

## INTEGRATION DE VANILLA PAY DANS VOTRE SITE WEB

Version de la plateforme VANILLA PAY : 2.0

Nécessite la librairie : phpseclib pour le cryptage/décryptage ou une librairie contenant le TripleDES.

Avant tout, vous devez déjà être enregistré auprès de la plateforme VANILLA PAY ( <https://pro.ariarynet.com/> ) et disposer des paramètres suivant :

- votre clé de sécurité privée, qu'il faut garder précieusement.
- votre clé de sécurité publique, qu'il faut garder précieusement.
- votre client\_Id et votre client\_secret (à créer une seule fois sur la plateforme lors de l'enregistrement de votre site web).




The screenshot shows the Vanilla Pay website interface. At the top, there's a navigation bar with the Vanilla Pay logo on the left and a login section on the right containing input fields for 'Nom d'utilisateur' and 'Mot de passe', and a 'Connexion' button. Below the navigation bar, the main content area is divided into two sections. On the left, there's a circular graphic with the Vanilla Pay logo in the center, surrounded by various e-commerce categories: e-commerce, e-business, e-tourisme, e-salaire, e-administration, e-GOV, e-écologie, e-agriculture, and e-énergie. On the right, there's a section titled 'Inscription pour les entreprises' with a link 'Créer un compte personnel'. Below this, there's a form for 'Etape 1 / 3' with the heading 'Informations sur le compte'. The form includes a dropdown menu for 'Type de compte' (currently set to 'Commercial'), input fields for 'Nom d'utilisateur', 'Adresse e-mail', and 'Mot de passe'.

Figure 1: Page d'inscription pour un compte pro

https://pro.ariarynet.com/compte/

**vanilla Pay** Récapitulatif Mon compte Bordereaux Tutoriel Déconnexion



**Pro1**  
Technicien

[Editer](#)

**A propos du compte**

Nom  
Collaborateur

Société Mes clés d'accès Mes sites

[Générer nouveaux clés d'accès](#)


Vos clés d'accès:

- Client\_ID: 208\_5pf1237hq0co00440k3oco0kugckgho0wcw8sokchg0004g044
- Client\_secret: 1fzkvwvc9gnm88w440ow0c0g084c4g4gogwwkmo08cov8k0k8sg [Enable](#)

Ces informations sont extrêmement importantes , veuillez bien les noter.

Figure 2: Clés d'accès

**vanilla Pay** Récapitulatif Mon compte Bordereaux Tutoriel Déconnexion



**Pro1**  
Technicien

[Editer](#)

**A propos du compte**

Nom  
Collaborateur

Prénom  
Ariary

Adresse e-mail  
pro@mail.com

Numero de téléphone  
+261351185678

Autres utilisateurs  
Aucun autre utilisateur n'utilise ce compte

Société Mes clés d'accès Mes sites

[Enregistrer mon site](#)

**Mon site**

Lien vers le site  
<https://monsite.com>

Lien de retour  
[https://monsite.com/paiement\\_retour](https://monsite.com/paiement_retour)

Lien en cas de notification du site  
<https://monsite.com/notif>

Lien en cas d'erreur  
<https://monsite.com/echo>

Adresse IP  
145.125.1.215

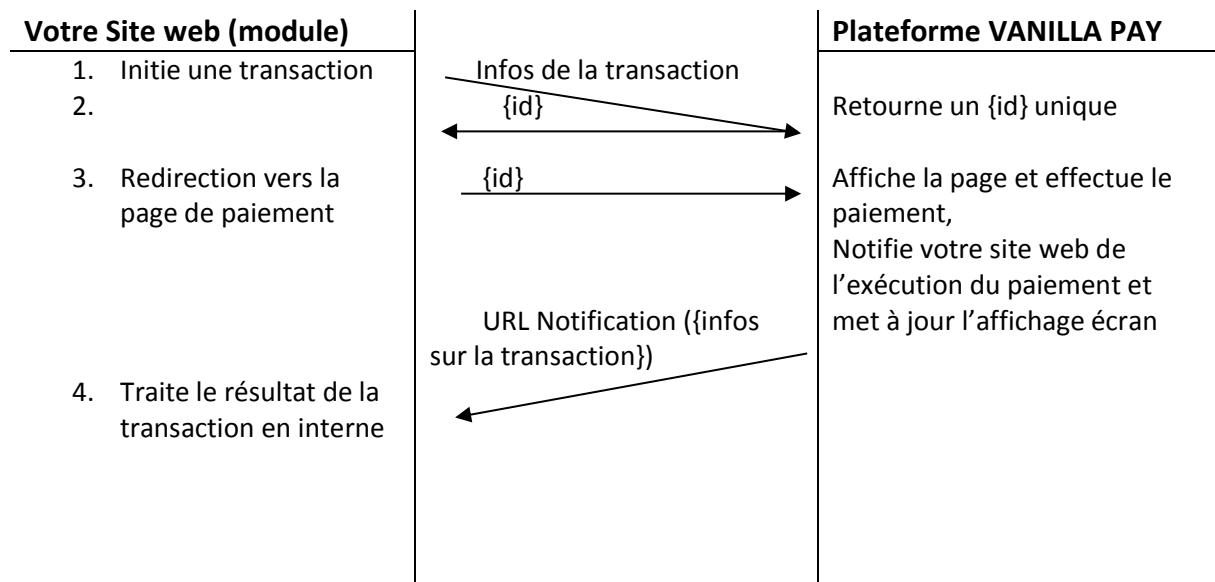
E-mail du site  
monsite@mail.com

Clé privée  
190405024283fa76c2ed121ff4d04c3a8b89783ecf0e158eb

Clé publique  
f913a480f2547e9d9bef816c079c14e3a9b3230b3ed82bf998

Figure 3: informations sur le site et clés

Une session de paiement se présente comme suit :



Ces appels webservice s'effectuent de manière automatique entre votre site web et la plateforme VANILLA PAY et s'exécute de façon transparente vis-à-vis du client cyberacheteur.

Tous ces échanges sont cryptés. A chaque appel webservice, votre site web doit crypter les paramètres avec votre clé publique. Chaque réponse envoyée par la plateforme VANILLA PAY doit être décryptée avec votre clé privée.

Le décryptage utilise les fonctions de la librairie phpseclib.

Pour une session de paiement en ligne, il faut protéger l'accès par un jeton (token).

### Demande d'accès (token)

Le jeton ou token permettra à votre site web d'accéder aux fonctionnalités de la plateforme de manière sécurisé.

Pour avoir le jeton, il faut que le site envoie une requête « GET » à l'url

<https://pro.ariarynet.com/oauth/v2/token>

Dans cette requête, il faut envoyer les paramètres suivant :

- 'client\_id' et 'client\_secret'. Les valeurs sont récupérées sur la plateforme.
- 'grant\_type' : 'client\_credentials' (tel quel)

En retour, la requête envoie le jeton (token). Ex : « **MzJmNDc3M2VjMmQzN** » pour toute la suite de ce document.

Ce token est dynamique donc a une durée de vie limitée sur la plateforme, juste pour réaliser un paiement en ligne. Il faut lancer cette requête à chaque nouveau paiement.

## Cryptage

Pour le cryptage en TripleDES, vous pouvez vous référer à ce code développer en NodeJS :

```
const crypto = require("crypto");

encrypt3DES: function(data, key) {

    var des_iv = Buffer.from("0000000000000000", 'hex');

    let cipher = crypto.createCipheriv('des-ede3-cbc', Buffer.from(key.substr(0, 24)), des_iv);

    let encrypted = cipher.update(data); encrypted = Buffer.concat([encrypted, cipher.final()]);

    return encrypted.toString('hex');

},
```

Il est à noter qu'il faut retourner la version cryptée en binaire et non en hexadécimal.

## Décryptage

Pour le décryptage en TripleDES, vous pouvez vous référer à ce code développer en NodeJS :

```
decrypt3DES: function(data, key) {

    var des_iv = Buffer.from("0000000000000000", 'hex');

    let encryptedText = Buffer.from(data, 'hex');

    let decipher = crypto.createDecipheriv('des-ede3-cbc', Buffer.from(key.substr(0, 24)), des_iv);

    let decrypted = decipher.update(encryptedText);

    decrypted = Buffer.concat([decrypted, decipher.final()]); return decrypted.toString();

},
```

Il est à noter que les données que nous envoyons sont en binaire et non en hexadécimal donc il faut convertir d'abord.

## Paieiment

Toutes les communications entre la plateforme et votre site web seront cryptées. Après inscription (à l'ouverture de votre compte sur VANILLA PAY), chaque client reçoit deux clés : clé publique (pour crypter) et clé privée (pour décrypter).

Pour accéder à une fonctionnalité de paiement, il faut envoyer une requête « POST » qui contiendra deux paramètres :

- 'site\_url' : le lien du site fourni lors de l'inscription (ex : « <http://www.moravidy.com> »), non crypté.
- 'params' : qui contient tous les paramètres requis pour la fonction demandée. Son contenu doit d'abord être encodé en json puis crypté avec la clé publique.

Le jeton d'identification (token) doit être obligatoirement mis en header de la requête comme ceci :

**Authorization: Bearer MzJmNDc3M2VjMmQzN**

### Initialisation du paiement

Avant d'effectuer un paiement, votre site web doit afficher une page de récapitulation. Cette page affiche au client cyberacheteur, un résumé complet de ce qu'il va vous payer, et un bouton « Payer avec VANILLA PAY ».

Pour initialiser un paiement sur la plateforme, il faut envoyer une requête « POST » à l'url

<https://pro.ariarynet.com/api/paiements>

Avec les paramètres suivants :

- 'unite\_monetaire' (ex : « Ar »)
- 'adresse\_ip' : l'adresse IP du client cyberacheteur qui va faire le paiement en ligne
- 'id\_panier' : l'identifiant de l'élément à payer
- 'montant' : le montant total à payer
- 'nom' : le nom du client cyberacheteur
- 'email' : l'adresse email du client cyberacheteur
- 'reference' : la référence de paiement pour votre gestion interne

A la fin de cette requête, votre site web recevra l'identifiant du paiement (« {id} ») qu'il faudra encore décrypter avec votre clé privée.

Cette requête « initialisation du paiement » est à envoyer avant de l'affichage de la page de récapitulation.

Dans cette page, le bouton « Payer avec VANILLA PAY » redirige le client cyberacheteur vers la plateforme de paiement en ligne.

L'url du paiement est

<https://moncompte.ariarynet.com/paiement/{id}> (pour les paiements par compte Vanilla Pay)

<https://moncompte.ariarynet.com/payer/{id}> (pour les paiements par mobile money direct)

Il faut remplacer le « {id} » par l'identifiant du paiement décrypté (en clair)

## Résultat du paiement

Lorsque le paiement a été effectué par le client cyberacheteur, la plateforme VANILLA PAY signalera votre site web via l'url de notification fournis lors de votre inscription que la transaction a bien été effectuée.

Le résultat du paiement, envoyé par la plateforme VANILLA PAY, est un objet encodé en json. Cet objet est toujours crypté. Pour rappel, il faut décrypter avec votre clé privée.

Il contient comme attribut :

- idpanier
- montant
- ref\_int (la référence que vous avez fourni)
- resultat ('success' si la transaction a réussi)
- nom (celui de l'acheteur si il l'a fourni)
- date
- ref\_arn (référence du paiement chez Vanilla Pay)

## Modules

Si votre projet est en **Symfony, CodeIgniter, WooCommerce, Odoo**, nous avons déjà développé des modules pour vous disponible dans :

[https://drive.google.com/drive/folders/1Y66rcvODvuGWAj8b6\\_VxQP9ba2HCONfX](https://drive.google.com/drive/folders/1Y66rcvODvuGWAj8b6_VxQP9ba2HCONfX) .

Sinon, vous pouvez développer seul ou avec nos développeurs le module correspondant à votre langage.