Prerequisites & Security

Security

In order to keep your communications with Payline secure, you must use:

- secure HTTPS connection with TLS 1.2 or higher.
- one of the two authentication methods proposed by Payline: access key or server certificate.

In addition, we recommend that you verify the authenticity of the server certificate that is presented to you during an HTTPS connection before sending your data or performing HTTP authentication. This is to ensure that:

- The certificate belongs to Payline,
- The certificate is signed by a trusted certification authority,
- The certificate is still valid (has not expired and is not revoked).

Depending on your environment, you may need to add the public key of Payline's "root" certificate to your "security store" (keystore). This is the certificate issued by the VeriSign Certification Authority, Inc. This allows your server to authenticate Payline servers and thus ensure highly secure server-to-server communication.

Authentication by access key

When you make payment requests to the Payline API, you must submit your Merchand ID and Merchant Access Key for HTTP authentication. Payline will not accept your requests if they are not properly authenticated. Never share your Merchant Access Key with a third party. Payline uses your access key to identify you as the sender of your payment requests. No one at Payline knows it and will not ask you for this information.

HTTP Basic Authentication Method

Payline uses the HTTP Basic Authentication mechanism to authenticate subscribed merchants.

If your merchant account ID is 1234567890 and your access key is DJMESHXYou6LmjQFdH, you must base6464456 7890: DJMESHXYou6LmjQFdH. The resulting string is to be added to the HTTP header as in the example below:

```
Authorization : Basic MTIzNDU2Nzg5MdpESk1FU0hYWW91NkxtalFGZEg=
```

Depending on the programming language, the identifier and access key are automatically encoded in base64 and added to the HTTP header.

Thanks to this mechanism, you optimally secure your computer exchanges between your applications and Payline and ensure:

- authentication of interlocutors: your servers and Payline servers,
- the integrity of the messages,
- data encryption.

Server certificate authentication

The implementation of certificate authentication type class 3.

The certificate used for signing must be present in the certificate store to grant access.

The certificate must take into account the PCI security requirements and the Payline payment solution:

- Algo of hash: SHA-256,
- Encryption keys: RSA (Length 2048 version V3). In addition, the associated private key must be greater than or equal to a 2048 bit encoding (the common name must be your merchant ID).

The CSR provided by the merchant will be signed by MONEXT, and this signed CSR certificate will be deposited with the private key generated when creating the csr in the merchant's keystore and it will be used during each web services call to the Payline payment solution. .

In case you use openSSL, the command to execute to generate the private key and the csr certificate:

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

Then you have to answer a certain number of questions. The most important thing is to put the merchant ID in the Common Name

If you want to check your CSR, you can use this command:

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

Then you must use the command described below, upon receipt of the certificate signed by Monext, this file generate the pkcs12, you will configure your server during each call 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"
```