Yowpay Hosted page manual

Purpose of the document :

Describing the calls to the payment hosted page

Returned values

Configure hosted page

1. Login with your account - https://yowpay.com/login
2. Go to E-Commerce menu and a new eCommerce (**name** and **site** are required). Your credentials will be automatically generated (**app token** + **secret key**). !!! Remember - never expose the secret key !!!

3. You can configure additional data (optional). This data can be configured automatically when using plugins for well known ecommerce systems

Return url : is the url on which Yowpay will redirect the client after he will have confirmed the submission of the payment (payment is not necessary credited yet).

Version 1.05 (14 Mar, 2023)

Cancel Url : is the url on which Yowpay will redirect the client in case he refuses to make the payment, this redirection is usually used for cascading purposes.

Webhook Url : this url is a secret url on merchant's web site to receive confirmation of accepted transaction. Usually this url is used to credit the end users of the services ordered or validate an order.

Start using the hosted page.

There are 2 ways to create transactions

1. Create from API

Post the following data to **https://yowpay.com/api/createTransaction/**

- these **headers** are needed in order to authenticate the merchant and validate the transaction

X-App-Access-Ts - the timestamp when the call is initiated (UTC must be used)
X-App-Token - the **app token** (part of ecommerce credentials explained above)
X-App-Access-Sig - the signature of the body (hash data). In order to receive you must use the **secret key** from credentials to hash the body content of the call

hash_hmac("sha256", "BodyWithParameters", "YOUR_SECRET_KEY");

The content of the **body** must be a json and this header will be needed too:

Content-type - application/json

- the **body** must contain the following parameters in json

- **amount** - (required - string)
- **currency** - EUR (required - string)
- **timestamp** - the same timestamp that is set in the header (required - int)
- **orderId** - end user reference (optional - string)
- **language** - end user language selection (optional - string)

2. Create from link

All parameters can be in the URL

https://yowpay.com/transaction/create?amount=%AMOUNT%&currency=%CURRENCY%&orderId=%ORDER_ID%&language=%LANGUAGE%&token=%APP_TOKEN%&timestamp=plained above%timestamp%&hash=%HASH%

Parameters are the same as explained above. The hash is built in a similar way based on previous parameters:

```
$data['amount']=$amount;
$data['currency']=$currency;
$data['orderId']=$orderId;
$data['language']=$language;
$data['token']=$token;
$data['timestamp'] = time();
$dataDecoded  = json_encode($data);

hash_hmac('sha256', $dataDecoded, $secret);
```

Update configuration URL

It is a server to server communication

URL : **https://yowpay.com/api/updateConfig/**

- these **headers** are needed in order to authenticate the merchant

X-App-Access-Ts - the timestamp when the call is initiated (UTC must be used)
X-App-Token - the **app token** (part of ecommerce credentials explained above)
X-App-Access-Sig - the signature of the body (hash data). In order to receive you must use the **secret key** from credentials to hash the body content of the call

hash_hmac("sha256", "BodyWithParameters", "YOUR_SECRET_KEY");

Also the content of the **body** must be a json so this header will be needed too:

Content-type - application/json

- the **body** must contain the following parameters in json

- **returnUrl** (required)
- **cancelUrl** - (required)
- **webhookUrl** - (required)
- **timestamp** - the same timestamp that is set in the header (required)

Get user's bank data information

It is a server to server communication

URL : **https://yowpay.com/api/getBankData/**

- these **headers** are needed in order to authenticate the merchant

X-App-Access-Ts - the timestamp when the call is initiated (UTC must be used)
X-App-Token - the **app token** (part of ecommerce credentials explained above)
X-App-Access-Sig - the signature of the body (hash data). In order to receive you must use the **secret key** from credentials to hash the body content of the call

hash_hmac("sha256", "BodyWithParameters", "YOUR_SECRET_KEY");

Also the content of the **body** must be a json so this header will be needed too:

Content-type - application/json

- the **body** must contain the following parameters in json

- **timestamp** - the same timestamp that is set in the header (required)

- the **API returns** the following data:

- **iban**
- **swift**
- **accountHolder**
- **consentExpirationTime**
- **remainingTime**

- **statusCode**

The parameter **statusCode** may have the following values:

0 - For still not provided consent.

1 - For active consent.

2 - For expired consent

3 - For lost consent

Webhooks

As explained above, you must configure webhooks in order to activate this feature. For every ecommerce we have generated credentials (**app token** and **secret key**) and a webhook URL can be added.

Webhooks are providing the following parameters as a json string in the body:

transactionId - unique id
amount
currency
reference
timestamp - (this is the time of the webhook in UTC, it can be used as a security feature)
language
orderId
createDate (transaction creation time - format ISO-8601 - e.g. 2023-02-15T10:40:24Z)
validateDate (transaction validation time - format ISO-8601 - e.g. 2023-02-15T10:40:24Z)
senderIban
senderSwift
senderAccountHolder
status
amountPaid
currencyPaid

- the **status** field can be equal to **1** or **2.**

1 - when the payment is validated and the paid amount is matching to transaction amount

2 - when the payment is validated but the amount and currency, that were paid, are not matching to amount and currency of the transaction. That is why we have also fields **amountPaid** and **currencyPaid** that are showing what amount was actually validated

In order to provide security of the webhooks we send the following headers:

X-App-Access-Ts - this the the same timestamp that is in the body as a parameter
X-App-Token - this is the **app token** (part of ecommerce credentials)
X-App-Access-Sig - this is the signature of the webhook (hash data)
Content-type: application/json

For creating the signature, the **secret key** from ecommerce credentials must be used. The secret key must not be exposed and it proves that data has not been manipulated.

hash_hmac('sha256', "BodyWithParameters", "YOUR_SECRET_KEY")

The following actions can be done to prove the validity of the webhook.

- the body must be hashed with the secret key and the result must be equal to the hash/signature of the header

- the timestamp in the body and in the header must be equal

- the timestamp should be relatively fresh (not older than 15 seconds for example). Be careful that UTC is used to avoid confusion with different server times.

We have an option with several retries of the webhooks in case of failure

We consider a webhook successfully accepted when a **http code 200** is returned and the body content is a string message "**ok**" or json reply **{"result":"ok"}**.