Prérequis & Sécurité

Sécurité

Dans l'objectif de conserver vos communications avec Payline sécurisées, vous devez obligatoirement utiliser :

- une connexion HTTPS sécurisé par TLS 1.2 ou supérieur.
- une des deux méthodes d'authentification proposées par Payline : clé d'accès ou certificat client

En complément, nous vous recommandons de vérifier l'authenticité du certificat serveur qui vous est présenté lors d'une connexion HTTPS avant d' envoyer vos données ou de réaliser une authentification HTTP. Cela consiste à s'assurer que :

- Le certificat appartient bien à Payline,
- Le certificat est signé par une autorité de certification digne de confiance,
- Le certificat est toujours valide (n'est pas expiré et n'est pas révoqué).

> En fonction de votre environnement, vous pouvez être amené à ajouter dans votre « **magasin de sécurité** » (keystore) la clé publique du certificat « root » de Payline. Il s'agit du certificat délivré par l'autorité de certification *VeriSign, inc*. Cela permet à votre serveur d' authentifier les serveurs Payline et donc d'assurer une communication de serveur à serveur fortement sécurisée.

Authentification par clé d'API

Lorsque vous réalisez des demandes de paiement à l'API Payline, vous devez obligatoirement présenter votre identifiant de compte commerçant (Merchand ID) et votre clé d'accès (Merchant Access Key) pour réaliser une authentification HTTP. Payline n'acceptera pas vos demandes si elles ne sont pas correctement authentifiées.

Ne communiquez jamais votre clé d'accès (Merchant Access Key) à une tierce personne. Payline utilise votre clé d'accès pour vous identifier en tant qu'expéditeur de vos demandes de paiement. Aucun interlocuteur chez Payline ne la connaît et ne vous demandera cette information.

Récupérer votre clé d'accès

Une fois connecter au centre administration Payline, vous pouvez générer une clé : Centre Administration - Gestion des clefs d'API

Méthode HTTP Basic Authentification

Payline utilise le mécanisme HTTP Basic Authentification pour authentifier les commerçants abonnés.

Si votre identifiant de compte commerçant est 1234567890 et votre clé d'accès est DJMESHXYou6LmjQFdH, vous devez encoder en base64 la valeur de 123456 7890:DJMESHXYou6LmjQFdH. La chaîne obtenue est à ajouter à l'entête HTTP comme dans l'exemple ci-dessous :

```
Authorization : Basic MTIzNDU2Nzg5MdpESk1FU0hYWW91NkxtalFGZEg=
```

En fonction du langage de programmation, l'identifiant et clé d'accès sont automatiquement encodés en base64 et ajoutés à l'entête HTTP.

Grâce à cette mécanique, vous sécurisez de façon optimale vos échanges informatiques entre vos applications et Payline et assurez :

- l'authentification des interlocuteurs : vos serveurs et les serveurs Payline,
- l'intégrité des messages,
- le cryptage des données.

Authentification par certificat client

La mise en place de l'authentification par certificat de type class 3.

Le certificat utilisé pour la signature devra être présent dans le magasin des certificats pour accorder l'accès.

Le certificat devra prendre en compte les exigences de sécurité PCI et de la solution de paiement Payline :

- Algo de hash : SHA-256,
- Clés de chiffrement : RSA (Longueur 2048 version V3). De plus la clef privée associée devra être supérieur ou égale à un encodage de 2048 bits (le common name doit être votre identifiant marchand).

Le CSR fournit par le commerçant sera signé par MONEXT, et ce certificat CSR signé sera déposé avec la clef privé généré lors de la création du csr dans le keystore du commerçant et il sera utilisé lors de chaque appels web services vers la solution de paiement Payline.

Dans le cas où vous utilisez openSSL, la commande à exécuter pour générer la clef privée et le certificat csr :

```
openssl req -out CSR.csr -sha256 -new -newkey rsa:2048 -nodes -keyout privateKey.key
```

Ensuite il faut répondre à un certain nombre de question. Le plus important est de mettre l'identifiant du commerçant dans le Common Name

Si vous souhaitez vérifier votre CSR, vous pouvez utiliser cette commande :

```
openssl req -text -noout -verify -in CSR.csr
```

Puis vous devez utiliser la commande décrite ci-dessous, dès réception du certificat signé par Monext, ce fichier générer le pkcs12, vous permettra de configurer votre serveur lors de chaque appel webservice

```
openssl pkcs12 -export -in cert_client_xxx.pem -inkey clef.key -certfile ca_inter.pem -out nom_du
fichier_de_sortie.p12 -name "Nom du certificat"
```

> ⚠ **point d'accès dédié**
>
> Se reporter à API Endpoints pour prendre connaissance des points d'accès dédiés à l'accès sécurisé par certificat client

Page Associée

- Demande d'une clef de chiffrement