, the way the chaining reference is handled is transparent to the merchant.

6.6. Payment by token

Payment by token allows to use a pre-registered token for making single or multiple payments without having to select a payment method and enter banking details.

In this case, a simple confirmation step is presented with a summary of the transaction (number and amount).

Simplified diagram



1. The merchant site submits a *payment request with reusing an alias*.

The buyer checks the information displayed on the payment page, enters the CVV of their card and confirms.



When the token is associated with an expired payment method, the gateway automatically suggests to the buyer to enter the new banking details in order to perform the payment and update the associated token.

2. The payment gateway initiates the cardholder's authentication process with the issuer.



For this use case, regulations require the CVV to be entered and the holder to be authenticated.

Authentication is performed for the payment amount.

3. Once the authentication (challenge or frictionless) is completed, the gateway proceeds with the authorization request by providing the cardholder's authentication details.
4. The issuer generates a unique transaction identifier and transmits it in the response to the authorization request.
5. The payment gateway notifies the merchant website about the *result*.

The gateway displays the receipt to the buyer.

If you have configured the corresponding notification rules, the buyer will receive an e-mail with payment confirmation.



The issuer transaction ID is stored by the payment gateway.

In case the merchant duplicates (*MIT*) the transaction, the gateway will automatically use this identifier as a chaining reference.

In this use case, the way the chaining reference is handled is transparent to the merchant.

6.7. Using a token to create a recurring payment

Once a token has been created, it is possible to add one or several additional recurring payments that will use this token.

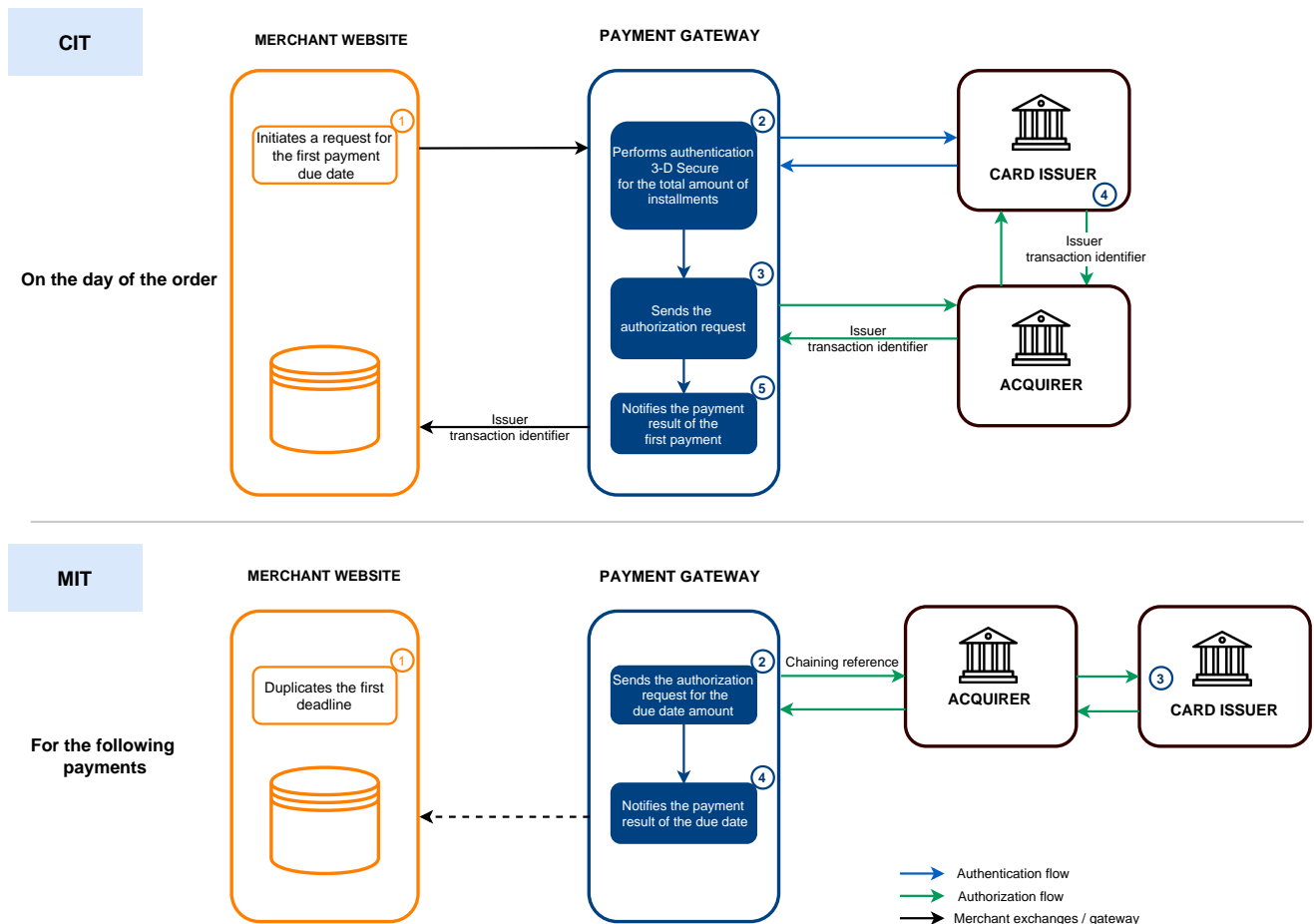
After a new recurring payment has been created, no banking detail entry will be requested. Only a confirmation on the buyer's part will be needed.



No payments will be made during the subscription. Only an information request will be made in order to validate the payment method details.

The first payment will be made once the due date is reached, between 12 a.m. and 5 a.m.

Simplified diagram



On the day of the order:

1. The merchant site submits a *subscription request using an existing alias*.

The buyer checks the recurring payment details and confirms.

2. The payment gateway notifies the merchant website about the *result*.

The gateway displays the receipt to the buyer. Among other things, it contains the recurring payment amounts.

If you have configured the corresponding notification rules, the buyer will receive an e-mail with the confirmation of the recurring payment registration.

Upon each installment:

1. The payment gateway performs an authorization request for the installment amount, providing the initial transaction identifier (ITC) as a chaining reference.
2. The issuer recognizes the transaction as a **MIT** that is part of a series of payments for which the cardholder has previously authenticated themselves and proceeds with the authorization request.

The transaction will not be rejected for lack of authentication (soft decline).

3. If the merchant has enabled the notification rule **Instant Payment Notification URL when creating recurring payments**, the payment gateway notifies the merchant site of the *payment result*.

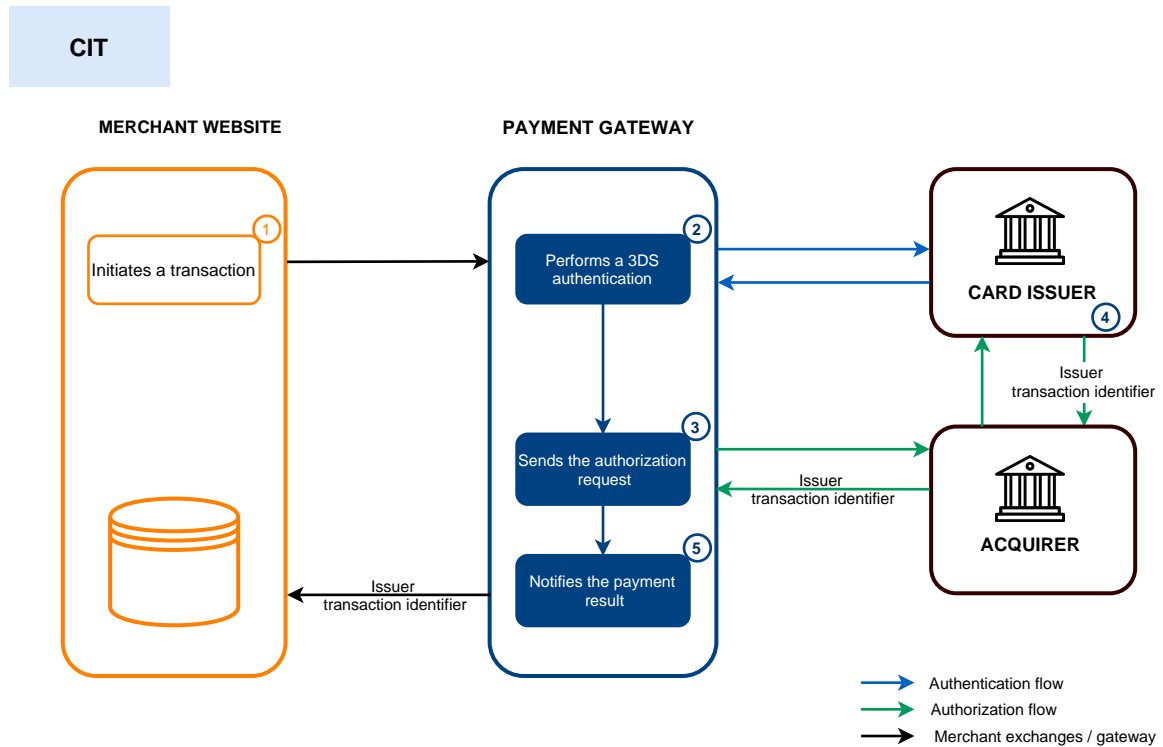


In this use case, the way the chaining reference is handled is transparent to the merchant.

6.8. Payment with the token creation option for the cardholder

At the moment of payment, the buyer has the possibility to remember the bank details for later by ticking the corresponding checkbox. This completely secure operation facilitates future purchases for the buyer.

Simplified diagram



1. The merchant site submits a *payment request*.

The buyer selects the payment method to register and enters their payment method details.

The buyer can check a box to give their consent for their payment method to be registered by the payment gateway. By default, this checkbox is unchecked.

2. The payment gateway initiates the cardholder's authentication process with the issuer.



If the buyer has checked the box, a payment method alias is created. Strong authentication is required by regulations.

Otherwise, the buyer is subject to authentication with or without interaction.

Regardless of the buyer's choice, authentication is performed for the payment amount.

3. Once the authentication is completed, the gateway proceeds with the authorization request by providing the cardholder's authentication details.

4. The issuer generates a unique transaction identifier and transmits it in the response to the authorization request.

5. The payment gateway notifies the merchant website about the *result*.



The token will not be created if the authorization or information request is rejected.

The gateway displays the receipt to the buyer. It contains:

- the payment result,
- the potentially created token.

If you have configured the corresponding notification rules, the buyer will receive an e-mail with:

- the payment receipt,
- the banking details registration confirmation on the payment gateway of the shop,
- the buyer's token that they can later use for another financial operation.



The issuer transaction identifier is stored by the payment gateway at the level of the alias and the transaction.

Depending on how you use the alias (1-click payment, 0-click payment, recurring payment, etc.) the gateway will use the issuer transaction ID as the default chaining reference if necessary.

In case the merchant duplicates (**MIT**) the transaction created on the day of the order, the gateway automatically uses this identifier as a chaining reference.

In this use case, the way the chaining reference is handled is transparent to the merchant.

7. LIFECYCLE OF A RECURRING PAYMENT

The recurring payment starts on its effective date.

The payment gateway starts creating payments following the schedule determined by the recurring payment rule sent in the form of recurring payment creation (vads_sub_desc field).

As part of the application of the PSD2, the payment gateway transmits a chaining reference in the authorization request, in order to avoid refusals for lack of authentication (soft decline).

Upon each installment, if the **Instant Payment Notification URL when creating a recurring payment** rule is enabled and correctly configured, the merchant website will receive the payment result via their notification URL (IPN).

The notification contains:

- The **vads_subscription** field that indicates the recurring payment reference.
- The **vads_recurrence_number** field that indicates the installment number.
- The **vads_occurrence_type** field that indicates the installment in question (first, nth or last installment).
- The **vads_trans_status** field that indicates the payment status (accepted or refused).

If the payment has been refused:

- the merchant will not be notified by e-mail,
- the payment will not be automatically presented once again.

If the payment method has reached its expiry date, a refused transaction is created without a call to the issuing bank. The error details (vads_payment_error) are set to 8 - The card expiration date does not allow this action.

If the payment method data has been purged following 15 months of inactivity, a refused transaction is created without a call to the issuing bank. The error description (vads_payment_error) is set to 107 - The payment method associated with the token is no longer valid.

Special case of daily recurrences

If you request the creation of a recurring payment to debit the payment method holder daily (RRULE:FREQ=DAILY;INTERVAL=1), and the requested effective date (vads_sub_effect_date) corresponds to the recurring payment creation date, then when the payment gateway processes this recurring payment the following morning (between midnight and 5a.m.), 2 payments will be created:

- The payment from the previous day (that corresponds to the effective date)
- And the payment from the current day

To avoid this, it is recommended to transmit an effective date on the day after the recurring payment is created.

8. LIFECYCLE OF A RECURRING PAYMENT WITH ANTICIPATED AUTHORIZATION

Thanks to this option, when a payment is rejected for a non-fraud related motive (see chapter [List of authorization request return codes](#)), the payment gateway can automatically make another daily authorization request up to two days before the expected capture date at the bank.

As soon as the option is enabled for the shop, recurring payments are created 6 days before the date anticipated by the recurring payment rule.

It is necessary to enable the **Instant Payment Notification URL on batch authorization** rule via your Merchant Back Office (see chapter [Setting up a notification on batch authorization](#)).

D-6: Creating a recurring payment

- The authorization request is accepted.
 - The payment status will remain **Waiting for capture** until the initially scheduled date.
 - A call to the notification URL will be triggered if the **Instant Payment Notification URL when creating a recurring payment** rule is enabled. The request will contain the following values:

Field name	Value
vads_url_check_src	REC
vads_trans_status	AUTHORISED

- The authorization request is rejected for a fraud-related reason.
 - The payment is definitively **Refused**.
 - A call to the notification URL will be triggered if the **Instant Payment Notification URL when creating a recurring payment** rule is enabled. The request will contain the following values:

Field name	Value
vads_url_check_src	REC
vads_trans_status	REFUSED

- The authorization request is rejected for a non fraud-related reason.
 - The payment status will remain **Waiting for authorization**.
 - A call to the notification URL will be triggered if the **Instant Payment Notification URL when creating a recurring payment** rule is enabled. The request will contain the following values:

Field name	Value
vads_url_check_src	REC
vads_trans_status	WAITING_AUTHORISATION

D-5, D-4, D-3: New authorization request triggered automatically

- The authorization request is accepted.
 - The payment status will remain **Waiting for capture** until the initially scheduled date.
 - A call to the notification URL will be triggered if the **Instant Payment Notification URL on batch authorization** rule is enabled. In this case, the request will contain the following values:

Field name	Value
vads_url_check_src	BATCH_AUTO
vads_trans_status	AUTHORISED

- The authorization request is rejected for a fraud-related reason.
 - The payment is definitively **Refused**.
 - A call to the notification URL will be triggered if the **Instant Payment Notification URL on batch authorization** rule is enabled. In this case, the request will contain the following values:

Field name	Value
vads_url_check_src	BATCH_AUTO
vads_trans_status	REFUSED

- The authorization request is rejected for a non fraud-related reason.
 - The payment status will remain **Waiting for capture** until the scheduled date.
 - A call to the notification URL will be triggered if the **Instant Payment Notification URL on batch authorization** rule is enabled. In this case, the request will contain the following values:

Field name	Value
vads_url_check_src	BATCH_AUTO
vads_trans_status	WAITING_AUTHORISATION

D-2: Last authorization request triggered automatically

- The authorization request is accepted.
 - The payment status will remain **Waiting for capture** until the initially scheduled date.
 - A call to the notification URL will be triggered if the **Instant Payment Notification URL on batch authorization** rule is enabled. In this case, the request will contain the following values:

Field name	Value
vads_url_check_src	BATCH_AUTO
vads_trans_status	AUTHORISED

- The authorization request is rejected (regardless of the reason).
 - The payment is definitively **Refused**.
 - A call to the notification URL will be triggered if the **Instant Payment Notification URL on batch authorization** rule is enabled. In this case, the request will contain the following values:

Field name	Value
vads_url_check_src	BATCH_AUTO
vads_trans_status	REFUSED

D: Capture of the transaction

The payment is automatically captured.

No calls to the Notification URL will be triggered.

Notes

- *Payment rejection between D-6 and D-2*

When the payment is definitively rejected, you must make sure that the access to the service for which the recurring payment was created is canceled on the scheduled date and not on the day when the payment rejection was received.

- *Cancellation of the recurring payment*

When the buyer cancels their recurring payment, the merchant must cancel the already scheduled payments.

8.1. List of authorization request return codes

The return codes of the authorization request are returned by the issuing bank (if available).

Value	Description	Authorized Retry
00	Approved or successfully processed transaction	
02	Contact the card issuer	
03	Invalid acceptor	YES
04	Keep the card	YES
05	Do not honor	YES
07	Keep the card, special conditions	YES
08	Confirm after identification	
12	Incorrect Transaction Code	YES
13	Invalid amount	YES
14	Invalid cardholder number	YES
15	Unknown issuer	YES
17	Canceled by the buyer	
19	Retry later	
20	Incorrect response (error on the domain server)	
24	Unsupported file update	
25	Unable to locate the registered elements in the file	
26	Duplicate registration, the previous record has been replaced	
27	File update edit error	
28	Denied access to file	
29	Unable to update	
30	Format error	
31	Unknown acquirer company ID	YES
33	Expired card	YES
34	Suspected fraud	YES
38	Expired card	
41	Lost card	YES
43	Stolen card	YES
46	Customer account closed	
51	Insufficient balance or exceeded credit limit	
54	Expired card	YES
55	Incorrect secret code	
56	Card absent from the file	YES
57	Transaction not allowed for this cardholder	YES
58	Transaction not allowed for this cardholder	
59	Suspected fraud	YES
60	The acceptor of the card must contact the acquirer	
61	Withdrawal limit exceeded	
63	Security rules unfulfilled	YES
65	Exceeded number of withdrawals	
68	Response not received or received too late	
75	Number of attempts for entering the secret code has been exceeded	
76	The cardholder is already blocked, the previous record has been saved	YES
78	Transaction blocked, first transaction on card not properly unblocked	
80	Contactless payment is not accepted by the issuer	
81	Unsecured payment is not accepted by the issuer	
82	CVV, dCVV, iCVV incorrect	
83	Revocation of all recurring payments for the card	

Value	Description	Authorized Retry
84	R1 - Revocation of recurring payment for the card of a specific Merchant or for the MCC and the card	
86	6P - Failure of the issuer to verify the data	
90	Temporary shutdown	
91	Unable to reach the card issuer	
94	Duplicate transaction	
96	System malfunction	
97	Overall monitoring timeout	
98	Server not available, new network route requested	
99	Initiator domain incident	

8.2. E-mail notification in case of installment rejection

Case of the option "Anticipated authorization"

When a payment is declined, a notification e-mail is sent to the merchant.

9. OFFERING ADDITIONAL PAYMENT ATTEMPTS

When a payment is refused, you have the possibility to offer the buyer to make another attempt with another payment method.

The number of additional attempts can be configured via the Merchant Back Office:

1. Go to **Settings > Shop**, then click on the name of the shop for which the configuration must be changed.
2. Select **Configuration**.
3. Enter the authorized number of additional attempts in case of a rejected payment.

If you configure 2 additional attempts, the buyer will be able to make 3 payment attempts in total.

4. If you wish, you can configure an IPN that will be sent upon each rejected attempt by checking **Instant Payment Notification URL on a declined attempt**.
5. Click **Save**.



Additional attempts are not offered:

- If the merchant has requested to automatically return to the shop via the **vads_redirect_error_timeout** field,
- If the payment is an installment payment,



Additional payment attempts and payment by token (1-Click).

If 1-Click payment is declined, the buyer will be prompted to choose a new payment method and enter their card details.

If the payment is accepted:

- the transaction will not be associated with the token transmitted in the request,
- the token will not be updated.

10. ESTABLISHING INTERACTION WITH THE PAYMENT GATEWAY

The merchant website and the payment gateway interact by exchanging data.

To create a payment, this data is sent in an HTML form via the buyer's browser.

At the end of the payment, the result is transmitted to the merchant website in two ways:

- Automatically by means of notifications called Instant Notification URLs (also called IPN or Instant Payment Notification), see chapter **Setting up notifications**.
- Via the browser, when the buyer clicks the button to return to the merchant website, see chapter **Managing the return to the merchant website**.

To guarantee the security of the exchange, the data is signed with a key known only to the merchant and the payment gateway.

10.1. Similarities with single payment

All the functionalities available for single payments are also available for payments by token and for recurring payments.

For more information, see the *Implementation Guide Hosted Payment Page*

Here is a non-exhaustive list:

- Single payment, completed in one transaction, or split payment.
- Management of several currencies.
- Management of several payment methods and associated MIDs.
- Payment page customization.
- Display in an iframe.

11. SETTING UP NOTIFICATIONS

The Merchant Back Office provides several types of notifications.

- Instant Payment Notification URL call
- E-mail sent to the merchant
- E-mail sent to the buyer
- SMS sent to the merchant
- SMS sent to the buyer

They allow to manage the events (payment accepted, payment abandoned by the buyer, payment canceled by the merchant, etc.) that will trigger a notification sent to the merchant website, the merchant or the buyer.



The notifications of Instant Payment Notification URL call type are very important as they represent the only reliable way for the merchant website to obtain the payment result.

If the payment gateway is unable to access the URL of your page, an e-mail will be sent to the shop administrator.

It contains:

- The HTTP code of the encountered error
- Parts of error analysis
- Its consequences
- Instructions via the Merchant Back Office to resend the request to the previously defined URL.

To access notification rule management:

Go to the following menu **Settings > Notification rules**.

Instant Payment Notification		<input checked="" type="checkbox"/> E-mail sent to the merchant	<input checked="" type="checkbox"/> E-mail sent to the buyer
Enabled	Reference		
✗	Instant Payment Notification URL on batch authorization		
✓	Instant Payment Notification URL at the end of the payment		
✗	Instant Payment Notification URL on batch change		
✗	Instant Payment Notification URL on cancellation		
✗	Instant Payment Notification URL on an operation coming from the Back Office		

11.1. Setting up the Instant Payment Notification

This rule allows to notify the merchant website in the following cases:

- Payment accepted
- Payment refused
- Token creation or update
- Creation of a recurring payment



This notification is required for communicating the result of a payment request, token or recurring payment creation.

It will inform the merchant website of the result even if the buyer has not clicked the “Return to the shop” button.

1. Right-click **Instant Payment Notification URL at the end of the payment**.
2. Select **Manage the rule**.
3. Enter the **E-mail address(es) to notify in case of failure** field in the **General settings** section.
To specify several e-mail addresses, separate them with a semi-colon.
4. Check the box **Automatic retry in case of failure** if you wish to authorize the gateway to automatically resend the notification in case of a failure (can be done up to 4 times).
For more information, please see chapter [Automatic retry in case of failure](#) on page 48.
5. In the **Instant Payment Notification URL of the API form V1, V2** section, specify the URL of your page in the fields **URL to notify in TEST mode** and **URL to notify in PRODUCTION mode** if you wish to receive notifications in the API form format.
6. Save the changes.

11.2. Setting up notifications in case of abandoned or canceled payments

This rule allows to notify the merchant website in the following cases:

- When the buyer abandons/cancels a payment - via the **Cancel and return to shop** button.
- When the buyer has not completed the payment and the payment session has expired.

The maximum length of a payment session is 10 minutes.

This rule is **disabled by default**.

1. Right-click **Instant Payment Notification URL on cancellation**.
2. Select **Manage the rule**.
3. Enter the **E-mail address(es) to notify in case of failure** field in the **General settings** section.
To specify several e-mail addresses, separate them with a semi-colon.
4. Check the box **Automatic retry in case of failure** if you wish to authorize the gateway to automatically resend the notification in case of a failure (can be done up to 4 times).
For more information, please see chapter [Automatic retry in case of failure](#) on page 48.
5. In the **Instant Payment Notification URL of the API form V1, V2** section, specify the URL of your page in the fields **URL to notify in TEST mode** and **URL to notify in PRODUCTION mode** if you wish to receive notifications in the API form format.
6. In the **REST API Instant Payment Notification URL** section, specify the URL of your page in the fields **Target URL of the IPN to notify in TEST mode** and **Target URL of the IPN to notify in PRODUCTION mode** if you are using the JavaScript client.
7. Save the changes.
8. Enable the rule by right-clicking **Instant Payment Notification URL on cancellation** and select **Enable the rule**.

11.3. Instant Payment Notification URL on an operation coming from the Back Office

This rule allows to notify the merchant website about every operation made via the Merchant Back Office:

- Creation of a manual payment (accepted or rejected)
- Transaction update
- Transaction duplication
- Transaction refund
- Transaction cancellation
- Transaction validation
- Token creation
- Token update

1. Right-click **Instant Payment Notification URL on an operation coming from the Back Office**.
2. Select **Manage the rule**.
3. Enter the **E-mail address(es) to notify in case of failure** field in the **General settings** section.
To specify several e-mail addresses, separate them with a semi-colon.
4. Check the box **Automatic retry in case of failure** if you wish to authorize the gateway to automatically resend the notification in case of a failure (can be done up to 4 times).
For more information, please see chapter [Automatic retry in case of failure](#) on page 48.
5. In the **Instant Payment Notification URL of the API form V1, V2** section, specify the URL of your page in the fields **URL to notify in TEST mode** and **URL to notify in PRODUCTION mode** if you wish to receive notifications in the API form format.
6. In the **REST API Instant Payment Notification URL** section, specify the URL of your page in the fields **Target URL of the IPN to notify in TEST mode** and **Target URL of the IPN to notify in PRODUCTION mode** if you are using the JavaScript client.
7. Save the changes.
8. Enable the rule by right-clicking **Instant Payment Notification URL on an operation coming from the Back Office** and select **Enable the rule**.

11.4. Setting up a notification upon creating a recurring payment

This rule allows to notify the merchant website in the following cases:

- When the payment gateway creates a new installment date of a recurring payment.
- Upon each new payment attempt, after a recurring payment installment has been refused.
Requires the activation of the anticipated authorization option.

This rule is **disabled by default**.

1. Right-click **Instant Payment Notification URL when creating a recurring payment**.
2. Select **Manage the rule**.
3. Enter the **E-mail address(es) to notify in case of failure** field in the **General settings** section.
To specify several e-mail addresses, separate them with a semi-colon.
4. Check the box **Automatic retry in case of failure** if you wish to authorize the gateway to automatically resend the notification in case of a failure (can be done up to 4 times).
For more information, please see chapter [Automatic retry in case of failure](#) on page 48.
5. In the **Instant Payment Notification URL of the API form V1, V2** section, specify the URL of your page in the fields **URL to notify in TEST mode** and **URL to notify in PRODUCTION mode** if you wish to receive notifications in the API form format.
6. In the **REST API Instant Payment Notification URL** section, specify the URL of your page in the fields **Target URL of the IPN to notify in TEST mode** and **Target URL of the IPN to notify in PRODUCTION mode** if you are using the JavaScript client.
7. Save the changes.
8. Enable the rule by right-clicking **Instant Payment Notification URL when creating a recurring payment** and select **Enable the rule**.

11.5. Setting up a notification on batch authorization

If the shop has the **Anticipated authorization** option, it is necessary to enable the **Instant Payment Notification URL on batch authorization** rule in order to receive the final payment result.

This rule is **disabled by default**.

1. Right-click **Instant Payment Notification URL on batch authorization**.
2. Select **Manage the rule**.
3. Enter the **E-mail address(es) to notify in case of failure** field in the **General settings** section.
To specify several e-mail addresses, separate them with a semi-colon.
4. Check the box **Automatic retry in case of failure** if you wish to authorize the gateway to automatically resend the notification in case of a failure (can be done up to 4 times).
For more information, please see chapter [Automatic retry in case of failure](#) on page 48.
5. In the **Instant Payment Notification URL of the API form V1, V2** section, specify the URL of your page in the fields **URL to notify in TEST mode** and **URL to notify in PRODUCTION mode** if you wish to receive notifications in the API form format.
6. In the **REST API Instant Payment Notification URL** section, specify the URL of your page in the fields **Target URL of the IPN to notify in TEST mode** and **Target URL of the IPN to notify in PRODUCTION mode** if you are using the JavaScript client.
7. Save the changes.
8. Enable the rule by right-clicking **Instant Payment Notification URL on batch authorization** and select **Enable the rule**.

11.6. Automatic retry in case of failure

Automatic retry does not apply to notifications manually triggered via the Merchant Back Office.

The merchant can enable a mechanism that allows the payment gateway to automatically return notifications when the merchant website is temporarily unavailable, **up to 4 times**.

A notification will be considered as failed if the HTTP code returned by the merchant site is not on the following list: **200, 201, 202, 203, 204, 205, 206, 301, 302, 303, 307, 308**.

Call attempts are scheduled at fixed intervals every 15 minutes (00, 15, 30, 45).

After each failed attempt, a notification e-mail is sent to the e-mail address specified in the configuration of the notification rule in question.

In this case, the subject of the e-mail contains the number corresponding to the notification retry attempt. It is presented as **attempt #** followed by the attempt number.

- Example of an e-mail subject following a first notification failure at the end of payment:

```
[MODE TEST] My Shop - Tr. ref. 067925 / FAILURE during the call to your IPN URL
[unsuccessful attempt #1]
```

- Example of an e-mail subject following a second failure:

```
[MODE TEST] My Shop - Tr. ref. 067925 / FAILURE during the call to your IPN URL
[unsuccessful attempt #2]
```

- Example of an e-mail subject following a third failure:

```
[MODE TEST] My Shop - Tr. ref. 067925 / FAILURE during the call to your IPN URL
[unsuccessful attempt #3]
```

- Example of an e-mail subject following the last failure:

```
[MODE TEST] My Shop - Tr. ref. 067925 / FAILURE during the call to your IPN URL
[unsuccessful attempt #last]
```

To notify the merchant website of the last notification attempt, the e-mail subject will contain the mention **attempt #last**.

During the automatic retry, certain details are not stored in the database or are modified.

Examples of fields not available/not registered in the database:

Field name	Description
vads_page_action	Completed operation
vads_payment_config	Payment type (immediate or installment).
vads_action_mode	Acquisition mode for payment method data.

Examples of fields sent with different values:

Field name	New value
vads_url_check_src	Always set to RETRY in case of automatic retry.
vads_trans_status	The transaction status may vary between the initial call and the automatic retry (cancellation by the merchant, transaction capture at the bank, etc.).
vads_hash	The value of this field is regenerated with each call.
signature	The signature value depends on the different statuses that may vary between the initial call and the automatic retry.

These e-mails contain:

- the encountered problem,
- parts of analysis depending on the error,
- its consequences,
- instructions for manually triggering the notification from the Merchant Back Office.



After the fourth attempt, it is still possible to retry the IPN URL **manually** via your Merchant Back Office.



Warning, during the automatic retry, any manual call to the IPN URL will affect the number of automatic attempts:

- a successful manual call will stop the automatic retry,
- a failed manual call will have no impact on the current automatic retry.

11.7. Configuring e-mails sent to the buyer



To use this service, please contact the E-commerce customer service to enable the necessary functions within your offer.

From the **E-mail sent to the buyer** tab:

1. Right-click the rule to be modified and select **Enable the rule**.
2. Right-click the rule again and select **Manage the rule**.
The rule management wizard appears.
3. In the General settings section, you can customize the label of the rule.
4. To customize the e-mail content:
 - a. Click **Buyer e-mail settings**.
 - b. Select the template of the e-mail to apply.
 - c. Select the language that you would like to update.
 - d. Click **Customize default text values** if you wish to edit the body and the subject of the "default" e-mail message.
 - e. Click on **Fields to include** to display the list of fields available for e-mail customization.
 - f. Select the fields that you wish to include. A detailed summary of the request processing will be added to the body of the e-mail.



To preview the changes, click **Preview the e-mail** at the bottom of the dialog box.

5. In order to change the events that trigger the notification:
 - a. Click the **Rule conditions** tab.
A condition is composed of a variable, a comparison operator and a reference value.
Example: "mode = TEST", "amount exceeding 1000". During the execution of a rule, the value of a variable is retrieved and compared to the reference value.
 - b. Double-click on an existing condition to edit it.
 - c. Click **Add** to create a new condition.
All the conditions must be validated for the rule to be executed.
6. Click **Save**.

In case your offer already comprises the feature of payment confirmation by e-mail and you have already configured it, we recommend to confirm payments by e-mail using the new functionality called "Advanced notifications" that can be entirely customized and configured. For this, make sure you delete the first configured rule in order to avoid sending two confirmations to your buyer..

12. GENERATING A PAYMENT FORM

To generate a payment request, you must create an HTML form as follows:

```
<form method="POST" action="https://paiement.systempay.fr/vads-payment/">
  <input type="hidden" name="parameter1" value="value1" />
  <input type="hidden" name="parameter2" value="value2" />
  <input type="hidden" name="parameter3" value="value3" />
  <input type="hidden" name="signature" value="signature"/>
  <input type="submit" name="pay" value="Pay"/>
</form>
```

It contains:

- The following technical elements:
 - The `<form>` and `</form>` tags that allow to create an HTML form.
 - The `method="POST"` attribute that defines the method used for sending data.
 - The `action="https://paiement.systempay.fr/vads-payment/"` attribute that defines where to send the form data.
- Form data:
 - The shop ID.
 - Information about the payment depending on the use case.
 - Additional information depending on your needs.
 - The signature that ensures the integrity of the form.

This data is added to the form by using the `<input>` tag:

```
<input type="hidden" name="parameter1" value="value1" />
```

For setting the `name` and `value` attributes, see the **Data dictionary** chapter also available in the online document archive.

All the data in the form must be encoded in **UTF-8**.

This will allow for the special characters (accents, punctuation marks, etc.) to be correctly interpreted by the payment gateway. Otherwise, the signature will be computed incorrectly and the form will be rejected.

- The **Pay** button for submitting the data:

```
<input type="submit" name="pay" value="Pay"/>
```

Different use cases are presented in the chapters below. They will allow you to adapt your payment form to your needs.

The following table lists the different formats that you can encounter when building your form.

Notation	Description
a	Alphabetic characters (from 'A' to 'Z' and from 'a' to 'z')
n	Numeric characters
s	Special characters
an	Alphanumeric characters
ans	Alphanumeric and special characters (except '<' and '>')
3	Fixed length of 3 characters
..12	Variable length up to 12 characters
json	<p>JavaScript Object Notation.</p> <p>Object containing key/value pairs separated by commas.</p> <p>It starts with a left brace "{" and ends with a right brace "}".</p> <p>Each key / value pair contains the name of the key between double-quotes followed by ":", followed by a value.</p> <p>The name of the key must be alphanumeric.</p> <p>The value can be:</p> <ul style="list-style-type: none"> • a chain of characters (in this case it must be framed by double-quotes) • a number • an object • a table • a boolean • empty <p>Example: {"name1":45,"name2":"value2", "name3":false}</p>
bool	Boolean. Can be populated with the true or false value.
enum	<p>Defines a field with a complete list of values.</p> <p>The list of possible values is given in the field definition.</p>
Enum list	<p>List of values separated by a ";".</p> <p>The list of possible values is given in the field definition.</p> <p>Example: vads_available_languages=fr;en</p>
map	<p>List of key / value pairs separated by a ";".</p> <p>Each key / value pair contains the name of the key followed by "=", followed by a value.</p> <p>The value can be:</p> <ul style="list-style-type: none"> • a chain of characters • a boolean • a json object • an xml object <p>The list of possible values for each key/value pair is provided in the field definition.</p> <p>Example: vads_theme_config=SIMPLIFIED_DISPLAY=true;RESPONSIVE_MODEL=Model_1</p>

12.1. Creating a 'Create a token without payment' form

Use case: creation of a token for making fast payments in the future.



Under PSD2, strong authentication is required when registering a card. The `vads_threeds_mpi` field is ignored and the `CHALLENGE_MANDATE` value is automatically applied.

1. Use all the fields presented in the table below to create your form.

Field name	Description	Format	Value
<code>vads_page_action</code>	Action to perform	enum	REGISTER
<code>vads_action_mode</code>	Acquisition mode for payment method data	enum	INTERACTIVE
<code>vads_currency</code>	Numeric currency code to be used for the payment, in compliance with the ISO 4217 standard (numeric code).	n3	E.g.: 978 for euro (EUR)
<code>vads_ctx_mode</code>	Mode of interaction with the payment gateway	enum	TEST or PRODUCTION
<code>vads_cust_email</code>	Buyer's e-mail address	ans..150	E.g.: abc@example.com
<code>vads_site_id</code>	Shop ID	n8	E.g.: 12345678
<code>vads_trans_date</code>	Date and time of the payment form in UTC format	n14	Respect the YYYYMMDDHHMMSS format E.g.: 20200101130025
<code>vads_version</code>	Version of the exchange protocol with the payment gateway	enum	V2
<code>signature</code>	Signature guaranteeing the integrity of the requests exchanged between the merchant website and the payment gateway.	ans..44	Compute the value of the signature field using all the fields of your form starting with <code>vads_</code> (see chapter Computing the signature).

2. Use the `vads_identifier` field if you wish to generate the identifier of the token associated with the payment method.

The token format must not be `ans..32`. This format is reserved for tokens generated by the payment gateway.

If you have activated the detection of token uniqueness, the value of the `vads_identifier` field transmitted in the form can be different from the one present in the notification if the payment method is already associated with another token.

3. Add optional fields according to your requirements (see chapter [Using additional features](#)).

The list of fields returned in the notification is described in the chapter [Creating a token without payment](#) on page 79.

12.2. Creating an 'Edit information associated with the token' form

Use case: update of bank information associated with a token.



Under PSD2, strong authentication is required when registering a card. The `vads_threeds_mpi` field is ignored and the `CHALLENGE_MANDATE` value is automatically applied.

1. Use all the fields presented in the table below to create your form.

Field name	Description	Format	Value
vads_page_action	Action to perform	enum	REGISTER_UPDATE
vads_ctx_mode	Mode of interaction with the payment gateway	enum	TEST or PRODUCTION
vads_cust_email	Buyer's e-mail address	ans..150	E.g.: abc@example.com
vads_action_mode	Acquisition mode for payment method data	enum	INTERACTIVE
vads_identifier	(unique) token associated with a payment method.	ans..50	E.g.: MyToken Note: two possible formats: <ul style="list-style-type: none"> an32: if the identifier is generated by the payment gateway ans..50: if the identifier is generated by the merchant.
vads_site_id	Shop ID	n8	E.g.: 12345678
vads_trans_date	Date and time of the payment form in UTC format	n14	Respect the YYYYMMDDHHMMSS format E.g.: 20200101130025
vads_version	Version of the exchange protocol with the payment gateway	enum	V2
signature	Signature guaranteeing the integrity of the requests exchanged between the merchant website and the payment gateway.	ans..44	Compute the value of the signature field using all the fields of your form starting with vads_ (see chapter Computing the signature).

2. Add optional fields according to your requirements (see chapter [Using additional features](#)).

The list of fields returned in the notification is described in the chapter [Updating token details](#) on page 83.

12.3. Creating a 'Create a token during a payment' form

Use case: creating a token during a payment.



Under PSD2, strong authentication is required when registering a card. The `vads_threeds_mpi` field is ignored and the `CHALLENGE_MANDATE` value is automatically applied.

1. Use all the fields presented in the table below to create your form.

Field name	Description	Format	Value
<code>vads_page_action</code>	Action to perform	enum	REGISTER_PAY
<code>vads_amount</code>	Payment amount in the smallest currency unit (cents for euro)	n..12	E.g.: 4525 for EUR 45.25
<code>vads_ctx_mode</code>	Mode of interaction with the payment gateway	enum	TEST or PRODUCTION
<code>vads_currency</code>	Numeric currency code to be used for the payment, in compliance with the ISO 4217 standard (numeric code).	n3	E.g.: 978 for euro (EUR)
<code>vads_cust_email</code>	Buyer's e-mail address	ans..150	E.g.: abc@example.com
<code>vads_action_mode</code>	Acquisition mode for payment method data	enum	INTERACTIVE
<code>vads_payment_config</code>	Payment type	enum	SINGLE
<code>vads_site_id</code>	Shop ID	n8	E.g.: 12345678
<code>vads_trans_date</code>	Date and time of the payment form in UTC format	n14	Respect the YYYYMMDDHHMMSS format E.g.: 20200101130025
<code>vads_trans_id</code>	Transaction number. Must be unique within the same day (from 00:00:00 UTC to 23:59:59 UTC). Warning: this field is not case sensitive.	an6	E.g.: xrT15p
<code>vads_version</code>	Version of the exchange protocol with the payment gateway	enum	V2
<code>signature</code>	Signature guaranteeing the integrity of the requests exchanged between the merchant website and the payment gateway.	ans..44	Compute the value of the signature field using all the fields of your form starting with vads_ (see chapter Computing the signature).

2. Use the `vads_identifier` field if you wish to generate the identifier of the token associated with the payment method.

The token format must not be an..32. This format is reserved for tokens generated by the payment gateway.

If you have activated the detection of token uniqueness, the value of the `vads_identifier` field transmitted in the form can be different from the one present in the notification if the payment method is already associated with another token.

3. Add optional fields according to your requirements (see chapter [Using additional features](#)).

The list of fields returned in the notification is described in the chapter [Creating a token during a payment](#) on page 86.

12.4. Creating a 'Create a token when making a recurring payment' form

Use case: subscription to a recurring payment with token creation.



Under PSD2, strong authentication is required when registering a card. The vads_threeds_mpi field is ignored and the CHALLENGE_MANDATE value is automatically applied.



No payments will be made during the subscription. Only a verification request will be made in order to validate the payment method details.

The first payment will be made once the due date is reached, between 12 a.m. and 5 a.m.

If you want the buyer to make the first installment at the moment of creating the recurring payment, see the following chapter: ['Create of a token when creating a subscription with payment' form on page 58.](#)

1. Use all the fields presented in the table below to create your form.

Field name	Description	Format	Value
vads_page_action	Action to perform	enum	REGISTER_SUBSCRIBE
vads_ctx_mode	Mode of interaction with the payment gateway	enum	TEST or PRODUCTION
vads_cust_email	Buyer's e-mail address	ans..150	E.g.: abc@example.com
vads_action_mode	Acquisition mode for payment method data	enum	INTERACTIVE
vads_site_id	Shop ID	n8	E.g.: 12345678
vads_sub_amount	Amount of installments (in the smallest currency unit) The amount of installments cannot be set to 0.	n..12	E.g.: 4525 for EUR 45.25
vads_sub_effect_date	Subscription start date (or effective date) in the UTC time zone, in YYYYMMDD format.	n8	E.g.: 20210601
vads_sub_currency	Code of the currency used for the recurring payment.	n3	E.g.: 978 for euro (EUR)
vads_sub_desc	<p>Rule for recurring payments to apply according to the iCalendar RFC5545 specification.</p> <p>If you request the creation of a recurring payment to debit the payment method holder daily (RRULE:FREQ=DAILY;INTERVAL and the requested effective date (vads_sub_effect_date) corresponds to the recurring payment creation date, then when the payment gateway processes this recurring payment the following morning (between midnight and 5a.m.), 2 payments will be created:</p> <ul style="list-style-type: none"> The payment from the previous day (that corresponds to the effective date) 	string	<p>Recurring payments can be made daily, weekly or monthly.</p> <p>It is possible to specify the number of the day or the month (e.g. "the 10th of the month", "every 3 months").</p> <p><i>Note: the string must not contain space characters.</i></p> <p>Examples:</p> <ul style="list-style-type: none"> In order to define a weekly recurring payment: <pre>RRULE:FREQ=WEEKLY</pre> In order to define a recurring payment every two weeks, on the same day and every 7 days: <pre>RRULE:FREQ=WEEKLY;INTERVAL=2</pre> To schedule installment payments on the last day of each month for 12 months: <pre>RRULE:FREQ=MONTHLY; BYMONTHDAY=28,29,30,31;</pre>

Field name	Description	Format	Value
	<ul style="list-style-type: none"> And the payment from the current day <p>To avoid this, it is recommended to transmit an effective date on the day after the recurring payment is created.</p>		<pre>BYSETPOS=-1;COUNT=12</pre> <ul style="list-style-type: none"> To schedule installment payments on the 10th of each month for 12 months: <pre>RRULE:FREQ=MONTHLY;COUNT=12;BYMONTHDAY=10</pre>
vads_trans_date	Date and time of the payment form in UTC format	n14	Respect the YYYYMMDDHHMMSS format E.g.: 20200101130025
vads_version	Version of the exchange protocol with the payment gateway	enum	V2
signature	Signature guaranteeing the integrity of the requests exchanged between the merchant website and the payment gateway.	ans..44	Compute the value of the signature field using all the fields of your form starting with vads_ (see chapter Computing the signature).



The **vads_sub_effect_date** time value must not be in the past.

2. Use the **vads_identifier** field if you wish to generate the identifier of the token associated with the payment method.

The token format must not be an..32. This format is reserved for tokens generated by the payment gateway.

If you have activated the detection of token uniqueness, the value of the **vads_identifier** field transmitted in the form can be different from the one present in the notification if the payment method is already associated with another token.

3. Add optional fields according to your requirements (see chapter [Using additional features](#)).

The list of fields returned in the notification is described in the chapter [Creating a token during a recurring payment](#) on page 90.

12.5. 'Create of a token when creating a subscription with payment' form

Use case: payment and creation of a recurring payment with token creation.



Under PSD2, strong authentication is required when registering a card. The vads_threeds_mpi field is ignored and the CHALLENGE_MANDATE value is automatically applied.

1. Use all the fields presented in the table below to create your form.

Field name	Description	Format	Value
vads_page_action	Action to perform	enum	REGISTER_PAY_SUBSCRIBE
vads_amount	Payment amount in the smallest currency unit (cents for euro)	n..12	E.g.: 4525 for EUR 45.25
vads_ctx_mode	Mode of interaction with the payment gateway	enum	TEST or PRODUCTION
vads_currency	Numeric currency code to be used for the payment, in compliance with the ISO 4217 standard (numeric code).	n3	E.g.: 978 for euro (EUR)
vads_cust_email	Buyer's e-mail address	ans..150	E.g.: abc@example.com
vads_action_mode	Acquisition mode for payment method data	enum	INTERACTIVE
vads_payment_config	Payment type	enum	SINGLE
vads_site_id	Shop ID	n8	E.g.: 12345678
vads_sub_amount	Amount of installments (in the smallest currency unit) The amount of installments cannot be set to 0.	n..12	E.g.: 4525 for EUR 45.25
vads_sub_currency	Code of the currency used for the recurring payment.	n3	E.g.: 978 for euro (EUR)
vads_sub_desc	<p>Rule for recurring payments to apply according to the iCalendar RFC5545 specification.</p> <p>If you request the creation of a recurring payment to debit the payment method holder daily (RRULE:FREQ=DAILY;INTERVAL and the requested effective date (vads_sub_effect_date) corresponds to the recurring payment creation date, then when the payment gateway processes this recurring payment the following morning (between midnight and 5a.m.), 2 payments will be created:</p> <ul style="list-style-type: none"> The payment from the previous day (that corresponds to the effective date) And the payment from the current day <p>To avoid this, it is recommended to transmit</p>	string	<p>Recurring payments can be made daily, weekly or monthly.</p> <p>It is possible to specify the number of the day or the month (e.g. "the 10th of the month", "every 3 months").</p> <p><i>Note: the string must not contain space characters.</i></p> <p>Examples:</p> <ul style="list-style-type: none"> In order to define a weekly recurring payment: <pre>RRULE:FREQ=WEEKLY</pre> In order to define a recurring payment every two weeks, on the same day and every 7 days: <pre>RRULE:FREQ=WEEKLY;INTERVAL=2</pre> To schedule installment payments on the last day of each month for 12 months: <pre>RRULE:FREQ=MONTHLY; BYMONTHDAY=28,29,30,31; BYSETPOS=-1;COUNT=12</pre>

Field name	Description	Format	Value
	an effective date on the day after the recurring payment is created.		<ul style="list-style-type: none"> To schedule installment payments on the 10th of each month for 12 months: <pre>RRULE:FREQ=MONTHLY; COUNT=12;BYMONTHDAY=10</pre>
vads_sub_effect_date	Subscription start date (or effective date) in the UTC time zone, in YYYYMMDD format.	n8	E.g.: 20210601
vads_trans_date	Date and time of the payment form in UTC format	n14	Respect the YYYYMMDDHHMMSS format E.g.: 20200101130025
vads_trans_id	Transaction number. Must be unique within the same day (from 00:00:00 UTC to 23:59:59 UTC). Warning: this field is not case sensitive.	an6	E.g.: xrT15p
vads_version	Version of the exchange protocol with the payment gateway	enum	V2
signature	Signature guaranteeing the integrity of the requests exchanged between the merchant website and the payment gateway.	ans..44	Compute the value of the signature field using all the fields of your form starting with vads_ (see chapter Computing the signature).



The **vads_sub_effect_date** time value must not be in the past.

2. Use the **vads_identifier** field if you wish to generate the identifier of the token associated with the payment method.

The token format must not be an..32. This format is reserved for tokens generated by the payment gateway.

If you have activated the detection of token uniqueness, the value of the **vads_identifier** field transmitted in the form can be different from the one present in the notification if the payment method is already associated with another token.

3. Add optional fields according to your requirements (see chapter [Using additional features](#)).

The list of fields returned in the notification is described in the chapter [Creating a token upon the creation of a subscription with payment](#) on page 94.

12.6. Creating a 'Payment by token' form

Use case: one-click payment (using an existing and valid token).



In the context of the application of the PSD2, the CVV entry as well as cardholder authentication are required during a payment by token, as long as the buyer is present. The `vads_threeds_mpi` field is taken into account to allow for potential authentication without buyer interaction.

1. Use all the fields presented in the table below to create your form.

Field name	Description	Format	Value
<code>vads_page_action</code>	Action to perform	enum	PAYMENT
<code>vads_amount</code>	Payment amount in the smallest currency unit (cents for euro)	n..12	E.g.: 4525 for EUR 45.25
<code>vads_ctx_mode</code>	Mode of interaction with the payment gateway	enum	TEST or PRODUCTION
<code>vads_currency</code>	Numeric currency code to be used for the payment, in compliance with the ISO 4217 standard (numeric code).	n3	E.g.: 978 for euro (EUR)
<code>vads_action_mode</code>	Acquisition mode for payment method data	enum	INTERACTIVE
<code>vads_identifier</code>	(unique) token associated with a payment method.	ans..50	E.g.: MyToken Note: two possible formats: <ul style="list-style-type: none"> an32: if the identifier is generated by the payment gateway ans..50: if the identifier is generated by the merchant.
<code>vads_payment_config</code>	Payment type	enum	SINGLE
<code>vads_site_id</code>	Shop ID	n8	E.g.: 12345678
<code>vads_trans_date</code>	Date and time of the payment form in UTC format	n14	Respect the YYYYMMDDHHMMSS format E.g.: 20200101130025
<code>vads_trans_id</code>	Transaction number. Must be unique within the same day (from 00:00:00 UTC to 23:59:59 UTC). Warning: this field is not case sensitive.	an6	E.g.: xrT15p
<code>vads_version</code>	Version of the exchange protocol with the payment gateway	enum	V2
<code>signature</code>	Signature guaranteeing the integrity of the requests exchanged between the merchant website and the payment gateway.	ans..44	Compute the value of the signature field using all the fields of your form starting with vads_ (see chapter Computing the signature).

2. Add optional fields according to your requirements (see chapter [Using additional features](#)).

The list of fields returned in the notification is described in the chapter [Payment by token](#) on page 98.

12.7. Creating a 'Use a token to create a recurring payment' form

Use case: using an existing and valid token to create a recurring payment.



No payments will be made during the subscription.

The first payment will be made once the due date is reached, between 12 a.m. and 5 a.m.

1. Use all the fields presented in the table below to create your form.

Field name	Description	Format	Value
vads_page_action	Action to perform	enum	SUBSCRIBE
vads_ctx_mode	Mode of interaction with the payment gateway	enum	TEST or PRODUCTION
vads_action_mode	Acquisition mode for payment method data	enum	INTERACTIVE
vads_identifier	(unique) token associated with a payment method.	ans..50	E.g.: MyToken Note: two possible formats: <ul style="list-style-type: none"> an32: if the identifier is generated by the payment gateway ans..50: if the identifier is generated by the merchant.
vads_site_id	Shop ID	n8	E.g.: 12345678
vads_sub_amount	Amount of installments (in the smallest currency unit) The amount of installments cannot be set to 0.	n..12	E.g.: 4525 for EUR 45.25
vads_sub_effect_date	Subscription start date (or effective date) in the UTC time zone, in YYYYMMDD format.	n8	E.g.: 20210601
vads_sub_currency	Code of the currency used for the recurring payment.	n3	E.g.: 978 for euro (EUR)
vads_sub_desc	Rule for recurring payments to apply according to the iCalendar RFC5545 specification. If you request the creation of a recurring payment to debit the payment method holder daily (RRULE:FREQ=DAILY;INTERVAL and the requested effective date (vads_sub_effect_date) corresponds to the recurring payment creation date, then when the payment gateway processes this recurring payment the following morning (between midnight and 5a.m.), 2 payments will be created: <ul style="list-style-type: none"> The payment from the previous day (that corresponds to the effective date) And the payment from the current day 	string	Recurring payments can be made daily, weekly or monthly. It is possible to specify the number of the day or the month (e.g. "the 10th of the month", "every 3 months"). Note: the string must not contain space characters. Examples: <ul style="list-style-type: none"> In order to define a weekly recurring payment: <pre>RRULE:FREQ=WEEKLY</pre> In order to define a recurring payment every two weeks, on the same day and every 7 days: <pre>RRULE:FREQ=WEEKLY;INTERVAL=2</pre> To schedule installment payments on the last day of each month for 12 months: <pre>RRULE:FREQ=MONTHLY; BYMONTHDAY=28,29,30,31;</pre>

Field name	Description	Format	Value
	To avoid this, it is recommended to transmit an effective date on the day after the recurring payment is created.		<pre>BYSETPOS=-1;COUNT=12</pre> <ul style="list-style-type: none"> To schedule installment payments on the 10th of each month for 12 months: <pre>RRULE:FREQ=MONTHLY;COUNT=12;BYMONTHDAY=10</pre>
vads_trans_date	Date and time of the payment form in UTC format	n14	Respect the YYYYMMDDHHMMSS format E.g.: 20200101130025
vads_version	Version of the exchange protocol with the payment gateway	enum	V2
signature	Signature guaranteeing the integrity of the requests exchanged between the merchant website and the payment gateway.	ans..44	Compute the value of the signature field using all the fields of your form starting with vads_ (see chapter Computing the signature).



The **vads_sub_effect_date** time value must not be in the past.

2. Add optional fields according to your requirements (see chapter [Using additional features](#)).

The list of fields returned in the notification is described in the chapter [Creating a recurring payment](#) on page 101.

12.8. Creating a 'Payment with option for the cardholder to create a token' form

Use case: offer the possibility to create a token during a payment.



Under PSD2, strong authentication is required when registering a card. The `vads_threeds_mpi` field is ignored and the `CHALLENGE_MANDATE` value is automatically applied.

1. Use all the fields presented in the table below to create your form.

Field name	Description	Format	Value
<code>vads_page_action</code>	Action to perform	enum	ASK_REGISTER_PAY
<code>vads_amount</code>	Payment amount in the smallest currency unit (cents for euro)	n..12	E.g.: 4525 for EUR 45.25
<code>vads_ctx_mode</code>	Mode of interaction with the payment gateway	enum	TEST or PRODUCTION
<code>vads_currency</code>	Numeric currency code to be used for the payment, in compliance with the ISO 4217 standard (numeric code).	n3	E.g.: 978 for euro (EUR)
<code>vads_cust_email</code>	Buyer's e-mail address	ans..150	E.g.: abc@example.com
<code>vads_action_mode</code>	Acquisition mode for payment method data	enum	INTERACTIVE
<code>vads_payment_config</code>	Payment type	enum	SINGLE
<code>vads_site_id</code>	Shop ID	n8	E.g.: 12345678
<code>vads_trans_date</code>	Date and time of the payment form in UTC format	n14	Respect the YYYYMMDDHHMMSS format E.g.: 20200101130025
<code>vads_trans_id</code>	Transaction number. Must be unique within the same day (from 00:00:00 UTC to 23:59:59 UTC). Warning: this field is not case sensitive.	an6	E.g.: xrT15p
<code>vads_version</code>	Version of the exchange protocol with the payment gateway	enum	V2
<code>signature</code>	Signature guaranteeing the integrity of the requests exchanged between the merchant website and the payment gateway.	ans..44	Compute the value of the signature field using all the fields of your form starting with vads_ (see chapter Computing the signature).

2. Use the `vads_identifier` field if you wish to generate the identifier of the token associated with the payment method.

The token format must not be an..32. This format is reserved for tokens generated by the payment gateway.

If you have activated the detection of token uniqueness, the value of the `vads_identifier` field transmitted in the form can be different from the one present in the notification if the payment method is already associated with another token.

3. Add optional fields according to your requirements (see chapter [Using additional features](#)).

The list of fields returned in the notification is described in the chapter [Payment with the token creation option for the cardholder](#) on page 103.

13. USING ADDITIONAL FEATURES

13.1. Defining a different amount for the first n installments

You wish to set up a recurring payment for which the amount of the first installment(s) would differ from the ones configured by the **vads_sub_amount** field.

Example: define a recurring payment with the first 3 installments equal to EUR 45.25 ,and the remaining installments equal to EUR 75.90.

To do so:

1. Use the fields required for your use case to create your payment form.
2. Use the fields below:

Field name	Description	Value
vads_sub_init_amount_number	Number of installments to which will be applied the amount defined by vads_sub_init_amount	3
vads_sub_init_amount	Amount of the first installments. The number of the first installments is defined by vads_sub_init_amount_number .	2500
vads_sub_amount	Amount of each installment except the ones that will be eventually defined by vads_sub_init_amount_number	3000
vads_sub_currency	Currency used for all of the installments.	E.g.: 978 for euro (EUR)



The **vads_sub_init_amount** and **vads_sub_amount** fields cannot be set to 0.



To define a recurring payment where the 3 first months are free, all you need to do is set the start date (**vads_sub_effect_date**) to 3 months later.

Form example:

```
<form method="POST" action="https://paiement.systempay.fr/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="Pay"/>
</form>
```

13.2. Defining the currency for creating or updating a token

If:

- you have a MID that supports several currencies,

- you have several shops,
- your shops are all linked to the same MID,
- each shop generates payments in a different currency,
(e.g.: US dollar for the first shop, Euro for the second shop)

it is possible that the currency used when creating or updating a token is not supported by the shop.

By default, the payment gateway uses alphabetical order when selecting the currency for performing the necessary checks with the payment method issuer.

In order to avoid IPN processing errors, you can transmit the information about the currency to use via the form.



It will always be possible to use the token for making payments in any currency supported by the agreement.

Field name	Description	Format	Value
vads_currency	Numeric currency code to be used for the payment, in compliance with the ISO 4217 standard (numeric code).	n3	E.g.: 978 for euro (EUR)

14. COMPUTING THE SIGNATURE

To be able to compute the signature, you must have:

- all the fields that start with **vads_**
- the signature algorithm chosen in the shop configuration
- the **key**

The key value is available in your Merchant Back Office via **Settings > Shop > Keys** tab.

The signature algorithm is defined in your Merchant Back Office via **Settings > Shop > Configuration** tab.



For maximum security, it is recommended to use HMAC-SHA-256 algorithm and an alphanumeric key.

The use of SHA-1 algorithm is deprecated but maintained for compliance reasons.

To compute the signature:

1. Sort the fields whose name begins with **vads_** alphabetical order.
2. Make sure that all the fields are encoded in UTF-8.
3. Concatenate the values of these fields separating them with the "+" character.
4. Concatenate the result with the test or production key separating them with the "+" character.
5. According to the signature algorithm defined in your shop configuration:
 - a. If your shop is configured to use "SHA-1", apply the **SHA-1** hash function to the chain obtained during the previous step. **Deprecated.**
 - b. If your shop is configured to use "HMAC-SHA-256", compute and encode in Base64 format the message signature using the **HMAC-SHA-256** algorithm with the following parameters:
 - the SHA-256 hash function,
 - the test or production key (depending on the value of the field **vads_ctx_mode**) as a shared key,
 - the result of the previous step as the message to authenticate.
6. Save the result of the previous step in the field **signature**.

Example of parameters sent to the payment gateway:

```
<form method="POST" action="https://paiement.systempay.fr/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="pay" value="Pay" />
</form>
```

This sample form is analyzed as follows:

1. We sort in **alphabetical** order the fields whose name begins with **vads_** :

- 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. We concatenate the value of these fields with the "+" character :

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

3. The value of the test key is added at the end of the chain and separated with the "+" character. In this example, the test key is **1122334455667788**

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

4. If you use the SHA-1 algorithm, apply it to the obtained chain.

The result that must be transmitted in the signature field is:
59c96b34c74b9375c332b0b6a32e6deeec87de2b

5. If your shop is configured to use "HMAC-SHA-256", compute and encode in Base64 format the message signature using the **HMAC-SHA-256** algorithm with the following parameters:

- the SHA-256 hash function,
- the test or production key (depending on the value of the field **vads_ctx_mode**) as a shared key,
- the result of the previous step as the message to authenticate.

The result that must be transmitted in the signature field is:

ycA5Do5tNvsnKdc/eP1bj2xa19z9q3iWPY9/rpesfS0=

15. SENDING THE PAYMENT REQUEST

The buyer will be able to finalize his/her purchase once he/she is redirected to the payment page.

The buyer's browser must transmit the payment form data.

15.1. Redirecting the buyer to the payment page

The URL of the payment gateway is:

<https://paiement.systempay.fr/vads-payment/>

Example of parameters sent to the payment gateway:

```
<form method="POST" action="https://paiement.systempay.fr/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="FR" />
<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="Pay"/>
</form>
```

15.2. Processing errors

If the payment gateway detects an error while receiving the form, an error message will appear and the buyer will not be able to proceed to the payment.

In TEST mode

The message indicates the source of the error and provides a link to the error code description to help you fix it.

In PRODUCTION mode

The message simply indicates to the buyer that a technical problem has occurred.

In both cases the merchant receives a notification e-mail.

It contains:

- the source of the error,
- a link to possible causes to facilitate its analysis,
- all the fields of the form.

The e-mail is sent to the company administrator.

If you wish to change this address or add an address, contact E-commerce customer service.

You can also create a personalized notification rule to receive this e-mail at another address.

To do this:

1. Sign in to your Merchant Back Office:
<https://paiement.systempay.fr/vads-merchant/>
2. Open the **Settings > Notification rules** menu.
3. Select **Advanced notification**.
4. Select the type of **E-mail sent to the merchant** notification.
5. Click **Next**.
6. Select the trigger event for **Invalid payment form**.
7. In the **General settings**, fill in the fields:
 - **Rule reference**
 - **E-mail address to notify**
8. Click **Create**.

A description of the error codes with their possible causes is available on our website

<https://paiement.systempay.fr/doc/en-EN/error-code/sitemap.html>

Other messages may appear during the payment process.

Here is a list of the most frequent messages:

Message	Description
This website does not currently accept payments.	"Seasonal service" is enabled in your shop. Payments are only authorized during the defined period. If you want to modify the opening period of your shop, please contact E-commerce customer service.
Your payment request has been declined by your financial institution.	<ul style="list-style-type: none"> • The buyer's bank has rejected the authorization or information request. • The risk assessment rules have triggered the rejection of the transaction.
Your registration request has been declined by your financial institution.	<ul style="list-style-type: none"> • The buyer's bank has rejected the authorization or information request. • The risk assessment rules have triggered the rejection of the transaction.
This payment order is expired. Please contact your shop.	The buyer clicked on the payment link after the payment order expiration date.
This payment order has already been paid.	The buyer clicked on the payment link one more time after having already made the payment.
An error occurred during the payment request, the merchant website has been informed of the impossibility to finalize the transaction.	The payment form has been rejected. The shop administrator has received an e-mail with the details about the origin of the error.
The transaction has already been made.	The merchant website sends a transaction identifier that has already been used for another transaction (accepted or rejected). The transaction identifier must be unique within the same day (00:00:00 at 23:59:59 UTC).
Sorry, you have been disconnected due to a long period of inactivity.	<ul style="list-style-type: none"> • The buyer attempts to validate the card number while the payment session is expired. The session is open for about 10 minutes. • The merchant website sends a transaction identifier that has already been used but that did not result in a transaction (e.g. abandoned payment). The transaction

Message	Description
	identifier must be unique within the same day (00:00:00 at 23:59:59 UTC).
Cookies are blocked by your browser. Make sure you authorize them before retrying the operation.	The buyer has disabled cookies in his or her browser. Cookies are necessary for the payment to be processed correctly.

15.3. Managing timeouts

Payment session concept

A "payment session" is the time spent by a buyer on the payment page.

The payment session begins as soon as the payment gateway receives the payment form.

The delay of payment session is 10 minutes (except for certain payment methods).

This delay is:

- **sufficient** to enable each buyer to make his or her payment
- **fixed in time**: it is not reset on each user action
- **non-modifiable**: it is fixed by the payment gateway due to technical constraints.

After this delay, the payment session times out and the session data is purged.

Expiration of the payment session

In some cases the payment session will expire while the buyer has not completed the payment.

Most frequent cases:

1. Once redirected to the payment page the buyer realizes that it is time to go to lunch, for example.

An hour later, the buyer decides to continue his or her payment and clicks on the logo corresponding to his or her payment method.

The buyer's payment session has already expired, the payment gateway displays an error message indicating that it was disconnected due to an extended period of inactivity.

The buyer then has the opportunity to click a button to return to the merchant website.

The return to the shop is done via the URL specified by the merchant:

- in the *vads_url_return* field transmitted in the payment form
 - in the "Return URL to the merchant website" field in the buyer's Merchant Back Office, no *vads_url_return* field is transmitted in his or her payment form
2. Once redirected to the payment page, the buyer closes the browser (by mistake or because he or she no longer wants to make the payment).

Notification in case of session expiration

It is possible to notify the merchant website in case of expiration of the payment session.

To do so, the merchant must configure and enable the **Instant Payment Notification URL on cancellation** notification rule (see chapter [Setting up notifications in case of abandoned or canceled payments](#) on page 44).

16. IMPLEMENTING THE IPN

The script must include at least the following steps:

- Retrieve the field list sent with the POST response
- Compute the signature taking into account the received data
- Compare the computed signature with the received signature
- Analyze the nature of the notification
- Retrieve the payment result

The script may check the order status (or any information of your choice) to see if it has not already been updated.

Once these steps are completed, the script can update the database (new order status, stock update, registration of payment information, etc.).

In order to facilitate support and diagnosis by the merchant in the event of a notification error, we recommend to write messages that will allow you to know at which stage of processing the error occurred.

The gateway reads and stores the first 256 bytes of the HTTP response.

You can write messages throughout the processing. Here are some examples of messages that you can use:

Message	Use case
Data received.	Message to display when retrieving data. Allows to confirm that the notification has been received by the merchant website.
POST is empty.	Message to display when retrieving data. Allows to bring out a possible redirection that would have caused the parameters posted by the payment gateway to be lost.
An error occurred while computing the signature.	Message to be displayed when the verification of the response signature has failed.
Order successfully updated.	Message to be displayed at the end of the file once your processing has been successfully completed.
An error occurred while updating the order.	Message to be displayed at the end of the file if an error occurred during your processing.

16.1. Preparing your environment



The notifications of Instant Payment Notification URL call type are very important as they represent the only reliable way for the merchant website to obtain the payment result.

It is therefore necessary to make sure the notifications function properly.

Here are some guidelines:

- In order for the dialog between the payment gateway and your merchant website to work, you must make sure, together with your technical teams, that the **194.50.38.0/24** IP address range is authorized on the various devices within your system (firewalls, apache server, proxy server, etc.)

Notifications are sent from an IP address in the 194.50.38.0/24 range **in Test and Production modes**.

- Using redirection leads to losing data presented in POST.

This is the case if there is a configuration on your devices or on the side of your host that redirects the URLs of “http://www.example.com” type to “http://example.com” or “http://example.com” to “https://example.com”.

- HTML must not be visible on the page. Access to images or CSS slows down the exchange between the payment gateway and the merchant website.

- Avoid integrating time-consuming tasks, such as PDF invoice generation or sending e-mails in your script.

The processing time has a direct influence on the time it takes to display the payment summary page.

The longer the processing of the notification, the greater the delay for displaying the page. After 35 seconds, the payment gateway considers that the call has failed (timeout).

- If your page is only accessible in https, test your URL on the Qualys SSL Labs website (<https://www.ssllabs.com/ssltest/>) and, if necessary, change your configuration if necessary in order to obtain the A score.

Your SSL certificate must be signed by a certification authority known and recognized on the market.

- Make sure that you use the latest version of the TLS protocol in order to maintain a high level of security.

16.2. Retrieving data returned in the response

The data returned in the response depends on the parameters sent in the payment request, the payment type, the settings of your shop and the notification format.

The data is always sent by the payment gateway using the **POST** method.

The first step consists in retrieving the contents received via the POST method.

Examples:

- In PHP, data is stored in the super global variable **\$_POST**,
- In ASP.NET (C#), you must use the **Form** property of the **HttpRequest** class,
- In Java, you must use the **getParameter** method of the **HttpServletRequest** interface.

The response consists of a field list. Each field contains a response value. The field list can be updated.

The script will have to create a loop to retrieve all the transmitted fields.

It is recommended to test the presence of the **vads_hash** field, which is only present during a notification.

```
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. Computing the IPN signature

The signature is computed by following the same logic as for creating the payment request.



The data submitted by the payment gateway is encoded in UTF-8. Any alteration of received data will result in signature computation error.

You must compute the signature with the fields received in the notification and not the ones that you transmitted in the payment request.

1. Take all the fields whose name starts with **vads_**.
2. Sort these fields alphabetically.
3. Concatenate the values of these fields separating them with the "+" character.
4. Concatenate the result with the test or production key separating them with the "+" character.
5. According to the signature algorithm defined in your shop configuration:
 - a. If your shop is configured to use "SHA-1", apply the **SHA-1** hash function to the chain obtained during the previous step. **Deprecated.**
 - b. If your shop is configured to use "HMAC-SHA-256", compute and encode in Base64 format the message signature using the **HMAC-SHA-256** algorithm with the following parameters:
 - the SHA-256 hash function,
 - the test or production key (depending on the value of the field **vads_ctx_mode**) as a shared key,
 - the result of the previous step as the message to authenticate.

Examples in PHP:

```
function getSignature ($params,$key)
{
    /**
     *Function that computes the signature.
     * $params: table containing the fields received in the IPN.
     * $key : TEST or PRODUCTION key
     */
    //Initialization of the variable that will contain the string to encrypt
    $signature_contents = "";

    //Sorting fields alphabetically
    ksort($params);
    foreach($params as $name=>$value){

        //Recovery of vads_ fields
        if (substr($name,0,5)=='vads_'){

            //Concatenation with "+"
            $signature_contents .= $value."+";

        }
    }
    //Adding the key at the end
    $signature_contents .= $key;

    //Encoding base64 encoded chain with HMAC-SHA-256 algorithm
    $sign = base64_encode(hash_hmac('sha256',$signature_contents, $key, true));
    return $sign;
}
```

16.4. Comparing signatures

To ensure the integrity of the response, you must compare the signature contained in the IPN with the value computed in the previous step.



You should not compare the signature of the IPN with the signature that you transmitted in your payment request.

If the signatures match

- You may consider the response as safe and proceed with the analysis.
- Otherwise, the script will have to raise an exception and notify the merchant about the anomaly.

Example in PHP:

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

The signatures may not match in case of:

- an implementation error (error in your calculation, problem with UTF-8 encoding, etc.),
- an error in the key value or in the **vads_ctx_mode** field (frequent issue when shifting to production mode),
- a data corruption attempt.

16.5. Analyzing the nature of the notification

The **vads_url_check_src** field allows to differentiate the notifications based on their triggering event:

- token creation (with or without the subscription of a recurring payment),
- installment payment,
- new notification sent by the merchant via the Merchant Back Office

It specifies the applied notification rule:

Value	Applied rule
PAY	<p>The PAY value is sent in the following cases:</p> <ul style="list-style-type: none"> • registration request for a mandate or a token (REGISTER) • registration request for a mandate or a token when subscribing to a recurring payment (REGISTER_SUBSCRIBE) • immediate payment (or first installment payment of a recurring payment) • payment abandoned or canceled by the buyer <p>Only if the merchant has configured the Instant Payment Notification URL on cancellation rule.</p>
BO	<p>Execution of the notification via the Merchant Back Office (right-click a transaction > Send the Instant Payment Notification).</p> <p>Check whether the vads_recurrence_number field is present:</p> <ul style="list-style-type: none"> • if yes, the notification concerns the result of a recurring payment (retry of a REC type notification), • if not, the notification concerns a notification at the end of payment.
BATCH	<p>The BATCH value is sent in case of an update of a transaction status after its synchronization on the acquirer side.</p> <p>This is the case of payments with redirection to the acquirer.</p> <p>Only if the merchant has configured the rule Instant Payment Notification URL on batch change.</p>
BATCH_AUTO	<p>The BATCH_AUTO value is sent in the following cases:</p> <ul style="list-style-type: none"> • payment deferred for more than 7 days • installments of a recurring payment (except the first one) <p>Only if the merchant has configured the Instant Payment Notification URL on batch authorization rule.</p> <p>The notification is sent with the authorization request for payments with "Waiting for authorization" status.</p>
REC	<p>The REC value is sent only for recurring payments if the merchant has configured the Instant Payment Notification URL when creating recurring payments rule.</p> <p>See the Installment payment on page 106 chapter for more information on the sent data.</p>
MERCH_BO	<p>The MERCH_BO value is sent:</p> <ul style="list-style-type: none"> • during an operation made via the Merchant Back Office (refund, cancellation, modification, validation, duplication, creation and/or update of token), only if the merchant has configured the following notification rule: Instant Payment Notification URL on an operation coming from the Back Office
RETRY	<p>Automatic retry of the IPN.</p> <p>Check whether the vads_recurrence_number field is present:</p> <ul style="list-style-type: none"> • if yes, the notification concerns the result of a recurring payment (retry of a REC type notification), • if not, the notification concerns a notification at the end of payment.

Table 1: Values associated with the vads_url_check_src field

After checking its value, the script can process differently depending on the nature of the notification.

For example:

If **vads_url_check_src** is set to **PAY** or **BATCH_AUTO**, the script will update the order status, etc.

If **vads_url_check_src** is set to **REC**, the script will retrieve the recurring payment reference and will increment the number of the expired installment payments in case the payment has been accepted, etc.

In the context of a recurring payment (from a REGISTER_SUBSCRIBE), the payment gateway notifies the creditor (merchant) when creating each transaction.


16.6. Processing the response data

- [Creating a token without payment](#) on page 79
- [Updating token details](#) on page 83
- [Creating a token during a payment](#) on page 86
- [Creating a token during a recurring payment](#) on page 90
- [Creating a token upon the creation of a subscription with payment](#) on page 94
- [Payment by token](#) on page 98
- [Creating a recurring payment](#) on page 101
- [Payment with the token creation option for the cardholder](#) on page 103
- [Installment payment](#) on page 106

16.6.1. Creating a token without payment

In order to understand the result, analyze the following fields:

Field name	Description
vads_page_action	Completed action. The returned value is REGISTER .
vads_identifier_status	Token creation status. Possible values are: <ul style="list-style-type: none"> • CREATED: the request for authorization or information, if supported by the acquirer is accepted. The token has been successfully created and gets displayed in the Merchant Back Office. • NOT_CREATED: the request for authorization or information has been rejected. The token is not created. • ABANDONED: action abandoned by the buyer. The token is not created.
vads_identifier	Token ID. The returned value is: <ul style="list-style-type: none"> • either the value transmitted in the request, regardless of the result of token creation, even in case of abandoned action, • or the value generated by the payment gateway, if the field is not transmitted in the request and the token has been successfully created (vads_identifier_status=CREATED). <p>Note</p> <p>If you have activated the token uniqueness check and the payment method is already registered with another token, then this token will be returned.</p> <p>The field vads_identifier will not be returned:</p> <ul style="list-style-type: none"> • if it has not been transmitted in the request and the buyer abandons the action (vads_identifier_status=ABANDONED),

Field name	Description
	<ul style="list-style-type: none"> if it has not been transmitted in the request and the token has not been created (vads_identifier_status=NOT_CREATED).
vads_identifier_previously_registered	Present only if both conditions are true: <ul style="list-style-type: none"> You have enabled the token uniqueness check. The used payment method is already registered with another token.
vads_initial_issuer_transaction_identifier	Unique transaction identifier generated by the issuer. <div>  <p>The issuer transaction identifier is stored by the payment gateway at the level of the alias. Depending on how you use the alias (1-click payment, 0-click payment, recurring payment, etc.) the issuer transaction ID will be used as a chaining reference if necessary.</p> </div>
vads_cust_email	Buyer's e-mail address transmitted in the request.
vads_site_id	Shop ID The returned value is the same as the one submitted in the form.
vads_ctx_mode	Operating mode. The returned value (TEST or PRODUCTION) is the same as the one submitted in the form.

A “create a token without a payment” request triggers the creation of a **VERIFICATION** transaction, visible in the Merchant Back Office.



The purpose of this transaction is to help the merchant, via their Back Office, understand the reasons for refusal of token creation.

Here are its characteristics:

Field name	Description
vads_operation_type	Transaction type Its value is VERIFICATION .
vads_trans_status	Status of the transaction. Possible values are: <ul style="list-style-type: none"> ACCEPTED The authorization or information request has been accepted. The token has been created and is visible in the Merchant Back Office. REFUSED The authorization or information request has been rejected. The token is not created.
vads_occurrence_type	Transaction occurrence type. Its value is UNITAIRE .
vads_amount	Possible values: <ul style="list-style-type: none"> 0 if the acquirer supports the inquiries, 100 otherwise.
vads_trans_id	Transaction identifier. Its value is generated by the payment gateway.
vads_trans_uuid	Unique transaction ID. Its value is generated by the payment gateway.
vads_auth_mode	Type of request made via authorization servers. Its value is MARK .
vads_auth_number	Authorization number returned by the authorization server. Empty if the authorization has failed.
vads_auth_result	Return code of the authorization request returned by the issuing bank. See chapter Managing the return codes of the authorization request . Empty in case of an error prior to the authorization.

Field name	Description
vads_risk_assessment_result	<p>List of actions made with the transaction, following the activation of the advanced risk assessment rules.</p> <p>The rules related to the amount, or whose action is “Validate manually”, do not apply in case of a VERIFICATION type transaction.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • ENABLE_3DS: 3D Secure enabled. • DISABLE_3DS: 3D Secure disabled. • CHALLENGE_REQUESTED: <ul style="list-style-type: none"> • 3DS1 card: The risk module has requested 3DS authentication. • 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge). • CHALLENGE_MANDATE: <ul style="list-style-type: none"> • 3DS1 card: The risk module has requested 3DS authentication. • 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge for regulatory reasons) for regulatory reasons. • REFUSE: The token is declined. • RUN_RISK_ANALYSIS: Result of the external risk analyzer. See the description of the vads_risk_analysis_result field for more information. • INFORM: A warning message appears. The merchant is notified that a risk has been identified via one or several notification center rules.

Details of the used payment method:

Field name	Note
vads_acquirer_network	Acquirer network code.
vads_bank_code	Code of the issuing bank.
vads_bank_label	Name of the issuing bank of the payment card.
vads_bank_product	Product code of the used card.
vads_brand_management	Allows to know the brand that was used, the list of available brands as well as whether the buyer has changed the default brand chosen by the merchant.
vads_card_brand	Used payment method. See chapter Compatible payment methods to see the list of possible values.
vads_card_country	Country code of the card used in compliance with the ISO 3166 standard.
vads_card_number	Truncated/masked card number.
vads_expiry_month	<p>Expiry month of the used card.</p> <div>  <p>It is advisable to use this data to check the expiration date of the token.</p> </div>
vads_expiry_year	<p>Expiry year of the used card.</p> <div>  <p>It is advisable to use this data to check the expiration date of the token.</p> </div>

Authentication details of the cardholder:


Field name	Note
vads_threeds_auth_type	Cardholder authentication type. Strong cardholder authentication is mandatory when registering a card. The field will therefore always be populated with CHALLENGE .
vads_threeds_enrolled	Enrollment status of the buyer to the 3D Secure program.

Field name	Note
	Possible values are: <ul style="list-style-type: none"> • Y: Authentication available. • N: Authentication not available. • U: Enrollment status to the 3D Secure program unknown. • empty: Incomplete 3DS authentication process (3DS disabled in the request, unregistered merchant or payment method not eligible for 3DS).
vads_threeds_status	3D Secure authentication result. Possible values are: <ul style="list-style-type: none"> • Y: Cardholder authentication success. • N: Cardholder authentication error. • U: Authentication impossible. • A: Authentication attempted but not completed. • empty: Unauthorized 3DS authentication (3DS disabled in the request, unregistered cardholder or payment method not eligible for 3DS).

The optional fields transmitted in the request are returned in the response with unmodified values.

16.6.2. Updating token details

In order to understand the result, analyze the following fields:

Field name	Description
vads_page_action	Completed action. The returned value is REGISTER_UPDATE .
vads_identifier_status	Token update status. Possible values are: <ul style="list-style-type: none"> UPDATED: the token has been successfully updated. NOT_UPDATED: the token has not been updated. ABANDONED: action abandoned by the buyer. The token has not been created, and therefore cannot be viewed in the Merchant Back Office.
vads_identifier	Token ID to be updated. The returned value is the same as the one submitted in the form.
vads_initial_issuer_transaction_identifier	Unique transaction identifier generated by the issuer. <div>  <p>The issuer transaction identifier is stored by the payment gateway at the level of the alias. Depending on how you use the alias (1-click payment, 0-click payment, recurring payment, etc.) the issuer transaction ID will be used as a chaining reference if necessary.</p> </div>
vads_cust_email	Buyer's e-mail address transmitted in the request.
vads_site_id	Shop ID The returned value is the same as the one submitted in the form.
vads_ctx_mode	Operating mode. The returned value (TEST or PRODUCTION) is the same as the one submitted in the form.

A “token update” request results in the creation of a **VERIFICATION** transaction, visible in the Merchant Back Office.


The purpose of this transaction is to help the merchant, via their Back Office, understand the reasons for refusal of token creation.


Here are its characteristics:

Field name	Description
vads_operation_type	Transaction type Its value is VERIFICATION .
vads_trans_status	Status of the transaction. Possible values are: <ul style="list-style-type: none"> ACCEPTED The authorization or information request has been accepted. The token has been created and is visible in the Merchant Back Office. REFUSED The authorization or information request has been rejected. The token is not created.
vads_occurrence_type	Transaction occurrence type. Its value is UNITAIRE .
vads_amount	Possible values: <ul style="list-style-type: none"> 0 if the acquirer supports the inquiries, 100 otherwise.
vads_trans_id	Transaction identifier. Its value is generated by the payment gateway.

Field name	Description
vads_trans_uuid	Unique transaction ID. Its value is generated by the payment gateway.
vads_auth_mode	Type of request made via authorization servers. Its value is MARK .
vads_auth_number	Authorization number returned by the authorization server. Empty if the authorization has failed.
vads_auth_result	Return code of the authorization request returned by the issuing bank. See chapter Managing the return codes of the authorization request . Empty in case of an error prior to the authorization.
vads_risk_assessment_result	<p>List of actions made with the transaction, following the activation of the advanced risk assessment rules.</p> <p>The rules related to the amount, or whose action is "Validate manually", do not apply in case of a VERIFICATION type transaction.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • ENABLE_3DS: 3D Secure enabled. • DISABLE_3DS: 3D Secure disabled. • CHALLENGE_REQUESTED: <ul style="list-style-type: none"> • 3DS1 card: The risk module has requested 3DS authentication. • 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge). • CHALLENGE_MANDATE: <ul style="list-style-type: none"> • 3DS1 card: The risk module has requested 3DS authentication. • 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge for regulatory reasons) for regulatory reasons. • REFUSE: The token is declined. • RUN_RISK_ANALYSIS: Result of the external risk analyzer. See the description of the vads_risk_analysis_result field for more information. • INFORM: A warning message appears. The merchant is notified that a risk has been identified via one or several notification center rules.

Details of the used payment method:

Field name	Note
vads_acquirer_network	Acquirer network code.
vads_bank_code	Code of the issuing bank.
vads_bank_label	Name of the issuing bank of the payment card.
vads_bank_product	Product code of the used card.
vads_brand_management	Allows to know the brand that was used, the list of available brands as well as whether the buyer has changed the default brand chosen by the merchant.
vads_card_brand	Used payment method. See chapter Compatible payment methods to see the list of possible values.
vads_card_country	Country code of the card used in compliance with the ISO 3166 standard.
vads_card_number	Truncated/masked card number.
vads_expiry_month	Expiry month of the used card. <div>  <p>It is advisable to use this data to check the expiration date of the token.</p> </div>
vads_expiry_year	Expiry year of the used card.

Field name	Note
	 It is advisable to use this data to check the expiration date of the token.

Authentication details of the cardholder:


Field name	Note
vads_threeds_auth_type	Cardholder authentication type. Strong cardholder authentication is mandatory when registering a card. The field will therefore always be populated with CHALLENGE .
vads_threeds_enrolled	Enrollment status of the buyer to the 3D Secure program. Possible values are: <ul style="list-style-type: none"> • Y: Authentication available. • N: Authentication not available. • U: Enrollment status to the 3D Secure program unknown. • empty: Incomplete 3DS authentication process (3DS disabled in the request, unregistered merchant or payment method not eligible for 3DS).
vads_threeds_status	3D Secure authentication result. Possible values are: <ul style="list-style-type: none"> • Y: Cardholder authentication success. • N: Cardholder authentication error. • U: Authentication impossible. • A: Authentication attempted but not completed. • empty: Unauthorized 3DS authentication (3DS disabled in the request, unregistered cardholder or payment method not eligible for 3DS).

The optional fields transmitted in the request are returned in the response with unmodified values.

16.6.3. Creating a token during a payment

In order to understand the result, analyze the following fields:

Field name	Description
vads_page_action	Completed action. The returned value is REGISTER_PAY .
vads_identifier_status	Token creation status. Possible values are: <ul style="list-style-type: none"> • CREATED: the request for authorization or information, if supported by the acquirer is accepted. Token has been successfully created. • NOT_CREATED: the request for authorization or information has been rejected. The token has not been created, and therefore cannot be viewed in the Merchant Back Office. • ABANDONED: action abandoned by the buyer. The token has not been created, and therefore cannot be viewed in the Merchant Back Office.
vads_trans_status	Status of the transaction. Possible values are: <ul style="list-style-type: none"> • AUTHORISED The authorization or information request has been accepted. The token has been created and is visible in the Merchant Back Office. • AUTHORISED_TO_VALIDATE The authorization or information request has been accepted. The merchant must manually validate the transaction. The token has been created and is visible in the Merchant Back Office. • CAPTURED The authorization or information request has been accepted. The transaction is visible in the "Captured transactions" tab of the Back Office. The token has been created and is visible in the Merchant Back Office. • WAITING_AUTHORISATION The capture delay in the bank exceeds the authorization validity period. The authorization request for the total amount has not yet been sent. The token has been created and is visible in the Merchant Back Office. • WAITING_AUTHORISATION_TO_VALIDATE To be validated and authorized The capture delay in the bank exceeds the authorization validity period. A EUR 1 (or information request about the CB network if the acquirer supports it) authorization has been accepted. The merchant must manually validate the transaction in order to trigger the authorization request and capture. • REFUSED The authorization or information request has been rejected. The token is not created. • ABANDONED Operation abandoned by the buyer. The transaction is then not visible via the Merchant Back Office. The token is not created.
vads_identifier	Token ID. The returned value is: <ul style="list-style-type: none"> • either the value transmitted in the request, regardless of the result of token creation, even in case of abandoned action, • or the value generated by the payment gateway, if the field is not transmitted in the request and the token has been successfully created (vads_identifier_status=CREATED).

Field name	Description
	<p>Note</p> <p>If you have activated the token uniqueness check and the payment method is already registered with another token, then this token will be returned.</p> <p>The field vads_identifier will not be returned:</p> <ul style="list-style-type: none"> if it has not been transmitted in the request and the buyer abandons the action (vads_identifier_status=ABANDONED), if it has not been transmitted in the request and the token has not been created (vads_identifier_status=NOT_CREATED).
vads_identifier_previously_registered	<p>Present only if both conditions are true:</p> <ul style="list-style-type: none"> You have enabled the token uniqueness check. The used payment method is already registered with another token.
vads_initial_issuer_transaction_identifier	<p>Unique transaction identifier generated by the issuer.</p> <div>  <ul style="list-style-type: none"> The issuer transaction identifier is stored by the payment gateway at the level of the alias and the transaction. Depending on how you use the alias (1-click payment, 0-click payment, recurring payment, etc.) the issuer transaction ID will be used as a chaining reference if necessary. In case the merchant duplicates (MIT) the transaction, the gateway will automatically use this identifier as a chaining reference. </div>
vads_cust_email	Buyer's e-mail address transmitted in the request.
vads_site_id	<p>Shop ID</p> <p>The returned value is the same as the one submitted in the form.</p>
vads_ctx_mode	<p>Operating mode.</p> <p>The returned value (TEST or PRODUCTION) is the same as the one submitted in the form.</p>


To view the payment details, see the parameters below:


Transaction details:

Field name	Description
vads_operation_type	<p>Transaction type</p> <p>Its value is DEBIT.</p>
vads_occurrence_type	<p>Transaction occurrence type.</p> <p>Its value is UNITAIRE.</p>
vads_amount	<p>Transaction amount.</p> <p>The returned value is the same as the one submitted in the form.</p>
vads_currency	Code of the currency used for the payment.
vads_trans_id	<p>Transaction identifier.</p> <p>The returned value is the same as the one submitted in the form.</p>
vads_trans_uuid	<p>Unique transaction ID.</p> <p>Its value is generated by the payment gateway.</p>
vads_contract_used	MID associated with the transaction.
vads_auth_mode	<p>Type of request made via authorization servers:</p> <ul style="list-style-type: none"> MARK: corresponds to an authorization of EUR 1 (or information request about the CB network if the acquirer supports it). Value also used if the period between the requested capture date and the current date is strictly greater than the authorization validity period. FULL: corresponds to an authorization of the total transaction amount. Value also used if the period between the requested capture date and the current date is strictly shorter than the authorization validity period.
vads_auth_number	<p>Authorization number returned by the authorization server.</p> <p>Empty if the authorization has failed.</p>

Field name	Description
vads_auth_result	Return code of the authorization request returned by the issuing bank. See chapter Managing the return codes of the authorization request . Empty in case of an error prior to the authorization.
vads_risk_control	Result of the risk assessment. If at least one verification process returns the ERROR value, the transaction is rejected. See the description of the vads_risk_analysis_result field for more information.
vads_risk_assessment_result	List of actions made with the transaction, following the activation of the advanced risk assessment rules. Possible values are: <ul style="list-style-type: none"> • ENABLE_3DS: 3D Secure enabled. • DISABLE_3DS: 3D Secure disabled. • CHALLENGE_REQUESTED: <ul style="list-style-type: none"> • 3DS1 card: The risk module has requested 3DS authentication. • 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge). • CHALLENGE_MANDATE: <ul style="list-style-type: none"> • 3DS1 card: The risk module has requested 3DS authentication. • 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge for regulatory reasons) for regulatory reasons. • MANUAL_VALIDATION: The transaction has been created via manual validation. The payment capture is temporarily blocked to allow the merchant to perform all the desired verification processes. • REFUSE: The transaction is refused. • RUN_RISK_ANALYSIS: Result of the external risk analyzer. See the description of the vads_risk_analysis_result field for more information. • INFORM: A warning message appears. The merchant is notified that a risk has been identified via one or several notification center rules.

Details of the used payment method:

Field name	Note
vads_acquirer_network	Acquirer network code.
vads_bank_code	Code of the issuing bank.
vads_bank_label	Name of the issuing bank of the payment card.
vads_bank_product	Product code of the used card.
vads_brand_management	Allows to know the brand that was used, the list of available brands as well as whether the buyer has changed the default brand chosen by the merchant.
vads_card_brand	Used payment method. See chapter Compatible payment methods to see the list of possible values.
vads_card_country	Country code of the card used in compliance with the ISO 3166 standard.
vads_card_number	Truncated/masked card number.
vads_expiry_month	Expiry month of the used card. <div> It is advisable to use this data to check the expiration date of the token.</div>
vads_expiry_year	Expiry year of the used card.

Field name	Note
	 It is advisable to use this data to check the expiration date of the token.


Authentication details of the cardholder:

Field name	Note
vads_threeds_auth_type	Cardholder authentication type. Strong cardholder authentication is mandatory when registering a card. The field will therefore always be populated with CHALLENGE .
vads_threeds_enrolled	Enrollment status of the buyer to the 3D Secure program. Possible values are: <ul style="list-style-type: none"> • Y: Authentication available. • N: Authentication not available. • U: Enrollment status to the 3D Secure program unknown. • empty: Incomplete 3DS authentication process (3DS disabled in the request, unregistered merchant or payment method not eligible for 3DS).
vads_threeds_status	3D Secure authentication result. Possible values are: <ul style="list-style-type: none"> • Y: Cardholder authentication success. • N: Cardholder authentication error. • U: Authentication impossible. • A: Authentication attempted but not completed. • empty: Unauthorized 3DS authentication (3DS disabled in the request, unregistered cardholder or payment method not eligible for 3DS).

The optional fields transmitted in the request are returned in the response with unmodified values.

16.6.4. Creating a token during a recurring payment

In order to understand the result, analyze the following fields:

Field name	Description
vads_page_action	Completed action. The returned value is REGISTER_SUBSCRIBE .
vads_identifier_status	Token creation status. Possible values are: <ul style="list-style-type: none"> • CREATED: the request for authorization or information, if supported by the acquirer is accepted. Token has been successfully created. See the value of the field vads_recurrence_status to determine whether the subscription has been created. • NOT_CREATED: the request for authorization or information has been rejected. The token has not been created, and therefore cannot be viewed in the Merchant Back Office. The recurring payment is not created. • ABANDONED: action abandoned by the buyer. The token has not been created, and therefore cannot be viewed in the Merchant Back Office. The recurring payment is not created.
vads_recurrence_status	Recurrence creation status. The possible values are: <ul style="list-style-type: none"> • CREATED: The recurring payment has been successfully created. • NOT_CREATED: The recurring payment is not created. • ABANDONED: The action has been abandoned by the buyer. The recurring payment is not created.
vads_identifier	Token ID. The returned value is: <ul style="list-style-type: none"> • either the value transmitted in the request, regardless of the result of token creation, even in case of abandoned action, • or the value generated by the payment gateway, if the field is not transmitted in the request and the token has been successfully created (vads_identifier_status=CREATED). <p>Note</p> <p>If you have activated the token uniqueness check and the payment method is already registered with another token, then this token will be returned.</p> <p>The field vads_identifier will not be returned:</p> <ul style="list-style-type: none"> • if it has not been transmitted in the request and the buyer abandons the action (vads_identifier_status=ABANDONED), • if it has not been transmitted in the request and the token has not been created (vads_identifier_status=NOT_CREATED).
vads_identifier_previously_registered	Present only if both conditions are true: <ul style="list-style-type: none"> • You have enabled the token uniqueness check. • The used payment method is already registered with another token.
vads_initial_issuer_transaction_identifier	Unique transaction identifier generated by the issuer. <div>  <p>The issuer transaction identifier is stored by the payment gateway at the level of the alias. Depending on how you use the alias (1-click payment, 0-click payment, recurring payment, etc.) the issuer transaction ID will be used as a chaining reference if necessary.</p> </div>
vads_cust_email	Buyer's e-mail address transmitted in the request.
vads_site_id	Shop ID

Field name	Description
	The returned value is the same as the one submitted in the form.
vads_ctx_mode	Operating mode. The returned value (TEST or PRODUCTION) is the same as the one submitted in the form.

To see the recurring payment details, see the parameters below:

Field name	Note
vads_subscription	Recurring payment token The returned value is: <ul style="list-style-type: none"> either the value transmitted in the request, regardless of the result of subscription creation, or the value generated by the payment gateway, if the field has not been transmitted in the request and the subscription has been successfully created (vads_recurrence_status=CREATED). The field vads_subscription will not be returned: <ul style="list-style-type: none"> if it has not been transmitted in the request and the buyer abandons the action (vads_recurrence_status=ABANDONED), if it has not been transmitted in the request and the recurring payment not been created (vads_recurrence_status=NOT_CREATED).
vads_sub_amount	Amount of installments (in the smallest currency unit)
vads_sub_currency	Code of the currency used for the recurring payment. E.g.: 978 for euro (EUR)
vads_sub_desc	Rule for recurring payments to apply according to the iCalendar RFC5545 specification. E.g.: RRULE:FREQ=MONTHLY
vads_sub_effect_date	Subscription start date (or effective date) in the UTC time zone, in YYYYMMDD format. E.g.: 20210601
vads_sub_init_amount	Amount of the first installments. The number of the first installments is defined by vads_sub_init_amount_number . E.g.: 1000
vads_sub_init_amount_number	Number of installments to which the amount, defined by vads_sub_init_amount , will be applied. E.g.: 3

A “create a token when subscribing to a recurring payment” request triggers the creation of a **VERIFICATION** type transaction, visible in the Merchant Back Office.

The purpose of this transaction is to help the merchant, via their Back Office, understand the reasons for refusal of token creation.



Here are its characteristics:

Field name	Description
vads_operation_type	Transaction type Its value is VERIFICATION .
vads_trans_status	Status of the transaction. Possible values are: <ul style="list-style-type: none"> ACCEPTED The authorization or information request has been accepted. The token has been created and is visible in the Merchant Back Office. REFUSED The authorization or information request has been rejected. The token is not created.
vads_occurrence_type	Transaction occurrence type.

Field name	Description
	Its value is UNITAIRE .
vads_amount	Possible values: <ul style="list-style-type: none"> • 0 if the acquirer supports the inquiries, • 100 otherwise.
vads_trans_id	Transaction identifier. Its value is generated by the payment gateway.
vads_trans_uuid	Unique transaction ID. Its value is generated by the payment gateway.
vads_auth_mode	Type of request made via authorization servers. Its value is MARK .
vads_auth_number	Authorization number returned by the authorization server. Empty if the authorization has failed.
vads_auth_result	Return code of the authorization request returned by the issuing bank. See chapter Managing the return codes of the authorization request . Empty in case of an error prior to the authorization.
vads_risk_assessment_result	List of actions made with the transaction, following the activation of the advanced risk assessment rules. The rules related to the amount, or whose action is "Validate manually", do not apply in case of a VERIFICATION type transaction. Possible values are: <ul style="list-style-type: none"> • ENABLE_3DS: 3D Secure enabled. • DISABLE_3DS: 3D Secure disabled. • CHALLENGE_REQUESTED: <ul style="list-style-type: none"> • 3DS1 card: The risk module has requested 3DS authentication. • 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge). • CHALLENGE_MANDATE: <ul style="list-style-type: none"> • 3DS1 card: The risk module has requested 3DS authentication. • 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge for regulatory reasons) for regulatory reasons. • REFUSE: The token is declined. • RUN_RISK_ANALYSIS: Result of the external risk analyzer. See the description of the vads_risk_analysis_result field for more information. • INFORM: A warning message appears. The merchant is notified that a risk has been identified via one or several notification center rules.

Details of the used payment method:

Field name	Note
vads_acquirer_network	Acquirer network code.
vads_bank_code	Code of the issuing bank.
vads_bank_label	Name of the issuing bank of the payment card.
vads_bank_product	Product code of the used card.
vads_brand_management	Allows to know the brand that was used, the list of available brands as well as whether the buyer has changed the default brand chosen by the merchant.
vads_card_brand	Used payment method. See chapter Compatible payment methods to see the list of possible values.
vads_card_country	Country code of the card used in compliance with the ISO 3166 standard.
vads_card_number	Truncated/masked card number.
vads_expiry_month	Expiry month of the used card.

Field name	Note
	 It is advisable to use this data to check the expiration date of the token.
vads_expiry_year	Expiry year of the used card.  It is advisable to use this data to check the expiration date of the token.

Authentication details of the cardholder:


Field name	Note
vads_threeds_auth_type	Cardholder authentication type. Strong cardholder authentication is mandatory when registering a card. The field will therefore always be populated with CHALLENGE .
vads_threeds_enrolled	Enrollment status of the buyer to the 3D Secure program. Possible values are: <ul style="list-style-type: none"> • Y: Authentication available. • N: Authentication not available. • U: Enrollment status to the 3D Secure program unknown. • empty: Incomplete 3DS authentication process (3DS disabled in the request, unregistered merchant or payment method not eligible for 3DS).
vads_threeds_status	3D Secure authentication result. Possible values are: <ul style="list-style-type: none"> • Y: Cardholder authentication success. • N: Cardholder authentication error. • U: Authentication impossible. • A: Authentication attempted but not completed. • empty: Unauthorized 3DS authentication (3DS disabled in the request, unregistered cardholder or payment method not eligible for 3DS).

The optional fields transmitted in the request are returned in the response with unmodified values.

16.6.5. Creating a token upon the creation of a subscription with payment

In order to understand the result, analyze the following fields:

Field name	Description
vads_page_action	Completed action. The returned value is REGISTER_PAY_SUBSCRIBE .
vads_identifier_status	Token creation status. Possible values are: <ul style="list-style-type: none"> • CREATED: the request for authorization or information, if supported by the acquirer is accepted. Token has been successfully created. See the value of the field vads_recurrence_status to determine whether the subscription has been created. • NOT_CREATED: the request for authorization or information has been rejected. The token has not been created, and therefore cannot be viewed in the Merchant Back Office. The recurring payment is not created. • ABANDONED: action abandoned by the buyer. The token has not been created, and therefore cannot be viewed in the Merchant Back Office. The recurring payment is not created.
vads_trans_status	Status of the transaction. Possible values are: <ul style="list-style-type: none"> • AUTHORISED The authorization or information request has been accepted. The token has been created and is visible in the Merchant Back Office. • AUTHORISED_TO_VALIDATE The authorization or information request has been accepted. The merchant must manually validate the transaction. The token has been created and is visible in the Merchant Back Office. • CAPTURED The authorization or information request has been accepted. The transaction is visible in the "Captured transactions" tab of the Back Office. The token has been created and is visible in the Merchant Back Office. • WAITING_AUTHORISATION The capture delay in the bank exceeds the authorization validity period. The authorization request for the total amount has not yet been sent. The token has been created and is visible in the Merchant Back Office. • WAITING_AUTHORISATION_TO_VALIDATE To be validated and authorized The capture delay in the bank exceeds the authorization validity period. A EUR 1 (or information request about the CB network if the acquirer supports it) authorization has been accepted. The merchant must manually validate the transaction in order to trigger the authorization request and capture. • REFUSED The authorization or information request has been rejected. The token is not created. • ABANDONED Operation abandoned by the buyer. The transaction is then not visible via the Merchant Back Office. The token is not created.
vads_recurrence_status	Recurrence creation status. Possible values are: <ul style="list-style-type: none"> • CREATED: The recurring payment has been successfully created.

Field name	Description
	<ul style="list-style-type: none"> NOT_CREATED: The recurring payment is not created. ABANDONED: action abandoned by the buyer. The recurring payment is not created.
vads_identifier	<p>Token ID. The returned value is:</p> <ul style="list-style-type: none"> either the value transmitted in the request, regardless of the result of token creation, even in case of abandoned action, or the value generated by the payment gateway, if the field is not transmitted in the request and the token has been successfully created (vads_identifier_status=CREATED). <p>Note If you have activated the token uniqueness check and the payment method is already registered with another token, then this token will be returned. The field vads_identifier will not be returned:</p> <ul style="list-style-type: none"> if it has not been transmitted in the request and the buyer abandons the action (vads_identifier_status=ABANDONED), if it has not been transmitted in the request and the token has not been created (vads_identifier_status=NOT_CREATED).
vads_identifier_previously_registered	<p>Present only if both conditions are true:</p> <ul style="list-style-type: none"> You have enabled the token uniqueness check. The used payment method is already registered with another token.
vads_initial_issuer_transaction_identifier	<p>Unique transaction identifier generated by the issuer.</p> <div>  <p>The issuer transaction identifier is stored by the payment gateway at the level of the alias and the transaction. Depending on how you use the alias (1-click payment, 0-click payment, recurring payment, etc.) the issuer transaction ID will be used as a chaining reference if necessary.</p> </div>
vads_cust_email	Buyer's e-mail address transmitted in the request.
vads_site_id	<p>Shop ID The returned value is the same as the one submitted in the form.</p>
vads_ctx_mode	<p>Operating mode. The returned value (TEST or PRODUCTION) is the same as the one submitted in the form.</p>

To see the recurring payment details, see the parameters below:

Field name	Note
vads_subscription	<p>Recurring payment token The returned value is:</p> <ul style="list-style-type: none"> either the value transmitted in the request, regardless of the result of subscription creation, or the value generated by the payment gateway, if the field has not been transmitted in the request and the subscription has been successfully created (vads_recurrence_status=CREATED). <p>The field vads_subscription will not be returned:</p> <ul style="list-style-type: none"> if it has not been transmitted in the request and the buyer abandons the action (vads_recurrence_status=ABANDONED), if it has not been transmitted in the request and the recurring payment not been created (vads_recurrence_status=NOT_CREATED).
vads_sub_amount	Amount of installments (in the smallest currency unit)
vads_sub_currency	Code of the currency used for the recurring payment.

Field name	Note
	E.g.: 978 for euro (EUR)
vads_sub_desc	Rule for recurring payments to apply according to the iCalendar RFC5545 specification. E.g.: RRULE:FREQ=MONTHLY
vads_sub_effect_date	Subscription start date (or effective date) in the UTC time zone, in YYYYMMDD format. E.g.: 20210601
vads_sub_init_amount	Amount of the first installments. The number of the first installments is defined by vads_sub_init_amount_number . E.g.: 1000
vads_sub_init_amount_number	Number of installments to which the amount, defined by vads_sub_init_amount , will be applied. E.g.: 3



To view the payment details, see the parameters below:

Transaction details:

Field name	Description
vads_operation_type	Transaction type Its value is DEBIT .
vads_occurrence_type	Transaction occurrence type. Its value is UNITAIRE .
vads_amount	Transaction amount. The returned value is the same as the one submitted in the form.
vads_currency	Code of the currency used for the payment.
vads_trans_id	Transaction identifier. The returned value is the same as the one submitted in the form.
vads_trans_uuid	Unique transaction ID. Its value is generated by the payment gateway.
vads_contract_used	MID associated with the transaction.
vads_auth_mode	Type of request made via authorization servers: <ul style="list-style-type: none"> MARK: corresponds to an authorization of EUR 1 (or information request about the CB network if the acquirer supports it). Value also used if the period between the requested capture date and the current date is strictly greater than the authorization validity period. FULL: corresponds to an authorization of the total transaction amount. Value also used if the period between the requested capture date and the current date is strictly shorter than the authorization validity period.
vads_auth_number	Authorization number returned by the authorization server. Empty if the authorization has failed.
vads_auth_result	Return code of the authorization request returned by the issuing bank. Empty in case of an error prior to the authorization.
vads_risk_control	Result of the risk assessment. If at least one verification process returns the ERROR value, the transaction is rejected. See the description of the vads_risk_analysis_result field for more information.
vads_risk_assessment_result	List of actions made with the transaction, following the activation of the advanced risk assessment rules. The possible values are: <ul style="list-style-type: none"> ENABLE_3DS: 3D Secure enabled. DISABLE_3DS: 3D Secure disabled. CHALLENGE_REQUESTED: <ul style="list-style-type: none"> 3DS1 card: The risk module has requested 3DS authentication.

Field name	Description
	<ul style="list-style-type: none"> 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge). CHALLENGE_MANDATE: <ul style="list-style-type: none"> 3DS1 card: The risk module has requested 3DS authentication. 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge for regulatory reasons) for regulatory reasons. MANUAL_VALIDATION: The transaction has been created via manual validation. The payment capture is temporarily blocked to allow the merchant to perform all the desired verification processes. REFUSE: The transaction is refused. RUN_RISK_ANALYSIS: Result of the external risk analyzer. See the description of the vads_risk_analysis_result field for more information. INFORM: A warning message appears. The merchant is notified that a risk has been identified via one or several notification center rules.

Details of the used payment method:

Field name	Note
vads_acquirer_network	Acquirer network code.
vads_bank_code	Code of the issuing bank.
vads_bank_label	Name of the issuing bank of the payment card.
vads_bank_product	Product code of the used card.
vads_brand_management	Allows to know the brand that was used, the list of available brands as well as whether the buyer has changed the default brand chosen by the merchant.
vads_card_brand	Used payment method. See chapter Compatible payment methods to see the list of possible values.
vads_card_country	Country code of the card used in compliance with the ISO 3166 standard.
vads_card_number	Truncated/masked card number.
vads_expiry_month	Expiry month of the used card.  It is advisable to use this data to check the expiration date of the token.
vads_expiry_year	Expiry year of the used card.  It is advisable to use this data to check the expiration date of the token.

Authentication details of the cardholder:

Field name	Note
vads_threeds_auth_type	Cardholder authentication type. Strong cardholder authentication is mandatory when registering a card. The field will therefore always be populated with CHALLENGE .
vads_threeds_enrolled	Enrollment status of the buyer to the 3D Secure program. Possible values are: <ul style="list-style-type: none"> Y: Authentication available. N: Authentication not available. U: Enrollment status to the 3D Secure program unknown.

Field name	Note
	<ul style="list-style-type: none"> empty: Incomplete 3DS authentication process (3DS disabled in the request, unregistered merchant or payment method not eligible for 3DS).
vads_threeds_status	<p>3D Secure authentication result. Possible values are:</p> <ul style="list-style-type: none"> Y: Cardholder authentication success. N: Cardholder authentication error. U: Authentication impossible. A: Authentication attempted but not completed. empty: Unauthorized 3DS authentication (3DS disabled in the request, unregistered cardholder or payment method not eligible for 3DS).

The optional fields transmitted in the request are returned in the response with unmodified values.

16.6.6. Payment by token

In order to understand the result, analyze the following fields:

Field name	Description
vads_page_action	Completed action. The returned value is PAYMENT .
vads_trans_status	<p>Status of the transaction. Possible values are:</p> <ul style="list-style-type: none"> AUTHORISED The authorization request has been accepted. AUTHORISED_TO_VALIDATE The authorization request has been accepted. The merchant must manually validate the transaction. CAPTURED The authorization request has been accepted. The transaction is visible in the "Captured transactions" tab of the Back Office. WAITING_AUTHORISATION The capture delay in the bank exceeds the authorization validity period. The authorization request for the total amount has not yet been sent. WAITING_AUTHORISATION_TO_VALIDATE To be validated and authorized The capture delay in the bank exceeds the authorization validity period. A EUR 1 (or information request about the CB network if the acquirer supports it) authorization has been accepted. The merchant must manually validate the transaction in order to trigger the authorization request and capture. REFUSED The authorization request has been declined. ABANDONED Operation abandoned by the buyer. The transaction is then not visible via the Merchant Back Office.
vads_identifier	Token ID to be debited. The returned value is the same as the one submitted in the form.
vads_cust_email	E-mail address of the buyer associated with the token.
vads_site_id	Shop ID The returned value is the same as the one submitted in the form.
vads_ctx_mode	Operating mode.

Field name	Description
	The returned value (TEST or PRODUCTION) is the same as the one submitted in the form.



To view the payment details, see the parameters below:

Transaction details:

Field name	Description
vads_operation_type	Transaction type Its value is DEBIT .
vads_occurrence_type	Transaction occurrence type. Its value is RECURRENT_INTERMEDIAIRE .
vads_amount	Transaction amount. The returned value is the same as the one submitted in the form.
vads_currency	Code of the currency used for the payment.
vads_trans_id	Transaction identifier. The returned value is the same as the one submitted in the form.
vads_trans_uuid	Unique transaction ID. Its value is generated by the payment gateway.
vads_initial_issuer_transaction_identifier	Unique transaction identifier generated by the issuer.
vads_contract_used	MID associated with the transaction.
vads_auth_mode	Type of request made via authorization servers: <ul style="list-style-type: none"> • MARK: corresponds to an authorization of EUR 1 (or information request about the CB network if the acquirer supports it). Value also used if the period between the requested capture date and the current date is strictly greater than the authorization validity period. • FULL: corresponds to an authorization of the total transaction amount. Value also used if the period between the requested capture date and the current date is strictly shorter than the authorization validity period.
vads_auth_number	Authorization number returned by the authorization server. Empty if the authorization has failed.
vads_auth_result	Return code of the authorization request returned by the issuing bank. See chapter Managing the return codes of the authorization request . Empty in case of an error prior to the authorization.
vads_risk_control	Result of the risk assessment. If at least one verification process returns the ERROR value, the transaction is rejected. See the description of the vads_risk_analysis_result field for more information.
vads_risk_assessment_result	List of actions made with the transaction, following the activation of the advanced risk assessment rules. Possible values are: <ul style="list-style-type: none"> • ENABLE_3DS: 3D Secure enabled. • DISABLE_3DS: 3D Secure disabled. • CHALLENGE_REQUESTED: <ul style="list-style-type: none"> • 3DS1 card: The risk module has requested 3DS authentication. • 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge). • CHALLENGE_MANDATE: <ul style="list-style-type: none"> • 3DS1 card: The risk module has requested 3DS authentication. • 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge for regulatory reasons) for regulatory reasons. • MANUAL_VALIDATION: The transaction has been created via manual validation.

Field name	Description
	<p>The payment capture is temporarily blocked to allow the merchant to perform all the desired verification processes.</p> <ul style="list-style-type: none"> • REFUSE: The transaction is refused. • RUN_RISK_ANALYSIS: Result of the external risk analyzer. See the description of the vads_risk_analysis_result field for more information. • INFORM: A warning message appears. The merchant is notified that a risk has been identified via one or several notification center rules.

Details of the used payment method:

Field name	Note
vads_acquirer_network	Acquirer network code.
vads_bank_code	Code of the issuing bank.
vads_bank_label	Name of the issuing bank of the payment card.
vads_bank_product	Product code of the used card.
vads_brand_management	Allows to know the brand that was used, the list of available brands as well as whether the buyer has changed the default brand chosen by the merchant.
vads_card_brand	Used payment method. See chapter Compatible payment methods to see the list of possible values.
vads_card_country	Country code of the card used in compliance with the ISO 3166 standard.
vads_card_number	Truncated/masked card number.
vads_expiry_month	Expiry month of the used card.  It is advisable to use this data to check the expiration date of the token.
vads_expiry_year	Expiry year of the used card.  It is advisable to use this data to check the expiration date of the token.

Details of strong authentication:

Field name	Note
vads_threeds_auth_type	<p>Cardholder authentication type. Possible values are:</p> <ul style="list-style-type: none"> • "Empty" if the buyer is not correctly authenticated. • FRICTIONLESS: cardholder authentication without interaction with the ACS. Value returned only in 3DS v2. • CHALLENGE: interactive cardholder authentication (entering an OTP or replying to a series of questions). Value returned in 3DS v1 and 3DS v2.
vads_threeds_enrolled	<p>Enrollment status of the buyer to the 3D Secure program. Possible values are:</p> <ul style="list-style-type: none"> • Y: Authentication available. • N: Authentication not available. • U: Enrollment status to the 3D Secure program unknown. • empty: Incomplete 3DS authentication process (3DS disabled in the request, unregistered merchant or payment method not eligible for 3DS).
vads_threeds_status	<p>3D Secure authentication result. Possible values are:</p> <ul style="list-style-type: none"> • Y: Cardholder authentication success.

Field name	Note
	<ul style="list-style-type: none"> • N: Cardholder authentication error. • U: Authentication impossible. • A: Authentication attempted but not completed. • empty: Unauthorized 3DS authentication (3DS disabled in the request, unregistered cardholder or payment method not eligible for 3DS).

The optional fields transmitted in the request are returned in the response with unmodified values.

16.6.7. Creating a recurring payment

In order to understand the result, analyze the following fields:



Field name	Description
vads_page_action	Completed action. The returned value is SUBSCRIBE .
vads_recurrence_status	Recurrence creation status. The possible values are: <ul style="list-style-type: none"> • CREATED: The recurring payment has been successfully created. • NOT_CREATED: The recurring payment is not created. • ABANDONED: action abandoned by the buyer. The recurring payment is not created.
vads_identifier	Token ID to be debited. The returned value is the same as the one submitted in the form.
vads_cust_email	E-mail address of the buyer associated with the token.
vads_site_id	Shop ID The returned value is the same as the one submitted in the form.
vads_ctx_mode	Operating mode. The returned value (TEST or PRODUCTION) is the same as the one submitted in the form.

To see the recurring payment details, see the parameters below:

Field name	Note
vads_subscription	Recurring payment token The returned value is: <ul style="list-style-type: none"> • either the value transmitted in the request, regardless of the result of subscription creation, • or the value generated by the payment gateway, if the field has not been transmitted in the request and the subscription has been successfully created (vads_recurrence_status=CREATED). The field vads_subscription will not be returned: <ul style="list-style-type: none"> • if it has not been transmitted in the request and the buyer abandons the action (vads_recurrence_status=ABANDONED), • if it has not been transmitted in the request and the recurring payment not been created (vads_recurrence_status=NOT_CREATED).
vads_sub_amount	Amount of installments (in the smallest currency unit)
vads_sub_currency	Code of the currency used for the recurring payment. E.g.: 978 for euro (EUR)
vads_sub_desc	Rule for recurring payments to apply according to the iCalendar RFC5545 specification. E.g.: RRULE:FREQ=MONTHLY

Field name	Note
vads_sub_effect_date	Subscription start date (or effective date) in the UTC time zone, in YYYYMMDD format. E.g.: 20210601
vads_sub_init_amount	Amount of the first installments. The number of the first installments is defined by vads_sub_init_amount_number . E.g.: 1000
vads_sub_init_amount_number	Number of installments to which the amount, defined by vads_sub_init_amount , will be applied. E.g.: 3

Details of the used payment method:

Field name	Note
vads_acquirer_network	Acquirer network code.
vads_bank_code	Code of the issuing bank.
vads_bank_label	Name of the issuing bank of the payment card.
vads_bank_product	Product code of the used card.
vads_brand_management	Allows to know the brand that was used, the list of available brands as well as whether the buyer has changed the default brand chosen by the merchant.
vads_card_brand	Used payment method. See chapter Compatible payment methods to see the list of possible values.
vads_card_country	Country code of the card used in compliance with the ISO 3166 standard.
vads_card_number	Truncated/masked card number.
vads_expiry_month	Expiry month of the used card.  It is advisable to use this data to check the expiration date of the token.
vads_expiry_year	Expiry year of the used card.  It is advisable to use this data to check the expiration date of the token.

Details of strong authentication performed when creating the token:

Field name	Note
vads_threeds_auth_type	Cardholder authentication type. Strong cardholder authentication is mandatory when registering a card. The field will therefore always be populated with CHALLENGE .
vads_threeds_enrolled	Enrollment status of the buyer to the 3D Secure program. Possible values are: <ul style="list-style-type: none"> Y: Authentication available. N: Authentication not available. U: Enrollment status to the 3D Secure program unknown. empty: Incomplete 3DS authentication process (3DS disabled in the request, unregistered merchant or payment method not eligible for 3DS).
vads_threeds_status	3D Secure authentication result. Possible values are: <ul style="list-style-type: none"> Y: Cardholder authentication success. N: Cardholder authentication error. U: Authentication impossible. A: Authentication attempted but not completed.

Field name	Note
	<ul style="list-style-type: none"> empty: Unauthorized 3DS authentication (3DS disabled in the request, unregistered cardholder or payment method not eligible for 3DS).

The optional fields transmitted in the request are returned in the response with unmodified values.

16.6.8. Payment with the token creation option for the cardholder

In order to understand the result, analyze the following fields:

Field name	Description
vads_page_action	Completed action. The returned value is ASK_REGISTER_PAY .
vads_identifier_status	<p>Token creation status.</p> <p>The field will not be sent if the buyer has not given the approval to register their card details.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> CREATED: the request for authorization or information, if supported by the acquirer is accepted. Token has been successfully created. NOT_CREATED: the request for authorization or information has been rejected. The token has not been created, and therefore cannot be viewed in the Merchant Back Office. ABANDONED: action abandoned by the buyer. The token has not been created, and therefore cannot be viewed in the Merchant Back Office.
vads_trans_status	<p>Status of the transaction.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> AUTHORISED The authorization or information request has been accepted. The token has been created and is visible in the Merchant Back Office. AUTHORISED_TO_VALIDATE The authorization or information request has been accepted. The merchant must manually validate the transaction. The token has been created and is visible in the Merchant Back Office. CAPTURED The authorization or information request has been accepted. The transaction is visible in the "Captured transactions" tab of the Back Office. The token has been created and is visible in the Merchant Back Office. WAITING_AUTHORISATION The capture delay in the bank exceeds the authorization validity period. The authorization request for the total amount has not yet been sent. The token has been created and is visible in the Merchant Back Office. WAITING_AUTHORISATION_TO_VALIDATE To be validated and authorized The capture delay in the bank exceeds the authorization validity period. A EUR 1 (or information request about the CB network if the acquirer supports it) authorization has been accepted. The merchant must manually validate the transaction in order to trigger the authorization request and capture. REFUSED The authorization or information request has been rejected. The token is not created. ABANDONED

Field name	Description
	Operation abandoned by the buyer. The transaction is then not visible via the Merchant Back Office. The token is not created.
vads_identifier	Token ID. The field will not be sent if the buyer has not given the approval to register their card details. The returned value is: <ul style="list-style-type: none"> either the value transmitted in the request, regardless of the result of token creation, even in case of abandoned action, or the value generated by the payment gateway, if the field is not transmitted in the request and the token has been successfully created (vads_identifier_status=CREATED). Note If you have activated the token uniqueness check and the payment method is already registered with another token, then this token will be returned. The field vads_identifier will not be returned: <ul style="list-style-type: none"> if it has not been transmitted in the request and the buyer abandons the action (vads_identifier_status=ABANDONED), if it has not been transmitted in the request and the token has not been created (vads_identifier_status=NOT_CREATED).
vads_cust_email	Buyer's e-mail address transmitted in the request.
vads_site_id	Shop ID The returned value is the same as the one submitted in the form.
vads_ctx_mode	Operating mode. The returned value (TEST or PRODUCTION) is the same as the one submitted in the form.



To view the payment details, see the parameters below:

Transaction details:

Field name	Description
vads_operation_type	Transaction type Its value is DEBIT .
vads_amount	Transaction amount. The returned value is the same as the one submitted in the form.
vads_currency	Code of the currency used for the payment.
vads_trans_id	Transaction identifier. The returned value is the same as the one submitted in the form.
vads_trans_uuid	Unique transaction ID. Its value is generated by the payment gateway.
vads_initial_issuer_transaction_identifier	Unique transaction identifier generated by the issuer.
vads_contract_used	MID associated with the transaction.
vads_auth_mode	Type of request made via authorization servers: <ul style="list-style-type: none"> MARK: corresponds to an authorization of EUR 1 (or information request about the CB network if the acquirer supports it). Value also used if the period between the requested capture date and the current date is strictly greater than the authorization validity period. FULL: corresponds to an authorization of the total transaction amount. Value also used if the period between the requested capture date and the current date is strictly shorter than the authorization validity period.
vads_auth_number	Authorization number returned by the authorization server. Empty if the authorization has failed.
vads_auth_result	Return code of the authorization request returned by the issuing bank. See chapter Managing the return codes of the authorization request .

Field name	Description
	Empty in case of an error prior to the authorization.
vads_risk_control	<p>Result of the risk assessment.</p> <p>If at least one verification process returns the ERROR value, the transaction is rejected.</p> <p>See the description of the vads_risk_analysis_result field for more information.</p>
vads_risk_assessment_result	<p>List of actions made with the transaction, following the activation of the advanced risk assessment rules.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • ENABLE_3DS: 3D Secure enabled. • DISABLE_3DS: 3D Secure disabled. • CHALLENGE_REQUESTED: <ul style="list-style-type: none"> • 3DS1 card: The risk module has requested 3DS authentication. • 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge). • CHALLENGE_MANDATE: <ul style="list-style-type: none"> • 3DS1 card: The risk module has requested 3DS authentication. • 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge for regulatory reasons) for regulatory reasons. • MANUAL_VALIDATION: The transaction has been created via manual validation. The payment capture is temporarily blocked to allow the merchant to perform all the desired verification processes. • REFUSE: The transaction is refused. • RUN_RISK_ANALYSIS: Result of the external risk analyzer. See the description of the vads_risk_analysis_result field for more information. • INFORM: A warning message appears. The merchant is notified that a risk has been identified via one or several notification center rules.

Details of the used payment method:

Field name	Note
vads_acquirer_network	Acquirer network code.
vads_bank_code	Code of the issuing bank.
vads_bank_label	Name of the issuing bank of the payment card.
vads_bank_product	Product code of the used card.
vads_brand_management	Allows to know the brand that was used, the list of available brands as well as whether the buyer has changed the default brand chosen by the merchant.
vads_card_brand	Used payment method. See chapter Compatible payment methods to see the list of possible values.
vads_card_country	Country code of the card used in compliance with the ISO 3166 standard.
vads_card_number	Truncated/masked card number.
vads_expiry_month	<p>Expiry month of the used card.</p> <div>  <p>It is advisable to use this data to check the expiration date of the token.</p> </div>
vads_expiry_year	<p>Expiry year of the used card.</p> <div>  <p>It is advisable to use this data to check the expiration date of the token.</p> </div>

Authentication details of the cardholder:

Field name	Note
vads_threeds_auth_type	Cardholder authentication type. Strong cardholder authentication is mandatory when registering a card. The field will therefore always be populated with CHALLENGE .
vads_threeds_enrolled	Enrollment status of the buyer to the 3D Secure program. Possible values are: <ul style="list-style-type: none"> • Y: Authentication available. • N: Authentication not available. • U: Enrollment status to the 3D Secure program unknown. • empty: Incomplete 3DS authentication process (3DS disabled in the request, unregistered merchant or payment method not eligible for 3DS).
vads_threeds_status	3D Secure authentication result. Possible values are: <ul style="list-style-type: none"> • Y: Cardholder authentication success. • N: Cardholder authentication error. • U: Authentication impossible. • A: Authentication attempted but not completed. • empty: Unauthorized 3DS authentication (3DS disabled in the request, unregistered cardholder or payment method not eligible for 3DS).

The optional fields transmitted in the request are returned in the response with unmodified values.

16.6.9. Installment payment

In order to understand the result, analyze the following fields:

Field name	Description
vads_page_action	Completed action. The returned value is PAYMENT .
vads_trans_status	Status of the transaction. Possible values are: <ul style="list-style-type: none"> • AUTHORISED The authorization request has been accepted. • AUTHORISED_TO_VALIDATE The authorization request has been accepted. The merchant must manually validate the transaction. • CAPTURED The authorization request has been accepted. The transaction is visible in the "Captured transactions" tab of the Back Office. • REFUSED The authorization request has been declined.
vads_identifier	Token ID.
vads_cust_email	Buyer's e-mail address.
vads_site_id	Shop ID
vads_ctx_mode	Operating mode.

To see the recurring payment details, see the parameters below:

Field name	Note
vads_subscription	Recurring payment token
vads_recurrence_number	Recurrence number of the recurring payment.



To view the payment details, see the parameters below:

Transaction details:

Field name	Description
vads_operation_type	Transaction type Its value is DEBIT .
vads_occurrence_type	Transaction occurrence type. Possible values: <ul style="list-style-type: none"> RECURRENT_INITIAL: First installment. RECURRENT_INTERMEDIAIRE: Nth installment. View the vads_recurrence_number field to know the installment number. RECURRENT_FINAL: Last installment.
vads_amount	Transaction amount. The returned value is the same as the one submitted in the form.
vads_currency	Code of the currency used for the payment.
vads_trans_id	Transaction identifier. The returned value is the same as the one submitted in the form.
vads_trans_uuid	Unique transaction ID. Its value is generated by the payment gateway.
vads_contract_used	MID associated with the transaction.
vads_auth_mode	Type of request made via authorization servers: <ul style="list-style-type: none"> MARK: corresponds to an authorization of EUR 1 (or information request about the CB network if the acquirer supports it). Value also used if the period between the requested capture date and the current date is strictly greater than the authorization validity period. FULL: corresponds to an authorization of the total transaction amount. Value also used if the period between the requested capture date and the current date is strictly shorter than the authorization validity period.
vads_auth_number	Authorization number returned by the authorization server. Empty if the authorization has failed.
vads_auth_result	Return code of the authorization request returned by the issuing bank. See chapter Managing the return codes of the authorization request . Empty in case of an error prior to the authorization.
vads_risk_control	Result of the risk assessment. If at least one verification process returns the ERROR value, the transaction is rejected. See the description of the vads_risk_analysis_result field for more information.
vads_risk_assessment_result	List of actions made with the transaction, following the activation of the advanced risk assessment rules. Possible values are: <ul style="list-style-type: none"> ENABLE_3DS: 3D Secure enabled. DISABLE_3DS: 3D Secure disabled. CHALLENGE_REQUESTED: <ul style="list-style-type: none"> 3DS1 card: The risk module has requested 3DS authentication. 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge). CHALLENGE_MANDATE: <ul style="list-style-type: none"> 3DS1 card: The risk module has requested 3DS authentication.

Field name	Description
	<ul style="list-style-type: none"> 3DS2 card: The risk module has requested an authentication with cardholder interaction (challenge for regulatory reasons) for regulatory reasons. MANUAL_VALIDATION: The transaction has been created via manual validation. The payment capture is temporarily blocked to allow the merchant to perform all the desired verification processes. REFUSE: The transaction is refused. RUN_RISK_ANALYSIS: Result of the external risk analyzer. See the description of the vads_risk_analysis_result field for more information. INFORM: A warning message appears. The merchant is notified that a risk has been identified via one or several notification center rules.

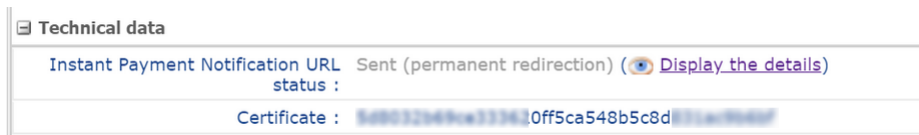
Details of the used payment method:

Field name	Note
vads_acquirer_network	Acquirer network code.
vads_bank_code	Code of the issuing bank.
vads_bank_label	Name of the issuing bank of the payment card.
vads_bank_product	Product code of the used card.
vads_brand_management	Allows to know the brand that was used, the list of available brands as well as whether the buyer has changed the default brand chosen by the merchant.
vads_card_brand	Used payment method. See chapter Compatible payment methods to see the list of possible values.
vads_card_country	Country code of the card used in compliance with the ISO 3166 standard.
vads_card_number	Truncated/masked card number.
vads_expiry_month	Expiry month of the used card. <div>  It is advisable to use this data to check the expiration date of the token. </div>
vads_expiry_year	Expiry year of the used card. <div>  It is advisable to use this data to check the expiration date of the token. </div>

16.7. Running tests and troubleshooting

In order to test the notifications, follow the steps below:

1. Make a payment (in TEST mode or in PRODUCTION mode).
2. Once the payment is complete, look for the transaction in your Back Office (**Management > Transactions** or **TEST Transactions** menu if you made the payment in TEST mode).
3. Double-click the transaction to view the **transaction details**.
4. In the transaction details, search for the section entitled **Technical data**.
5. Check the status of the Instant Payment Notification URL:



The list of possible statuses is provided below:

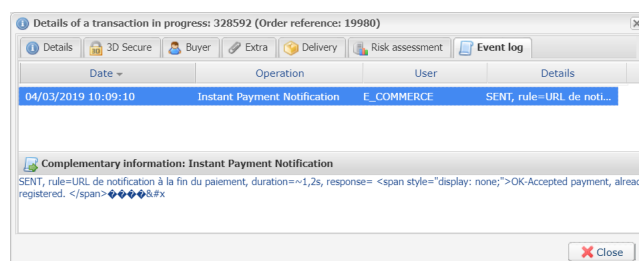
Status	Description
N/A	The transaction did not result in a notification or no notification rules have been enabled.
Undefined URL	An event has triggered the end of payment notification rule but the URL is not configured.
Call in progress	The notification is in progress. This status is temporary.
Sent	The notification has been successfully sent and a remote device returned an HTTP 200, 201, 202, 203, 204, 205 or 206 response status code.
Sent (permanent redirection)	The merchant website has returned an HTTP 301 or 308 response status code with a new URL to contact. A new call in POST mode has been made to the new URL.
Sent (temporary redirection)	The merchant website has returned an HTTP 302 or 307 response status code with a new URL to contact. A new call in POST mode has been made to the new URL.
Sent (redirection to another page)	The merchant website has returned an HTTP 303 response status code with a new URL to contact. A new call in GET mode has been made to the new URL.
Failed	Generic error different from the codes described below.
Server unavailable	The notification has lasted more than 35s.
SSL handshake failure	Your server is incorrectly configured. Run a test on the Qualys website (https://www.ssllabs.com/ssltest/) and correct the errors.
Connection interrupted	Communication error.
Connection refused	Communication error.
Server error 300	Case of redirection not supported by the gateway.
Server error 304	Case of redirection not supported by the gateway.
Server error 305	Case of redirection not supported by the gateway.
Server error 400	The merchant website returned a HTTP 400 Bad Request code.
Server error 401	The merchant website returned a HTTP 401 Unauthorized code. Make sure that the resource is not protected by an .htaccess file.
Server error 402	The merchant website returned a HTTP 402 Payment Required code.
Server error 403	The merchant website returned a HTTP 403 Forbidden code. Make sure that the resource is not protected by an .htaccess file.
Server error 404	The merchant website returned a HTTP 404 Not Found code. Make sure that the URL is correctly specified in the rule configuration. Make sure that the file is present on your server.
Server error 405	The merchant website returned a HTTP 405 Method Not allowed code.
Server error 406	The merchant website returned a HTTP 406 Not Acceptable code.
Server error 407	The merchant website returned a HTTP 407 Proxy Authentication Required code.

Status	Description
Server error 408	The merchant website returned a HTTP 408 Request Time-out code.
Server error 409	The merchant website returned a HTTP 409 Conflict code.
Server error 410	The merchant website returned a HTTP 410 Gone code.
Server error 411	The merchant website returned a HTTP 411 Length Required code.
Server error 412	The merchant website returned a HTTP 412 Precondition Failed code.
Server error 413	The merchant website returned a HTTP 413 Request Entity Too Large code.
Server error 414	The merchant website returned a HTTP 414 Request-URI Too long code.
Server error 415	The merchant website returned a HTTP 415 Unsupported Media Type code.
Server error 416	The merchant website returned a HTTP 416 Requested range unsatisfiable code.
Server error 417	The merchant website returned a HTTP 417 Expectation failed code.
Server error 419	The merchant website returned a HTTP 419 Authentication Timeout code.
Server error 421	The merchant website returned a HTTP 421 Misdirected Request code.
Server error 422	The merchant website returned a HTTP 422 Unprocessable Entity code.
Server error 423	The merchant website returned a HTTP 423 Locked code.
Server error 424	The merchant website returned a HTTP 424 Failed Dependency code.
Server error 425	The merchant website returned a HTTP 425 Too Early code.
Server error 426	The merchant website returned a HTTP 426 Upgrade Required code.
Server error 429	The merchant website returned a HTTP 431 Request Header Fields Too Large code.
Server error 431	The merchant website returned a HTTP 415 Unsupported Media Type code.
Server error 451	The merchant website returned a HTTP 451 Unavailable For Legal Reasons code.
Server error 500	The merchant website returned a HTTP 500 Internal Server Error code. An application error has occurred on the level of the server hosting your shop. See the logs of your HTTP server (usually apache). The issue can only be corrected by performing an action on your server.
Server error 501	The merchant website returned a HTTP 501 Not Implemented code.
Server error 502	The merchant website returned a HTTP 502 Bad Gateway / Proxy Error code.
Server error 503	The merchant website returned a HTTP 503 Service Unavailable code.
Server error 504	The merchant website returned a HTTP 504 Gateway Time-out code. The merchant server has not accepted the call within the time limit of 10s.
Server error 505	The merchant website returned a HTTP 505 HTTP Version not supported code.

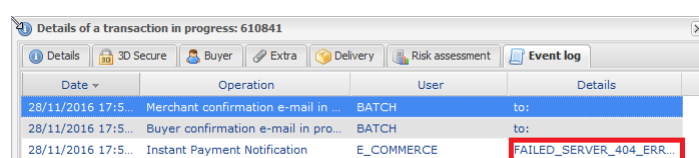
For more information on a notification, click the link **Display the details** or click the **Event log** tab and search for the line **Notification URL call**.

In order to help the merchant identify the source of the error, the gateway systematically analyses the 512 first characters returned by the merchant website and displays them in the **Details** column.

- Example of a successfully processed notification:



- Example of a failed notification:



If the payment gateway is unable to access the URL of your page, an e-mail alert will be sent to the shop administrator.

It contains:

- The HTTP code of the encountered error
- Parts of error analysis
- Its consequences
- Instructions to follow via the Merchant Back Office for resending the request to the URL specified in step 4

17. OBTAINING HELP

Looking for help? Check our FAQ on our website

<https://paiement.systempay.fr/doc/en-EN/faq/sitemap.html>

For any technical inquiries or if you need any help, contact [technical support](#).

In view of facilitating the processing of your requests, please specify your shop ID (an 8-digit number) in your query

This information is available in the “registration of your shop” e-mail or in the Merchant Back Office (**Settings > Shop > Configuration**).

18. APPENDIX

18.1. Automatically creating a recurring payment via Web services

Use the **Charge/CreateSubscription** method to make recurring payments (subscription) using an existing and valid token.

For more information, see the description of the [Charge/CreateSubscription](#) method.

18.2. Automatically canceling a recurring payment via Web services

Use the **Subscription/Cancel** method to cancel a recurring payment.

For more information, see the description of the [Subscription/Cancel](#) method.

18.3. Test cards

Test cards are available on the payment page.

Depending on the test scenario associated with the card, they allow:

- To create a token and/or a recurring payment only if the test result is "Payment accepted".
- To not create a token if the test result is "Payment refused".

In order to test the behavior when an installment is refused, you must use the following test card:

Card number	Test card checked
4970101000001002	Token creation OK - Payment refused due to exceeded limit if the installment amount is higher than 0.

Note

This card is not offered on the payment page upon token creation.