Manuel page de paiement hébergée

Objet du document

Description des appels à la page de paiement hébergée

Valeurs retournées

Configurer la page de paiement hébergée

1. Authentification sur le compte - https://merchant.yowpay.com/login
2. Allez au menu E-Commerce menu et créez un nouveau site E-Commerce (**nom** et **url** sont requis). Vos certificats seront automatiquement générés (**jeton d'application + clef secrète**) !!! Attention - ne jamais fournir ces information à des tiers !!!

3. Vous pouvez configurer des informations supplémentaires (en option). Ces informations peuvent être configurées automatiquement lors de l'utilisation de plugins E-Commerce connus.

Version 1.06 (15 Mar, 2024)

Retours à l'URL du site : il s'agit de l'url sur laquelle Yowpay redirige le client après un paiement confirmé par celui ci comme envoyé (le paiement n'est pas forcément crédités).

URL d'annulation : il s'agit de l'url sur laquelle Yowpay redirige le client dans le cas ou il refuse de faire le paiement, cette redirection est utilisée pour faire du cascading.

URL de rappel HTTP : il s'agit d'une url secrete sur le site web du commerçant destinée a recevoir les confirmations des transactions acceptées et ainsi de pouvoir créditer les clients de leurs commandes.

Commencer à utiliser la page de paiement hébergée.

Il y a 2 façons de créer des transactions

1. Création depuis l'API

Poster les données à l'url suivante :**https://api.yowpay.com/transaction/create**

- ces entêtes sont nécessaires pour authentifier le commerçant et valider la transaction

X-App-Access-Ts - le « timestamp » de l'appel (format UTC)
X-App-Token - le **jeton d'application** (dans la section E-Commerce, Certificats expliquée ci dessus)
X-App-Access-Sig - la signature du corps (donnée hachée). Pour recevoir vous devez utiliser la clef secrètre disponible dans la section E-Commerce, Certificats pour hacher le corps du contenu de l'appel.

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

Le contenu du **corps** doit être un json et son entête doit être aussi :

Content-type - application/json

- le **corps** doit contenir le paramètres suivant dans le json

- **amount** - (requis - chaine)
- **currency** - EUR (requis - chaine)

- **timestamp** - le même timestamp qui est configuré dans l'entête (requis - entier)
- **orderId** - référence client final (optionnel - chaîne)
- **language** - langue du client final (optionnel - chaîne

2. Création depuis un lien

Tous les paramètres peuvent être dans l'URL

https://secure.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:

Les paramètres sont les mêmes que ceux expliqués au dessus, les données hachées sont générées sur la base des mêmes paramètres.

```
$data['amount']=$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);
```

Mise à jour de l'URL de configuration

La communication s'effectue directement entre serveurs.

URL : **https://api.yowpay.com/config/update**

- ces entêtes sont nécessaires pour authentifier le commerçant

X-App-Access-Ts - le « timestamp » de l'appel (format UTC)
X-App-Token - le **jeton d'application** (dans la section E-Commerce, Certificats expliquée ci dessus)
X-App-Access-Sig - la signature du corps (donnée hachée). Pour recevoir vous devez utiliser la clef secrètre disponible dans la section E-Commerce, Certificats pour hacher le corps du contenu de l'appel.

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

Le contenu du **corps** doit être un json et son entête doit être aussi :

Content-type - application/json

- le **corps** doit contenir le paramètres suivant dans le json

- **returnUrl** (requis)
- **cancelUrl** - (requis)

- **webhookUrl** - (requis)
- **timestamp** - le même timestamp qui est configuré dans l'entête (requis - entier)

Accéder aux données bancaires commerçant

La communication s'effectue directement entre serveurs.

URL : **https://api.yowpay.com/bankData/get**

- ces entêtes sont nécessaires pour authentifier le commerçant

X-App-Access-Ts - le « timestamp » de l'appel (format UTC)
X-App-Token - le **jeton d'application** (dans la section E-Commerce, Certificats expliquée ci dessus)
X-App-Access-Sig - la signature du corps (donnée hachée). Pour recevoir vous devez utiliser la clef secrètre disponible dans la section E-Commerce, Certificats pour hacher le corps du contenu de l'appel.

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

Le contenu du **corps** doit être un json et son entête doit être aussi :

Content-type - application/json

- le **corps** doit contenir le paramètres suivant dans le json

- **timestamp** - le même timestamp qui est configuré dans l'entête (requis - entier)

- l' **API retourne** les informations suivantes :

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

Le paramètre **statusCode** peut prendre les valeurs suivantes :

0 - Pour consentement toujours pas fourni

1 - Pour consentement actif

2 - Pour consentement expiré

3 - Pour consentement perdu

Webhooks

Comme expliqué ci dessus, vous devez configurer les webhooks pour activer cette fonctionnalité. Pour chaque E-Commerce, nous avons générés des Certificats (jeton d'application et clef secrète) et une url de webhook peut être ajoutée.

Les Webhooks fournissent les paramètres suivants dans une chaîne json dans le corps :

transactionId - unique id
amount
currency
reference
timestamp - (le timestamp du webhook format UTC, peut être utilisé pour sécuriser les échanges)
language
orderId
createDate (date de création transaction - format ISO-8601 - e.g. 2023-02-15T10:40:24Z)
validateDate (date de validation transaction - format ISO-8601 - e.g. 2023-02-15T10:40:24Z)
senderIban
senderSwift
senderAccountHolder
status
amountPaid
currencyPaid

- le champ **status** peut prendre les valeurs **1 ou 2.**

1 - quand le paiement est validé et que le montant matche avec le montant de la transaction

2 - quand le paiement est validé et que le montant ne matche pas avec le montant de la transaction. C'est pourquoi les champs **amountPaid et currencyPaid** renvoient les montants réel qui a été validé

Afin de sécuriser les webhooks nous envoyons les entêtes suivantes :

X-App-Access-Ts - le « timestamp » est le même que dans le corps en paramètre
X-App-Token - le **jeton d'application** (dans la section E-Commerce, Certificats expliquée ci dessus)
X-App-Access-Sig - la signature du corps (donnée hachée). Pour recevoir vous devez utiliser la clef secrètre disponible dans la section E-Commerce, Certificats pour hacher le corps du contenu de l'appel.

Content-type: application/json

Pour créer la signature, la **clef secrète** disponible dans E-Commmerce Certificats doit être utilisée. La clef secrète ne doit pas être publiée et cela prouve que les données n'ont pas été manipulées.

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

Les actions suivantes peuvent être réalisées pour prouver la validité des webhooks

- le corps doit être haché avec la clé secrète et le résultat doit être égal au hachage/signature de l'en-tête

- le timestamp dans le corps et dans l'en-tête doit être égal

- le timestamp doit être relativement récent (pas plus de 15 secondes par exemple). Attention, UTC est utilisé pour éviter toute confusion avec les différentes heures du serveur.

Nous avons une option avec plusieurs tentatives des webhooks en cas d'échec

Nous considérons qu'un webhook a été accepté avec succès lorsqu'un **http code 200** est renvoyé et que le contenu du corps est un message de chaîne « ok » ou une réponse json **{"result":"ok"}**.