



IMPLEMENTATION OF FLIK PAYMENT METHOD FOR E-COMMERCE

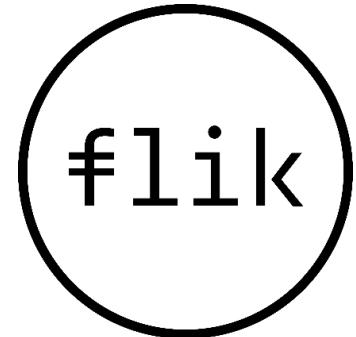
April 2024

Table of contents

What is Flik?	3
TECHNICAL INTEGRATION OF FLIK PAYMENT METHOD	5
Basic information	6
Flow of message exchange between the merchant's system and the Bankart Payment Gateway	6
Specification of API calls for Flik remote payments	7
Initial API call	8
API call response – customer redirection	9
API call response - without redirection	11
Payment result	12
Structured and unstructured payment reference	13
INSTRUCTIONS FOR TESTING AND TRANSITION TO PRODUCTION	14
Basic information	15
Data for the connecting to the Payment Gateway	15
Testing payments with the simulator	18
Testing payments without redirection	20
Transition to production environment	21
Validation of the alias input format	21
Declined transaction due to non-existent alias	23
BANKART PAYMENT GATEWAY: THE USER INTERFACE	24
Access to the portal	25
Overview of the graphical interface	25
Review of transaction details (logs)	26
Refund of the transaction amount	28
Export of the list of completed transactions	29
Frequently Asked Questions by Traders (FAQ)	31

What is Flik?

Flik is a modern and simple method of payments and transfers between customers of various banks in Slovenia and enables various payment options (transferring money between people in everyday life or at physical or online stores, etc...). Each Flik payment is a SEPA instant payment, meaning that the transfer of money from the debtor's account to the creditor's account takes place in a few seconds, even outside bank working hours - 24 hours, 7 days a week, 365 days a year. Flik payments can be initiated and received by customers of all banks in Slovenia within the application that each bank offers for this purpose (in the following: Flik application). For this purpose debtor has to register his phone number or email address as contact information (in the following: alias) with which he is reachable between Flik users. Alias is linked to his payment account and consequently entering the bank details of the creditor or debtor is not required.



Various options are available to companies and retailers within Flik. One of these is Flik remote payment or Flik online.

Flik online

Support for Flik remote payments on the merchant's side is part of Bankart Payment Gateway, which, in addition to Flik, also supports card payments. In the Flik area, it offers two options, these are: receiving Flik payments (Flik P2eM) and initiating Flik payouts (Flik B2P).

Flik P2eM payments enable a very good user experience, as the debtor receives a request to pay in the form of a push notification in the Flik application based on the given alias, which he confirms or rejects. This completes the payment process, and the money is in the creditor's account in a few seconds. Flik P2eM provides three implementation options depending on the point of sale where Flik P2eM is implemented.

P2eM payment types are:

- Online payment (**E-Commerce P2eM**): *In the online store, the merchant offers the option of paying for the purchase with the Flik payment method. The request to pay that the debtor receives in their Flik application is valid for **5 minutes**.*
- Payment via loyalty cards at physical stores (**In-Person P2eM**): *A merchant offering a loyalty card to its customers can connect the loyalty card to the Flik alias of the individual debtor with the Flik P2eM integration. When the customer presents the loyalty card at the checkout, a request to pay is automatically forwarded to the Flik application. The request to pay is valid for **90 seconds**.*
- Bill payment and mobile wallet top-up (**Out-of-Band P2eM**): *The merchant/top-up wallet initiates a payment request based on a prior agreement with the debtor. The debtor has **72 hours** to confirm the request to pay in his Flik application. Examples of use are subscriptions, monthly bills, filling wallets.*

Flik B2P enables the refund of funds previously paid by a person to the creditor. For a refund, the merchant only needs a reference to the first transaction or purchase made with Flik. The refund cannot be higher than the amount paid for the original purchase.

B2P payment type is:

- *Refund (B2P Refund): Resolving complaints, refunding overpayments. To perform a refund, the merchant needs to send a reference to the original transaction (purchase) in the API call, thus ensuring that the amount of the refund cannot be higher than the original transaction.*
- *Payout (Payout B2P): This type of transaction is used when the merchant wants to use the possibility of direct immediate payment to the customer's account. Withdrawal uses the customer's alias and the money is in the account within seconds. This type of transaction differs from a refund in a way that it has no upper limit on the amount and does not require any reference to the original transaction.*

Mini-dictionary:

Payment Gateway: A system that enables the acceptance of payments by payment cards or Flik for merchants. It is a system that connects websites (online stores) with issuers of payment methods and customers. Part of the Payment gateway is the web interface that the merchant uses to review completed transactions.

P2eM: Flik payment made by a person at an online merchant.

B2P: Flik payment made by an online merchant to a person, e.g. refund of purchase price.

Flik application: An application that allows paying with Flik. More information is available at <https://flik.si>.

Alias: Contact information (phone number or e-mail) with which the user registers with Flik and through which he can make Flik payments.

RTP: Request to pay, which in the case of P2eM Flik payments, is sent by the merchant to the debtor's alias.

TECHNICAL INTEGRATION OF FLIK PAYMENT METHOD

(instructions for developers)

Basic information

For the successful integration of Flik remote payments, it is necessary to implement appropriate API calls to Bankart's Payment Gateway on the merchant's side. Bankart's Payment Gateway supports both card and Flik payments, both of which use the same API interface. The content is in JSON format, and an OpenApi v3 scheme is also available.

- **Basic documentation**
<https://gateway.bankart.si/documentation/apiv3>
- **General API specification**
<https://gateway.bankart.si/documentation/gateway>
- **API specification for Flik Payments**

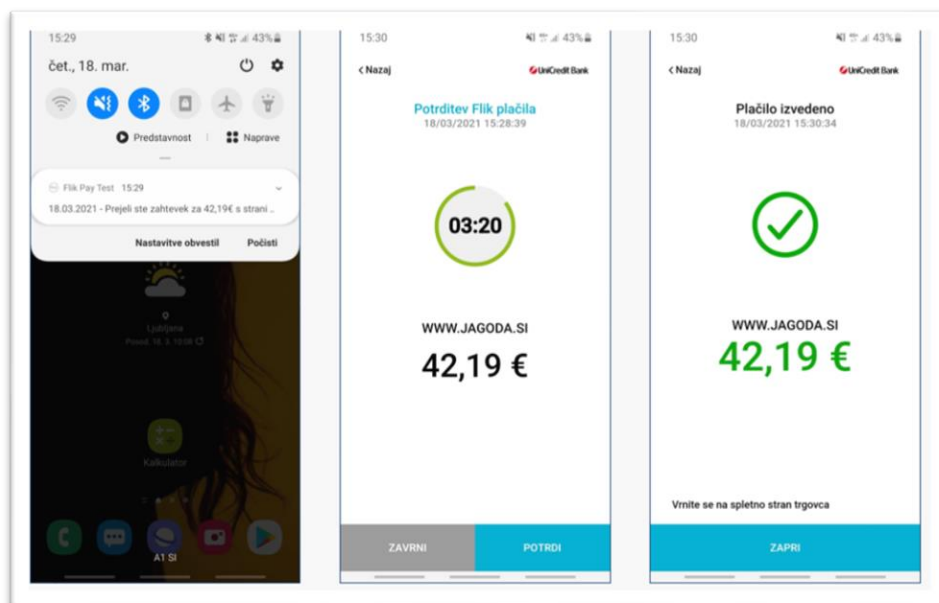
Flik specifics are given via fields in the extraData element.

Example: "extraData":{"alias":"my@mail.si"}

All API calls must contain a signature that is generated based on the sent content and the shared secret. Callbacks are also signed, so you can check the authenticity of the received content yourself. It is necessary to emphasize that when initiating a transaction with an API call in JSON, the merchant must not forget to send the callbackURL field, because the result of the transaction will be sent to this URL address when it is completed.

Flow of message exchange between the merchant's system and the Bankart Payment Gateway

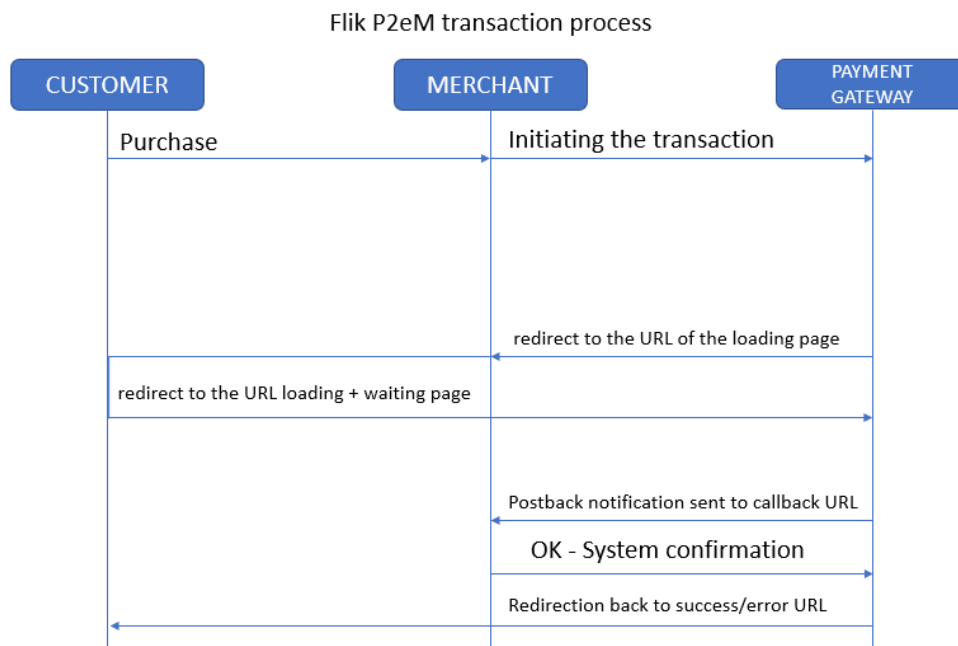
The customer fills the shopping cart in the online store. Select the Flik payment method at the checkout. The merchant initiates a Request To Pay (RTP) by executing an API call. The Payment Gateway redirects the customer to the information screen, where he is asked to confirm the request in the Flik application.



The customer then confirms the request (he also has the option of rejecting it). The merchant's system receives the transaction result at the given callback URL. The customer is redirected to the appropriate merchant's site.

In case the customer is not shown the information page, instead of being redirected, the merchant only receives the Pending status, which means that the transaction is in progress.

For easier representation, the graphic below shows the entire Flik P2eM transaction process. It is an asynchronous transaction, as the response (confirmation by the customer) can take a long time (depending on the validity period of the RTP).



The merchant can initiate transactions via the Payment Gateway only for the online store or the URL address that was provided during onboarding with the bank. The bank registers this URL address in Bankart's system, then the URL appears on the input mask for Flik alias at the time of purchase, and in the Flik application for confirming payments. Therefore, if a company has several online stores with different URL addresses, it is necessary to register a new merchant with the bank for each URL address.

Specification of API calls for Flik remote payments

The following pages show some API messages that outline the operation of the system and contain guidelines for the technical connection to the Bankart Payment Gateway. In general, we distinguish between two basic courses:

- If the merchant has the debtor's alias, the API call is made without redirection. Immediately after making the call, the debtor will receive a Request to pay in the Flik application.
- If the merchant does not have the debtor's contact information or alias, an API call is made with redirection. After making the call, the customer will be redirected to a page where he would enter his contact information or alias, after which he will receive a Request to pay in his Flik application. The merchant can also implement the page for entering contact information in his website.

Initial API call

The Flik request to pay uses an API call for a DEBIT transaction, which must be sent to the correct address: <https://gateway.bankart.si/api/v3/transaction/api-key/debit> (You can get the API Key as part of the access data for connecting to Bankart Payment Gateway)

Example of the content of the call to the gateway:

```
{
  "merchantTransactionId": "Flik-20210413133336-d3898",
  "amount": "11.11",
  "currency": "EUR",
  "successUrl": "https://merchants.address.si/success",
  "errorUrl": "https://merchants.address.si/error",
  "cancelUrl": "https://merchants.address.si/cancel",
  "callbackUrl": "https://merchants.address.si/callback",
  "description": "sporočilo kupcu",
  "extraData": {
    "alias": "0038641147148",
  },
  "customer": {
    "ipAddress": "46.123.232.123"
  },
  "language": "sl"
}
```

Content instructions for providing key data for the execution of the transaction:

Field name	Description
merchantTransactionId	Unique transaction ID assigned by merchant. If the transaction ID is not unique, the gateway will reject the transaction.
amount	In the amount use a decimal point and a maximum of two decimal places.
currency	The currency should always be EUR!
Success/error/cancelUrl	URL Addresses for redirecting the customer back to your online store after the purchase on Bankart's site ends.
callbackUrl	You receive the result of the payment to this address.
description	In this field, you write a message that will be displayed to the customer in the Flik payment application. This message will also be visible as a transaction description in bank statements.
extradata: alias	In the extraData element, add the user's contact information (alias) for Flik (GSM or e-mail). If the data is not sent by the merchant when initiating the transaction, the Payment Gateway retrieves it by displaying a dynamic entry page to the customer - a common approach.
customer: ipAddress	In this field the IP address of the user who confirmed the purchase must be provided. The data is used for security purposes to prevent fraud.
Language	Value: sl (static)

For URL addresses, *query strings* can also be used. Example:

- succesUrl: <https://merchants.address.si/redirect?status=success&transactionId=1234>
- errorUrl: <https://merchants.address.si/redirect?status=error&transactionId=1234>
- cancelUrl: <https://merchants.address.si/redirect?status=cancel&transactionId=1234>
- CallbackUrl: <https://merchants.address.si/callback?transactionId=1234>

Depending on the agreement between the merchant and the bank, Bankart can enable sending of the following additional parameters in the extraData set:

Title	Description
enableWaitingScreen	Value: yes/no determines the mode of operation, with or without redirection. Redirection of the customer is the default mode of operation only for e-commerce transactions.
merchantMID	Merchants with multiple branches/stores or pick-up locations can set the same code as they use for card payments.
merchantTerminalId	Merchants who will be using the in-person mode can set up a terminal ID to make it easier to pair a payment with a specific registry.
ultimateCreditorName	The name of the point of sale, which is displayed to the customer in the application.

API call response – customer redirection

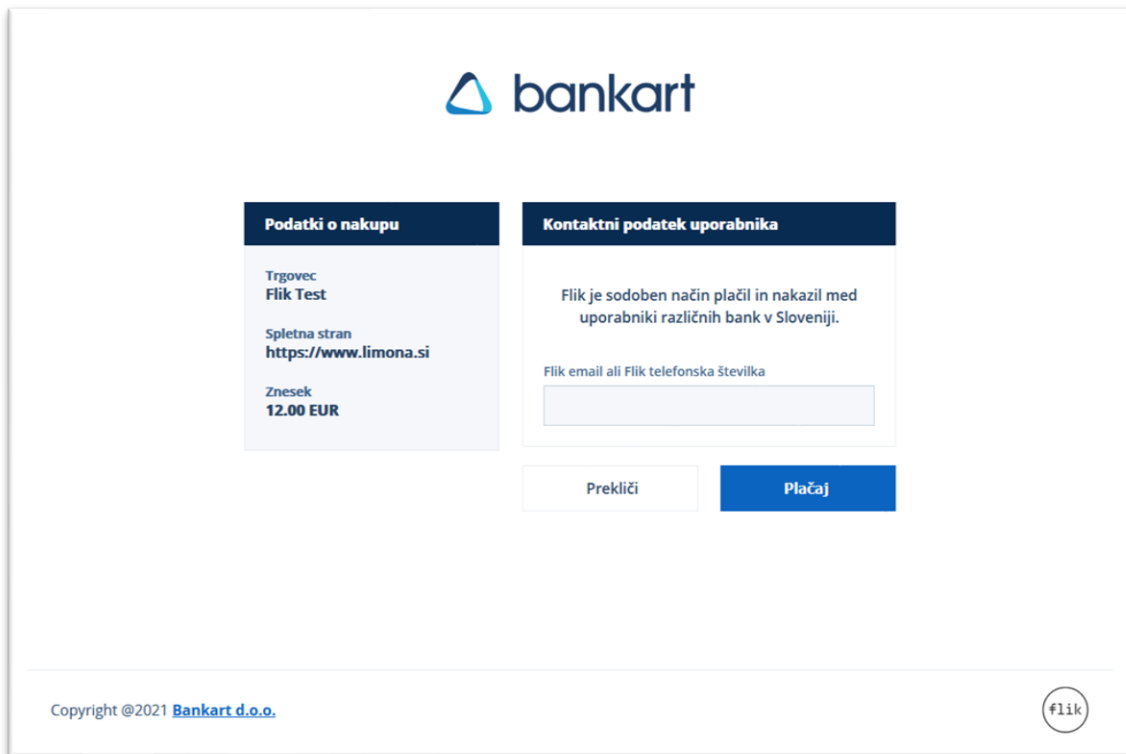
This is the default way the online store works - the merchant receives an URL address as an answer to the initial API call to where he redirects customer.

An example of a customer redirect response to the initial merchant API call:

```
{
  »success«: true,
  »uuid«: »c5b92e902dc9e4b0edea«,
  »purchaseId«: »20210413-c5b92e902dc9e4b0edea«,
  »returnType«: »REDIRECT«,
  »redirectUrl«:
    »https://bankart.paymentsandbox.cloud/redirect/c5b92e902dc9e4b0edea/N2JkZThiNWZmN2Vi
    ZTMxXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX2ODZiMTlyMGEyMjM3NjA2NGEwM2M2MGQzM2M1Mzc5Zjc2NjN
    mMjYxYWRjOGU4Y2ZiZDEyZhiNDNINzRjM2ZmMjQ=«,
  »paymentMethod«: »FlikPayments«,
  »extraData«: {
    »expiresDateTime«: »2021-04-13 11:35:07«,
    »adapterReferenceId«: »PGTASI20IT5100410416121751eIbN05«
  }
}
```

An explanation of the meaning of individual fields is given in the table, which is located after both examples of results.

Redirection of the customer to the provided redirectUrl can be done as a full page redirect or you can display the page in an iFrame element. If the alias is not provided in the API call, the customer will be shown an input mask where he will be asked to enter the alias or contact information for Flik as shown in the image below.



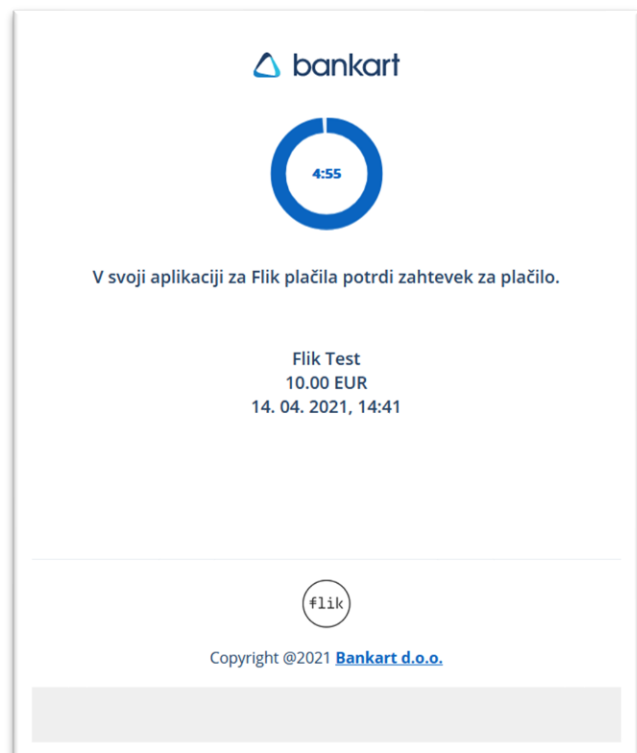
The screenshot shows the Bankart payment gateway interface. At the top, the Bankart logo is displayed. Below it, there are two main sections: 'Podatki o nakupu' (Purchase Data) and 'Kontaktne podatke uporabnika' (User Contact Data). The 'Podatki o nakupu' section contains the merchant name 'Trgovec: Flik Test', the website 'Spletna stran: https://www.limona.si', and the amount 'Znesek: 12.00 EUR'. The 'Kontaktne podatke uporabnika' section contains the instruction 'Flik je sodoben način plačil in nakazil med uporabniki različnih bank v Sloveniji.' and a text input field for 'Flik email ali Flik telefonska številka'. Below these sections are two buttons: 'Prekliči' (Cancel) and 'Plačaj' (Pay). At the bottom, there is a copyright notice 'Copyright ©2021 Bankart d.o.o.' and a small Flik logo.

Picture 1: An example of a mask for entering contact data

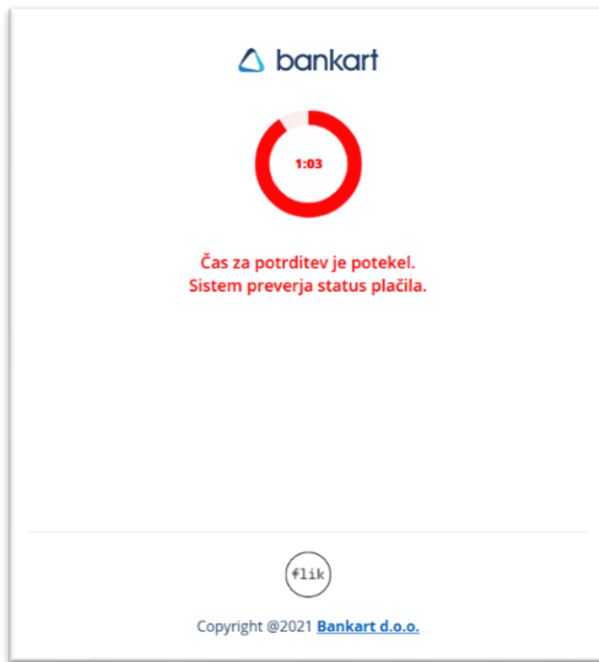
After providing the contact information (in the merchant's API call or via the Payment Gateway input mask), the customer is asked to confirm (or reject) the request to pay in the Flik application via the information page on the web store. The Payment Gateway shows the customer a window with a timer (*picture on the right*).

Once the customer confirms or declines the request to pay, they will be redirected back to the merchant's site. The URL addresses for redirection are defined in the initial API call:

- `successUrl` – the customer confirmed the request to pay and the payment was successfully made
- `cancelUrl` – the customer rejected the request to pay
- `errorUrl` – an error occurred when making the payment (technical error, insufficient funds for payment, ...)



The screenshot shows the Bankart payment gateway interface during a payment confirmation. At the top, the Bankart logo is displayed. Below it, there is a large blue circular timer showing '4:55'. The text 'V svoji aplikaciji za Flik plačila potrdi zahtevek za plačilo.' (Confirm the payment request in your Flik application) is displayed. Below this, the merchant name 'Flik Test', the amount '10.00 EUR', and the date and time '14. 04. 2021, 14:41' are shown. At the bottom, there is a small Flik logo, the copyright notice 'Copyright ©2021 Bankart d.o.o.', and a grey bar.



In the event that the customer does not confirm the payment, or the Payment Gateway does not receive a result on the payment status, the Payment Gateway will try to obtain the information again after the expiration of the validity of the request to pay and send the request again after at least 45 seconds have passed. During this time, the customer's display is refreshed with a new countdown timer. This applies only in the case of *e-commerce* transaction type.

In the case of in-person and oob transactions, the countdown timer is not displayed due to the payment method or due to the long validity period of the request. At the last one, only a screen is displayed where you can see the payment amount and until when the request is valid.

API call response - without redirection

This is the default mode of operation of the In-Person and Out-of-Band (oob) point of sale - the merchant receives status "PENDING" on the initial API call.

Example of a response to the merchant's initial API call:

```
{
  "success": true,
  "uuid": "c5b92e902dc9e4b0edea",
  "purchaseId": "20210413-c5b92e902dc9e4b0edea",
  "returnType": "PENDING",
  "paymentMethod": "FlikPayments",
  "extraData": {
    "expiresDateTime": "2021-04-13 11:35:07",
    "adapterReferenceId": "PGTASI20ITS100410416121751elbN05"
  }
}
```

The result of the payment is returned to the callbackUrl that was specified in the initial API call. An example of the API call for the payment result is shown below.

The table below contains explanation of individual fields that are included in API response messages.

Field Name	Description
success	Result of the API call result.
uuid	An unique transaction ID that is generated on the Bankart Payment Gateway. This information can be used to search for a specific transaction on the PG user interface.
purchaseId	An ID that is generated in the backend systems and also includes the date.

returnType	The field tells what type of call it is - with or without redirection forwarding.
redirectUrl	Only in the case of a redirect transaction , this field is filled with the URL address where the merchant redirects the customer to enter the alias.
paymentMethod	The field tells us that it is a payment with the Flik payment method.
extradata: expiresDateTime	It is informative. After the transaction, the system sends the result to the merchant's system, or after the expiration, it reports a failed transaction to the callbackUrl that you provided in the initial API call.
extradata: adapterReferenceld	A unique transaction ID that is sent across all backend systems.

Payment result

The result of the payment is received at the callbackUrl which was provided by the merchant in the initial API call:

```
{
  "result": "OK",
  "uuid": " c5b92e902dc9e4b0edea",
  "merchantTransactionId": " Flik-20210413133336-d3898",
  "purchaseId": "20210413-c5b92e902dc9e4b0edea",
  "transactionType": "DEBIT",
  "paymentMethod": "FlikPayments",
  "amount": "11.11",
  "currency": "EUR",
  "extraData": {
    "adapterReferenceld": " PGTASI20IT5100410416121751elbN05"
  }
}
```

The Gateway will make the first attempt to send a response to the callback address before redirecting the customer to the merchant's page (success/error/cancelUrl). In case of unsuccessful confirmation of the result, the Gateway will periodically resend the payment status to the callback address.

The response can be combined with the request based on:

- **merchantTransactionID** – provided by the merchant in the initial API call
- **uuid** – unique ID that the gateway provides in response to the initial API call

NOTE

Query for transaction status: Based on the values above, a manual query can be made using the status call (Status API call): <https://gateway.bankart.si/documentation/apiv3#status-request>.

NOTE

Tips for integrating the countdown timer: The countdown timer can be displayed in a modal window, and the redirect address simply returns a page with javascript code that will forward the result to the main page: <https://javascript.info/cross-window-communication>

It is also possible to display an intermediate page in the success/cancel/errorUrl addresses passed for redirection, which redirects the entire page to the actual success/cancel/error display: `windop.top.location.href = "https://address.merchant.si/success/cancel/error"`.

Structured and unstructured payment reference

Flik payments enable two types of references, that provide the buyer with information on what the individual transaction is related to.

- **unstructured reference:** is sent in the "description" field (marked below in blue), and this field can be filled with any description of the purpose of the transaction. In this case, it is not necessary to send additional indicators. Example of the initial API call:

```
{
  "merchantTransactionId": "Flik-20210413133336-d3898",
  "amount": "11.11",
  "currency": "EUR",
  "successUrl": "https://naslov.trgovca.si/success",
  "errorUrl": "https://naslov.trgovca.si/error",
  "cancelUrl": "https://naslov.trgovca.si/cancel",
  "callbackUrl": "https://naslov.trgovca.si/callback",
  "description": "unstructured message to the buyer",
  "extraData": {
    "alias": "0038641147148",
  },
  "customer": {
    "ipAddress": "46.123.232.123"
  },
  "language": "sl"
}
```

- **structured reference:** also a description of the purpose of the transaction is sent in the "description" field. Since this is a structured reference, it is necessary to send two additional indicators in the "extraData" array. The first is "referenceType" (marked below in red), which is filled with the value "structured" and thus the message is changed to the desired type, taking the value from the field "description" (marked below in red) as a reference. If desired, a field indicating the purpose of the payment "purposeCode" (marked below in red) can be added, which is filled with the four-digit purpose code "XXXX", as when filling out a UPN order (e.g. WEBI). This changes the payment intent from "OTHR" which is set by default to desired. Example of the initial API call:

```
{
  "merchantTransactionId": "Flik-20210413133336-d3898",
  "amount": "11.11",
  "currency": "EUR",
  "successUrl": "https://naslov.trgovca.si/success",
  "errorUrl": "https://naslov.trgovca.si/error",
  "cancelUrl": "https://naslov.trgovca.si/cancel",
  "callbackUrl": "https://naslov.trgovca.si/callback",
  "description": "structured reference",
  "extraData": {
    "alias": "0038641147148",
    "referenceType": "structured",
    "purposeCode": "XXXX",
  },
  "customer": {
    "ipAddress": "46.123.232.123"
  },
  "language": "sl"
}
```

INSTRUCTIONS FOR TESTING AND TRANSITION TO PRODUCTION

Basic information

Before Flik payment method can be used in a production environment, it is necessary to successfully pass a test that confirms the correct operation of the merchant's system. The payment flow for an online purchase is initiated by a request to pay with a customer's purchase through the merchant's system.

The payment flow can be carried out by redirecting the customer to the timer (for example: e-commerce transaction type) or without redirection. In the case of testing with redirection, the use of a simulator is available. In the case of testing without redirection, the assigned aliases are given below in the table to cover each test scenario (in the section Testing payments without redirection).

Before the start of the test, Bankart provided you with a username and password with which you will connect to the Bankart Payment Gateway, where you will be able to access other important data and thus you can start the test (described in the next subsection). The table below describes all the main information a merchant needs to connect. The data marked in red must be downloaded separately for each of the defined connectors or terminals, both simulation and production. In your current case this relates to the Flik connector(s).

Naziv	Opis
API username	Access to the API interface - the developer uses this in the code.
API password	Access to the API interface.
API Key	Key for the payment method.
Shared Secret)	Shared secret for signing and authenticating the content of API calls.
<u>Web access to download data and access to review transactions:</u>	
URL	Web address to access the portal and review transactions
Username	Assigned username to access the portal
Password	Assigned password for first login (must be changed after first login!)

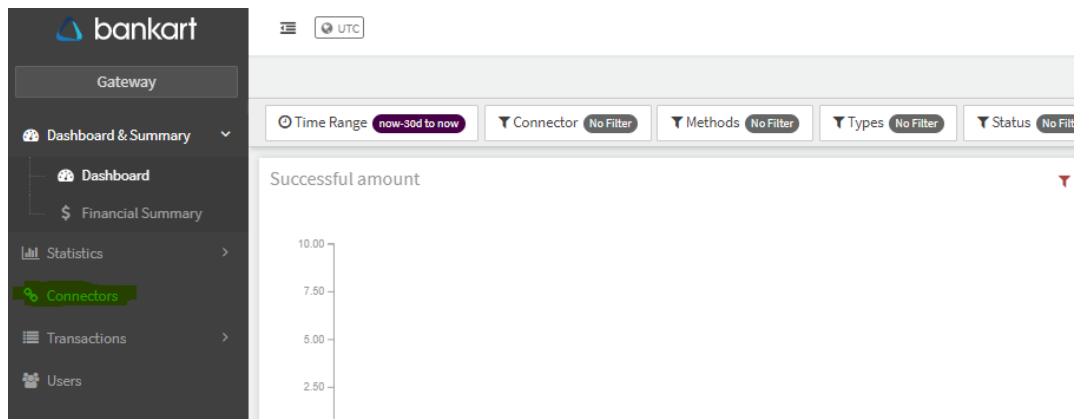
Data for the connecting to the Payment Gateway

Data for entering the Payment Gateway portal is sent via two channels (**upcoming feature, currently we are sending below data in one email message**)

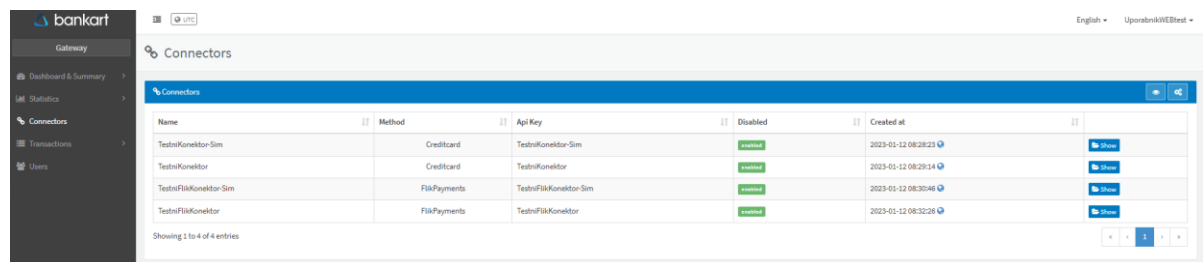
- **e-mail address**, which is given when the merchant is input into the Bankart system. Through this channel, instructions for integration will be sent, as well as the password for accessing the portal, which must be changed immediately upon registration.
- **SMS text message** to the number provided when inputting merchant into the Bankart system. The username to access the portal will be sent via this channel.

When you receive data from Bankart for logging into the portal, you also need to collect data for connecting/integrating terminals on merchants side, which is shown step by step below:

1. **Step:** After logging in to the Payment Gateway portal, select the "Connectors" tab on the left (marked in green):



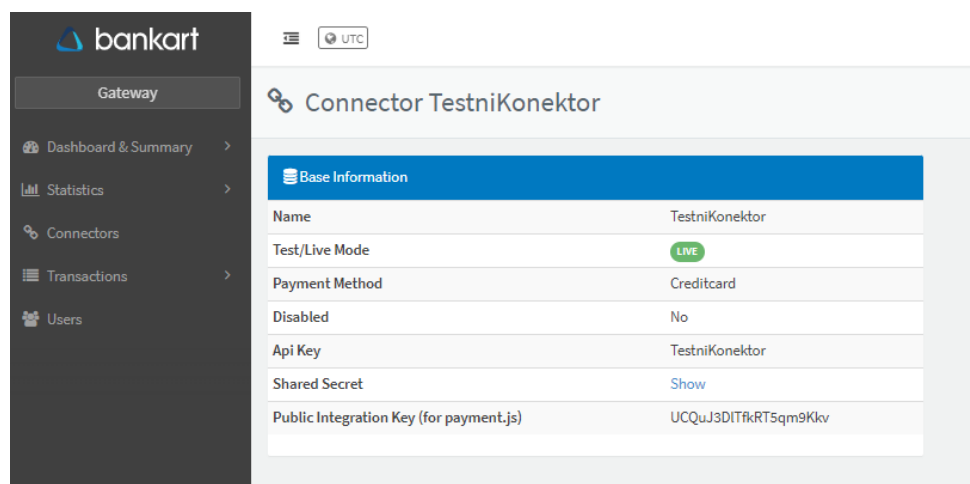
2. **Step:** A list of all terminals or connectors is displayed. For each of these connectors, by clicking on the "Show" button on the right, you will find information that is important for integration or connection to the Payment Gateway. Connectors that end with "Sim" are simulation connectors and are used for integration testing before the merchant goes into production. In your case, the data for Flik connectors should be copied to your system. More about this is written in the next subsection.



Name	Method	Api Key	Disabled	Created at	
TestniKonektor-Sim	Creditcard	TestniKonektor-Sim	enabled	2023-01-12 08:28:23	Show
TestniKonektor	Creditcard	TestniKonektor	enabled	2023-01-12 08:28:14	Show
TestniFlikKonektor-Sim	FlikPayments	TestniFlikKonektor-Sim	enabled	2023-01-12 08:30:46	Show
TestniFlikKonektor	FlikPayments	TestniFlikKonektor	enabled	2023-01-12 08:32:26	Show

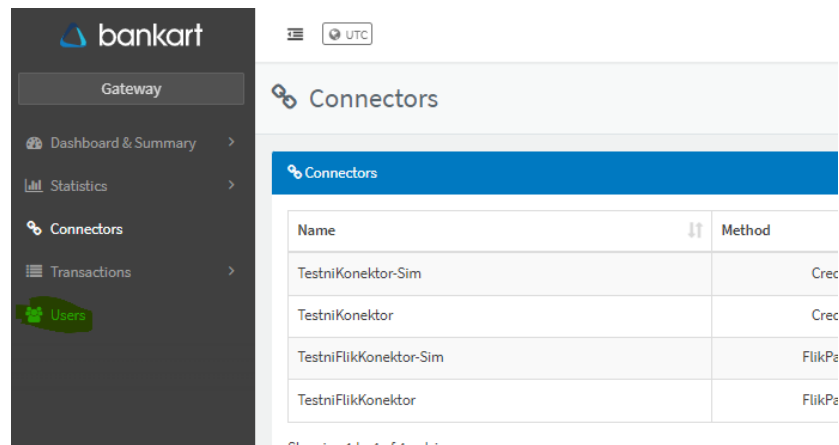
Showing 1 to 4 of 4 entries

3. **Step:** The image below shows all the information about the connector, but the main information that the merchant needs in this menu to connect to the Gateway is:
 - a. API Key
 - b. Shared Secret (it is necessary to click on "show" to show the whole string)



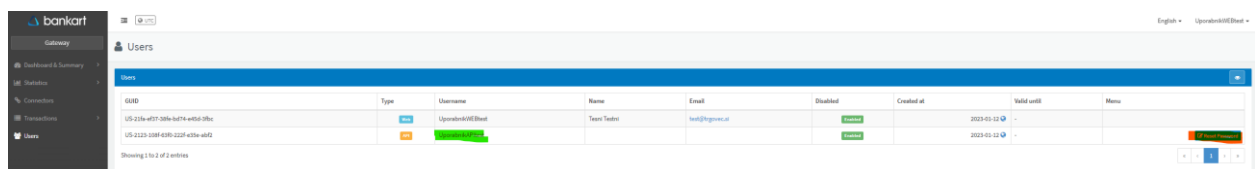
Base Information	
Name	TestniKonektor
Test/Live Mode	LIVE
Payment Method	Creditcard
Disabled	No
Api Key	TestniKonektor
Shared Secret	Show
Public Integration Key (for payment.js)	UCQuJ3DITrkRT5qm9Klv

4. **Step:** after the data for each of the desired connectors has been copied to the merchant's system, you must select the "Users" tab on the left side of the menu:

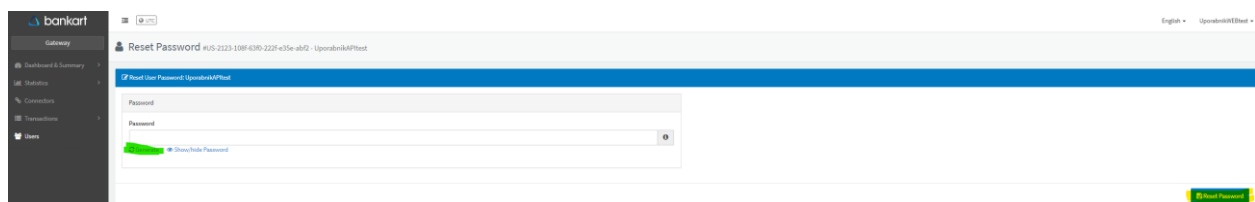


5. **Step:** A list of all users that the merchant has is displayed. There can be more users of the WEB type, as these are users for whom the merchant provides access to the Payment Gateway portal and review of transactions (we suggest a maximum of 3 created by Bankart). There is usually only one API type user, as the connection to the Payment Gateway is enabled only through this user.

We have already sent the data for the WEB main user, so at the end, the merchant must also copy the API username (marked in green). For the same API user the merchants web user must click on the "Reset Password" button (marked in red) on the right side.



6. **Step:** The API password generation menu appears. By clicking on the "Generate" option (marked in green) under the Password field, a password is generated. This password must be copied into the merchant's systems, and then click the "Reset Password" button (marked in yellow) on the bottom right. This saves the password in the Payment Gateway system.



IMPORTANT: The generation of the new API password should be done **only once, or at the first login**. Before the password generation process is completed, it must be saved and copied to the merchant's backend systems so that the merchant can connect to the Payment Gateway. If the API password is changed after the merchant has been in production for a long time and uses the API password generated at the initial login, the connection between the merchant and the Payment Gateway will be **TERMINATED** after the subsequent password change, and the transactions can **NOT be initiated** and executed correctly!

Testing payments with the simulator

In the test environment, a test merchant is defined, that is used to test the configuration and if it's backend systems for processing the Flik messages work as they should. On the debtor's side, the response will be simulated. For an example of payment confirmation on the debtor's side, the merchant selects "Successful payment" from the scenario. "Canceled payment" represents the response that the system receives in the event that the debtor rejects the purchase in their application. "Failed Payment" is a payment that has failed due to technical issues. If the merchant is granted the right by the bank to trigger "Refund" transactions (that is, the return of money to the customer's account), the additional scenarios "Successful payment for a subsequent successful refund" and "Successful payment for a subsequent unsuccessful refund" are performed, where after a successful payment the merchant subsequently initiates a refund, once with a successful outcome and the second with an unsuccessful outcome.

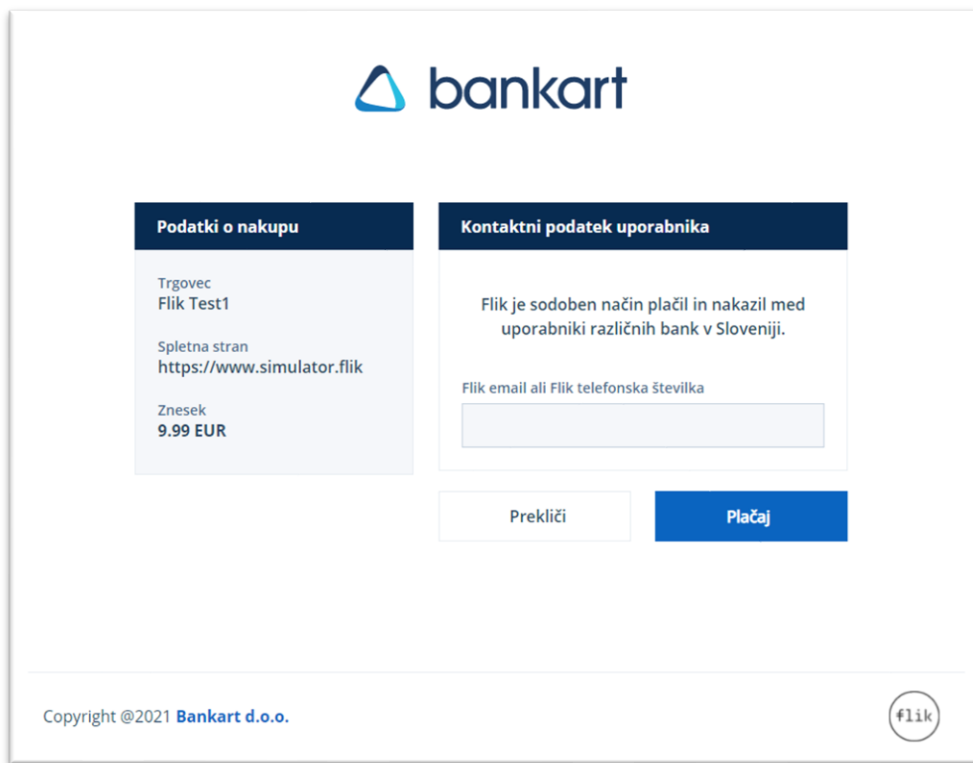
The merchant checks the operation of it's system - receiving the payment result on the callbackUrl via test scenarios:

- **Successful payment** (E-Commerce, In-Person, Out-of-Band)
- **Canceled payment** (E-Commerce, In-Person, Out-of-Band)
- **Failed payment** (E-Commerce, In-Person, Out-of-Band)
- **Successful payment for subsequent successful refund** (E-Commerce, In-Person, Out-of-Band, Refund)
- **A successful payment for a subsequent unsuccessful refund** (E-Commerce, In-Person, Out-of-Band, Refund)

To use the simulator for testing purposes, the test aliases below are available.

Key	Value	Parameter description	Scenario
alias	redirect@bankart.flik	E-mail	Successful payment Canceled payment Payment failed Successful payment for subsequent successful refund Successful payment for a subsequent unsuccessful refund
alias	0038670999999	Mobile phone number	

In the event that the initial call to the Payment Gateway does not contain an alias value, the debtor is redirected and asked to enter contact information via the form to perform the Flik payment:



Podatki o nakupu

Trgovec
Flik Test1

Spletna stran
<https://www.simulator.flik>

Znesek
9.99 EUR

Kontaktne podatke uporabnika

Flik je sodoben način plačil in nakazil med uporabniki različnih bank v Sloveniji.

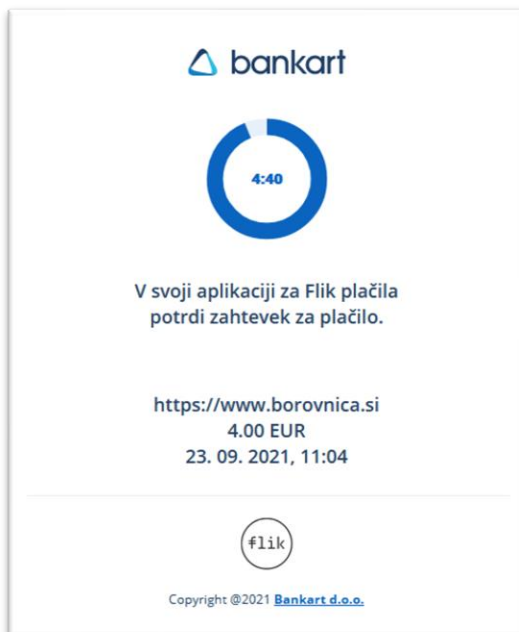
Flik email ali Flik telefonska številka

[Prekliči](#) [Plačaj](#)

Copyright ©2021 Bankart d.o.o.



After entering the alias and its confirmation, in the production environment, the debtor will receive a push message to confirm the online purchase (RTP) in their Flik application. The image below shows an example of a timer page.



bankart

4:40

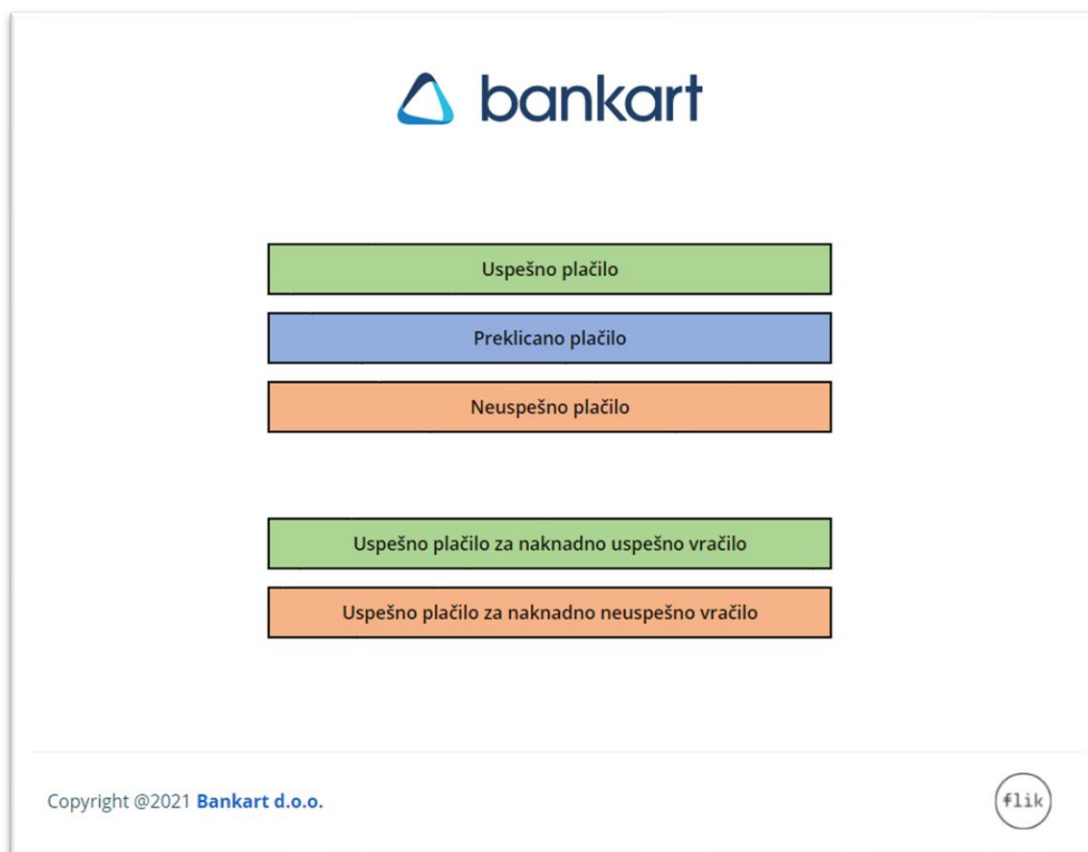
V svoji aplikaciji za Flik plačila
potrdi zahtevek za plačilo.

<https://www.borovnica.si>
4.00 EUR
23. 09. 2021, 11:04



Copyright ©2021 Bankart d.o.o.

In test mode there is no possibility to perform a validation in the Flik application. For testing purposes, this timer is replaced by a page with a set of test scenarios.



- **Successful payment** – The debtor confirms the payment in their Flik application, which is then successfully executed.
- **Canceled payment** – The debtor refuses the payment in their Flik application.
- **Unsuccessful payment** – Unsuccessful payment due to technical problems on the system, overdue claim.
- **Successful payment for a subsequent successful refund** – The debtor confirms the payment in their Flik application, which is then successfully executed. The refund is made by the merchant subsequently with a call in which he refers to the original transaction. The refund is successfully completed when the merchant receives a response about the success of this transaction to the "callbackUrl" parameter in the Refund API call. Due to the nature of the simulator's operation, expect an asynchronous call with answer about the completion of the payment within two minutes.
- **Successful payment for a subsequent unsuccessful refund** - The debtor confirms the payment in their Flik application, which is successfully executed. The merchant subsequently makes a refund attempt with a call in which he refers to the original transaction. The refund is completed unsuccessfully when the merchant receives a response about the failure of this transaction to the "callbackUrl" parameter in the Refund API call. Due to the nature of the simulator, expect an asynchronous call for a payment response within two minutes.

Testing payments without redirection

The set of aliases below is used to initiate In-Person or Out-of-Band transactions, or in the case of payments without redirecting the debtor to the alias input page in the case of an E-Commerce transactions.

E-mail	Phone number	Scenario
<i>success.debit@bankart.flik</i>	0038670999000	Successful payment
<i>cancel.debit@bankart.flik</i>	0038670999111	Canceled payment
<i>error.debit@bankart.flik</i>	0038670999222	Failed payment
<i>success.debit_success.refund@bankart.flik</i>	0038670999333	Successful payment for a subsequent successful refund
<i>success.debit_error.refund@bankart.flik</i>	0038670999444	Successful payment for a subsequent unsuccessful refund

- **Successful payment** – The debtor confirms the payment in their Flik application, which is then successfully executed.
- **Canceled payment** – The debtor refuses the payment in their Flik application.
- **Unsuccessful payment** – Unsuccessful payment due to technical problems on the system, overdue claim.
- **Successful payment for a subsequent successful refund** – The debtor confirms the payment in their Flik application, which is then successfully executed. The refund is made by the merchant subsequently with a call in which he refers to the original transaction. The refund is successfully completed when the merchant receives a response about the success of this transaction to the "callbackUrl" parameter in the Refund API call. Due to the nature of the simulator's operation, expect an asynchronous call to answer about the completion of the payment within two minutes.
- **Successful payment for a subsequent unsuccessful refund** - The debtor confirms the payment in their Flik application, which is successfully executed. The merchant subsequently makes a refund attempt with a call in which he refers to the original transaction. The refund is completed unsuccessfully when the merchant receives a response about the failure of this transaction to the "callbackUrl" parameter in the Refund API call. Due to the nature of the simulator, expect an asynchronous call for a payment response within two minutes.

Transition to production environment

- **Bankart's customer support checks the integration status via the logs on the Payment gateway:** Before we grant production access, our customer support checks the payment gateway logs if the payment flows are executed correctly on the simulation adapter. If everything is fine or if the transactions are correctly executed and marked, Bankart's customer support team will manually enable the ability to use the production terminal.
- **Technical support during business hours only:** Technical support is only available during business hours (8:00-15:00) on business days.
- **Merchants should NOT test in a production environment!**
If the merchant makes any significant changes to the settings in the production environment, especially outside of business hours, we cannot provide you with immediate technical support. All possible problems in the execution of the transactions that are consequence of such changes are merchant's responsibility and will be dealt with during business hours.

Validation of the alias input format

To avoid errors that would result from an incorrectly entered alias in the case of using the integrated field for entering the alias in the online store itself, we recommend validating the input format.

All phone numbers in the Flik scheme are registered with the format 00386*****, so it is necessary to ensure that the information is forwarded in this format. In the case when Bankart's input mask is in use, this validation is not required.

Example of the code, which can be helpful when performing alias validation when using integrated field for entering alias is provided below:.

```
function validateAlias(alias) {  
    if (alias == "") {  
        return 'empty';  
    }  
    var testCase = "";  
    var aliasError = "";  
  
    if (alias.indexOf("@") == -1) {  
        testCase = checkAndFormatNumber(alias);  
    } else if (alias.indexOf("@") > -1) {  
        aliasError = !alias.match(/^[a-zA-Z0-9_\-\.]+\@([a-zA-Z0-9_\-\.]+\.[a-zA-Z]{2,5})$/g);  
    }  
    if (testCase == 'invalid' || aliasError) {  
        return 'invalid';  
    }  
  
    return 'valid';  
}  
  
function checkAndFormatNumber(phoneNumber) {  
    phoneNumber = phoneNumber.split("(").join("");  
    phoneNumber = phoneNumber.split(")").join("");  
    phoneNumber = phoneNumber.split("-").join("");  
  
    if (phoneNumber.match(/\d{13}/g) && phoneNumber.substring(0, 5) == "00386") {  
        return phoneNumber;  
    } else if (phoneNumber.match(/\+\d{11}/g) && phoneNumber.substring(0, 4) == "+386") {  
        return phoneNumber.replace("+", "00");  
    } else if (phoneNumber.match(/\d{11}/g) && phoneNumber.substring(0, 3) == "386") {  
        return "00" + phoneNumber;  
    } else if (phoneNumber.match(/\d{9}/g) && phoneNumber[0] == "0") {  
        return "00386" + phoneNumber.substring(1, 9);  
    } else {  
        return "invalid";  
    }  
}
```

Declined transaction due to non-existent alias

If the customer who wants to make a payment via Flik does not have his alias registered (he is not yet a Flik user) or if he made a typo when entering the alias, the merchant receives the following error in the transaction result at the callbackURL:

```
<errors>
<error>
<message>Alias does not exist</message>
<code>2007</code>
<adapterMessage>Did not exist</adapterMessage>
<adapterCode>03</adapterCode>
</error>
</errors>
```

In the case of receiving the mentioned error, it is recommended that the merchant informs the debtor about the reason for the error and directs him to the page with information about the registration process. The example of the text that could be shown to the customer on the errorURL page that merchant sent in the initial call is shown below:

You have entered the wrong contact information (alias). You can check your alias in the settings in the Flik Payments app. This is usually a phone number or e-mail.

If you do not yet have Flik payment enabled, the registration process is described at the following link: <https://www.flik.si/#zacni-z-uporabo>

In this way, the debtor is given the complete information about the reason for the unsuccessful payment and instructions if he wants to make the purchase with Flik.

An example from one of the existing merchants:

Napaka pri plačilu s Flikom

Vnesli ste napačen kontaktni podatek (alias). Kakšen je vaš alias, lahko preverite v nastavitvah v svoji aplikaciji za Flik plačila. Ponavadi je to telefonska številka ali e-mail.

V primeru, da še nimate omogočenega Flik plačevanja je postopek registracije opisan na sledeči povezavi: <https://www.flik.si/#zacni-z-uporabo>.

Opis napake:
(2007) Alias does not exist

[Nazaj v košarico](#)

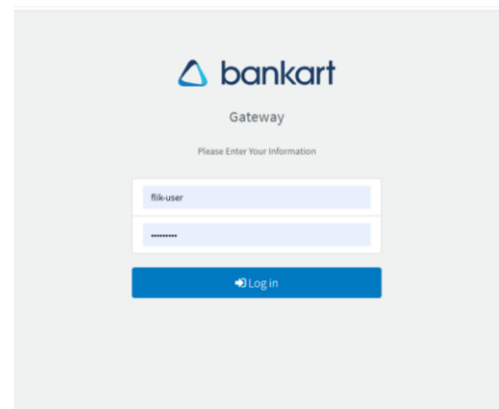
BANKART PAYMENT GATEWAY: THE USER INTERFACE

Access to the portal

The portal for merchants is accessible via the URL addresses below:

- Sandbox portal:
<https://bankart.paymentsandbox.cloud/en>
- Production portal:
<https://gateway.bankart.si/en/login>

The login page shown in the right image will appear, with the option to enter the username and password that you get from Bankart (described in the previous chapters).



Overview of the graphical interface

After entering the data and login, the home page or dashboard of the portal opens.

On the left side, in the dark gray part, there are various tabs where you can choose to display the desired details.

At the top, in the area marked in yellow, the time zone is given (Europe/Ljubljana is appropriate), which is important for the proper display of transactions.

The most important tabs are **Dashboard & Summary** and **Transactions**.

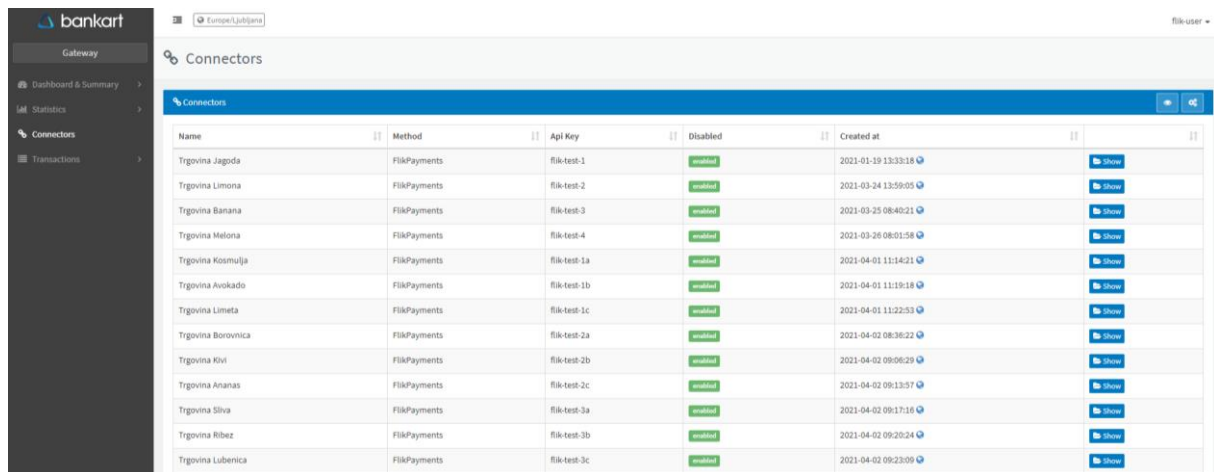


By default, the **Dashboard & Summary** tab is opened.

The **Dashboard** subtab displays graphical and numerical statistics of transactions for a certain period. This page can be customized with various filters in the top row (marked in red), which the user can also personalize. On the right side next to the "Refresh" button, you can select the time interval in which the data is refreshed.

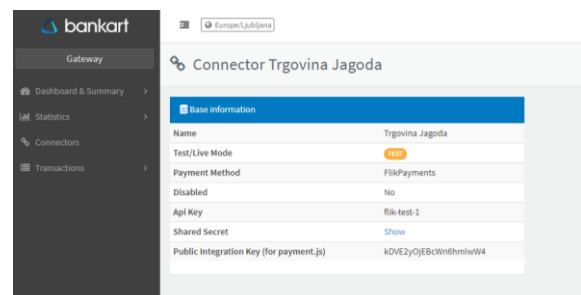
In the **Connectors** tab, all sales points of merchants are visible (for example, for easier pickup or delivery), if a merchant has more than one. If the merchant has only one online store/sales point through which all transactions are triggered, there will be only one connector.

The data for the individual connector/point of sale is input by Bankart and sent to the merchant as described in the chapters above. The connector definition requires: merchant name, payment method, API call name, status and enrollment date.



Name	Method	Api Key	Disabled	Created at	
Trgovina Jagoda	FlikPayments	flik-test-1	enabled	2021-01-19 13:33:18	Show
Trgovina Limona	FlikPayments	flik-test-2	enabled	2021-03-24 13:59:05	Show
Trgovina Banana	FlikPayments	flik-test-3	enabled	2021-03-25 08:40:21	Show
Trgovina Melona	FlikPayments	flik-test-4	enabled	2021-03-26 08:01:58	Show
Trgovina Kosmulja	FlikPayments	flik-test-1a	enabled	2021-04-01 11:14:21	Show
Trgovina Avokado	FlikPayments	flik-test-1b	enabled	2021-04-01 11:19:18	Show
Trgovina Limeta	FlikPayments	flik-test-1c	enabled	2021-04-01 11:22:53	Show
Trgovina Borovnica	FlikPayments	flik-test-2a	enabled	2021-04-02 08:36:22	Show
Trgovina Kivi	FlikPayments	flik-test-2b	enabled	2021-04-02 09:06:29	Show
Trgovina Ananas	FlikPayments	flik-test-2c	enabled	2021-04-02 09:13:57	Show
Trgovina Silva	FlikPayments	flik-test-3a	enabled	2021-04-02 09:17:16	Show
Trgovina Ribez	FlikPayments	flik-test-3b	enabled	2021-04-02 09:20:24	Show
Trgovina Lubenica	FlikPayments	flik-test-3c	enabled	2021-04-02 09:23:09	Show

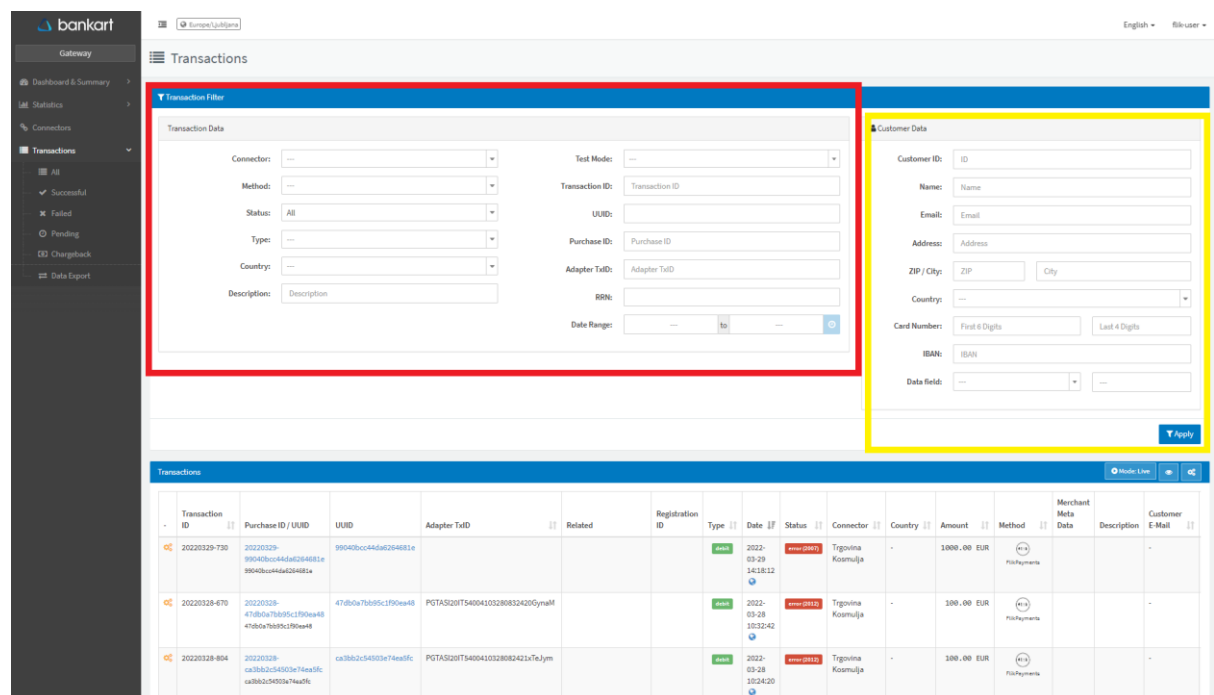
After clicking on the "Show" option (blue button on the right), basic information about each connector/sales point is displayed, such as the name, the mode in which it works (test or production), the payment method (Flik or card), the name of the API key and connection passwords.



Base information	
Name	Trgovina Jagoda
Test/Live Mode	TEST
Payment Method	FlikPayments
Disabled	No
Api Key	flik-test-1
Shared Secret	Show
Public Integration Key (for payment.js)	kDVE2yOjEBcImdHmlw04

Review of transaction details (logs)

In the **Transactions** tab, the All subtab displays the history of all enabled transactions in the online store.



Transaction Filter

Transaction Data

Connector:

Method:

Status:

Type:

Country:

Description:

Test Mode:

Transaction ID:

UUID:

Purchase ID:

Adapter TxID:

BRN:

Date Range: to

Customer Data

Customer ID:

Name:

Email:

Address:

ZIP / City:

Country:

Card Number: First 6 Digits Last 4 Digits

IBAN:

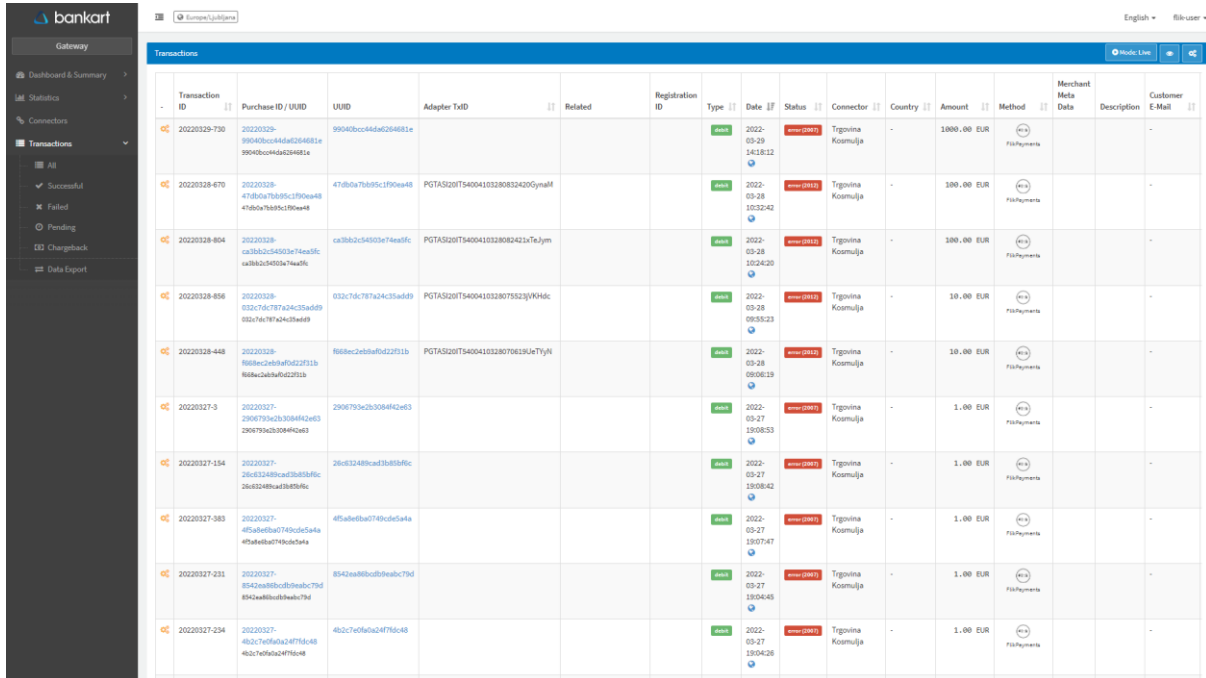
Date Field:

Transaction ID	Purchase ID / UUID	UUID	Adapter TxID	Related	Registration ID	Type	Date	Status	Connector	Country	Amount	Method	Merchant Meta Data	Description	Customer E-Mail
20220329-730	20220329-8904b0cc44d6264681e	8904b0cc44d6264681e				card	2022-03-29 14:18:12	error (2013)	Trgovina Kosmulja	-	1000.00 EUR	FlikPayments			
20220329-670	20220329-47db0a7b85fc1f9e4e8	47db0a7b85fc1f9e4e8	PGTAS201754004103280832420fymH			card	2022-03-28 10:32:42	error (2013)	Trgovina Kosmulja	-	100.00 EUR	FlikPayments			
20220328-804	20220328-ca3b62c34503e74eaf5c	ca3b62c34503e74eaf5c	PGTAS201754004103280832421a7aJym			card	2022-03-28 10:24:20	error (2013)	Trgovina Kosmulja	-	100.00 EUR	FlikPayments			

In the upper part, there are filters for simplified search of desired transactions. In the "Transaction Data" section (highlighted in red) there are fields to limit the set of searched transactions.

In the "Customer Data" section (highlighted in yellow), you can filter transactions based on debtor's information. Fields from both sections can be filled in at once. You can activate the filters by pressing the "Apply" button.

In the lower part, in the "Transactions" section, all activated transactions are displayed.

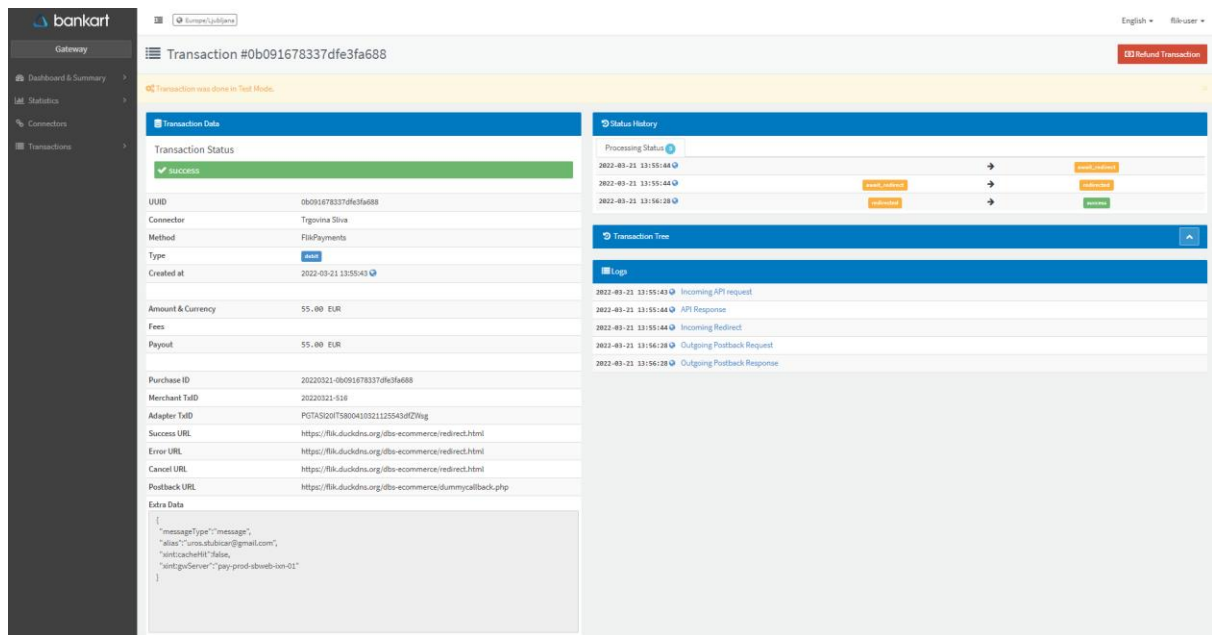


Transaction ID	Purchase ID / UUID	UUID	Adapter TxID	Related	Registration ID	Type	Date	Status	Connector	Country	Amount	Method	Merchant Meta Data	Description	Customer E-Mail
20220329-730	20220329-39040b0c4d4d204681e 39040b0c4d4d204681e	99040b0c4d4d204681e				success	2022-03-29 14:18:12	success (2022)	Trgovina Kosmija	-	1000.00 EUR	Payments			-
20220328-470	20220328-47db0a7b895c1f90ea48 47db0a7b895c1f90ea48	47db0a7b895c1f90ea48	PGTAS20T54004103280832420GynaM			success	2022-03-28 10:32:42	success (2022)	Trgovina Kosmija	-	300.00 EUR	Payments			-
20220328-804	20220328-ca3b6c2c54030e74ea3fc ca3b6c2c54030e74ea3fc	ca3b6c2c54030e74ea3fc	PGTAS20T5400410328080421uTeJym			success	2022-03-28 10:24:20	success (2022)	Trgovina Kosmija	-	300.00 EUR	Payments			-
20220328-856	20220328-032c7dc787a24c35ad49 032c7dc787a24c35ad49	032c7dc787a24c35ad49	PGTAS20T5400410328073523jVKh4c			success	2022-03-28 08:55:23	success (2022)	Trgovina Kosmija	-	10.00 EUR	Payments			-
20220328-448	20220328-868ec2eb8af0d22f11b 868ec2eb8af0d22f11b	868ec2eb8af0d22f11b	PGTAS20T5400410328070619uTeTyNI			success	2022-03-28 08:06:19	success (2022)	Trgovina Kosmija	-	10.00 EUR	Payments			-
20220327-3	20220327-290679362b3084f2e403 290679362b3084f2e403	290679362b3084f2e403				success	2022-03-27 19:08:53	success (2022)	Trgovina Kosmija	-	1.00 EUR	Payments			-
20220327-154	20220327-26c63248bca0b0b0b0c 26c63248bca0b0b0b0c	26c63248bca0b0b0b0c				success	2022-03-27 19:08:42	success (2022)	Trgovina Kosmija	-	1.00 EUR	Payments			-
20220327-583	20220327-4f5a5eb8a0749c3e5a5a 4f5a5eb8a0749c3e5a5a	4f5a5eb8a0749c3e5a5a				success	2022-03-27 19:07:47	success (2022)	Trgovina Kosmija	-	1.00 EUR	Payments			-
20220327-231	20220327-8542ea8b0c0b0b0b0c79d 8542ea8b0c0b0b0b0c79d	8542ea8b0c0b0b0b0c79d				success	2022-03-27 19:04:45	success (2022)	Trgovina Kosmija	-	1.00 EUR	Payments			-
20220327-234	20220327-462c7e0f6a24f76e48 462c7e0f6a24f76e48	462c7e0f6a24f76e48				success	2022-03-27 19:04:26	success (2022)	Trgovina Kosmija	-	1.00 EUR	Payments			-

The most important fields in the transaction list are:

- **Transaction ID:** transaction identifier specified by the merchant. Transaction ID must be unique for each transaction.
- **Purchase ID/UUID:** UUID is a unique transaction ID set by the payment gateway itself.
- **Type:** Transaction type. Debit means an online purchase, and Refund means a refund linked to an individual transaction.
- **Status:** the result of the transaction
- **Amount:** the amount paid in the transaction

Clicking on the number in the UUID field opens a more detailed view for the individual transaction, where some messages exchanged between the merchant and the Payment Gateway (Logs section) are also displayed - displayed on the next page.



Transaction #0b091678337dfe3fa688

Transaction was done in Test Mode.

Transaction Data

Transaction Status: **success**

UUID: 0b091678337dfe3fa688

Connector: Trgovina Silva

Method: FilkPayments

Type: **test**

Created at: 2022-03-21 13:55:43

Amount & Currency: 55.00 EUR

Fees: 55.00 EUR

Payout: 55.00 EUR

Purchase ID: 20220321-0b091678337dfe3fa688

Merchant TxID: 20220321-518

Adapter TxID: PGTAS207580043021125543dZWig

Success URL: https://rik.duckdns.org/dbs-e-commerce/redirect.html

Error URL: https://rik.duckdns.org/dbs-e-commerce/redirect.html

Cancel URL: https://rik.duckdns.org/dbs-e-commerce/redirect.html

Postback URL: https://rik.duckdns.org/dbs-e-commerce/dummycallback.php

Extra Data:

```
{
  "messageType": "message",
  "alias": "uros.stubicar@gmail.com",
  "merchantId": "1818",
  "url": "https://rik.duckdns.org/dbs-e-commerce/dummycallback.php"
}
```

Status History

Processing Status: 1

2022-03-21 13:55:44 Incoming API request

2022-03-21 13:55:44 API Response

2022-03-21 13:55:44 Incoming Redirect

2022-03-21 13:56:28 Outgoing Postback Request

2022-03-21 13:56:28 Outgoing Postback Response

Transaction Tree

Logs

2022-03-21 13:55:43 Incoming API request

2022-03-21 13:55:44 API Response

2022-03-21 13:55:44 Incoming Redirect

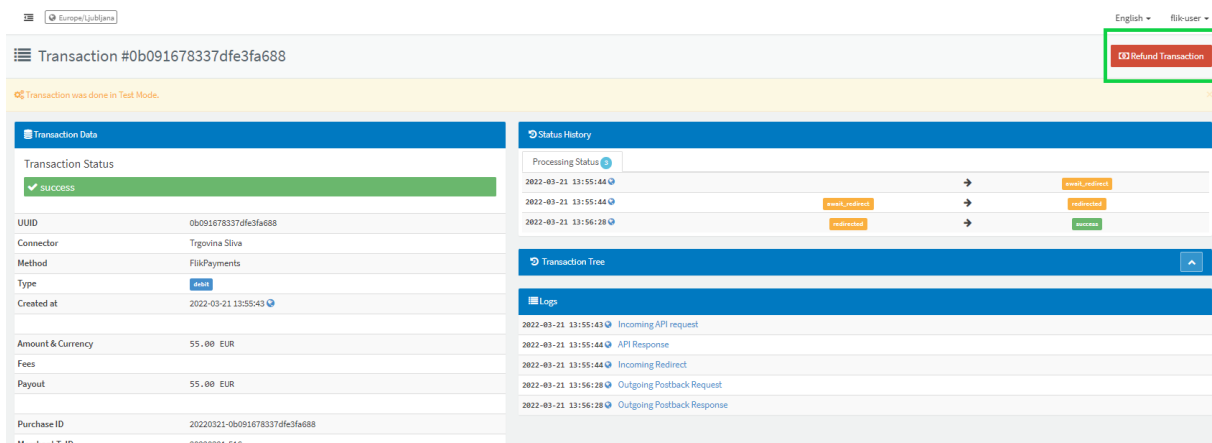
2022-03-21 13:56:28 Outgoing Postback Request

2022-03-21 13:56:28 Outgoing Postback Response

Refund Transaction

Refund of the transaction amount

Merchants who have the option of refunding the amount for purchases can initiate it via the user interface with the button located at the top right (*marked in green*).



Transaction #0b091678337dfe3fa688

Transaction was done in Test Mode.

Transaction Data

Transaction Status: **success**

UUID: 0b091678337dfe3fa688

Connector: Trgovina Silva

Method: FilkPayments

Type: **test**

Created at: 2022-03-21 13:55:43

Amount & Currency: 55.00 EUR

Fees: 55.00 EUR

Payout: 55.00 EUR

Purchase ID: 20220321-0b091678337dfe3fa688

Merchant TxID: 20220321-518

Status History

Processing Status: 1

2022-03-21 13:55:44 Incoming API request

2022-03-21 13:55:44 API Response

2022-03-21 13:55:44 Incoming Redirect

2022-03-21 13:56:28 Outgoing Postback Request

2022-03-21 13:56:28 Outgoing Postback Response

Transaction Tree

Logs

2022-03-21 13:55:43 Incoming API request

2022-03-21 13:55:44 API Response

2022-03-21 13:55:44 Incoming Redirect

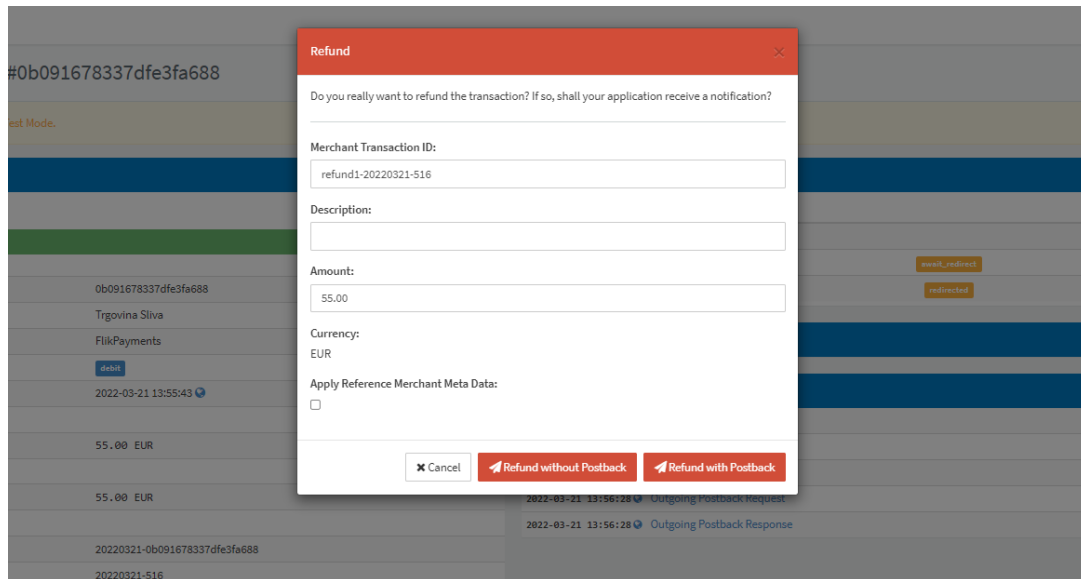
2022-03-21 13:56:28 Outgoing Postback Request

2022-03-21 13:56:28 Outgoing Postback Response

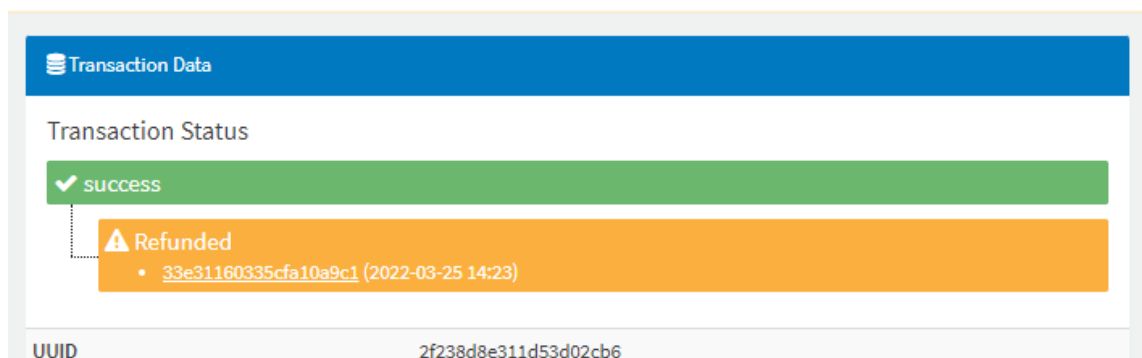
Refund Transaction

When a refund is initiated via the user interface, a pop-up opens that offers two options: "Refund without Postback" and "Refund with Postback".

The "with Postback" option sends the new transaction status to the merchant's Callback URL. If this option is not selected, the merchant does NOT get a change in the status of the transaction when making a refund via the Payment gateway user interface.

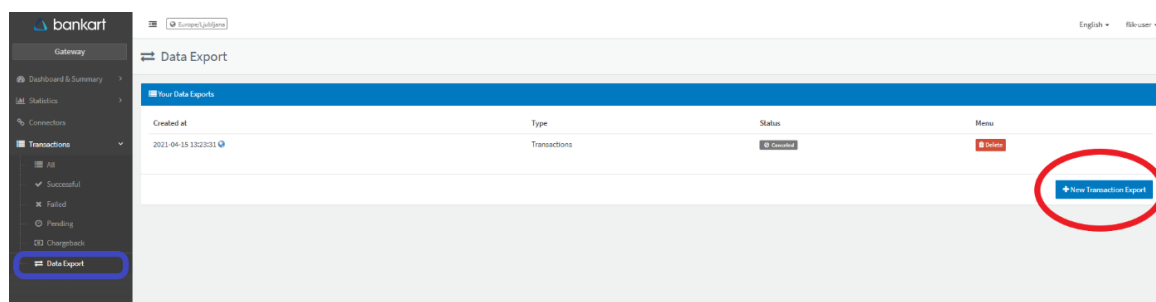


If a refund has already been made for an individual transaction, this is shown in the "Transaction status" section, where there is also a link to the refunded transaction.



Export of the list of completed transactions

In the **Data Export** subtab (marked in red in the image below), you can filter transactions and export them to a .csv or .xlsx file (Excel format).

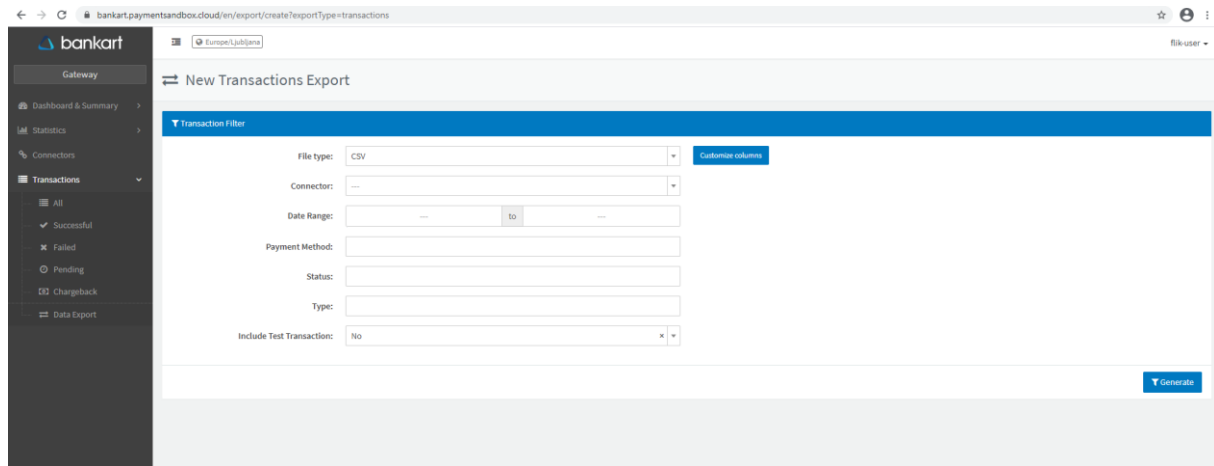


When you click on the subtab, all the documents that have been generated for export up to a certain moment are displayed. For each document, the transaction export date, the type of data in the export document, the status and the possibility of deletion or download are visible.

A new export document is created by clicking the "New Transaction Export" button (marked in red in the image above).

When a new window opens, the desired filters and file type for export are set, by clicking the button "Generate" the file for export is generated. After clicking on the button, the user is redirected to the previous page, where it is necessary to wait a few moments for the document to be generated and the option to download/delete is offered.

If these options do not appear after 30 seconds, the user can refresh the page himself.



The screenshot shows the 'New Transactions Export' page in the Bankart system. The interface includes a sidebar with navigation options: Gateway, Dashboard & Summary, Statistics, Connectors, and Transactions. The Transactions section is expanded, showing filters for All, Successful, Failed, Pending, Chargeback, and Data Export. The main area is titled 'New Transactions Export' and contains a 'Transaction Filter' section. This section includes fields for File type (set to CSV), Connector, Date Range, Payment Method, Status, Type, and Include Test Transaction (set to No). A 'Generate' button is located at the bottom right of the filter section.

Frequently Asked Questions by Traders (FAQ)

1. What data are used to identify the debtor?

The debtor is identified by the so-called alias (contact information) with which he registered as a user in the Flik scheme, i.e. phone number and/or email address.

2. What is the process of paying/buying with Flik?

When the debtor chooses Flik when choosing a payment option, an API call is sent to Bankart by the merchant, which returns Bankart's dynamic page with an input mask to the merchant and shows the debtor the possibility of entering an alias (phone number or email) with which Flik is activated at his bank. After entering the alias, the customer receives a push notification on their phone in their Flik application, where they must confirm the request to pay. When the debtor confirms the online payment, the payment gateway redirects him to a page where he is informed about the success of the payment. The debtor is also shown the status of the transaction success in the application.

3. Is there a possibility to return the amount of the initial purchase with the Flik method?

Yes, refunds are also available. A reference to the original purchase is required for the refund, and the refund amount cannot exceed the amount from the original transaction, but can be lower.

4. Is it possible to payout from the customer's account using the Flik method and what is the process?

We are still improving this option so that it meets all security requirements, which will probably be fixed within a few months. At the moment, therefore, we only offer payment and the option of refund. Otherwise, the customer could choose the option of payout of the desired amount from his user account via an alias, i.e. a number or email, which would be confirmed on the customer's user account. However, with payout confirmation, the money would be credited to the customers's TRR within seconds.

5. What is the request and response structure used in backend system releases?

The structure of requests and responses in the backend system is of JSON type.

6. What technology is used for data exchange?

API calls are used for data exchange, the specifications are available at the addresses below:

<https://gateway.bankart.si/documentation/apiv3>

<https://gateway.bankart.si/documentation/gateway>