Mode Intégré - Direct

< Précédent Suivant >

Contenu :

Introduction

Objet du document

Ce document décrit la procédure d'intégration de la solution de paiement sécurisé en ligne Payline en mode API DIRECT dans votre site commerçant.

Ce document est destiné aux commerçants et intégrateurs qui souhaitent utiliser le mode d'intégration « API DIRECT » la solution de paiement Payline.

Liste des documents de référence

Nos documents sont disponibles sur notre site internet www.payline.com ou sur simple demande auprès de notre service support.

Contactez le support Payline.

Principe général

Présentation

Le commerçant récupère les données carte sur la page récapitulative de commande hébergée sur ses serveurs. Ce mode permet l'exécution de la demande d'autorisation en mode synchrone ou asynchrone (via stockage temporaire du CVV), l'usage des fonctionnalités de portefeuille. Le commerçant devra se mettre en conformité PCI-DSS.

Sécurité

La collecte des données de paiement par le site marchand implique un risque plus élevé pour le commerçant. Ce mode d'intégration nécessite donc une application rigoureuse des standards de sécurité.

En outre, deux éléments importants sont à mettre en œuvre par le marchand :

1. La page de collecte des données de paiement ne doit stocker (fichiers logs, …) à aucun moment les informations « numéro de carte » et « CVV » saisies par l'acheteur. Ces données seront transmis à Payline au travers des appels webservices ;
2. Le numéro de commande fourni lors de l'appel à la fonction *getToken* doit être bien retrouvé à l'identique lors de l'analyse de la réponse. Ce contrôle garantit que les données n'ont pas été détournées dans le but de procéder à un autre paiement que celui prévu initialement.

Prérequis techniques

Pour les serveurs PHP les exemples de code fonctionnent :

- Avec la bibliothèque *gzdecode.php*. qui est optionnelle jusqu'à la version 5.4.0 (disponible en standard pour les versions supérieures) ;
- Avec les modules *mcrypt* et *php_soap*. Ils doivent être à activer.

Pour les serveurs J2E, afin de pouvoir accéder aux fonctions de chiffrement avec des clés supérieures à 128 bits, il faut installer le package *Java Cryptography Extension* (JCE) *Unlimited Strength Jurisdiction Policy* (http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html).

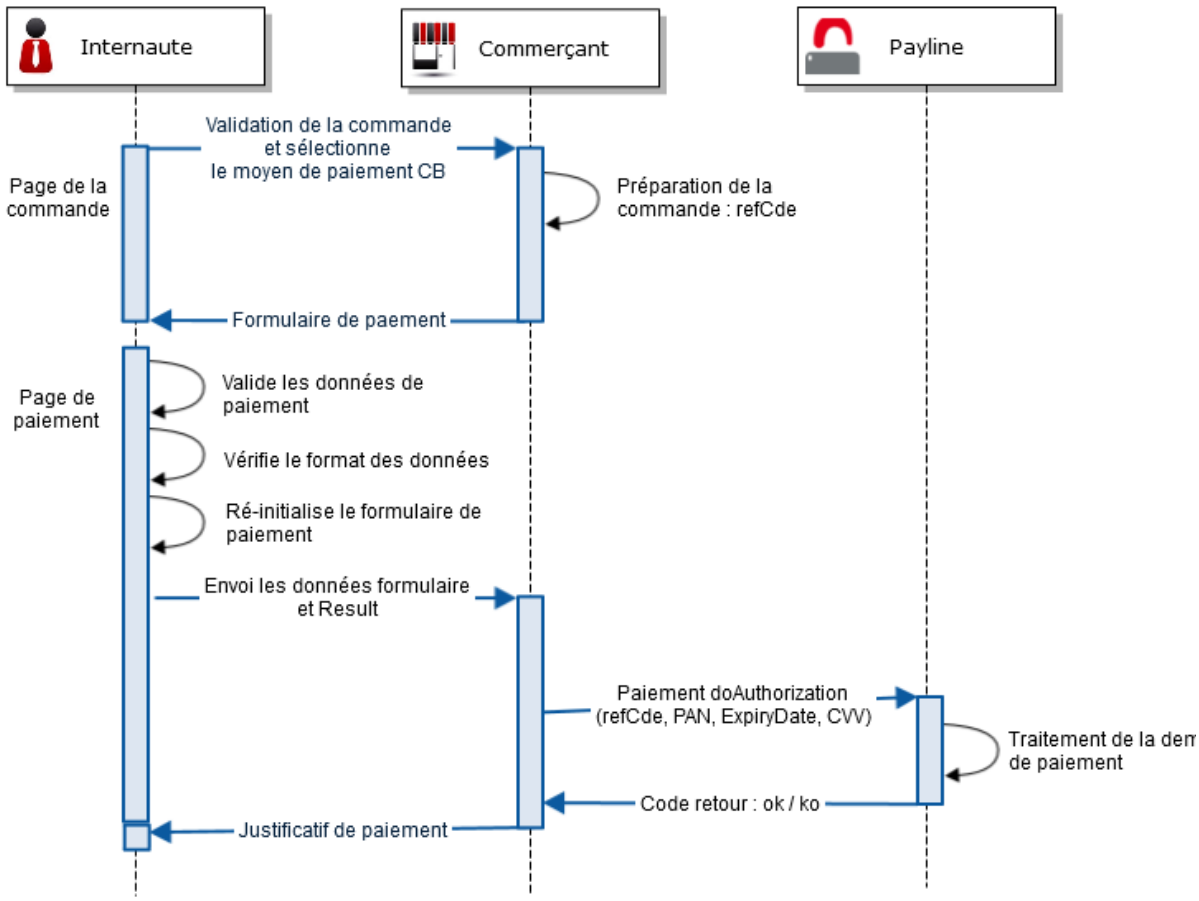
Description fonctionnelle

Cinématique d'un paiement simple

Voici les étapes principales d'un paiement avec cette nouvelle interface :

1. L'acheteur valide son panier, le navigateur envoie une requête http sur le serveur commerçant ;
2. Le serveur commerçant :
    a. génère une référence unique de commande ;
    b. chiffre avec sa clé d'accès la chaine composée de la référence commande et du numéro de contrat ;
    c. construit et renvoie le formulaire au navigateur ;
3. L'acheteur saisit et valide ses données (paiement, adresse de facturation, etc…) ;
4. Le serveur commerçant appelle le WS Payline « doAuthorization » avec les données de paiement ;
5. Le WS Payline « doAuthorization » :
    a. appelle la banque du commerçant pour réaliser une demande d'autorisation ;
    b. réalise les contrôles anti-fraude ;
    c. retourne le résultat au commerçant.

Figure 1 : Cinématique d'un paiement simple (sans 3DS)

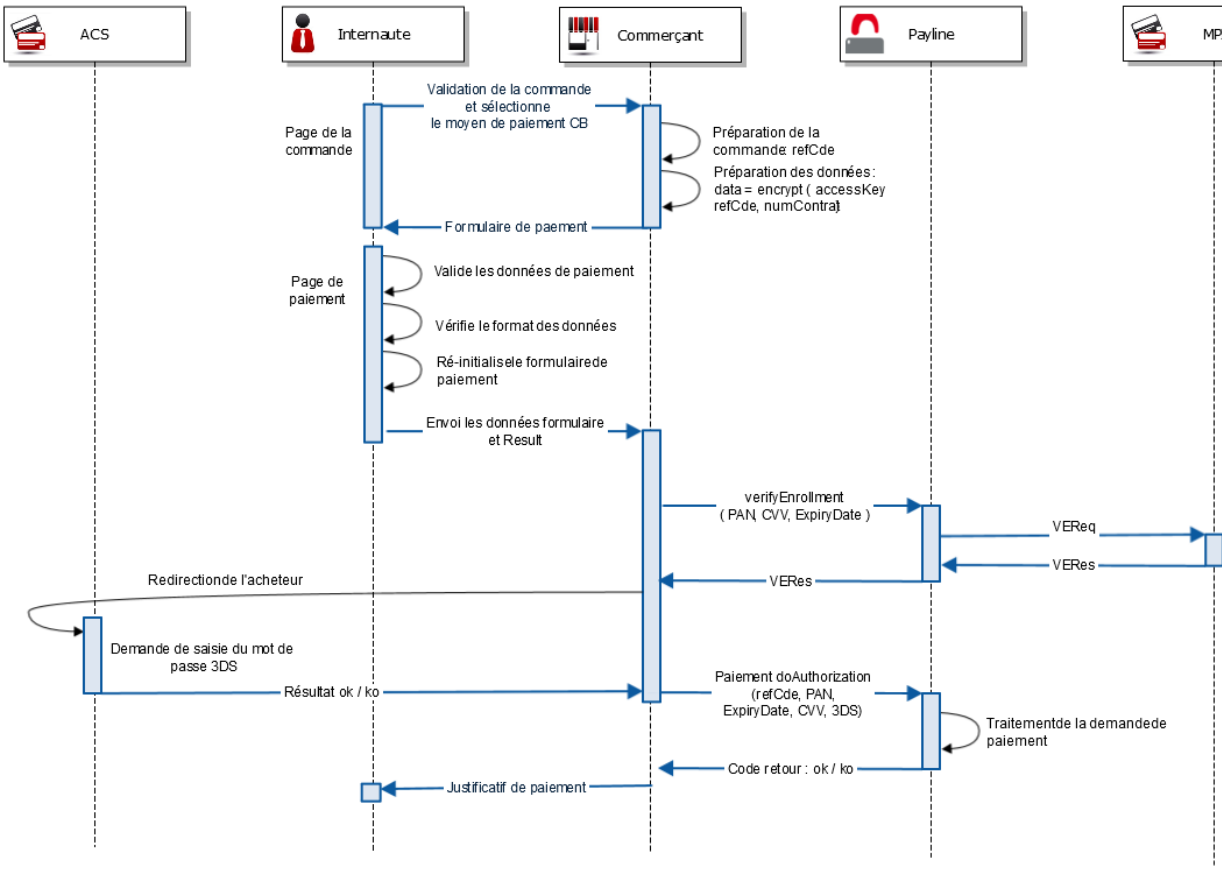


Cinématique d'un paiement 3DSecure

Voici les étapes principales pour un paiement 3DSecure :

1. L'acheteur valide son panier, le navigateur envoie une requête http sur le serveur commerçant ;
2. Le serveur commerçant génère un formulaire comme dans la cinématique précédente.
3. L'acheteur saisit et valide ses données (paiement, adresse de facturation, etc…).
4. Le serveur du commerçant :
    a. déchiffre les données Payline pour récupérer le numéro de la carte, la date d'expiration et le CVV ;
    b. stocke dans la session de l'acheteur ces données ;
    c. appelle le WS Payline « verifyEnrollment » avec le numéro de la carte, CVV et la date d'expiration.
5. Le WS Payline « verifyEnrollment » demande au MPI l'adresse de l'ACS de l'acheteur.
6. L'acheteur :
    a. est redirigé sur l'ACS de sa banque ;
    b. s'identifie ;
    c. est redirigé sur le site du commerçant (cf. TERM_URL).
7. Le serveur commerçant appelle le WS Payline « doAuthorization » avec le numéro de la carte, la date d'expiration, le CVV et le PARes.
8. Le WS Payline « doAuthorization » :
    a. appelle le MPI pour vérifier le PARes ;
    b. appelle la banque du commerçant pour réaliser une demande d'autorisation ;
    c. réalise les contrôles anti-fraude ;
    d. retourne le résultat au commerçant.

Figure 2 : Cinématique d'un paiement simple avec 3DSecure



Cinématique d'un paiement 3DSecure déclenché par le module anti-fraude

Voici les étapes principales pour un paiement 3DSecure déclenché par le module anti-fraude :

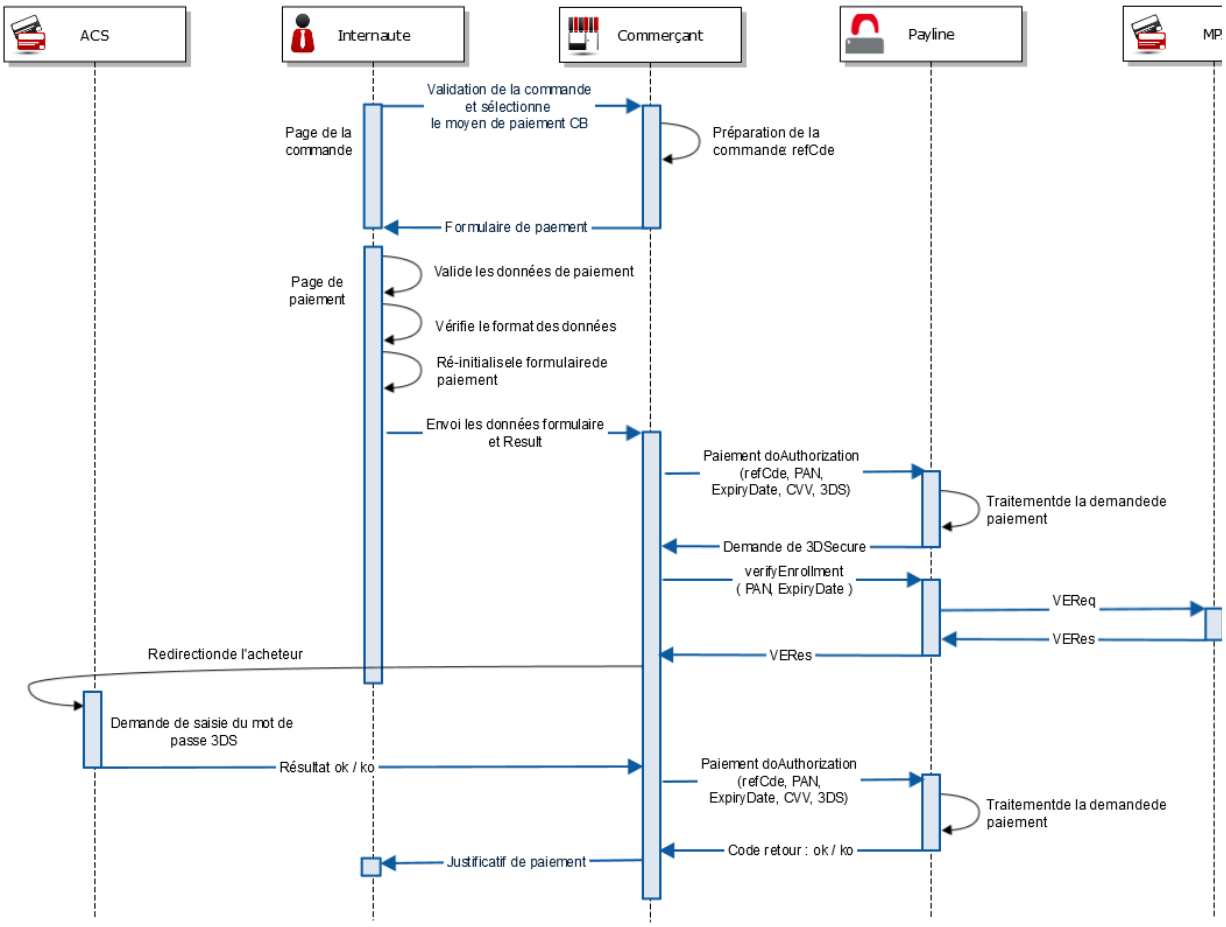
1. L'acheteur valide son panier, le navigateur envoie une requête http sur le serveur commerçant.
2. Le serveur commerçant génère un formulaire comme dans la cinématique précédente.
3. L'acheteur saisit et valide ses données (paiement, adresse de facturation, etc…).
4. Le navigateur appelle le serveur du commerçant avec les données de paiement.
5. Le serveur du commerçant :

    a. stocke dans la session de l'acheteur ses données ;
    b. appelle le WS Payline « doAuthorization » avec le numéro de la carte, la date d'expiration et le CVV.
6. Le WS Payline « doAuthorization » :
    a. réalise les contrôles 3DSecure ;
    b. renvoie un code d'erreur 02715 « Authentication3DSecure is mandatory ».
7. Le serveur du commerçant appelle le WS Payline « verifyEnrollment » avec le numéro de la carte et la date d'expiration.

Le traitement reprend à partir de l'étape 6 de la cinématique 3DS précédente :

1. Le WS Payline verifyEnrollment demande au MPI l'adresse de l'ACS de l'acheteur.
2. L'acheteur :
    a. est redirigé sur l'ACS de sa banque ;
    b. s'identifie ;
    c. est redirigé sur le site du commerçant (cf. TERM_URL).
3. Le serveur commerçant appelle le WS Payline « doAuthorization » avec le numéro de la carte, la date d'expiration, le CVV et le PARes.
4. Le WS Payline « doAuthorization » :
    a. appelle le MPI pour vérifier le PARes ;
    b. appelle la banque du commerçant pour réaliser une demande d'autorisation ;
    c. réalise les contrôles anti-fraude ;
    d. retourne le résultat au commerçant.

Figure 3 : Cinématique d'un paiement avec 3DSecure déclenché par le module LCLF



Cinématique d'enregistrement d'une carte dans un portefeuille

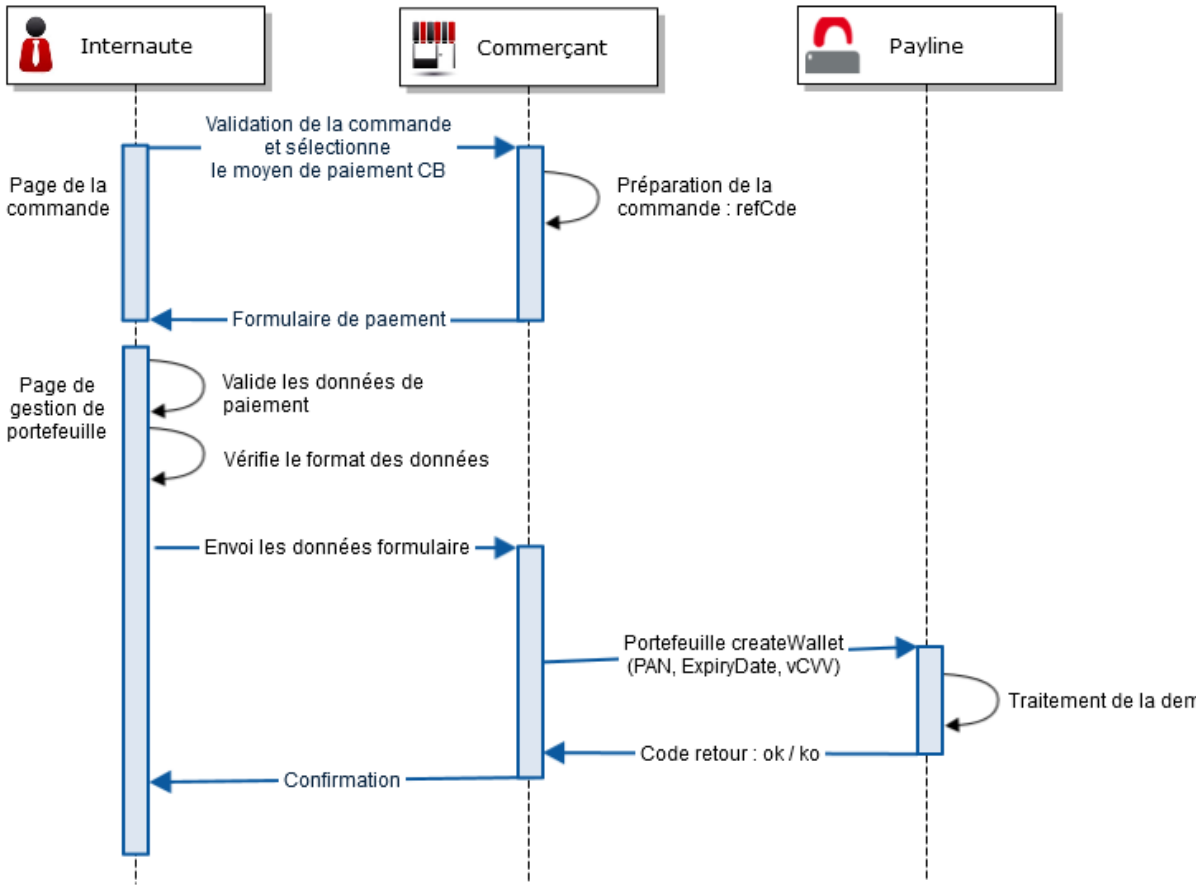
Dans ce scénario, aucun paiement n'est réalisé.

Lorsque l'acheteur valide :

1. Le navigateur de l'acheteur envoie les données de la carte à Payline (sur le module des pages Web de paiement).
2. Le navigateur retourne ces données au serveur commerçant.
3. Le serveur commerçant appelle le WS Payline « createWallet ».

4. Le WS Payline « createWallet » envoie une demande d'autorisation pour scoring à la banque du commerçant (ex : autorisation à 1 euro ou demande d'information selon la banque).

Figure 4 : Cinématique d'un enregistrement de carte dans le portefeuille Payline

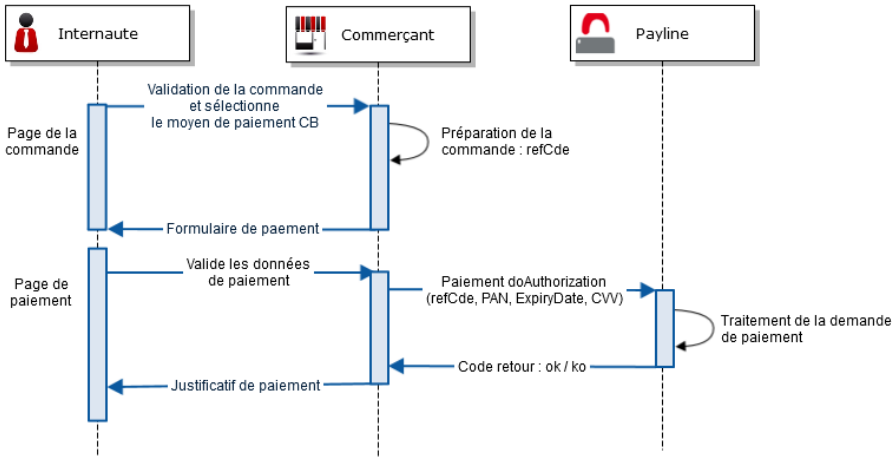


Cinématique d'un second paiement

Dans cette cinématique, le commerçant a conservé au préalable le PAN de la carte et la date d'expiration dans sa base de données lors du premier paiement. La page de paiement affiche les cartes associées à ce compte acheteur.
Le commerçant a la possibilité de collecter le CVV auprès de son acheteur et le fournir lors de l'appel « doAuthorization » ou d'effectuer une transaction sans CVV.

Lorsque l'acheteur valide la commande :

1. Le serveur commerçant :
    a. recherche le numéro de la carte associé au client ;
    b. appelle WS Payline « doAuthorization » avec la carte, avec ou sans CVV et un code action 120 ou 121.
2. Le WS Payline « doAuthorization » envoie une autorisation à la banque du commerçant.


Internaute
Commerçant
Payline
Validation de la commande
et sélectionne
le moyen de paiement CB
Page de la
commande
Préparation de la
commande : refCde
Formulaire de paement
Page de
paiement
Valide les données
de paiement
Paiement doAuthorization
(refCde, PAN, ExpiryDate, CVV)
Traitement de la demande
de paiement
Code retour : ok / ko
Justificatif de paiement