Transaction management

Back Office user manual

Document version 2.11

DEVELOPPONS ENSEMBLE
L'ESPRIT D'EQUIPE

Contents

1. HISTORY OF THE DOCUMENT

Version	Author	Date	Comment
2.11	Société Générale	2/7/2024	- Update of the *Refunding a transaction* chapter - Update of the *Searching for a transaction in progress* chapter - Update of the *Searching for a captured transaction* chapter - Update of the *Viewing buyer details* chapter - Update of the document structure
2.10	Société Générale	3/30/2023	- Chapter updates in *Transaction lifecycle*. - Update of the chapter *Transaction with failed 3D Secure authentication*.
2.9	Société Générale	1/23/2023	- Modification of the *Configuring the display of the counter value currency* chapter: currency conversion is now performed in the company's currency, not just in euros. - Update of the chapter *Refunding a transaction*.

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 Société Générale. All rights reserved.

2. VIDEO TUTORIAL

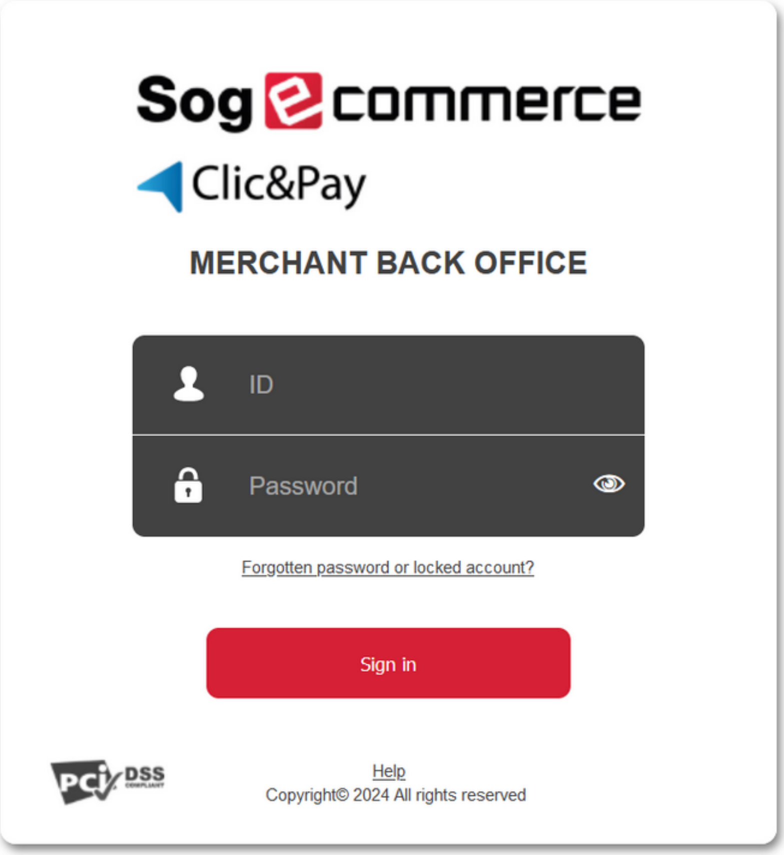
For more information, go to *our video tutorials page* available on the documentary site.

Video tutorials

3. SIGNING IN TO THE MERCHANT BACK OFFICE

Your Back Office is accessible via:

https://sogecommerce.societegenerale.eu/vads-merchant/


Sogecommerce
Clic&Pay
MERCHANT BACK OFFICE
ID
Password
Forgotten password or locked account?
Sign in
PCI DSS
Help
Copyright© 2024 All rights reserved

1. Enter your username.

   Your connection identifiers (username and password) are sent to you in an e-mail with the subject **Connection identifiers - [your shop name]**.

2. Enter your password.

   Your connection identifiers (username and password) are sent to you in an e-mail with the subject **Connection identifiers - [your shop name]**.

3. Click **Sign in**.

   The user account is blocked after 3 wrong password entries. If your account is blocked, click **Forgotten password or locked account** to reset it.

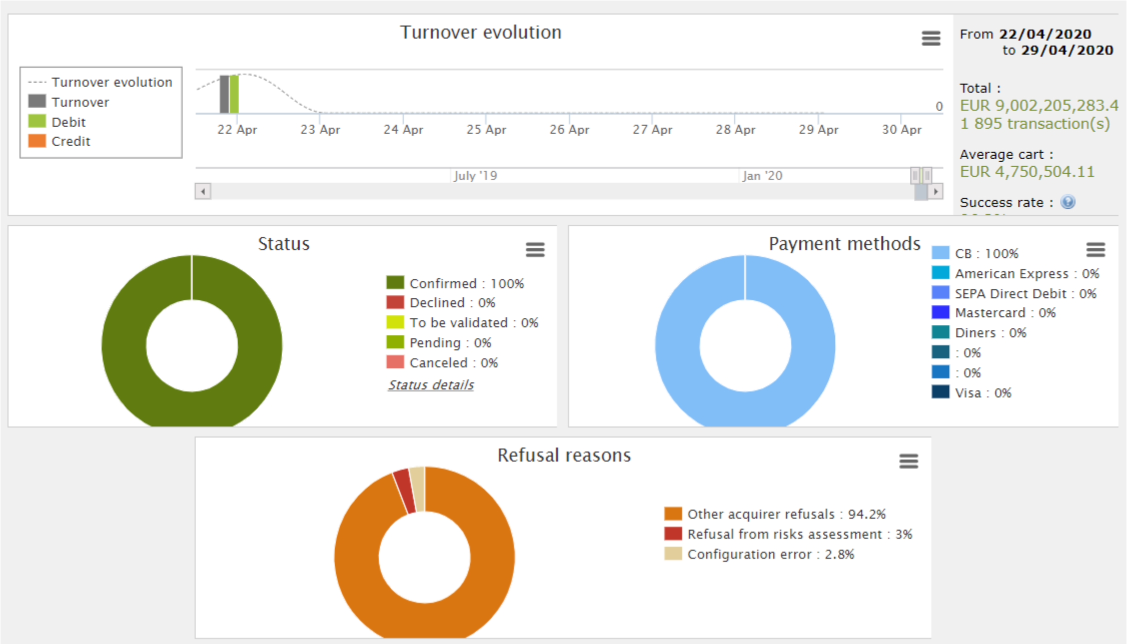
   > The user password is valid for 90 days. After this period, the user must modify it by logging into their account.

4. VIEWING THE DASHBOARD

Access to the **Dashboard** requires to be configured. If the **Dashboard** menu does not appear in your Merchant Back Office, please contact your customer advisorSociété Générale.

To display the dashboard, click **Management** > **Dashboard**

The graph page appears.



From **22/04/2020**
to **29/04/2020**

Total :
EUR 9,002,205,283.4
1 895 transaction(s)

Average cart :
EUR 4,750,504.11

Success rate :

The shops chosen in this dashboard example are in **mono currency** but these graphs also work in **multi currency** cases.

4 types of data are analyzed:

- **The evolution of the number of transactions and/or of the turnover.**

  The graphs are presented as a histogram. The data is analyzed and compared over a specific period of time.

  At any moment, the user can hover the cursor over a specific period of time to display a tooltip with the amounts and/or transactions analyzed in this period.

- **The different payment statuses.**

  The graphs are presented as a circle. The data is analyzed and compared in real time over a specific period of time.

  At any moment, the user can hover the cursor over a payment status to display a tooltip with the desired amounts and transactions.

  The different analyzed statutes are:

  - Canceled
  - To be validated
  - Confirmed
  - Failed
  - Pending
  - Refused

- **The different payment methods used during the transactions.**

  The graphs are presented as a circle. The data is analyzed and compared in real time over a specific period of time.

  At any moment, the user can hover the cursor over a payment method to display a tooltip with the amounts and transactions performed using this payment method.

- **The different reasons for refusal.**

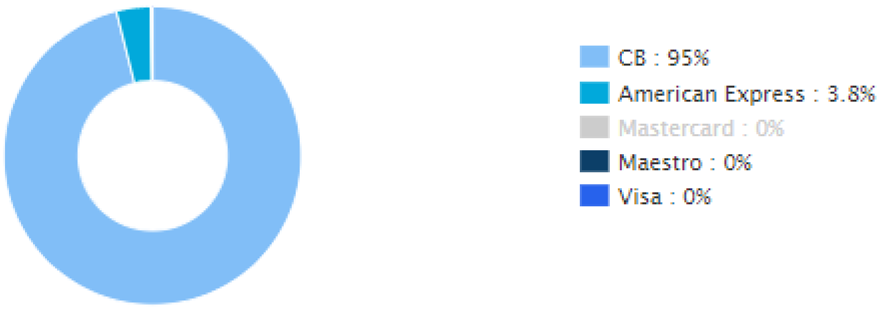
  The graphs are presented as a circle. The data is analyzed and compared in real time over a specific period of time.

  At any moment, the user can hover the cursor over a refusal motive to display a tooltip with the amounts and the number of transactions concerned by this refusal.

  The different categories of the analyzed reasons for refusal are:

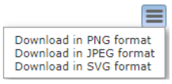
  - 3D Secure abandonment
  - Other acquirer refusals
  - Invalid card
  - Lost or stolen card
  - Configuration error
  - Suspected fraud
  - Do not honor
  - Limit exceeded / insufficient funds
  - 3D Secure refusal
  - Refusal from risk assessment
  - Transaction not allowed

At any moment, the user can apply filters to a graph by clicking on one or more elements in its caption.



Example: in this screenshot, the user does not want to analyze the transactions made with **Mastercard**. He or she clicks on the payment method to set it to zero (**0**) and exclude it from the analysis. All the user needs to do to reintegrate the payment method into the graph is click on the payment method once again.

The user can download each graph in PNG, JPEG or SVG format.
To do this, the user needs to click the download icon and choose its format.



5. VIEWING TRANSACTIONS

Via the **Management** menu, the merchant has access to real and TEST transactions.

Note:

Depending on the access rights, TEST transactions (e.g.: developer profile) and/or real transactions (e.g.: accountant profile) can be displayed.

The user interface is presented as follows:

- **Dashboard**

  History of the turnover

- **Search tool**

  - Transactions is progress

  Allows you to search for all the transactions that have not yet been captured (e.g. expired, refused, waiting for authorization, to be validated, pre-authorized, waiting for capture, etc.).

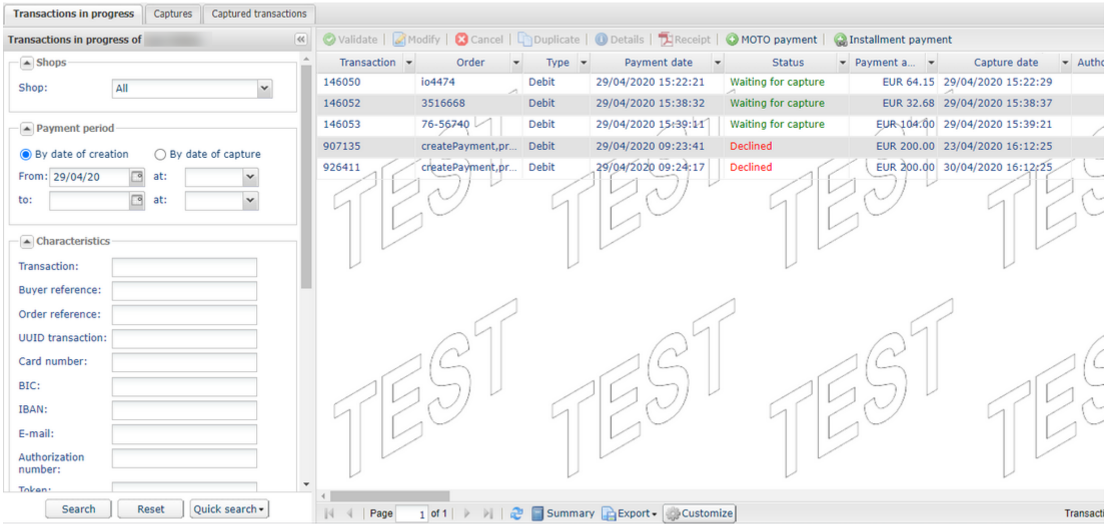
  - Captures

  Allows to find the list of all the captures sorted by the acquirer contract.

  - Captured transactions

  Allows to find all the transactions captured by the acquirer.

- **Transaction details view**



Transactions in progress of [redacted]

Shop: All

● By date of creation ○ By date of capture

From: 29/04/20 at:

to: at:

Transaction:

Buyer reference:

Order reference:

UUID transaction:

Card number:

BIC:

IBAN:

E-mail:

Authorization number:

Token:

Transaction	Order	Type	Payment date	Status	Payment a...	Capture date	Autho
146050	io4474	Debit	29/04/2020 15:22:21	Waiting for capture	EUR 64.15	29/04/2020 15:22:29	
146052	3516668	Debit	29/04/2020 15:38:32	Waiting for capture	EUR 32.68	29/04/2020 15:38:37	
146053	76-56740	Debit	29/04/2020 15:39:11	Waiting for capture	EUR 104.00	29/04/2020 15:39:21	
907135	createPayment,pr...	Debit	29/04/2020 09:23:41	Declined	EUR 200.00	23/04/2020 16:12:25	
926411	createPayment,pr...	Debit	29/04/2020 09:24:17	Declined	EUR 200.00	30/04/2020 16:12:25	

The content of the **Transactions in progress** tab is displayed by default. All the transactions of the day are listed. Old transactions can be accessed via search.

Click on the **Captured transactions** tab to display captured payments.

You always have the possibility to make exports.

6. CUSTOMIZING THE DISPLAY OF THE TRANSACTION TABLE

You can modify the page display for captured or in-progress transactions by adding, deleting or modifying the column order.

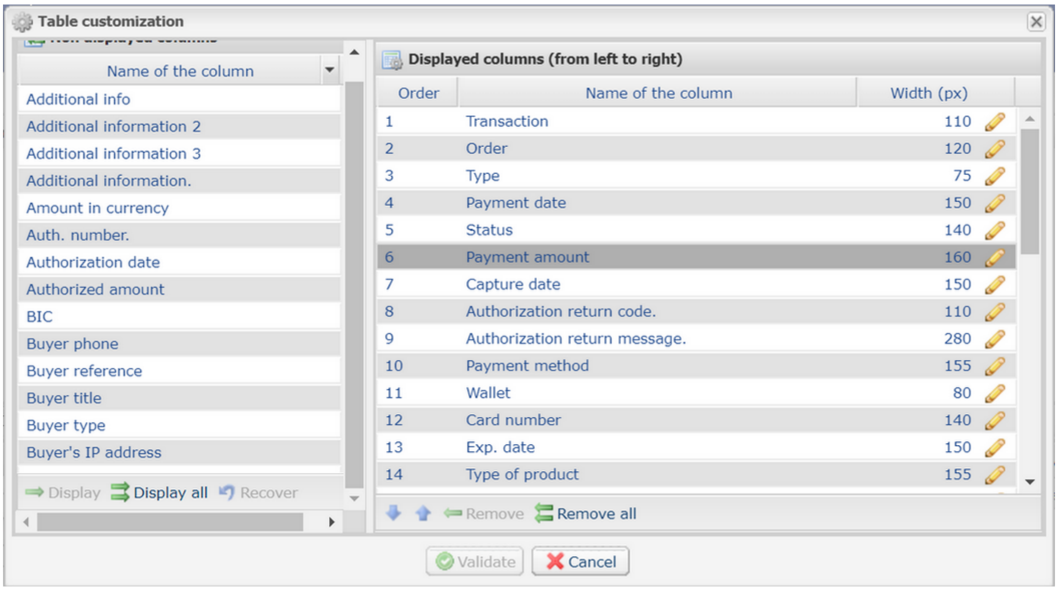
The new display will be used for:

- exporting transactions
- generating transaction logs

In order to modify the column display

1. Select the tab of your choice
2. Click on **Customize** at the bottom of the page

   The following window appears.



Name of the column
Additional info
Additional information 2
Additional information 3
Additional information.
Amount in currency
Auth. number.
Authorization date
Authorized amount
BIC
Buyer phone
Buyer reference
Buyer title
Buyer type
Buyer's IP address

Order	Name of the column	Width (px)
1	Transaction	110
2	Order	120
3	Type	75
4	Payment date	150
5	Status	140
6	Payment amount	160
7	Capture date	150
8	Authorization return code.	110
9	Authorization return message.	280
10	Payment method	155
11	Wallet	80
12	Card number	140
13	Exp. date	150
14	Type of product	155

To display a column:

1. Select the column in the **Non-displayed columns** area.
2. Click **Display** or drag-and-drop the column to **Displayed columns**.

To remove a column:

1. Select the column in the **Displayed columns** area.
2. Click **Remove** or drag-and-drop the column to **Non-displayed columns**.

To move a column:

Select the column in the **Displayed columns** area.

Click ⬇ or ⬆ until you obtain the desired position.

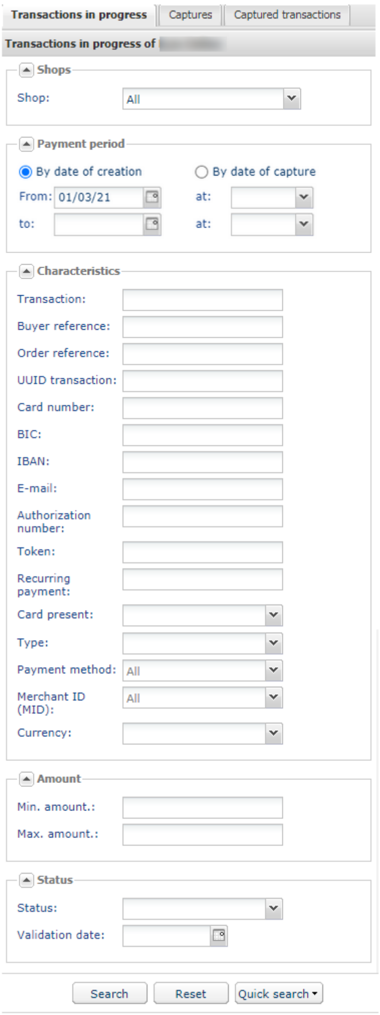
Click the **Validate** button to save the changes.

The following table provides the meaning of the different icons used in the **Table customization** window. You can use them to facilitate your customization.

Icon	Description	Icon	Description
⬇	Move the selected column to the bottom	⬆	Move the selected column to the top
⇉	Display all columns	⇇	Hide all columns
⇨	Display the selected column(s)	⇦	Hide the selected column(s)
↶	Restore tables to their initial state		

Table 1: Icons used in the Table customization

7. SEARCHING FOR A TRANSACTION IN PROGRESS



Transactions in progress of [redacted]

Shops

Shop: All

Payment period

● By date of creation ○ By date of capture

From: 01/03/21 at:

to: at:

Characteristics

Transaction:

Buyer reference:

Order reference:

UUID transaction:

Card number:

BIC:

IBAN:

E-mail:

Authorization number:

Token:

Recurring payment:

Card present:

Type:

Payment method: All

Merchant ID (MID): All

Currency:

Amount

Min. amount.:

Max. amount.:

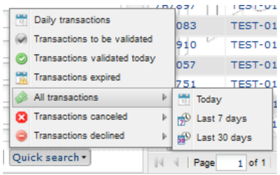
Status

Status:

Validation date:

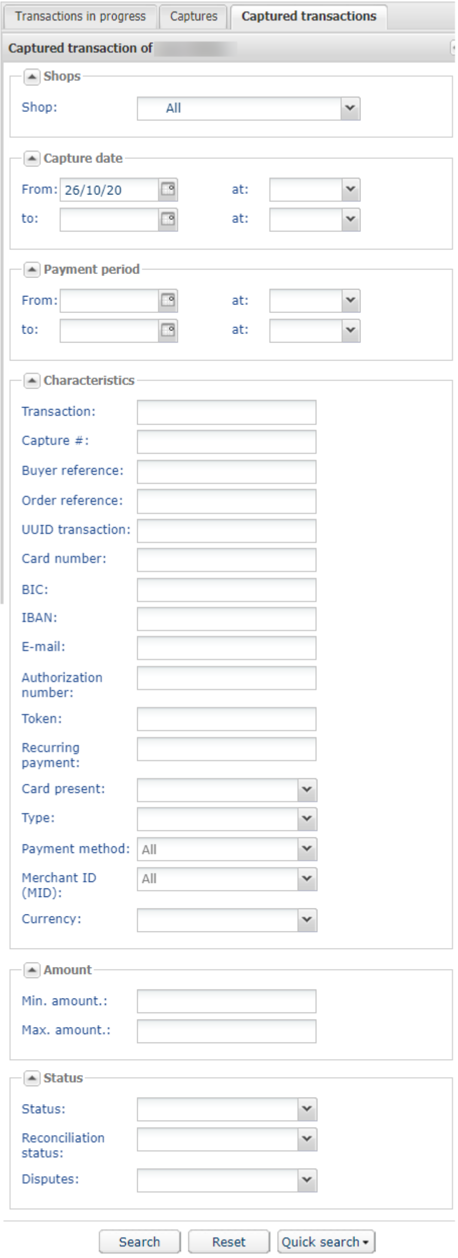
Via the search tool:

1. Select **Transactions is progress**.
2. Fill in your search criteria.
   There can be multiple search criteria. There are no restrictions to the number of criteria. However, the more criteria there are, the longer the response time will be. In the event of a time-out, the merchant is prompted to limit his/her search range.
   The search criteria are:
   - Shops ('all' by default)
   - Date/time of creation
   - Date/time of capture in the bank
   - Merchant order reference (provided by the merchant in the form)
   - Buyer's e-mail address
   - Buyer reference (buyer code provided by the merchant)
   - UUID (unique payment reference generated by the payment gateway and returned to the merchant website at the end of the payment)
   - Payment card number, BIC or IBAN
   - Transaction number
   - Authorization number
   - Token (Buyer ID or UMR)
   - Recurring payment reference associated with the token
   - Card presence
   - Type of operation:
     - **debit**: the merchant account is credited,
     - **credit**: the buyer's account is credited,
     - **verification**: operation allowing to check the card validity. It never results in a debit or a credit.
     - **pre-authorization**
   - Payment mode
     - Single payment
     - Payment in installments
     - etc.
   - Payment method (search is restricted to the payment method used)
   - Merchant ID (MID): allows to restrict the search to the merchant ID or the wallet
   - Amount (allows to define minimum and maximum amounts)
   - Transaction status (restricts search to transaction status)
3. Click the **Quick search** button.
   A list of quick searches is also available to the merchant:



Results are displayed in the transaction details view.

8. SEARCHING FOR A CAPTURED TRANSACTION



Shop: All

From: 26/10/20

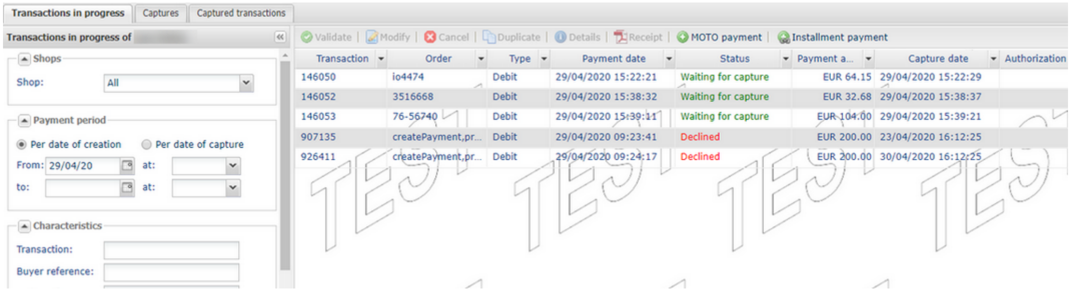
Payment method: All

Merchant ID (MID): All

1. Select **Captured transactions**.
2. Fill in your search criteria.
   There can be multiple search criteria. There are no restrictions to the number of criteria. However, the more criteria there are, the longer the response time will be. In the event of a time-out, the merchant is prompted to limit his/her search range.
   The search criteria are:
   - Shops ('all' by default)
   - Date/time of capture in the bank
   - Date/time of creation
   - Order reference (provided by the merchant)
   - Capture number
   - Buyer’s e-mail address
   - Buyer reference (buyer code provided by the merchant)
   - UUID (unique payment reference generated by the payment gateway and returned to the merchant website at the end of the payment)
   - Payment card number, BIC or IBAN
   - Authorization number
   - Token (Buyer ID or UMR)
   - Transaction number
   - Recurring payment reference associated with the token
   - Type of operation:
     - **debit**: the merchant account is credited,
     - **credit**: the buyer’s account is credited,
     - **verification**: operation allowing to check the card validity. It never results in a debit or a credit.
     - **pre-authorization**
   - Payment mode
     - Single payment
     - Payment in installments
     - etc.
   - Payment method (search is restricted to the payment method used)
   - Merchant ID (MID): allows to restrict the search to the merchant ID or the wallet
   - Currency
   - Amount (allows to define minimum and maximum amounts)
   - Status of the operation
   - Reconciliation status
   - Legal dispute (allows to identify chargeback transactions)

3. Click the **Quick search** button.
   Results are displayed in the transaction details view.

9. VIEWING TRANSACTION DETAILS



Transactions in progress of [redacted]

Shop: All

● Per date of creation ○ Per date of capture

From: 29/04/20 at:

to: at:

Transaction:

Buyer reference:

Transaction	Order	Type	Payment date	Status	Payment a...	Capture date	Authorization
146050	io4474	Debit	29/04/2020 15:22:21	Waiting for capture	EUR 64.15	29/04/2020 15:22:29	
146052	3516668	Debit	29/04/2020 15:38:32	Waiting for capture	EUR 32.68	29/04/2020 15:38:37	
146053	76-56740	Debit	29/04/2020 15:39:11	Waiting for capture	EUR 104.00	29/04/2020 15:39:21	
907135	createPayment,pr...	Debit	29/04/2020 09:23:41	Declined	EUR 200.00	23/04/2020 16:12:25	
926411	createPayment,pr...	Debit	29/04/2020 09:24:17	Declined	EUR 200.00	30/04/2020 16:12:25	

Figure 1: List of transactions in progress

Double-click a transaction to display its details.

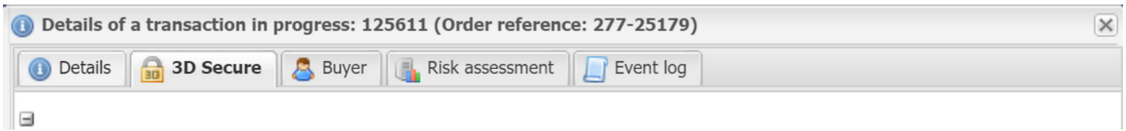

Details of a transaction in progress: 125611 (Order reference: 277-25179)

Figure 2: Example of tabs in transaction details

In transaction details, there are as many tabs as the details transmitted in the form.

The presence of a red exclamation mark to the left of a tab name indicates that the reason of payment rejection is related to the information presented in that tab.

The main displayed tabs:

- **Details**

  Displays the payment characteristics.

- **Authentication**

  The name of the authentication tab varies depending on the authentication type:

  - 3D Secure
  - PayPal authentication
  - American Express Safekey authentication
  - MasterPass authentication
  - etc.

- **Buyer**

  Displays the buyer’s personal details.

- **Event log**

  Provides the history of the operations made throughout the transaction process.

Additional tabs:

- **Extra**

  Displays additional information that the merchant can send in his or her payment request.

- **Shipping**

This tab is available only if the merchant transmits the information about the shipping address to the payment gateway (required by certain payment methods).

- **Shopping cart**

  This tab is available only if the merchant transmits the contents of the shopping cart to the payment gateway.

- **Risk assessment**

  This tab is only available if the merchant has opted for **Risk assessment**.

- **Advanced risk assessment**

  This tab is only available if the merchant has opted for **Advanced risk assessment** module.

  Note:

  In the event of a refusal, the tab is marked with a red exclamation mark.

- **Multiple attempts**

  This tab is available only if the buyer has made several payment attempts. It provides a table with all the attempts.

  The row in bold corresponds to the current transaction.

  By double-clicking a row of the table, you can switch to the detailed summary of the corresponding payment attempt.

- **Split payment**

  This tab lists the used payment methods.

  The row in bold corresponds to the current transaction.

  By double-clicking a row of the table, you can switch to the detailed summary of the corresponding payment attempt, paid with a different payment method.

- **Installment payment**

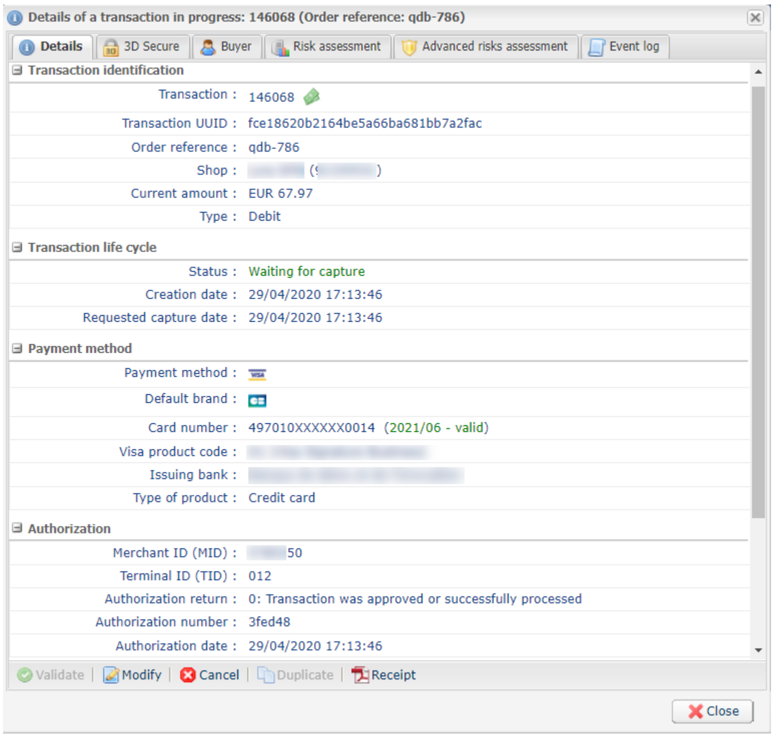
  This tab is available only if the buyer has made an installment payment. It provides a table with all the installments.

  The row in bold corresponds to the current transaction.

  By double-clicking a row of the table, you can switch to the detailed summary of the corresponding installment.

9.1. Viewing payment characteristics

Payment characteristics are displayed by default.



Details of a transaction in progress: 146068 (Order reference: qdb-786)

Transaction identification

Transaction : 146068

Transaction UUID : fce18620b2164be5a66ba681bb7a2fac

Order reference : qdb-786

Shop : [redacted] ([redacted])

Current amount : EUR 67.97

Type : Debit

Transaction life cycle

Status : Waiting for capture

Creation date : 29/04/2020 17:13:46

Requested capture date : 29/04/2020 17:13:46

Payment method

Payment method : VISA

Default brand : CB

Card number : 497010XXXXXX0014 (2021/06 - valid)

Visa product code : [redacted]

Issuing bank : [redacted]

Type of product : Credit card

Authorization

Merchant ID (MID) : [redacted]50

Terminal ID (TID) : 012

Authorization return : 0: Transaction was approved or successfully processed

Authorization number : 3fed48

Authorization date : 29/04/2020 17:13:46

The **Details** tab contains the following information:

- Transaction identification and the UUID

  Displays the unique transaction number generated by the payment gateway, the merchant order reference (if transmitted), the name of the shop, the shop ID, the amount, the transaction currency and the type of operation (debit or credit).

- Information about the transaction lifecycle

  Displays the current status of the transaction, the creation date of the transaction (may be different from the authorization date), the requested capture date and the reconciliation status if the transaction already has the **Captured by the acquirer** status.

- Payment method

  Provides information about the used payment method.

- Information about authorization data

  Regardless of the used payment method, the acquirer return code is returned unchanged (important for private and foreign acquirers). This section contains the acquirer contract that was used for the authorization (can be overridden by the form or if the ON US rules apply), the authorization number, information about the imprint if a pre-authorization has been made, the date and time of the authorization.

- Technical data

  Provides the status of the IPN URL and a key generated by the payment gateway that validates the integrity of all the returned data.

- Source details

  Provides the version of the used browser, the details of the payment module version (if provided), the version of the used e-commerce solution and the payment source (e-commerce, Back Office, Web Services with the used version).

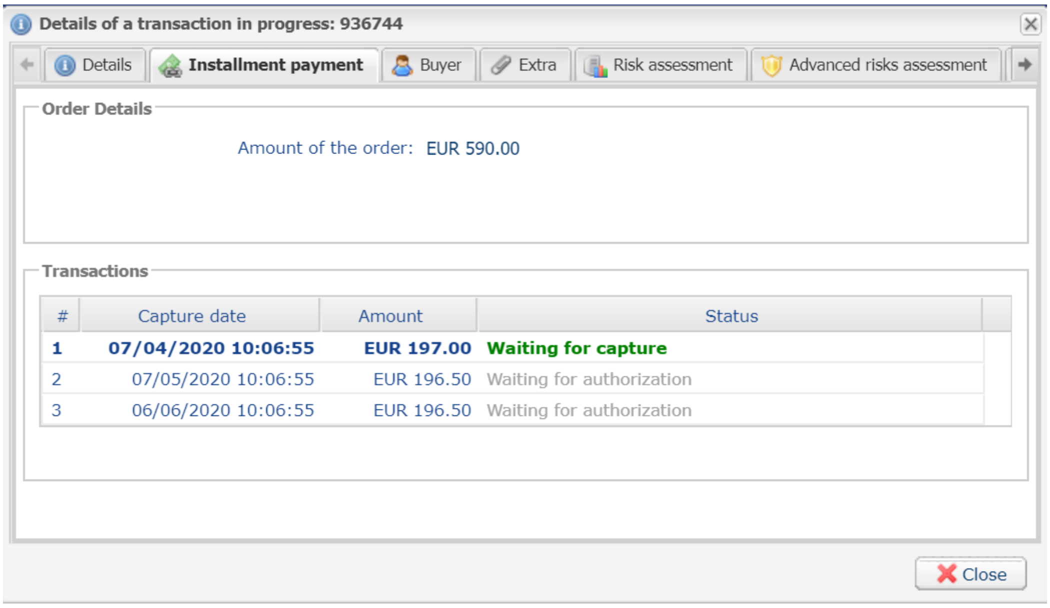
9.2. Viewing installment payment details

A payment is considered to be an “installment payment” if the amount for the purchase is debited to the buyer’s account in several installments.

If the authorization (or information) request is accepted on the day of the order, a transaction is created for each Installment payment due date.

Otherwise, only one rejected transaction is created. The transaction **History** tab then indicates the number of installments initially planned.

Therefore, the **Installment payment** tab is only displayed for this transaction type.



Details of a transaction in progress: 936744

Order Details

Amount of the order: EUR 590.00

Transactions

#	Capture date	Amount	Status
1	**07/04/2020 10:06:55**	**EUR 197.00**	**Waiting for capture**
2	07/05/2020 10:06:55	EUR 196.50	Waiting for authorization
3	06/06/2020 10:06:55	EUR 196.50	Waiting for authorization

Figure 3: Example of the Installment payment tab

An installment payment is not credit, but a payment solution offered by the merchant.

The merchant alone bears the risk of non-payment of the installment payments.

The first installment can be subject to strong authentication and benefit from a payment guarantee.

This is not the case for the subsequent installments.

The **Installment payment** tab contains the following information:

- Total amount of the order,
- The payment schedule detailing the number of installments, the amount of each installment, the installment dates and the status of the associated transactions.

  The highlighted line indicates which installment you are currently looking at.

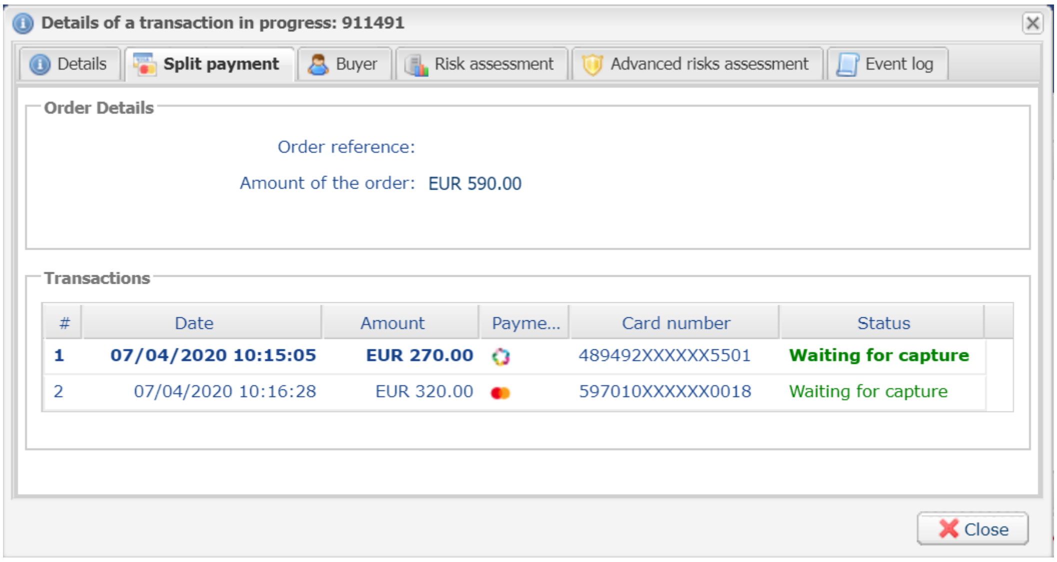
Double-clicking an installment opens the details of the associated transaction.

9.3. Viewing cascading payment details

A payment is considered to be “cascading” when the buyer has used several payment methods to pay for his or her purchase.

A transaction is created for each payment made with a different payment method.

The **Split payment** tab is only displayed for this transaction type.


Details of a transaction in progress: 911491
Details
Split payment
Buyer
Risk assessment
Advanced risks assessment
Event log
Close

Order Details

Order reference:

Amount of the order: EUR 590.00

Transactions

#	Date	Amount	Payme...	Card number	Status
1	**07/04/2020 10:15:05**	**EUR 270.00**	○	489492XXXXXX5501	**Waiting for capture**
2	07/04/2020 10:16:28	EUR 320.00	●	597010XXXXXX0018	Waiting for capture

Figure 4: Example of the Cascading payment tab

The **Split payment** tab contains the following information:

- The reference and total amount of the order,
- The list of transactions and their details:
  - their capture date,
  - their amount,
  - the type of used payment method,
  - the number of the used card or account,
  - their status.

  The highlighted line indicates which installment you are currently looking at.

Double-clicking an installment opens the details of the associated transaction.

9.4. Viewing the 3D Secure authentication result

Click the **3D Secure** tab.

In the **Recap** section, you have:

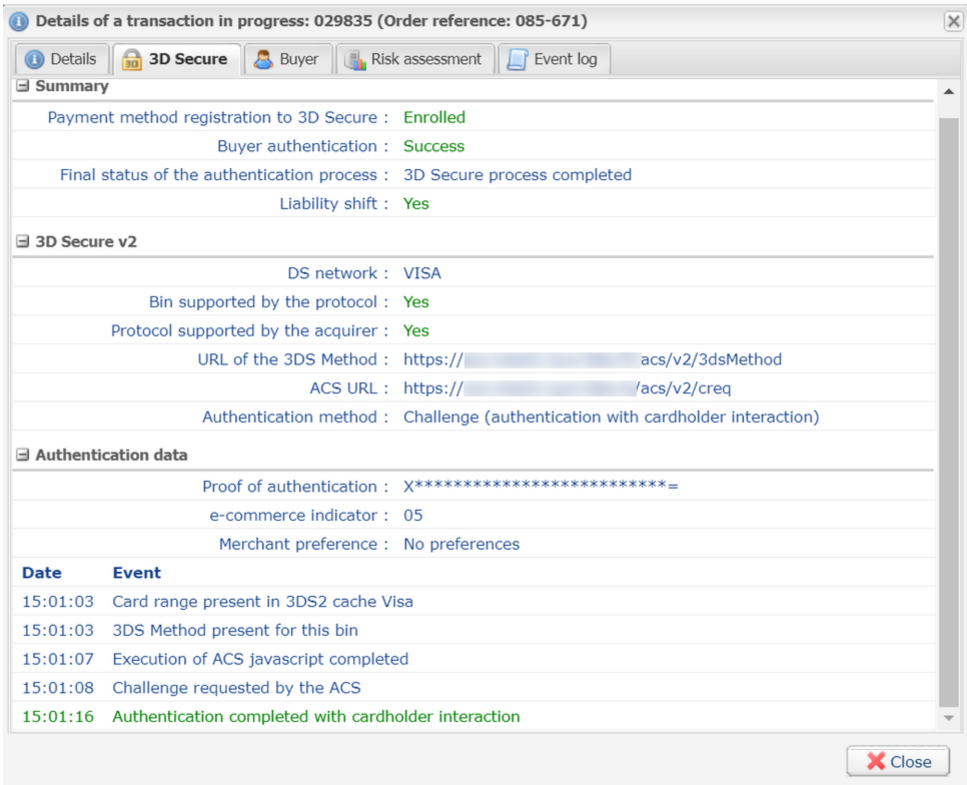
- The enrollment status of the payment method in the 3D Secure program;
- The authentication status of the cardholder;
- The final status of 3D Secure process;
- The result of the liability shift assessment

The other sections provide technical information on the authentication process:

- **3D Secure v2**: indicates the authentication method of the cardholder (frictionless or challenge);
- **Authentication data**: indicates, the merchant’s preference and the reason for the error received from the authentication service in 3DS2.
- **Authentication details**: lists the various events that occurred during authentication.

The following chapters will help you to interpret this information according to the different use cases.

9.4.1. Transaction with successful strong authentication



Details of a transaction in progress: 029835 (Order reference: 085-671)

Summary

Payment method registration to 3D Secure :	Enrolled
Buyer authentication :	Success
Final status of the authentication process :	3D Secure process completed
Liability shift :	Yes

3D Secure v2

DS network :	VISA
Bin supported by the protocol :	Yes
Protocol supported by the acquirer :	Yes
URL of the 3DS Method :	https://[redacted]acs/v2/3dsMethod
ACS URL :	https://[redacted]/acs/v2/creq
Authentication method :	Challenge (authentication with cardholder interaction)

Authentication data

Proof of authentication :	X**************************=
e-commerce indicator :	05
Merchant preference :	No preferences

Date	Event
15:01:03	Card range present in 3DS2 cache Visa
15:01:03	3DS Method present for this bin
15:01:07	Execution of ACS javascript completed
15:01:08	Challenge requested by the ACS
15:01:16	Authentication completed with cardholder interaction

- **Overview**:

  The payment method is enrolled and the buyer has authenticated him or herself correctly on his or her bank’s authentication page (ACS).

  The absence of a red exclamation mark in the various tabs indicates that the payment was successful.

  The Liability shift section is set to **Yes**. Thus, in the event of fraud, the merchant will not be charged.

- **Authentication**:

The DS network responsible for the security is presented.

The payment method *bin* supports the v2 3D Secure protocol.

The v2 3D Secure protocol is also supported by the acquirer.

A challenge (strong authentication with interaction) has been required and successfully performed for the transaction.

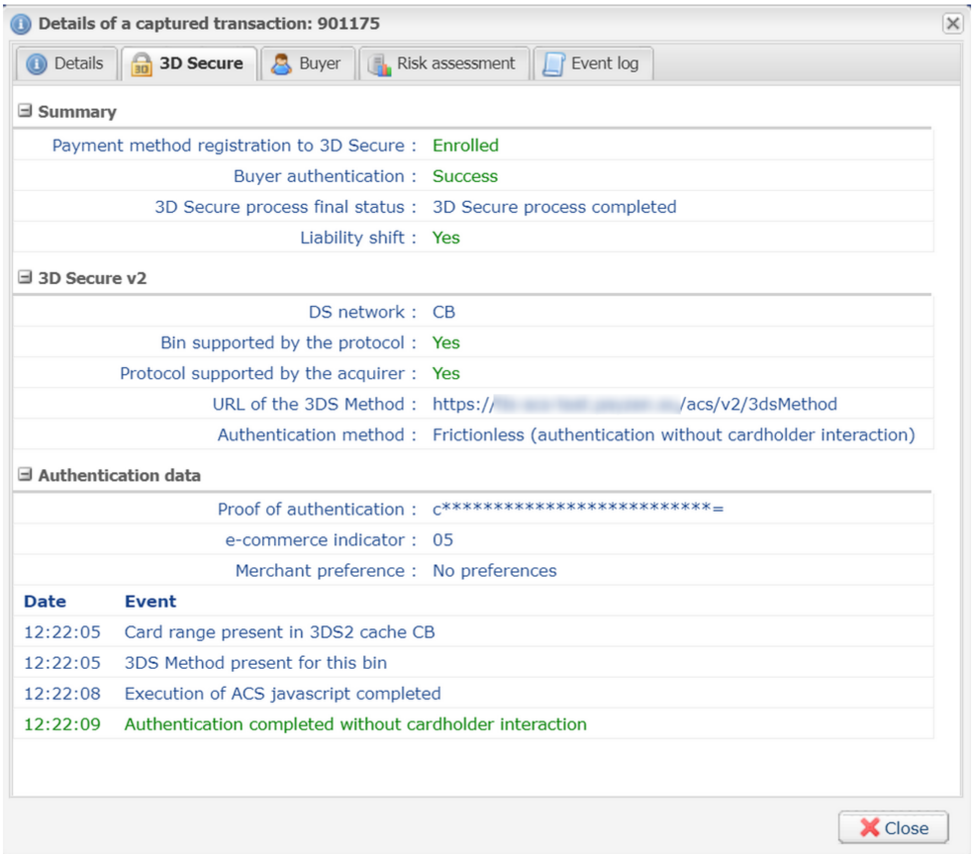
- **Authentication data**:
  - Proof of authentication: sensitive data (CAVV, AEVV or AAV) that proves cardholder authentication by the ACS is present and masked.
  - E-commerce indicator: the buyer has correctly authenticated him or herself. The **05** value indicates successful authentication for **CB**, **VISA** and **AMEX**. The **02** value indicates successful authentication for **MasterCard**.
  - Merchant preference: the **No preference** value indicates that the merchant has not chosen the authentication method.
- **Authentication details**:

  The detailed timeline of the events is displayed for better traceability in case technical assistance is required.

9.4.2. Transaction with successful frictionless authentication

There are two cases for a transaction with successful frictionless authentication:

1. The issuer has received a choice of "No Preference" or "Challenge Requested". They assessed the transaction risk and decided that an authentication without interaction was sufficient.



Details of a captured transaction: 901175

Summary

Payment method registration to 3D Secure : Enrolled

Buyer authentication : Success

3D Secure process final status : 3D Secure process completed

Liability shift : Yes

3D Secure v2

DS network : CB

Bin supported by the protocol : Yes

Protocol supported by the acquirer : Yes

URL of the 3DS Method : https://[redacted]/acs/v2/3dsMethod

Authentication method : Frictionless (authentication without cardholder interaction)

Authentication data

Proof of authentication : c**************************=

e-commerce indicator : 05

Merchant preference : No preferences

Date	Event
12:22:05	Card range present in 3DS2 cache CB
12:22:05	3DS Method present for this bin
12:22:08	Execution of ACS javascript completed
12:22:09	Authentication completed without cardholder interaction

- **Overview** :

The payment method is enrolled and the buyer has authenticated him or herself correctly on his or her bank's authentication page (ACS).

The absence of a red exclamation mark in the various tabs indicates that the payment was successful.

The Liability shift section is set to **Yes**. Thus, in the event of fraud, the merchant will not be charged.

- **Authentification** :

  The DS network responsible for the security is presented.

  The payment method *bin* supports the v2 3D Secure protocol.

  The v2 3D Secure protocol is also supported by the acquirer.

  Authentication without cardholder interaction (frictionless) was granted by the bank but not requested by the merchant.

  The transaction benefits from liability shift.

- **Authentication data**:
  - Proof of authentication: sensitive data (CAVV, AEVV or AAV) that proves cardholder authentication by the ACS is present and masked.
  - E-commerce indicator: the buyer has correctly authenticated him or herself. The **05** value indicates successful authentication for **CB**, **VISA** and **AMEX**. The **02** value indicates successful authentication for **MasterCard**.
  - Merchant preference: the **No preference** value indicates that the merchant has not chosen the authentication method.

- **Authentication data**:
  - Proof of authentication: sensitive data (CAVV, AEVV or AAV) that proves cardholder authentication by the ACS is present and masked.
  - E-commerce indicator: the buyer has correctly authenticated him or herself. The **05** value indicates successful authentication for **CB**, **VISA** and **AMEX**. The **02** value indicates successful authentication for **MasterCard**.
  - Merchant preference: the **No preference** value indicates that the merchant has not chosen the authentication method.
  - Reason for exemption: the reason for authentication without bearer interaction.

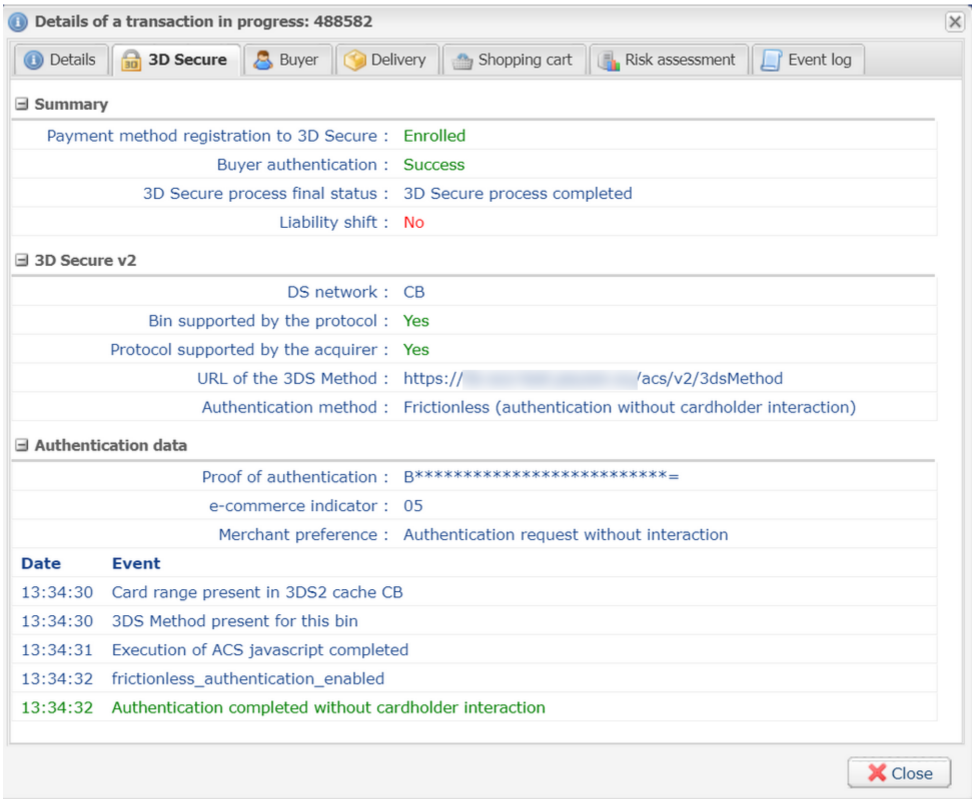
    In this example, the reason is transmitted by the issuer. *View the exemption list*.

- **Authentication details**:

  The detailed timeline of the events is displayed for better traceability in case technical assistance is required.

2. The merchant has the “Frictionless 3DS2” option and has requested authentication without cardholder interaction. The card issuer has accepted the request.

   - **Overview**:



Details of a transaction in progress: 488582

Summary

Payment method registration to 3D Secure :	Enrolled
Buyer authentication :	Success
3D Secure process final status :	3D Secure process completed
Liability shift :	No

3D Secure v2

DS network :	CB
Bin supported by the protocol :	Yes
Protocol supported by the acquirer :	Yes
URL of the 3DS Method :	https://[redacted]/acs/v2/3dsMethod
Authentication method :	Frictionless (authentication without cardholder interaction)

Authentication data

Proof of authentication :	B**************************=
e-commerce indicator :	05
Merchant preference :	Authentication request without interaction

Date	Event
13:34:30	Card range present in 3DS2 cache CB
13:34:30	3DS Method present for this bin
13:34:31	Execution of ACS javascript completed
13:34:32	frictionless_authentication_enabled
13:34:32	Authentication completed without cardholder interaction

The payment method is enrolled and the buyer has authenticated him or herself correctly on his or her bank's authentication page (ACS).

The absence of a red exclamation mark in the various tabs indicates that the payment was successful.

The Liability shift section is set to **No**. Thus, in the event of buyer fraud, the merchant will not be charged.

- **Authentification** :

  The DS network responsible for the security is presented.

  The payment method *bin* supports the v2 3D Secure protocol.

  The v2 3D Secure protocol is also supported by the acquirer.

  An authentication without cardholder interaction has requested by the merchant and the request has been accepted by the bank. This authentication mode is valid in 3DS2 for an amount in euro lower than €30.

  The transaction does not benefit from liability shift.

- **Authentication data**:
  - Proof of authentication: sensitive data (CAVV, AEVV or AAV) that proves cardholder authentication by the ACS is present and masked.
  - E-commerce indicator: the buyer has correctly authenticated him or herself. The **05** value indicates successful authentication for **CB**, **VISA** and **AMEX**. The **02** value indicates successful authentication for **MasterCard**.
  - Merchant preference: In this example, the merchant requested authentication without interaction with the bearer. Based on the store's options and the characteristics of the transaction, the gateway transmitted the request to the issuer.
  - Reason for exemption: the reason for authentication without bearer interaction.

    In this example, the reason is transmitted by the payment gateway. *View the exemption list*.

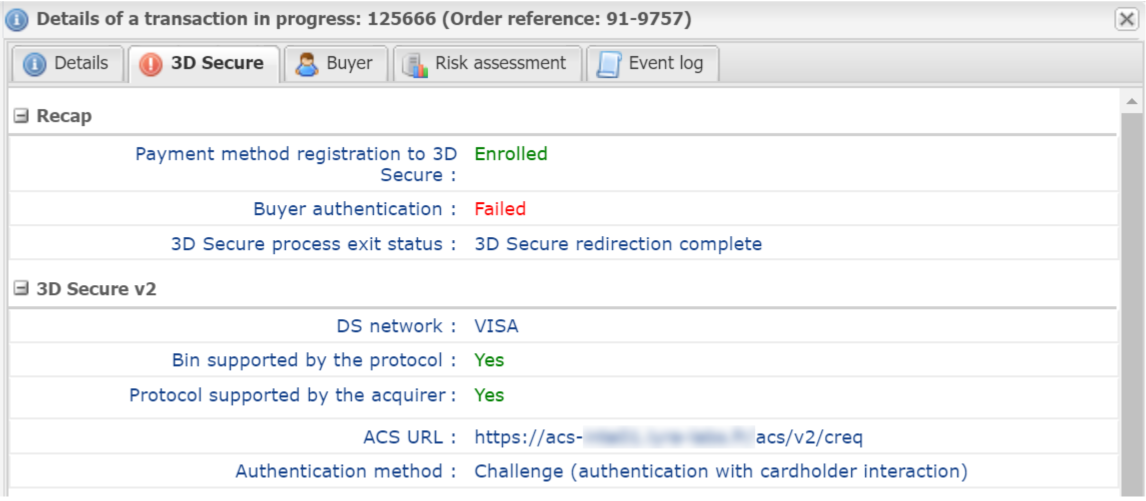
- **Authentication details**:

  The detailed timeline of the events is displayed for better traceability in case technical assistance is required.

Exemption list:

- Risk analysis by the issuer;
- Risk analysis by the acquirer;
- Strong authentication delegated to a third party;
- Low value transaction;
- Fixed recurring payments with a fixed term;
- The merchant participates in CB's Low Risk Merchant program;
- Other exemption cases;
- A technical error prevents cardholder authentication;
- Trusted beneficiaries;
- Payment devices;
- Payment by corporate card;
- Transaction not concerned by the SCA (Strong Customer Authentication);
- Another exemption received from the DS.

9.4.3. Transaction with failed 3D Secure authentication



Details of a transaction in progress: 125666 (Order reference: 91-9757)

Recap

Payment method registration to 3D Secure :	Enrolled
Buyer authentication :	Failed
3D Secure process exit status :	3D Secure redirection complete

3D Secure v2

DS network :	VISA
Bin supported by the protocol :	Yes
Protocol supported by the acquirer :	Yes
ACS URL :	https://acs-[redacted]acs/v2/creq
Authentication method :	Challenge (authentication with cardholder interaction)

The red exclamation mark to the left of the tab name indicates that the reason for rejection is related to 3D Secure authentication.

The payment method is enrolled for 3D Secure and strong authentication (challenge) was required.

The Authentication Status ("**Failed**") indicates that the cardholder has not authenticated correctly on his or her bank's authentication site (ACS).

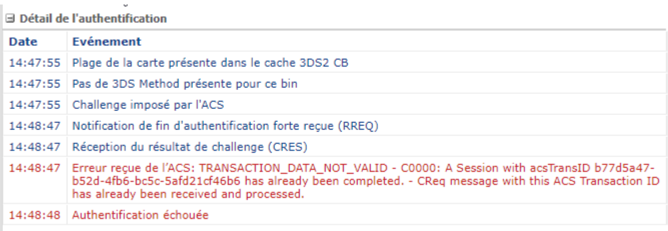
Example of reasons for refusal:

- "39: 3D Secure was declined for this transaction": corresponds to an incorrect entry of the authentication code, which resulted in the payment being refused.

- "206: 3D Secure - A technical error occurred during the process":

This type of error can occur when the buyer performs the transaction using a cell phone with insufficient memory. The transaction fails during the authentication phase and the ACS shows us an error message visible in the transaction details.

Example: “Error received from the ACS: TRANSACTION_DATA_NOT_VALID"



⊟ Détail de l'authentification

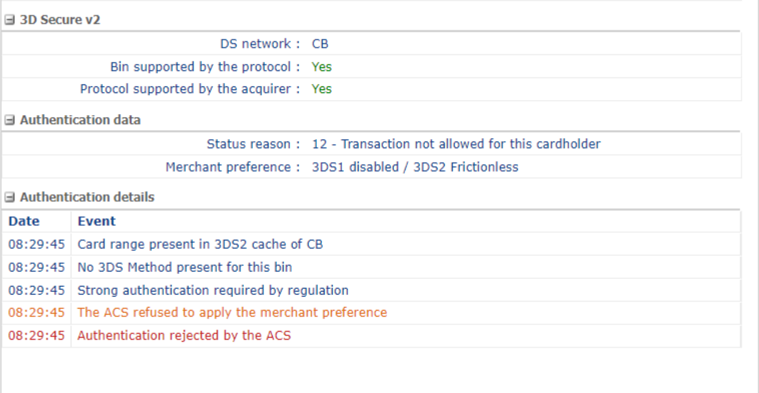
Date	Evénement
14:47:55	Plage de la carte présente dans le cache 3DS2 CB
14:47:55	Pas de 3DS Method présente pour ce bin
14:47:55	Challenge imposé par l'ACS
14:48:47	Notification de fin d'authentification forte reçue (RREQ)
14:48:47	Réception du résultat de challenge (CRES)
14:48:47	Erreur reçue de l'ACS: TRANSACTION_DATA_NOT_VALID - C0000: A Session with acsTransID b77d5a47-b52d-4fb6-bc5c-5afd21cf46b6 has already been completed. - CReq message with this ACS Transaction ID has already been received and processed.
14:48:48	Authentification échouée

- “207: Refusal of the authentication by the issuer (Transaction not allowed for this cardholder)”:

  This error appears when the authentication servers (ACS) reject the authentication.

  The buyer must ask their bank if the card used for the payment allows payments with 3DS2 authentication and/or payments via an e-commerce website.

  Status reason: "12-Transaction not allowed for this cardholder"



⊟ 3D Secure v2

DS network :	CB
Bin supported by the protocol :	Yes
Protocol supported by the acquirer :	Yes

⊟ Authentication data

Status reason :	12 - Transaction not allowed for this cardholder
Merchant preference :	3DS1 disabled / 3DS2 Frictionless

⊟ Authentication details

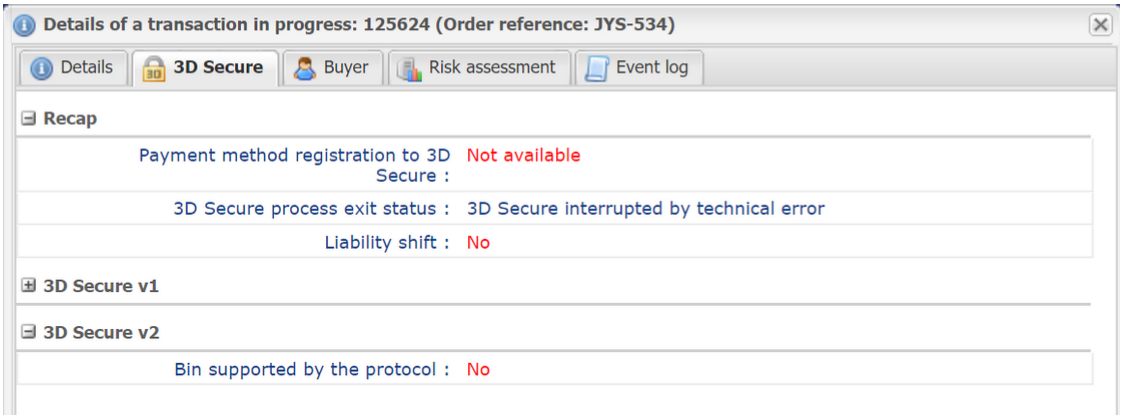
Date	Event
08:29:45	Card range present in 3DS2 cache of CB
08:29:45	No 3DS Method present for this bin
08:29:45	Strong authentication required by regulation
08:29:45	The ACS refused to apply the merchant preference
08:29:45	Authentication rejected by the ACS

9.4.4. Transaction with a technical error during the authentication

This can happen when:

- the payment method enrollment status is unknown;
- the buyer’s authentication status in unknown.

Example of “the payment method enrollment status is unknown” case:



Details of a transaction in progress: 125624 (Order reference: JYS-534)

⊟ Recap

Payment method registration to 3D Secure :	Not available
3D Secure process exit status :	3D Secure interrupted by technical error
Liability shift :	No

⊞ 3D Secure v1

⊟ 3D Secure v2

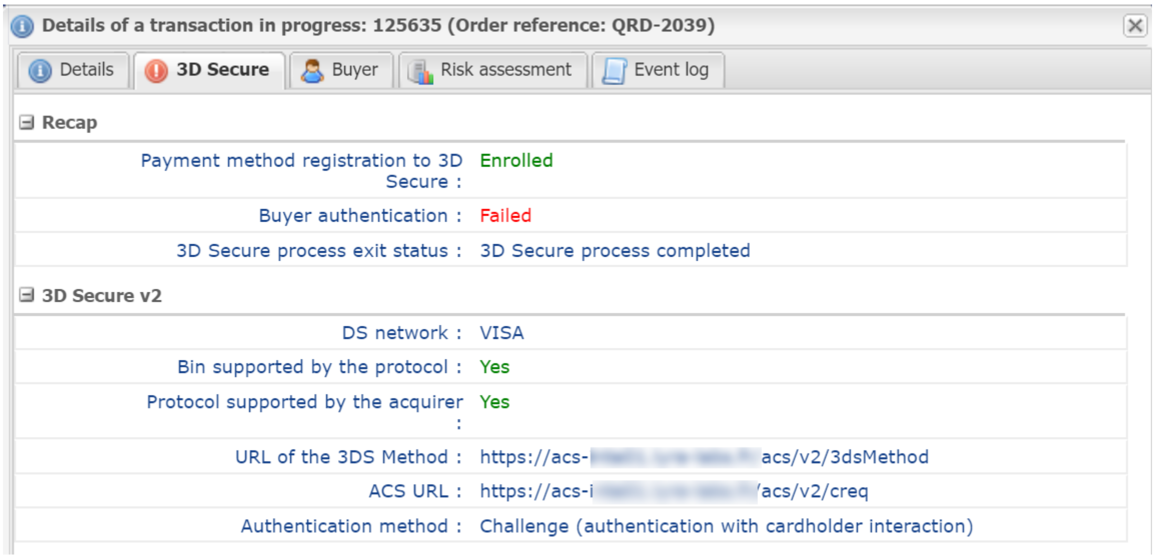
Bin supported by the protocol :	No

In this case, an error occurred when checking the payment method enrollment status.

The 3D Secure process was aborted.

Payment continued without authentication of the cardholder. In accordance with the rules of the network concerned, this resulted in the loss for the liability shift to the card issuer.

9.4.5. Payment session expiration



Details of a transaction in progress: 125635 (Order reference: QRD-2039)

Recap

Payment method registration to 3D Secure : Enrolled

Buyer authentication : Failed

3D Secure process exit status : 3D Secure process completed

3D Secure v2

DS network : VISA

Bin supported by the protocol : Yes

Protocol supported by the acquirer : Yes

URL of the 3DS Method : https://acs-[redacted]acs/v2/3dsMethod

ACS URL : https://acs-i[redacted]/acs/v2/creq

Authentication method : Challenge (authentication with cardholder interaction)

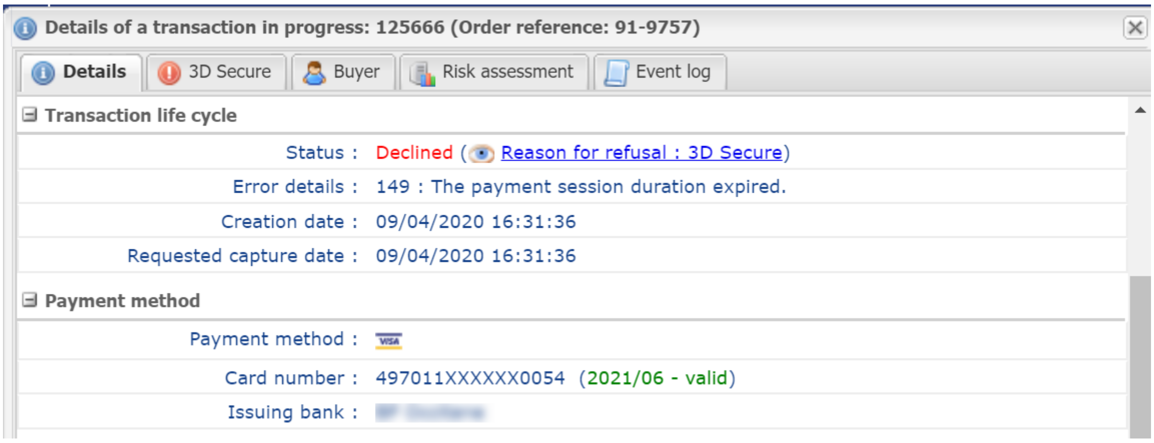
The payment method is enrolled for 3D Secure and strong authentication (challenge) was required.

The buyer’s browser was redirected to the buyer’s bank’s authentication website (ACS).

The URL of the authentication website (ACS) is indicated in the 3D Secure section corresponding to the protocol used for authentication.

At this stage the payment gateway is still waiting for the browser to return.

After 10 minutes without a response (duration of the payment session), the payment is refused with the “149 - payment session expired” error.



Details of a transaction in progress: 125666 (Order reference: 91-9757)

Transaction life cycle

Status : Declined (Reason for refusal : 3D Secure)

Error details : 149 : The payment session duration expired.

Creation date : 09/04/2020 16:31:36

Requested capture date : 09/04/2020 16:31:36

Payment method

Payment method : VISA

Card number : 497011XXXXXX0054 (2021/06 - valid)

Issuing bank : [redacted]

Here are some of the possible causes:

- the buyer took too long to authenticate;
- the buyer has closed the authentication window;
- the buyer has not received the authentication code by SMS;
- the buyer has installed a plugin on his or her browser or an antivirus that prevents the ACS page from being opened;

- the ACS page was not displayed because the ACS server is unavailable;
- the ACS page is not displayed correctly.

The payment gateway is never to blame for these errors. It does not manage the banks' authentication servers, and is never in contact with them.

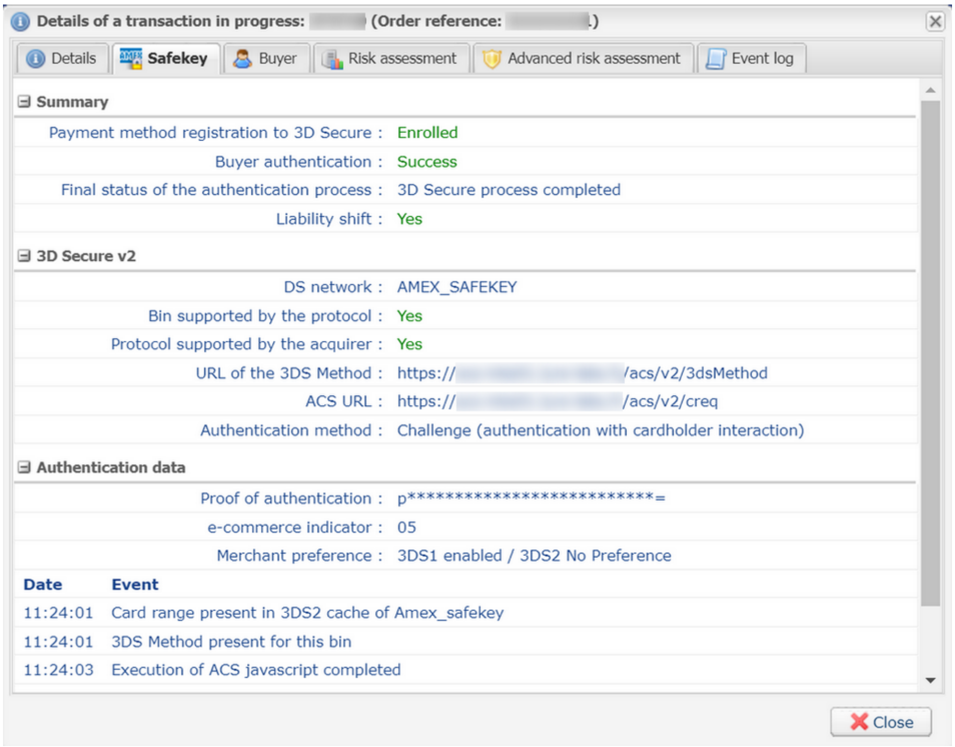
Only the buyer's browser interacts with the banks' authentication servers.

9.5. Viewing the American Express SafeKey authentication result

American Express SafeKey relies on 3D Secure technology to authenticate the cardholder during online payments.

The interpretation on the SafeKey tab information is identical to that presented in the chapter *Viewing the 3D Secure authentication result on page 21*.

Click on the **SafeKey** tab.



Details of a transaction in progress: [redacted] (Order reference: [redacted])

Summary

Payment method registration to 3D Secure : Enrolled
Buyer authentication : Success
Final status of the authentication process : 3D Secure process completed
Liability shift : Yes

3D Secure v2

DS network : AMEX_SAFEKEY
Bin supported by the protocol : Yes
Protocol supported by the acquirer : Yes
URL of the 3DS Method : https://[redacted]/acs/v2/3dsMethod
ACS URL : https://[redacted]/acs/v2/creq
Authentication method : Challenge (authentication with cardholder interaction)

Authentication data

Proof of authentication : p*************************=
e-commerce indicator : 05
Merchant preference : 3DS1 enabled / 3DS2 No Preference

Date	Event
11:24:01	Card range present in 3DS2 cache of Amex_safekey
11:24:01	3DS Method present for this bin
11:24:03	Execution of ACS javascript completed

In the **Recap** section, you will find:

- The enrollment status of the payment method in the 3D Secure program
- The authentication status of the cardholder.
- The final status of 3D Secure process
- The result of the liability shift assessment

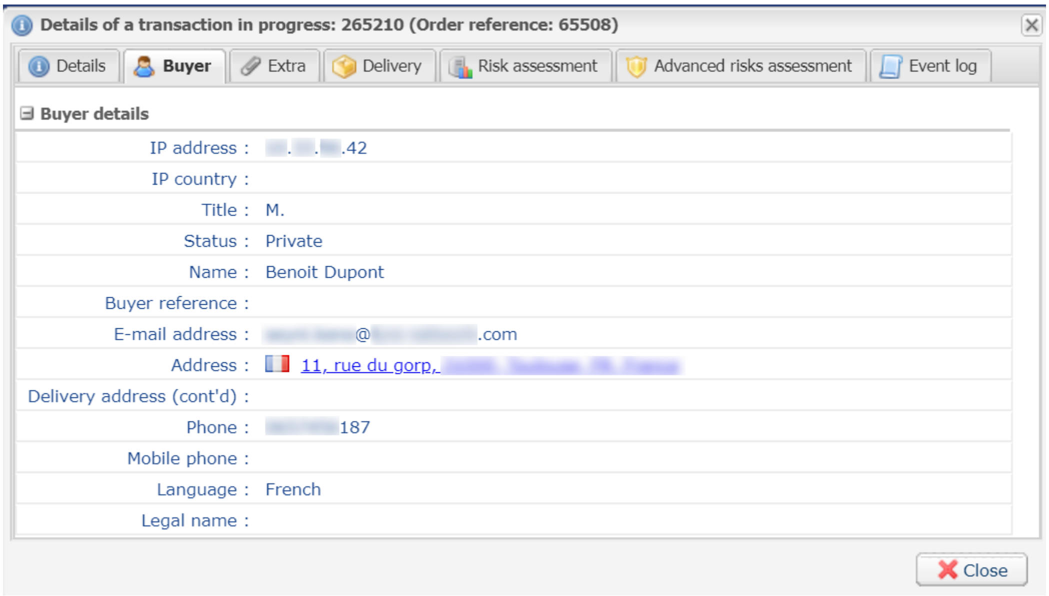
The other sections provide technical information on the authentication process, useful in the event of a customer support request:

- **3D Secure v2**: Indicates the authentication method of the cardholder (frictionless or challenge).
- **Authentication data:** Indicates the merchant preference in 3DS2, the reason for refusal if transmitted by the ACS, or the validity of the message containing the result of cardholder authentication (PaRes) in 3DS1.
- **Authentication details**: Lists the various events that occurred during authentication.

For more information, see chapter *Viewing the 3D Secure authentication result on page 21*.

9.6. Viewing buyer details

Buyer details are available via the **Buyer** tab.



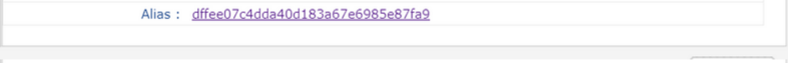
Details of a transaction in progress: 265210 (Order reference: 65508)

Buyer details

IP address :	[redacted].[redacted].[redacted].42
IP country :	
Title :	M.
Status :	Private
Name :	Benoit Dupont
Buyer reference :	
E-mail address :	[redacted]@[redacted].com
Address :	11, rue du gorp, [redacted]
Delivery address (cont'd) :	
Phone :	[redacted]187
Mobile phone :	
Language :	French
Legal name :	

This tab contains the following information:

- the IP address from which the buyer made the purchase,
- the IP address host country,
- the buyer's title*,
- the client type (private or company)*,
- the buyer reference in the merchant's system*,
- the buyer's personal data (full name, national identifier, address, telephone number, etc.)*,
- the language used to display the payment page and payment confirmation e-mails to the buyer,
- the company name if the buyer is a company*,
- the payment method token, if applicable*.



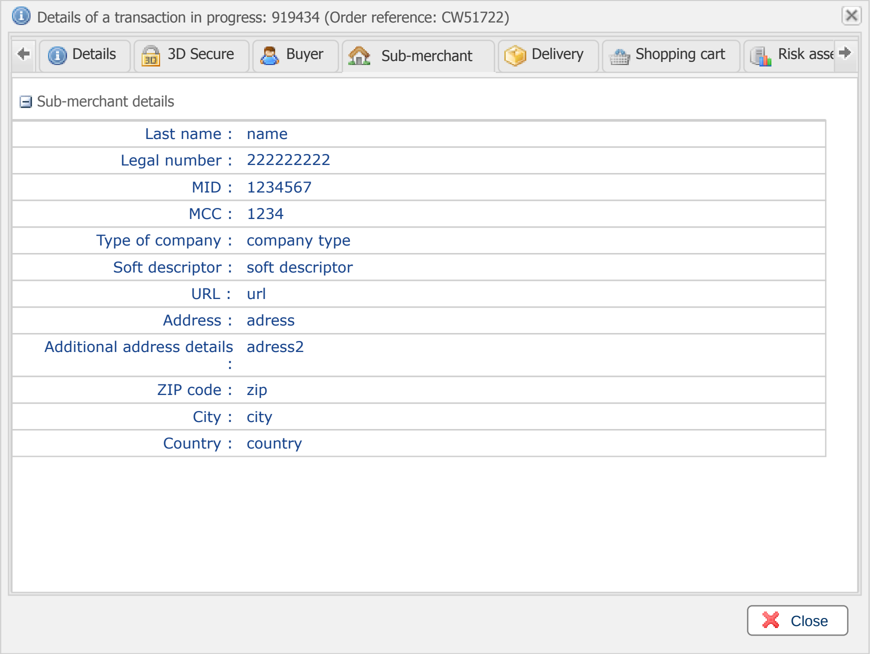
Alias : dffee07c4dda40d183a67e6985e87fa9

  - You can click on the token to view its details.

*Only if the merchant has transmitted the information in his or her payment request.

9.7. Viewing sub-merchant details

The sub-merchant details transmitted in the payment request are accessible via the **Sub-merchant** tab.



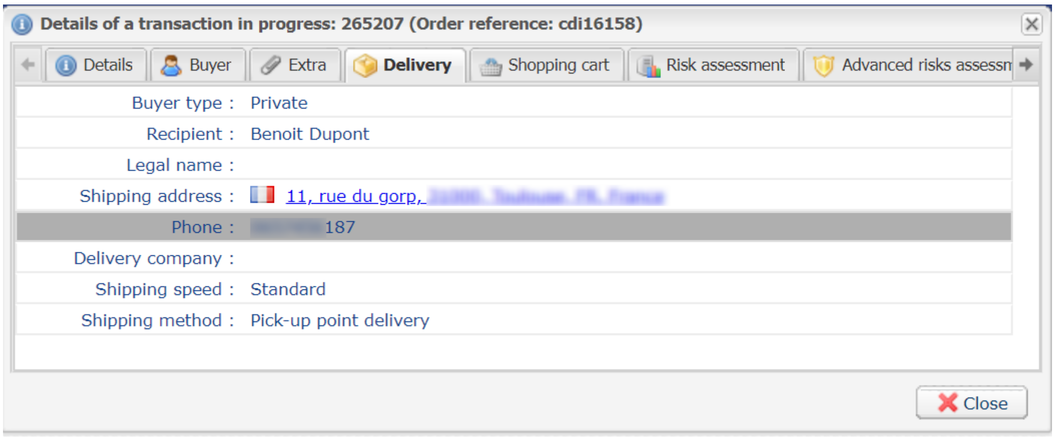
Details of a transaction in progress: 919434 (Order reference: CW51722)

Sub-merchant details

Last name :	name
Legal number :	222222222
MID :	1234567
MCC :	1234
Type of company :	company type
Soft descriptor :	soft descriptor
URL :	url
Address :	adress
Additional address details :	adress2
ZIP code :	zip
City :	city
Country :	country

9.8. Viewing shipping details

This tab is present only if the merchant has transmitted at least one piece of information about shipping in his or her payment request.



Buyer type :	Private
Recipient :	Benoit Dupont
Legal name :	
Shipping address :	11, rue du gorp, [redacted]
Phone :	[redacted]187
Delivery company :	
Shipping speed :	Standard
Shipping method :	Pick-up point delivery

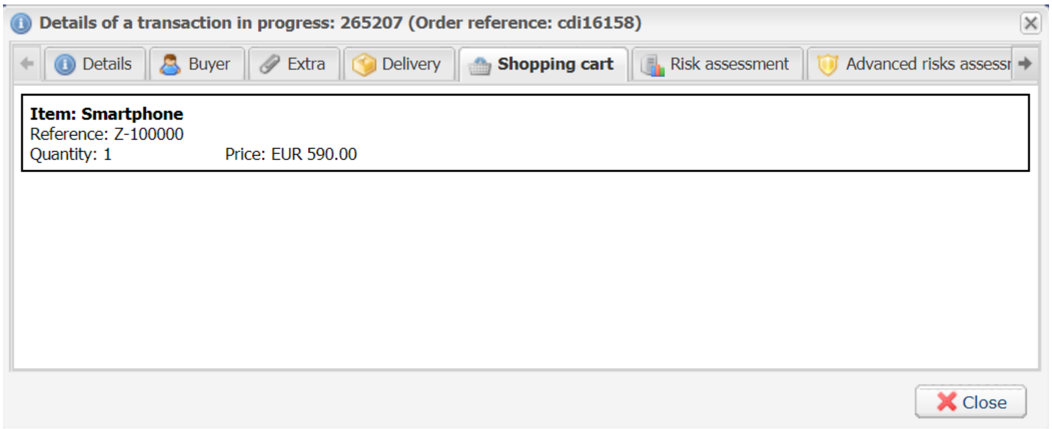
Figure 5: Example of the Delivery tab

This tab contains the following information:

- the client type (private or company),
- the recipient,
- the legal name in case of shipping to a relay point or a shop,
- the first and last names in case of shipping to a private address,
- the shipping address,
- the contact phone number,
- the transporter’s name,
- the speed of delivery,
- the shipping type.

9.9. Viewing shopping cart details

This tab is present only if the merchant has transmitted at least one piece of information about the contents of the shopping cart in his or her payment request.



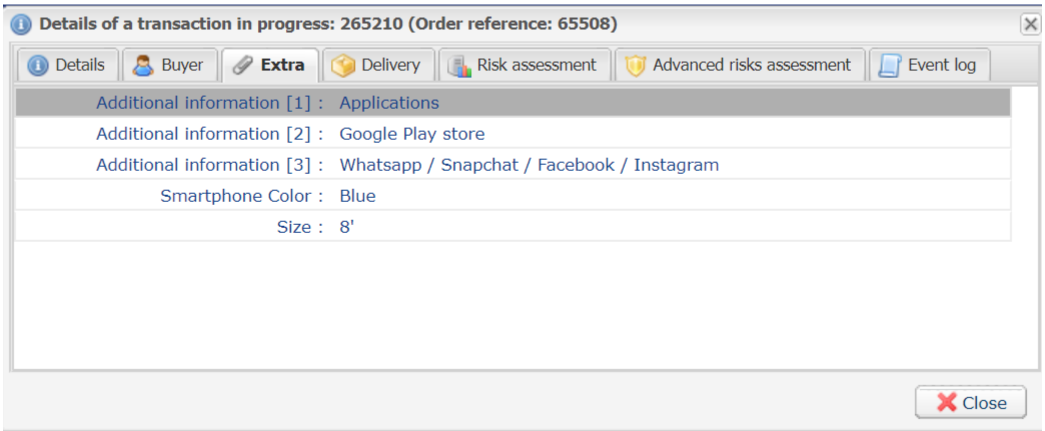
Item: Smartphone
Reference: Z-100000
Quantity: 1 Price: EUR 590.00

Figure 6: Example of the Shopping cart details tab

For each item in the shopping cart, you will find:

- its reference,
- its name,
- its price,
- its quantity,
- its category,
- the VAT amount.

9.10. Viewing extra details



Details of a transaction in progress: 265210 (Order reference: 65508)

Additional information [1] :	Applications
Additional information [2] :	Google Play store
Additional information [3] :	Whatsapp / Snapchat / Facebook / Instagram
Smartphone Color :	Blue
Size :	8'

Figure 7: Example of the Extra tab

The **Extra** tab only appears:

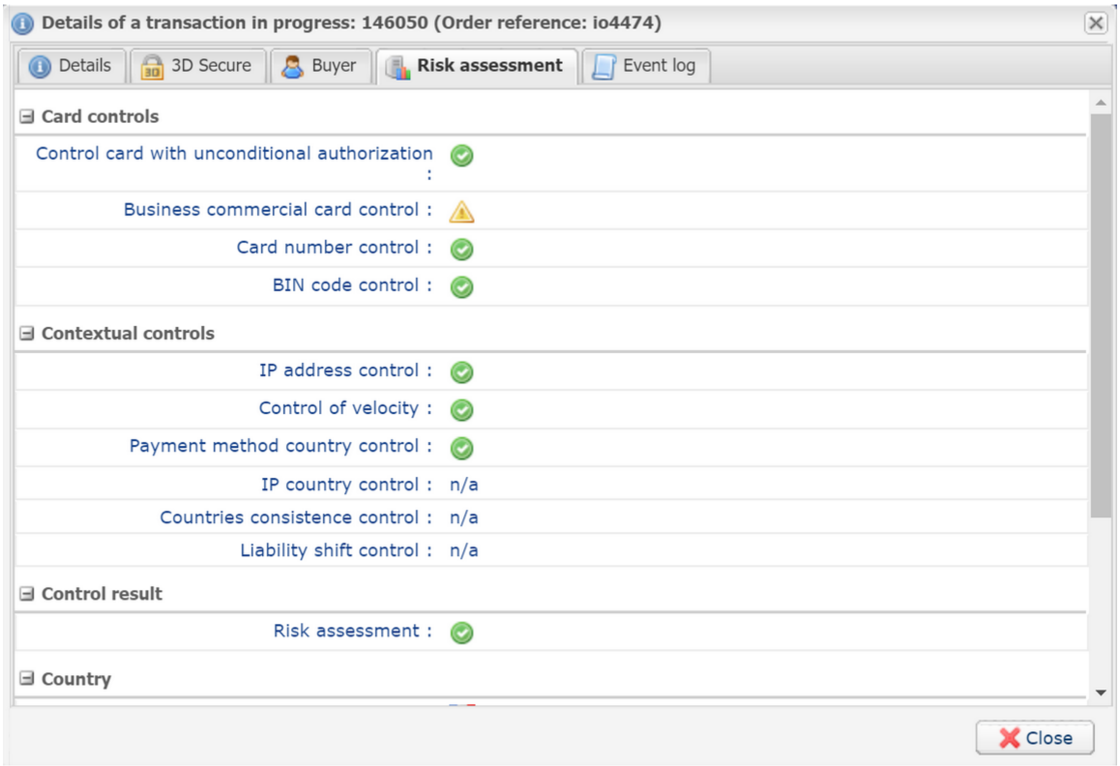
- if at least one additional piece of information describing the order has been transmitted in the payment request
  - via the vads_order_info, vads_order_info2, vads_order_info3 fields of the Hosted Payment Page
  - via the attributes orderInfo, orderInfo2, orderInfo3 of the REST API metadata object
- if at least one custom field was transmitted in the payment request
  - vads_ext_info_xxxx of the Hosted Payment Page
  - via the metadata of the REST API
- if the transaction is made using the data collection form and the merchant has added supplementary fields

9.11. Viewing completed transaction controls

This tab is present only if you have opted for the *Risk assessment* service.

By default, all controls are disabled. Controls must be configured individually for each shop (Settings > Risk assessment).

To see the controls performed on the transaction, go to the **Risk assessment** tab.



Details of a transaction in progress: 146050 (Order reference: io4474)

Card controls

Control card with unconditional authorization : ✓

Business commercial card control : ⚠

Card number control : ✓

BIN code control : ✓

Contextual controls

IP address control : ✓

Control of velocity : ✓

Payment method country control : ✓

IP country control : n/a

Countries consistence control : n/a

Liability shift control : n/a

Control result

Risk assessment : ✓

Country

Controls are classified by risk category (map controls, contextual controls, country, etc.).

For each control, the result can be:

- **n/a**: control not performed or non applicable,
- **green icon**: control successfully completed – no alerts raised,
- **yellow icon**: alert raised,
- **red icon**: control failed.

The **Control result** section provides the overall control result:

- **n/a**: all the not completed or non applicable controls,
- **green icon**: all the successfully completed controls – no alerts raised,
- **yellow icon**: one or more alerts raised,
- **red icon**: one or more controls failed.

If one or more controls fail, the payment is refused and a red exclamation mark appears in the tab name.

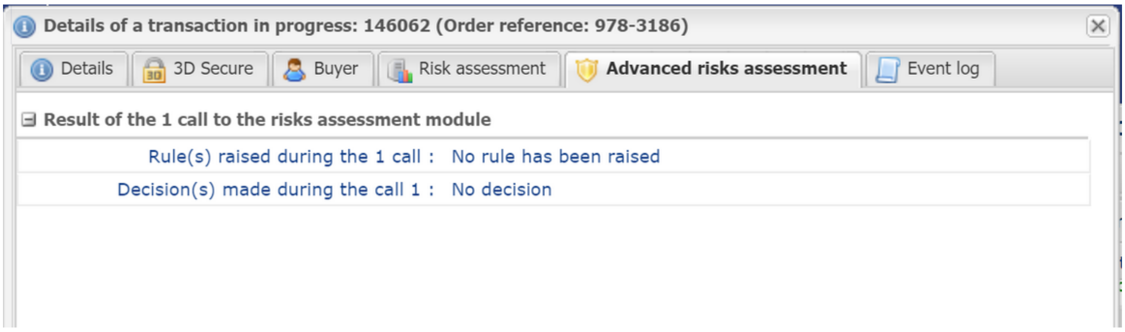
9.12. Viewing the advanced risk assessment result

The **Advanced risk assessment** tab lists the controls carried out throughout the payment and the decisions that have been made.

For the **Advanced risk assessment** tab to be visible, you must enable transaction redirection to the risk management module.

For more information on configuring risk assessment, see the Advanced Risk Assessment Back Office user guide.

- **No rules raised**



Details of a transaction in progress: 146062 (Order reference: 978-3186)

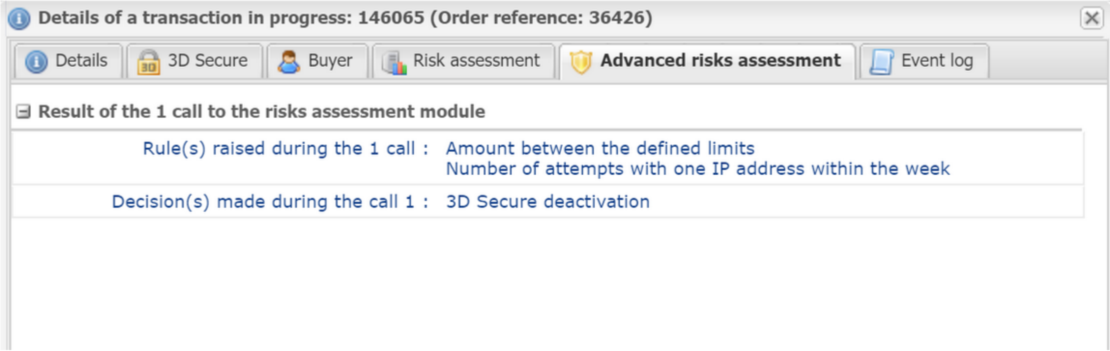
Result of the 1 call to the risks assessment module

Rule(s) raised during the 1 call : No rule has been raised

Decision(s) made during the call 1 : No decision

The transaction does not match the criteria configured in Advanced Risk Assessment, or no rules have been configured or enabled.

- **1 or more rules raised**



Details of a transaction in progress: 146065 (Order reference: 36426)

Result of the 1 call to the risks assessment module

Rule(s) raised during the 1 call : Amount between the defined limits
Number of attempts with one IP address within the week

Decision(s) made during the call 1 : 3D Secure deactivation

Depending on the rules enabled by the merchant, the payment gateway can make several calls to the fraud management module during the payment:

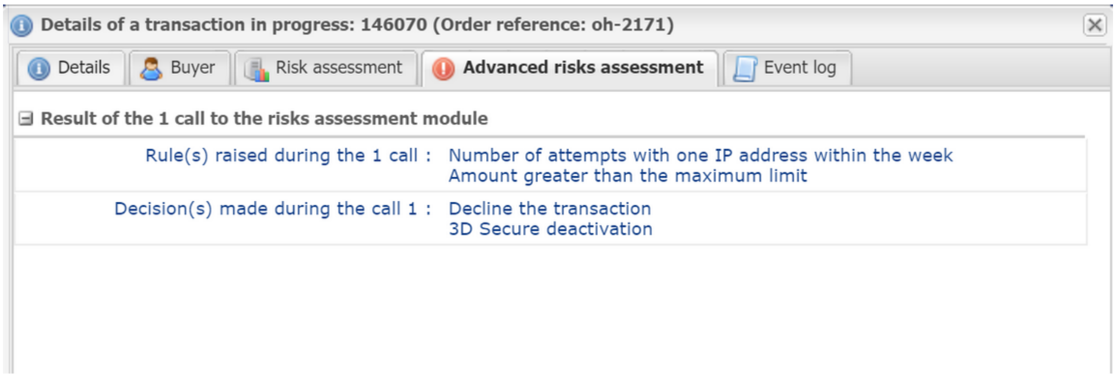
- After validation of the input data
- after completing strong authentication
- after the authorization request

For each call, 2 pieces of information are available:

- The **Rule raised during the call x** which lists the rules for which the transaction matches the criteria of the controls enabled by the merchant.
- The **Decision made during the call x** which lists the actions that have been carried out in accordance with the rules defined by the merchant.

- **Payment rejected by the fraud management module**

When a control results in a rejected payment, a red exclamation mark is displayed to the left of the tab name:

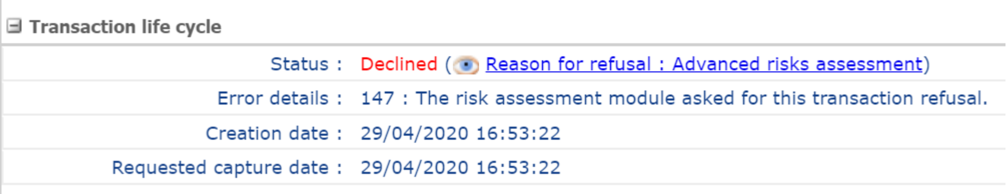


Details of a transaction in progress: 146070 (Order reference: oh-2171)
Details
Buyer
Risk assessment
Advanced risks assessment
Event log

Result of the 1 call to the risks assessment module

Rule(s) raised during the 1 call :	Number of attempts with one IP address within the week Amount greater than the maximum limit
Decision(s) made during the call 1 :	Decline the transaction 3D Secure deactivation

The error detail visible in the **Details** tab is then populated with **147**:

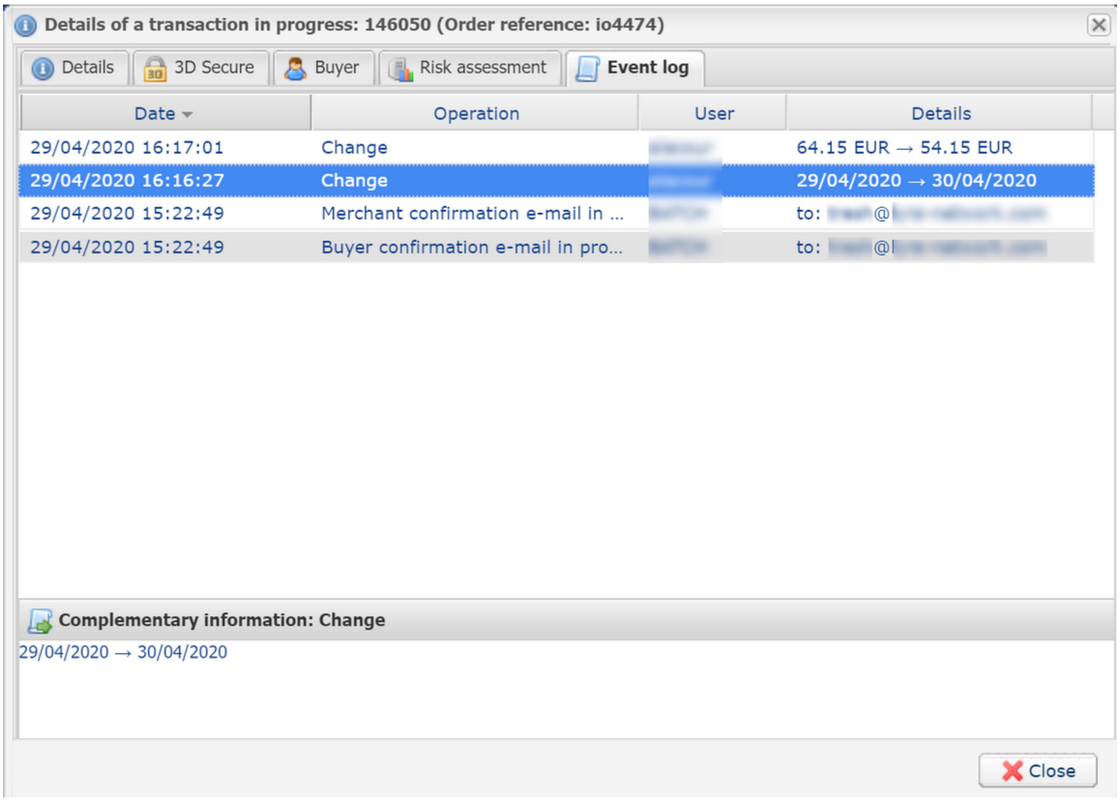


Transaction life cycle

Status :	Declined (Reason for refusal : Advanced risks assessment)
Error details :	147 : The risk assessment module asked for this transaction refusal.
Creation date :	29/04/2020 16:53:22
Requested capture date :	29/04/2020 16:53:22

9.13. Viewing transaction history

To view the history of operations performed within the transaction, go to the **Event log** tab.



Details of a transaction in progress: 146050 (Order reference: io4474)

Date	Operation	User	Details
29/04/2020 16:17:01	Change	[redacted]	64.15 EUR → 54.15 EUR
29/04/2020 16:16:27	Change	[redacted]	29/04/2020 → 30/04/2020
29/04/2020 15:22:49	Merchant confirmation e-mail in ...	[redacted]	to: [redacted]
29/04/2020 15:22:49	Buyer confirmation e-mail in pro...	[redacted]	to: [redacted]

Complementary information: Change

29/04/2020 → 30/04/2020

All events are presented with as many details as possible.

- All the updates performed on the transaction (capture date, amount, cancellation, refund, etc.),
- History of the e-mails sent to the merchant and the receipt confirmation,
- History of the e-mails sent to the buyer and the receipt confirmation,
- History of the calls to the IPN URL at the end of payment,

  The recorded date and time of the call, processing time of the IPN by the merchant website, and the 200 first bytes read from the socket of the merchant website.
- Information about the capture time and the associated capture number, if it exists.

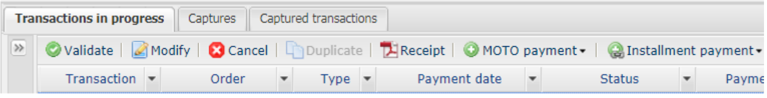
10. PERFORMING AN OPERATION WITH YOUR TRANSACTIONS

The list of authorized operations within a transaction depends on its status (and on the user rights).

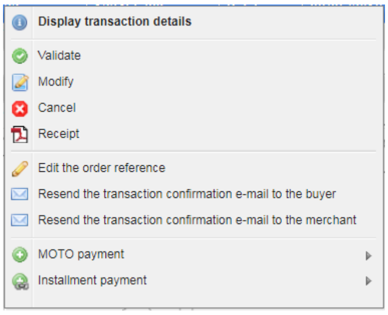
This list varies whether you place yourself in the **Transactions in progress** or in the **Captured transactions** tab.

The list of authorized operations can be viewed:

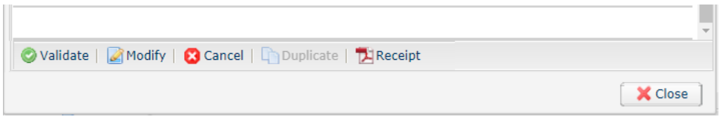
- via the menu bar,



- using right click,


Display transaction details
Validate
Modify
Cancel
Receipt
Edit the order reference
Resend the transaction confirmation e-mail to the buyer
Resend the transaction confirmation e-mail to the merchant
MOTO payment
Installment payment

- at the bottom of the **Transaction details**.



10.1. Validating a transaction

This operation allows to indicate that the transaction can be captured on the scheduled presentation date.

Only the transactions with the following statuses can be validated:

- **To be validated**
- **To be validated and authorized**

In order to validate a transaction:

1. Click on the tab **Transactions is progress**
2. Select the transaction.
3. Click **Validate**.

Once the transaction has been validated, the status changes to "**Waiting for capture**" or "**Waiting for authorization**" depending on the initial transaction status.

Even if it is not validated before the scheduled capture date, the payment status will remain To be validated until the authorization expires.

In the meantime, you will still be able to validate and/or modify it even if the initial capture date has passed.

Case of installment payments created in manual validation mode:

When a user validates the first installment, a window appears to request confirmation of validation and offer simultaneous validation of all the remaining installments.

Upon each installment validation, and as long as the user has not validated all the remaining installments, this simultaneous validation of remaining installments is suggested.

10.2. Canceling one or several transactions

This operation allows to cancel the transaction entirely before the actual debit.

It does not allow for partial cancellation. If you wish to partially cancel a transaction, see the chapter *Editing a transaction*.

Depending on the acquirer, cancellation is possible:

- Before the capture date (particularly on the CB network).
- After the capture date, as long as the transaction is not cleared.

Cancellation is not suggested if the capture process is already in progress. In this case, you must proceed with a refund.

When a cancellation request is accepted, the transaction status changes to **Cancelled** (CANCELLED).

It is impossible to cancel a cancellation request.

Reversal request

If the acquirer supports it, when the merchant cancels a transaction, the payment gateway automatically requests the cancellation of the authorization request.

If the card issuer accepts the request, the authorization limit of the cardholder's card is restored.

Otherwise, or if the acquirer does not support the reversal, the transaction is canceled and the card limit is restored when the authorization request expires.

If a reversal request is made upon cancellation, it will appear in the transaction details (History tab).

To request a transaction cancellation:

- Go to the **Transactions is progress** tab to cancel a transaction in progress.

1. Select the transaction.
2. Click **Cancel**.

   A confirmation message of cancellation appears.
3. Click **Yes** to confirm the cancellation of the transaction or **No** to undo your action.

An error message may appear if the transaction cannot be cancelled. In this case, follow the instructions in the message.

Case of installment payments:

If you cancel a transaction with installments, you have the option of canceling only the selected transaction or canceling all associated installments. Simply check "**Cancel all scheduled payments**".

Cancellation of multiple transactions

It is possible to cancel several transactions at the same time:

1. Select all the transactions to be canceled.

*Hold down the **Ctrl** key and the **left mouse button** simultaneously to select several transactions.*

2. Click **Cancel** and confirm your choice.

The status of the transactions will change to **Cancelled**.

10.3. Modifying a transaction

The **Edit** action is available when the transaction has one of the following statuses:

- To be validated
- To be validated and authorized
- Waiting for authorization
- Waiting for capture

This action allows to modify the amount and the capture date at the bank with respect to the following constraints:

- the modified amount cannot be greater than the initial amount
- when the transaction has not yet been authorized, the capture date can be defined anytime between the current date and the capture date specified by the merchant during the payment.

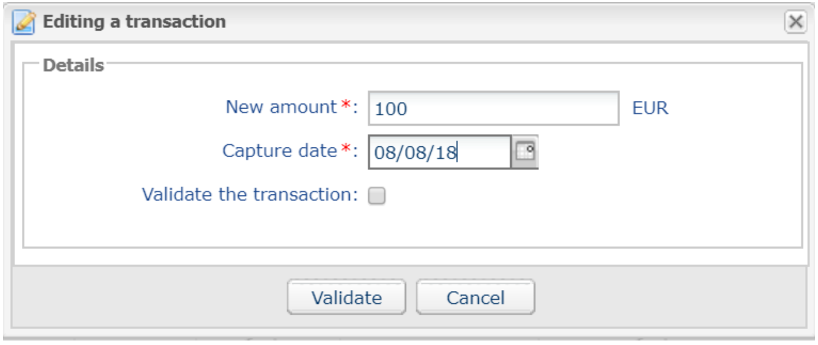
  An authorization request will be automatically triggered if the selected capture date is between the current date and the expiry date of the authorization request (e.g.: 7 days for Visa).
- when the transaction has already been authorized, the capture date at the bank cannot be later than the expiry date of the authorization (e.g.: 7 days for Visa).
- the card type authorizes to modify the amount or the capture date.

To modify a transaction:

1. Select the transaction.

2. Click on **Modify**

   The dialog box **Editing a transaction** appears.



Editing a transaction

Details

New amount*: 100 EUR

Capture date*: 08/08/18

Validate the transaction: □

   *It is also possible to validate transactions with the **To be validated** or **To be validated and authorized** status by checking **Validate the transaction**.*

3. Enter a new amount.

   Reminder: the new amount must be lower than the initial amount.

4. Enter the capture date.

   The calendar will show the authorized slot for the capture date. The slot is calculated based on when the authorization expires. The authorization validity period depends on the payment method and the network that was used for the authorization requeste.g.: 7 days for Visa).

5. Click **Sign in**.

Once the transaction has been modified:

- the payment amount corresponds to the modified amount,
- the initial amount corresponds to the amount before the modification.

10.4. Duplicating a transaction

This function allows to create a new transaction with the exact same characteristics (e.g. card number) as the transaction that was used for duplication.

A duplicated transaction has the same characteristics as all the other transactions, and it can be duplicated itself.

During duplication of a transaction, a new authorization request is made with the card number that corresponds to the original transaction. This transaction does not have a payment guarantee.

The payment receipt will be sent to the buyer if the e-mail is specified for the transaction used for duplication and if the notification rule associated with sending an e-mail to the buyer is active.

Transactions that can be subject to duplication must have one of the following status(es):

- Captured
- Expired
- Cancelled
- Refused

The duplication of refused transactions made with Mastercard cards (Mastercard, Maestro, Mastercard Debit) is forbidden when one of the following reasons is mentioned:

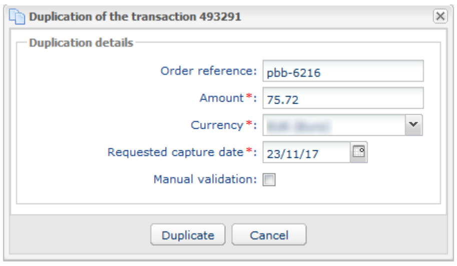
- 04 - Please hold card
- 14 - Invalid cardholder number
- 15 - Unknown card issuer
- 41 - Lost card
- 43 - Stolen card
- 54 - Exp. date of the card passed

To duplicate a transaction:

1. Select the transaction.

2. Click **Duplicate**.

   The dialog box **Duplication of the transaction** appears. All of the fields are pre-populated.



Duplication of the transaction 493291

Duplication details

Order reference: pbb-6216

Amount*: 75.72

Currency*: [redacted]

Requested capture date*: 23/11/17

Manual validation: □

You can modify:

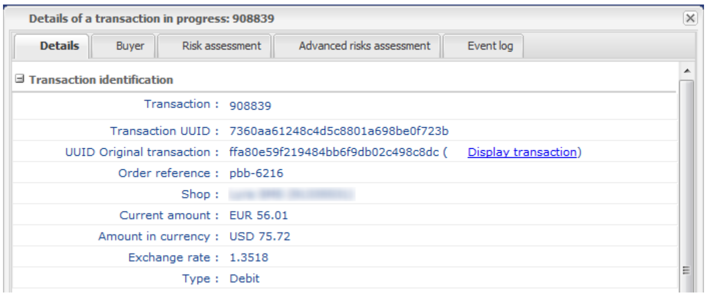
- The order reference

- The amount
- The currency

  If the selected currency is not supported the following message is displayed: ***Currency not supported by this Merchant ID (MID) and/or shop***.

  If the selected currency is supported and multi-currency is possible in your contract, the conversion rate will be applied. The details of the new transaction will be displayed with both currencies: local currency and new currency.

  Example



Details of a transaction in progress: 908839

Transaction identification

Transaction : 908839
Transaction UUID : 7360aa61248c4d5c8801a698be0f723b
UUID Original transaction : ffa80e59f219484bb6f9db02c498c8dc (Display transaction)
Order reference : pbb-6216
Shop : [redacted]
Current amount : EUR 56.01
Amount in currency : USD 75.72
Exchange rate : 1.3518
Type : Debit

- The requested capture date

  It can not be earlier than the transaction modification date.
- The validation mode by (un)checking **Manual validation**.

3. Click **Duplicate** to continue or **Cancel** to cancel the duplication.

The transaction can be viewed in the **Transactions is progress** tab.

10.5. Refunding a transaction

This operation makes it possible to re-credit a customer's account after a transaction.

The customer account is credited with the refunded amount, the merchant account is debited with the same amount.

The refund is only available for captured transactions. Depending on the acquirer, it is possible to partially or fully refund the transaction amount.

The refund delay after the initial transaction date also depends on the acquirer or the network.

For example:

- Until the card expiry within the CB network. Refund forbidden to an expired card.
- 180 days within the PAYPAL network.
- 15 months within the AMEXGLOBAL network.
- 20 days within the ONEY_API network.

For more information, see the reference documentation for the payment method in question.

Case of chargebacks: any attempt to refund an unpaid transaction will be rejected.

Case of refund refusal:

A system called **credit online** has recently been impletented. This system includes a systematic authorization request sent to the buyer's bank for each refund request.

This lets you know whether the refund is accepted, and if not, the reason why it is blocked.

In case of refusal at the time of the authorization request, the buyer’s bank returns a reason to us, and we present it to you.

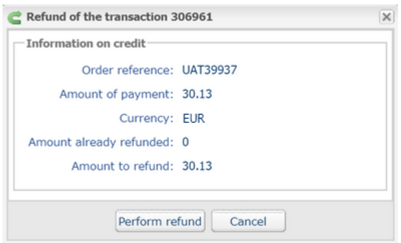
For the CB network, we indicate the code and the refusal reason sent by the buyer's bank. If the refund request is made from the Merchant Back Office, a warning message is also displayed to inform that the buyer’s financial institution is the cause of this refusal for its own reason.

For example, if the refund request is made on a blocked card, the code and refusal reason will be “59: suspected fraud” for some acquirers. See: *List of specific return codes* for the CB network for more details.

You must then refund your buyer **by another payment method** (cheque, wire transfer, etc.).

1. Go to the **Captured transactions** tab.
2. Select the transaction.
3. Click **Making a refund**. The **Refund of the transaction** dialog box appears.

Example of a full refund

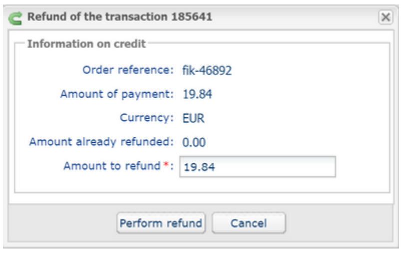


Refund of the transaction 306961

Information on credit

Order reference: UAT39937
Amount of payment: 30.13
Currency: EUR
Amount already refunded: 0
Amount to refund: 30.13

Example of a partial refund



Refund of the transaction 185641

Information on credit

Order reference: fik-46892
Amount of payment: 19.84
Currency: EUR
Amount already refunded: 0.00
Amount to refund *: 19.84

4. Enter the amount that you want to refund. The input field appears if partial refund is possible.
5. Click **Perform refund**. Details of this operation appear.

10.6. Manual reconciliation

This operation allows you to manually reconcile merchant's payments from an account statement.

1. Search for the relevant transaction via the **Captured transactions** tab.
2. Right-click the transaction.
3. Select **Manual reconciliation**.
4. Click **Yes** to confirm the manual reconciliation of the selected transaction.
   The **Comment** dialog box appears.
5. Enter a comment for this reconciliation.
6. Click **OK**.

The transaction status changes to **Reconciled**.

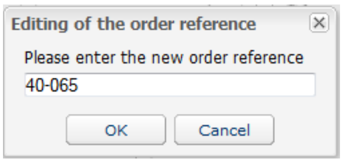
10.7. Editing the order reference

This operation allows the merchant to change the order reference.

To edit the order reference of a transaction:

1. Right-click the transaction.

2. Select **Editing the order reference**.



Editing of the order reference

Please enter the new order reference

40-065

3. Enter the new order reference.

4. Click **OK**.

10.8. Creating a token using a transaction

This action allows the user to create a token of the payment method used for the payment.

This action is authorized only if the original transaction status is:

- accepted
- to be validated
- waiting for capture
- captured
- capture in progress

The payment method used for the original transaction must:

- support payment by token,
- be supported by a non-terminated MID associated with the shop.

Token creation leads to creating a transaction of **VERIFICATION** type and sending the following notifications (if the Merchant has enabled the corresponding rules):

- Instant Payment Notification URL on an operation coming from the Back Office,
- Confirmation e-mail of token creation sent to the merchant,
- Confirmation e-mail of token creation sent to the buyer.

A line will be added to the detail summary of the original transaction in order to track the transaction.

To create a token:

1. Right-click the transaction.

2. Select **Create a token using a transaction**.
   The token creation wizard appears.

3. Enter the **Buyer's e-mail** e-mail address.

4. A token is generated by default in the **Token ID** field. You can click on the button **Generate a new identifier** if you wish.

   You also can enter your own token. You must, however, make sure it is unique.

5. If you wish, you can select the used currency when checking the payment method.

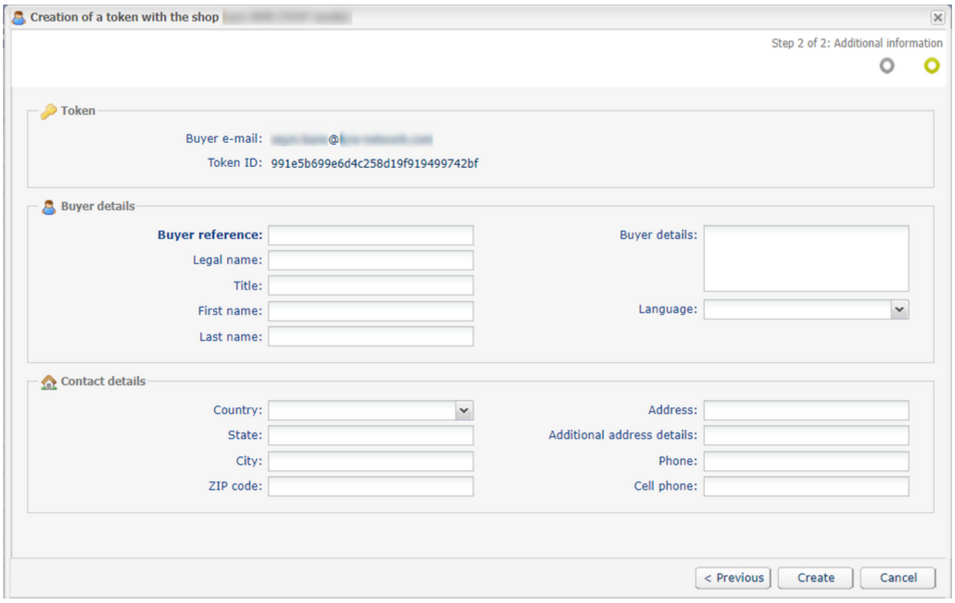
   This choice is useful when you have a multi-currency agreement associated with several shops, where each shop only supports one currency.

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

6. Click **Next**.

   The buyer detail entry page appears.

   The **Token** section reminds you of the specified e-mail and the created token.



Creation of a token with the shop [redacted]

Step 2 of 2: Additional information

Token

Buyer e-mail: [redacted]@[redacted]

Token ID: 991e5b699e6d4c258d19f919499742bf

Buyer details

Buyer reference:

Legal name:

Title:

First name:

Last name:

Buyer details:

Language:

Contact details

Country:

State:

City:

ZIP code:

Address:

Additional address details:

Phone:

Cell phone:

7. Fill in the information about the buyer.

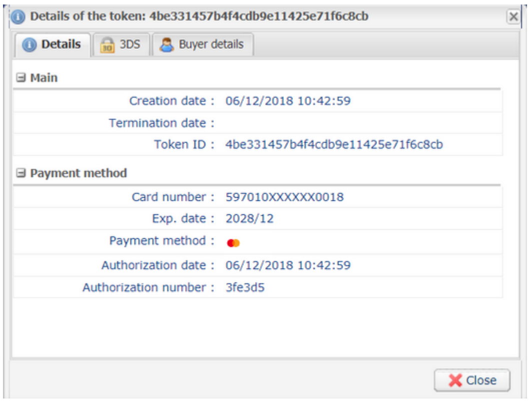
   These details are useful for buyer identification.

   Fields marked with an asterisk (*) are required.

   The buyer’s “First name” and “Last name” are mandatory when creating a SEPA mandate.

8. Click **Create** to complete the process.

If all the payment method verification processes have been successfully completed, the token detail window appears.



Details of the token: 4be331457b4f4cdb9e11425e71f6c8cb

Main

Creation date : 06/12/2018 10:42:59

Termination date :

Token ID : 4be331457b4f4cdb9e11425e71f6c8cb

Payment method

Card number : 597010XXXXXX0018

Exp. date : 2028/12

Payment method : ●

Authorization date : 06/12/2018 10:42:59

Authorization number : 3fe3d5

It mentions the **Token ID**. It corresponds to the newly created token. Later on, it can be used for another financial operation in your shop(s).

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

10.9. Downloading the payment receipt

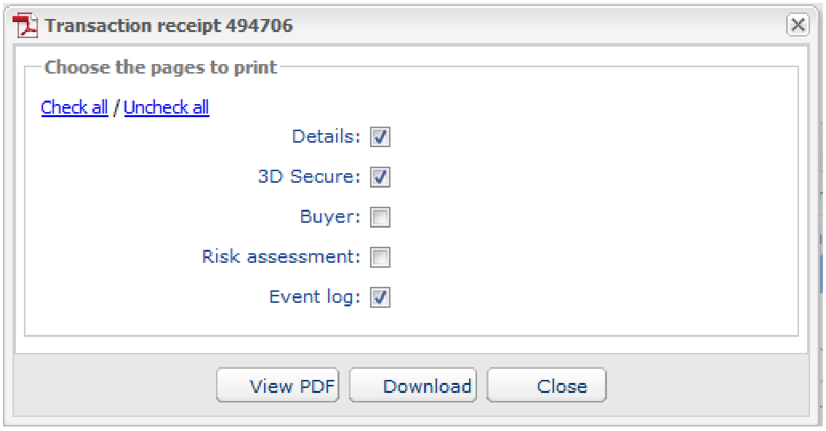
Payment receipt is a transaction proof binding merchant to buyer and may be presented in case of dispute or information request to the issuer or acquirer.

You can download the transaction receipt in PDF format.

This operation is available both for **transactions in progress** and **captured transactions**:

1. Locate and select the transaction,
2. Click **Receipt,**

   The page **page selection for printing** is displayed.



Transaction receipt 494706

Choose the pages to print

Check all / Uncheck all

Details: ☑

3D Secure: ☑

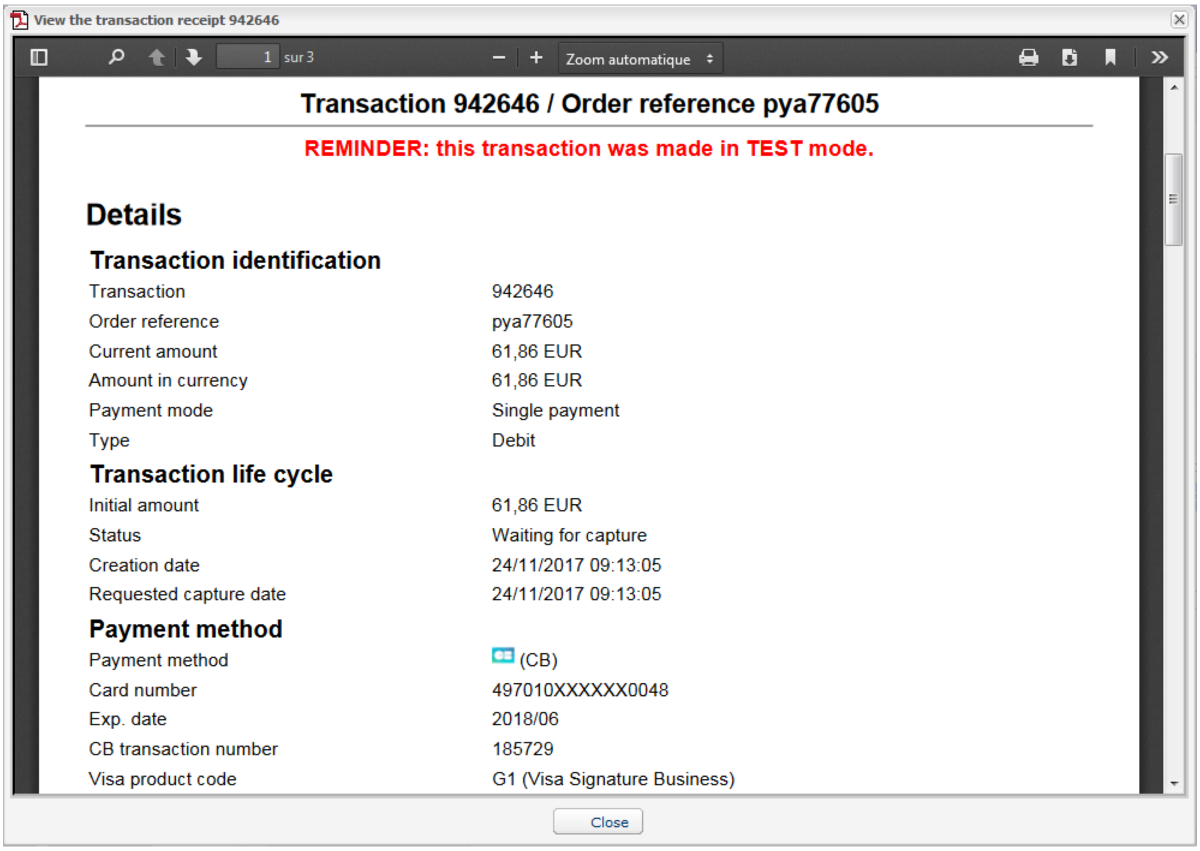
Buyer: □

Risk assessment: □

Event log: ☑

   The available choices depend on the tabs available for the transaction,

3. Check the details you want to print,
4. Click **View PDF** to view the information before downloading the file.



View the transaction receipt 942646

Transaction 942646 / Order reference pya77605

REMINDER: this transaction was made in TEST mode.

Details

Transaction identification

Transaction	942646
Order reference	pya77605
Current amount	61,86 EUR
Amount in currency	61,86 EUR
Payment mode	Single payment
Type	Debit

Transaction life cycle

Initial amount	61,86 EUR
Status	Waiting for capture
Creation date	24/11/2017 09:13:05
Requested capture date	24/11/2017 09:13:05

Payment method

Payment method	(CB)
Card number	497010XXXXXX0048
Exp. date	2018/06
CB transaction number	185729
Visa product code	G1 (Visa Signature Business)

5. Click **Download** to print or save the document file.

10.10. Sending a payment order from a declined transaction

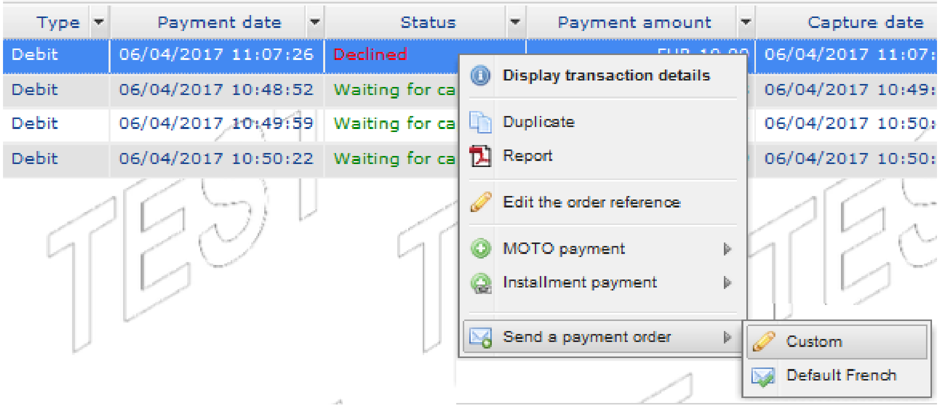
After a declined payment, you have the option to send a payment order from the declined payment to your buyer.

During this second attempt, the buyer will have, for example, the possibility to change the payment method.

Note

To use this option, your offer must include payment by e-mail.

1. Display the **Transactions in progress** tab.
2. Select the declined transaction.
3. Right click on the transaction.



Type	Payment date	Status	Payment amount	Capture date
Debit	06/04/2017 11:07:26	Declined	EUR 10.00	06/04/2017 11:07:
Debit	06/04/2017 10:48:52	Waiting for ca		06/04/2017 10:49:
Debit	06/04/2017 10:49:59	Waiting for ca		06/04/2017 10:50:
Debit	06/04/2017 10:50:22	Waiting for ca		06/04/2017 10:50:

4. Select **Send a payment order** from the menu.

   Several possibilities in choosing the e-mail template:

   - The **Default** e-mail template allows you to send e-mails without personalization and in the language of the Merchant Back Office.
   - The **Custom** template allows you to go to the payment order editor by e-mail and personalize your e-mail (subject, content, validity period, selective 3DS on the order).
   - Other templates allow you to send the email directly by just selecting the template name.

   Sending the e-mail is immediate without going through the mail payment order editor if you select a template. A confirmation page is displayed.

5. Confirm by clicking **Yes**.

Your buyer will receive a payment order with the declined amount. He or she simply needs to follow the link to resume the payment.

11. MANUALLY RESENDING A NOTIFICATION

The merchant can manually resend a notification via a transaction present in the table of transactions (in progress or captured).

11.1. Resending the end of payment notification (IPN)

This functionality allows to manually resend a notification at the end of payment to the notification URL of the shop.

It is useful when the initial notification failed, whichever rule was triggered.

To use this functionality, the merchant must have configured the Instant Payment Notification URL at the end of payment rule.

The Send the Instant Payment Notification option is not available in the context menu if you have not configured the IPN rule or if your user account has not been allowed to perform this action.

1. In the transaction table, search for the transaction for which you would like to resend the notification.
2. Right-click the transaction and select **Send the Instant Payment Notification**.

   If your application becomes available once again, you will see a message confirming that the URL has been successfully executed.

   In any case, you can view the result of your action in the event history of the transaction and analyze the error messages if the problem persists.

Characteristics of manual execution

When an IPN is manually executed, some fields will not be sent or will have a different value.

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

- **vads_page_action**
- **vads_payment_config**
- **vads_action_mode**

Examples of fields sent with different values:

- **vads_url_check_src**

  Will be set to **BO** in case of a manual retry.
- **vads_trans_status**

  The transaction status may differ between the initial call and the retry.
- **vads_hash**
- **signature**

11.2. Resending the payment confirmation e-mail to the merchant

Before you resend the transaction confirmation e-mail to the merchant, the merchant must have configured the Payment confirmation e-mail sent to the merchant rule.

1. In the transaction table, search for the transaction for which you would like to resend the payment confirmation e-mail.
2. Right-click the transaction and click **Resending the transaction confirmation e-mail to the merchant**.

   A confirmation message appears.
3. Click **OK**.

11.3. Resending the payment confirmation e-mail to the buyer

To resend the payment confirmation e-mail to the buyer in case it has not been received or if the email address has changed:

1. In the transaction table, search for the transaction for which you would like to resend the confirmation e-mail to the buyer.
2. Right-click the transaction and click **Resend the transaction confirmation e-mail to the buyer**.

   The dialog box for entering the e-mail address appears.

   The entry field is pre-populated with the buyer's e-mail address that was saved during the transaction.
3. Enter another e-mail address if necessary.
4. Click **OK**.

12. RECONCILING TRANSACTIONS AND CHARGEBACKS

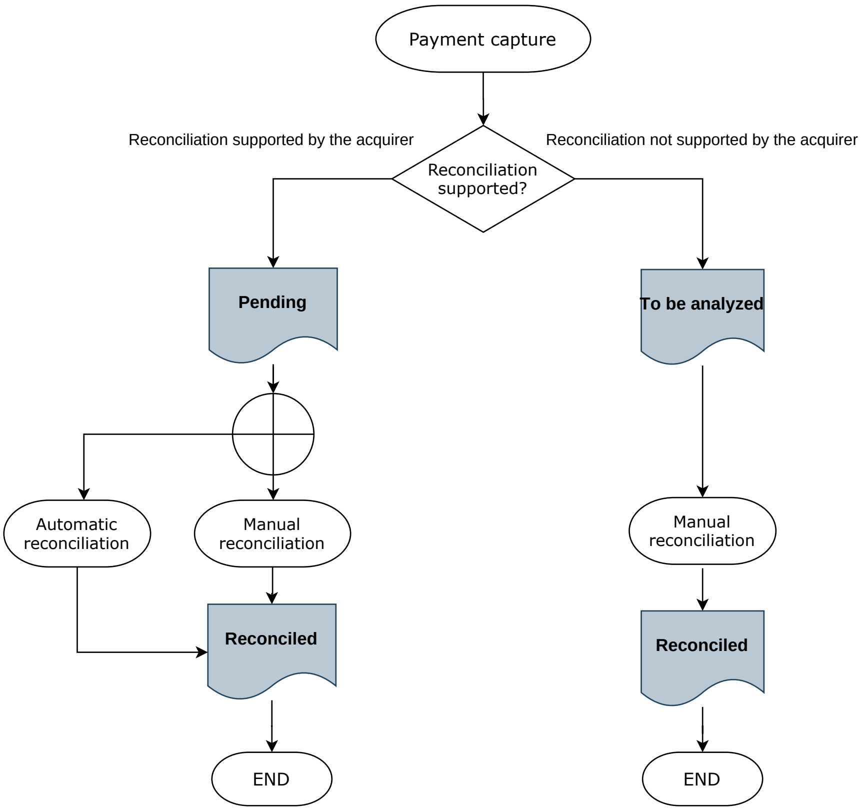
If you have selected the corresponding options in your Sogecommerce offer, you benefit from the following services:

- Visual transaction reconciliation
- Visual chargeback reconciliation
- Bank reconciliation report
- Chargeback reconciliation report

12.1. The “Visual reconciliation” service

The visual reconciliation service allows merchants to benefit from automatic reconciliation of transactions made on the payment gateway with the payments that appear on their bank statement.

Operating principle



If the acquirer supports reconciliation, each captured transaction gets the “**Pending**” reconciliation status.

If the acquirer does not support reconciliation, captured transactions get the “**To be analyzed**” reconciliation status.

As soon as the service is enabled, automatic processing is set up to check the transactions acquired on the payment gateway and the bank statement entries.

Successfully reconciled transactions get the “**Reconciled**” status.

Transactions with the "**Pending**" or "**To be analyzed**" status may be reconciled manually by the merchant via the **Captured transactions** tab (see chapter *Manual reconciliation* on page 44).

Liste des acquéreurs supportant la réconciliation :

CODE Réseau	Acquéreur
AMEXGLOBAL	American Express Global
CB	Société Générale
PAYPAL	PayPal
SEPA	Société Générale

Special case: SEPA Direct Debit request

The reconciliation status of a SDD transaction is set to "**Reconciled**" as soon as the direct debit file is submitted to the bank.

This status is not definitive and can change within the day.

12.2. The "Visual chargeback reconciliation" service

The visual chargeback reconciliation service allows merchants to benefit from automatic reconciliation of chargeback transactions.

Operating principle

Each captured transaction has an chargeback reconciliation status. Possible values in **Dispute**:

- **Yes**

  the visual chargeback reconciliation service is disabled. A dispute has been received on the transaction.
- **No**

  The visual chargeback reconciliation service is enabled and no disputes have been filed for the transaction.
- **n/a**

  The visual chargeback reconciliation service is disabled.

As soon as the service is enabled, automatic processing is set up to check the transactions acquired on the payment gateway and any potential chargebacks.

Transactions that have been the subject of an chargeback reconciliation are valued at **Yes** in **Dispute** data.

Transactions that are not subject to chargeback reconciliation, while the option is selected, are valued at **No**.

The "**N/A**" status corresponds to transactions of a merchant that has not opted for the visual chargeback reconciliation service.

List of acquirers supporting chargeback reconciliation:

Network CODE	Acquirer
AMEXGLOBAL	American Express Global
CB	Société Générale
SEPA	Société Générale

12.3. The “Reconciliation reports” service

This service provides the merchant with a file containing a list of automatically reconciled transactions. The report provides additional bank details (amount credited to the account, commission fees, etc.).

See the *corresponding documentation* in our online document archive.

12.4. The “Chargeback reconciliation report” service

This service provides the merchant with a file containing a list of automatically reconciled chargeback transactions. The report provides additional bank details (reason of the chargeback, etc.).

See *corresponding documentation* in our online document archive.

13. TRANSACTION RETENTION PERIOD

Transactions are stored in the Merchant Back Office for a limited period of time.

- In TEST mode, each transaction is stored for a period of 30 days after the transaction date. It will be automatically deleted after the deadline.
- In PRODUCTION mode, the transaction storage rule is established according to PCI-DSS mode. Each transaction is stored for 15 months after the transaction date. It will be automatically deleted after the deadline.

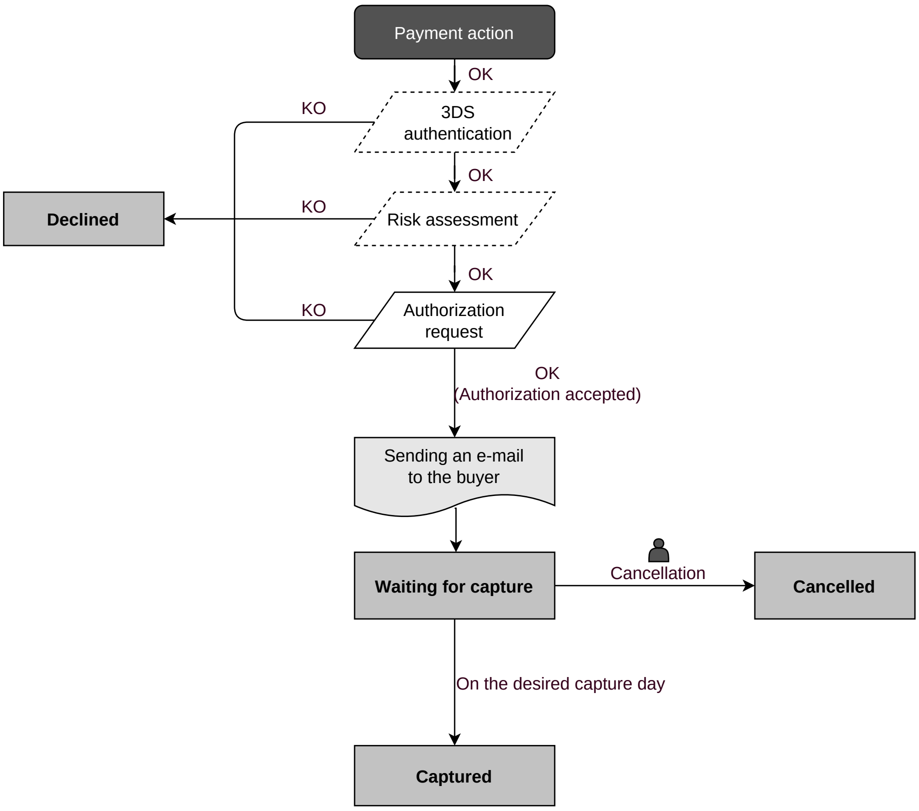
14. TRANSACTION LIFECYCLE

In all the following diagrams, the following caption is used:

👤 Action required from the merchant - manual (Merchant Back Office) or automatic (Web Services)

14.1. Immediate payment

14.1.1. Automatic validation



Once the payment request has been made, several verification processes start automatically:

- The 3D Secure authentication.
- Different verification processes performed by the payment gateway (these potentially include local checks, risk rules configured by the merchant) or by an external risk analyzer.
- An authorization request is also made by the buyer's bank on the day of payment, independently of the requested capture date at the bank.

If one of the verification processes fails, the payment request will not be accepted. The buyer is informed of the rejection on the screen. In the Merchant Back Office, the transaction appears with the **Refused** status.

Otherwise, the transaction takes the **Waiting for capture** status.

The buyer is informed about the acceptance of the payment request and receives a confirmation e-mail.

The transaction will be automatically submitted for capture on the day requested by the merchant and will take the **Captured** status. The **Captured** status is final.

Once the capture is made, the arrival of the transaction to the merchant account depends on the interbank processing time.

Before the capture date, the buyer can modify it together with the amount (only smaller amounts can be entered in case of partial delivery by the merchant).

If necessary, the buyer can also cancel the transaction: the transaction will then appear with the **Cancelled** status.

14.1.2. Manual validation

Following a payment request, the verification process starts automatically:

- The 3D Secure authentication.
- Different verification processes performed by the payment gateway (these potentially include local checks, risk rules configured by the merchant) or by an external risk analyzer.
- An authorization request is also made by the buyer's bank.

If one of the verification processes fails, the payment request will not be accepted. The buyer is informed of the rejection on the screen. In the Merchant Back Office, the transaction appears with the **Refused** status.

Otherwise, the payment is accepted and the transaction appears in the Merchant Back Office with the **To be validated** status.

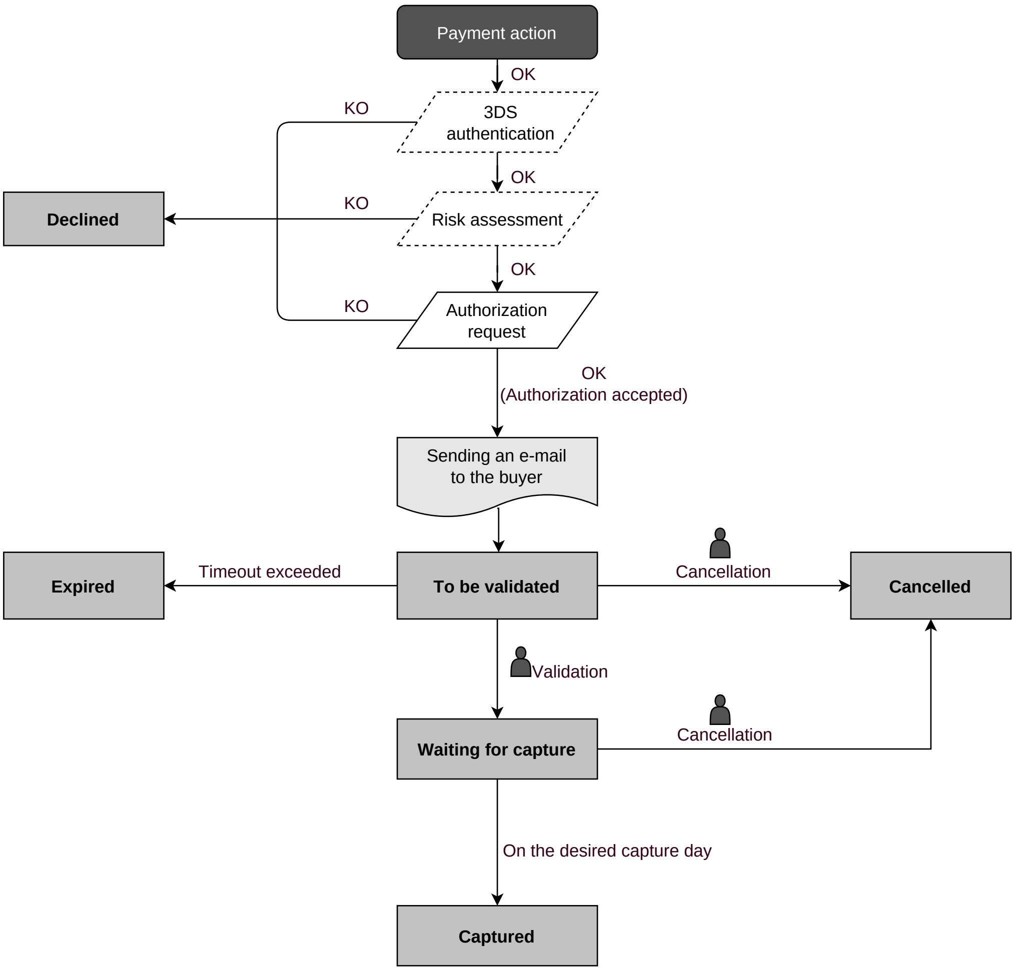
In this case, the merchant must validate the transaction before the expiry date of the authorization request. If the validation is made after this date, the transaction appears as **Expired** and cannot be captured in the bank.

As soon as the transaction is validated, its status changes to **Waiting for capture**.

The transaction will be automatically submitted for capture on the day requested by the merchant and will take the **Captured** status. The **Captured** status is final.

Once the capture is made, the arrival of the transaction to the merchant account depends on the interbank processing time.

The merchant can also cancel the transaction, if necessary. In this case, the transaction takes the **Cancelled** status.


Payment action
OK
KO
3DS authentication
OK
KO
Declined
Risk assessment
OK
KO
Authorization request
OK (Authorization accepted)
Sending an e-mail to the buyer
Expired
Timeout exceeded
To be validated
Cancellation
Cancelled
Validation
Cancellation
Waiting for capture
On the desired capture day
Captured

14.2. Deferred payment

14.2.1. Automatic validation

Capture delay shorter than the authorization validity period

(See the diagram “The life cycle of an immediate payment transaction”).

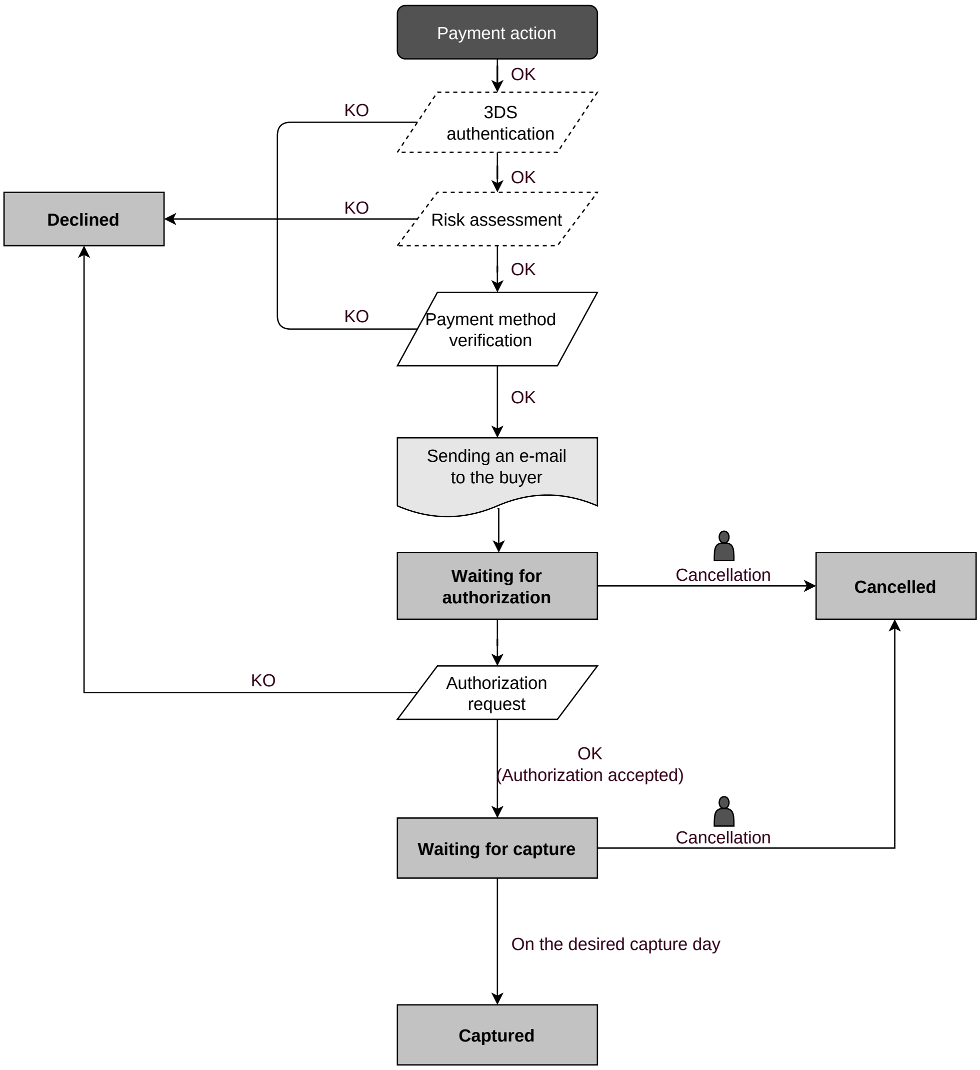
Capture delay longer than the authorization validity period

All the transactions for deferred payments made in automatic validation mode with a successfully completed verification request can be viewed in the Merchant Back Office with the **Waiting for authorization** status.

The authorization request is automatically sent:

- By default: the day before the desired capture date,
- With anticipated authorization: depending on the selected payment method, on D-Δ before the desired capture date (see chapter *The “Anticipated authorizations” service* on page 62).

A deferred payment goes through the steps in the diagram below:



14.2.2. Manual validation

Capture delay shorter than the authorization validity period

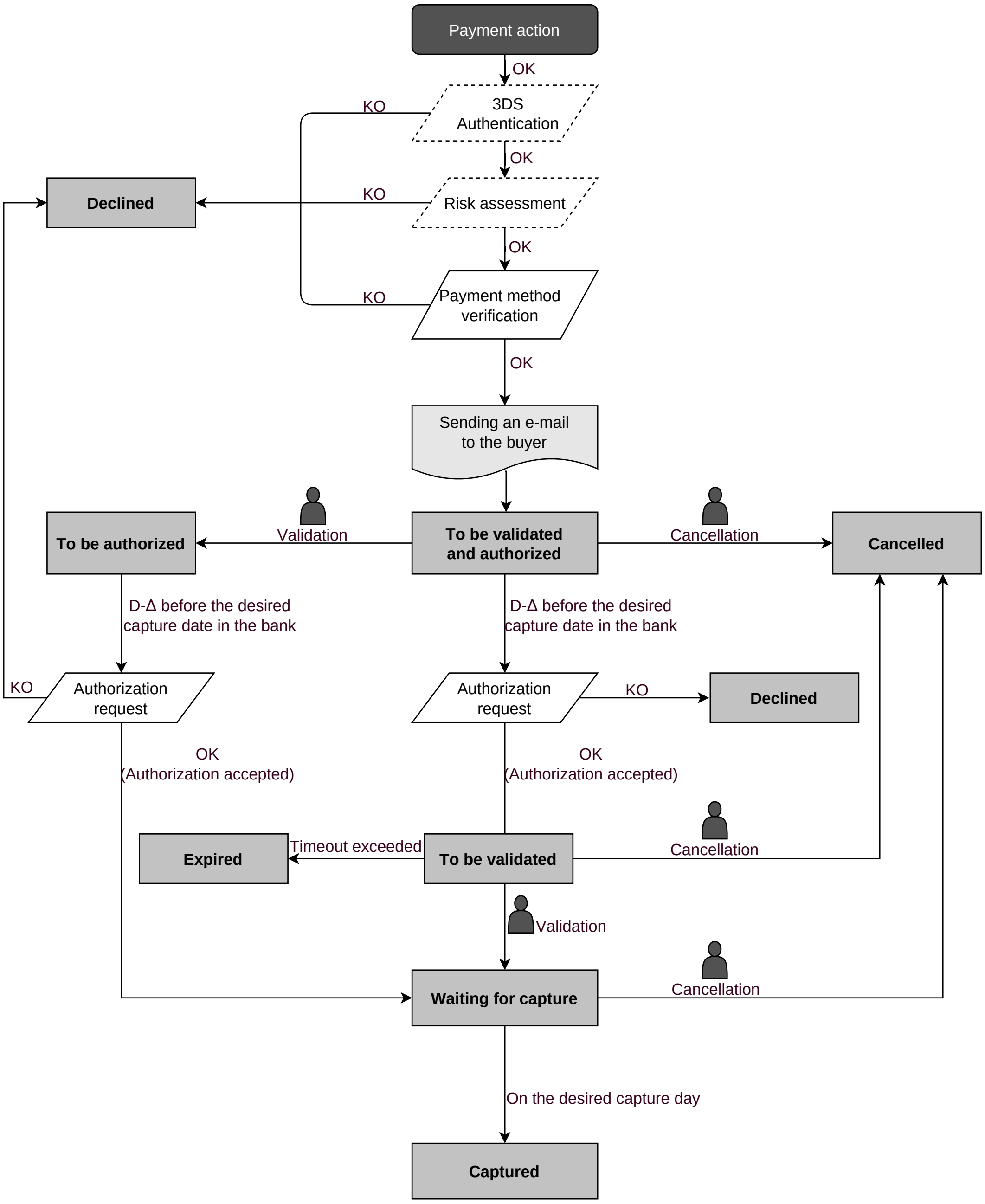
(See the diagram "The life cycle of an immediate payment transaction").

Capture delay longer than the authorization validity period

All the transactions for deferred payments made in automatic validation mode with a successfully completed authorization request for EUR 1 (or information request about the CB network if the acquirer supports it) can be viewed in the Merchant Back Office with the **To be validated and authorized** status.

The authorization request is automatically sent on the requested capture day, on the condition that the merchant has already validated the transaction.

In the meantime, the merchant may cancel the transaction or change its amount (only smaller amounts can be entered) and/or the capture date. These transactions go through the steps in the diagram below:



14.3. Payment in installments

14.3.1. Automatic validation

The activation of the payment in installments feature is subject to the prior agreement of Société Générale.

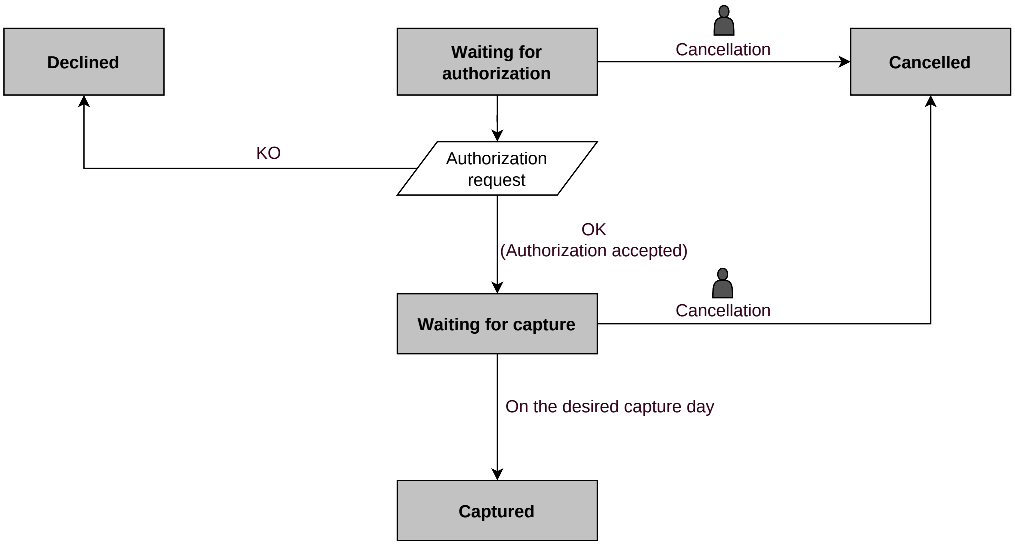
Depending on the capture date, the first installment will have exactly the same features as an immediate payment or a deferred payment.

By default, the following installments will have the **Waiting for authorization** status. The buyer's bank will be able to reject the authorization request. The payment gateway will then inform the merchant by e-mail that the transaction has been declined.

The authorization requests for the upcoming installments are automatically sent as a transaction for a deferred payment, with two possible dates:

- By default: the day before the desired capture date,
- With anticipated authorization: depending on the selected payment method, on D-Δ before the desired capture date (see chapter *The "Anticipated authorizations" service* on page 62).

The following installments go through the steps specified in the diagram below (case of an authorization request that is not resent):



In any case, canceling an installment never implies that the upcoming installments will be canceled.

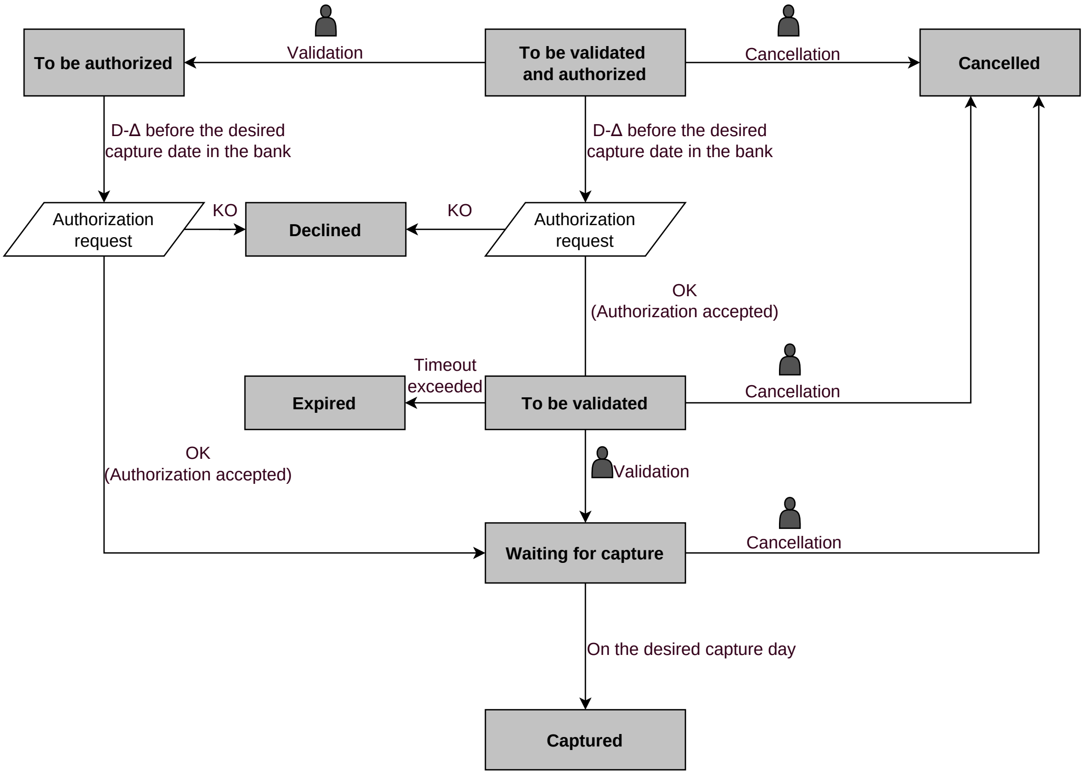
14.3.2. Manual validation

The activation of the payment in installments feature is subject to the prior agreement of Société Générale.

Depending on the capture date, the first installment will have exactly the same features as an immediate payment or a deferred payment.

By default, the upcoming installments have the **To be validated and authorized** status as long as the first installment has not been validated by the merchant. The successful execution of the installments is not guaranteed to the merchant. The buyer's bank may reject the authorization request.

Validation of the first installment implies that all the other installments will be validated as well. However, canceling an installment does not cancel the upcoming installments.


To be authorized
Validation
To be validated and authorized
Cancellation
Cancelled
D-Δ before the desired capture date in the bank
D-Δ before the desired capture date in the bank
Authorization request
KO
Declined
KO
Authorization request
OK (Authorization accepted)
Timeout exceeded
Expired
To be validated
Cancellation
OK (Authorization accepted)
Validation
Waiting for capture
Cancellation
On the desired capture day
Captured

14.4. The “Anticipated authorizations” service

This service allows to trigger the authorization on D-Δ (see *Authorization validity period* for each payment method) before the desired capture date at the bank.

In case of refusal by the issuing bank, exclusively for a non-fraud related reason, a process automatically reissues authorization requests until up to 2 days prior to the desired capture date at the bank.

The merchant may cancel the transaction or change its amount (only smaller amounts can be entered) and/or the capture date at any moment.

This process applies to:

- recurring payments,
- deferred payments,
- installments, other than the first one, in case of payment in installments.

In case of refusal for fraud-related reasons, the transaction is considered as permanently rejected.

Here is a list of fraud-related reasons that do not allow authorization reruns.

Network	Authorization return code	Label
CB	03	Invalid acceptor
	04	Keep the card
	05	Do not honor
	07	Keep the card, special conditions
	12	Incorrect Transaction Code
	13	Invalid amount
	14	Invalid cardholder number
	15	Unknown issuer
	31	Unknown acquirer company ID
	33	Expired card
	34	Suspected fraud
	41	Lost card
	43	Stolen card
	54	Expired card
	56	Card absent from the file
	57	Transaction not allowed for this cardholder
	59	Transaction not allowed for this cardholder
	63	Security rules unfulfilled
	76	The cardholder is already blocked, the previous record has been saved
	80	Contactless payment is not accepted by the issuer
	81	Unsecured payment is not accepted by the issuer
	82	Revocation of recurring payment for the card of a specific Merchant or for the MCC and the card
	83	Revocation of all recurring payments for the card

Contact your customer advisorSociété Générale if you would like to enable anticipated authorizations.

14.5. Authorization request validity period

Network code	Payment method	Card types (vads_payment_cards)	Authorization validity period (in days)
ACCORD	Illicado gift Card	ILLICADO	0
ACCORD	PicWic brand card	PICWIC	0
ACCORD_SANDBOX	Illicado gift cards - Sandbox mode	ILLICADO_SB	0
ACCORD_SANDBOX	PicWic brand card - Sandbox mode	PICWIC_SB	0
AMEXGLOBAL	American Express	AMEX	7
AURORE	Cpay card	AURORE-MULTI	29
CB	CB	CB	7
CB	e-Carte Bleue virtual card	E-CARTEBLEUE	7
CB	Maestro	MAESTRO	30
CB	Mastercard	MASTERCARD	7
CB	Visa	VISA	7
CB	Visa Electron	VISA_ELECTRON	7
CB	VPay	VPAY	7
CB	Bimpli Meal Voucher card (ex Apetiz)	APETIZ	7
CB	Chèque Déjeuner Meal Voucher card	CHQ_DEJ	7
CB	1st generation Mastercard electronic meal voucher	EDENRED	7
CB	Sodexo Meal Voucher card	SODEXO	7
CONECS	Bimpli Meal Voucher card (ex Apetiz)	APETIZ	30
CONECS	Chèque Déjeuner Meal Voucher card	CHQ_DEJ	30
CONECS	Conecs Meal Voucher card	CONECS	30
CONECS	Sodexo Meal Voucher card	SODEXO	30
CVCONNECT	Chèque-Vacances Connect	CVCO	6
FRANFINANCE	Franfinance payment in 3X	FRANFINANCE_3X	0
FRANFINANCE	Franfinance payment in 4X	FRANFINANCE_4X	0
FRANFINANCE_SB	Franfinance payment in 3X - Sandbox mode	FRANFINANCE_3X	0
FRANFINANCE_SB	Franfinance payment in 4X - Sandbox mode	FRANFINANCE_4X	0
FULLCB	Payment in 3 installments with no fees with BNPP PF	FULLCB3X	7
FULLCB	Payment in 4 installments with no fees with BNPP PF	FULLCB4X	7
MASTERPASS	MasterPass	MASTERPASS	0
ONEY_API	Oney 3x 4x payment	ONEY_3X_4X	0
ONEY_API	Payment 10x 12x Oney	ONEY_10X_12X	0
ONEY_API	Payment Oney Pay Later	ONEY_PAYLATER	0
ONEY_API	Oney partner brand cards	ONEY_ENSEIGNE	0
ONEY_API_SANDBOX	Oney 3x 4x payment (Sandbox mode)	ONEY_3X_4X	0
ONEY_API_SANDBOX	Oney 10x 12x payment (Sandbox mode)	ONEY_10X_12X	0
ONEY_API_SANDBOX	Payment Oney Pay Later (Sandbox mode)	ONEY_PAYLATER	0
ONEY_API_SANDBOX	Oney partner brand cards in Sandbox mode	ONEY_ENSEIGNE	0

Network code	Payment method	Card types (vads_payment_cards)	Authorization validity period (in days)
PAYPAL	PayPal	PAYPAL	3
PAYPAL_SB	PayPal - Mode sandbox	PAYPAL_SB	3
PLANET_DCC	MASTERCARD	MASTERCARD	0
PLANET_DCC	VISA	VISA	0
SEPA	SEPA DIRECT DEBIT	SDD	15

15. OBTAINING HELP

Looking for help? See our FAQ:

https://sogecommerce.societegenerale.eu/doc/fr-FR/faq/faq-homepage.html

For any technical inquiries or if you need any help, contact *technical support*.

In view of facilitating the processing of your requests, please have your shop ID ready (an 8-digit number).

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