3D Secure

Contenu

Le principe

3D Secure est un protocole d'authentification fourni par les systèmes de cartes de crédit.
Le marchand peut demander un mot de passe au consommateur pour confirmer le paiement. Cette procédure permet d'authentifier le consommateur comme étant le porteur de la carte utilisée pour le paiement. Elle permet de renforcer la sécurité et de transférer la responsabilité au consommateur de la carte en cas d'impayé.

L'authentification se fait en deux étapes :

- vérification de l'enrôlement de la carte au système 3D Secure ;
- demande d'authentification du consommateur.

La mise en place de 3D Secure doit permettre aux e-marchands de réduire le montant de leurs impayés dus à la fraude, mais cette procédure réduit également le taux des paiements acceptés.

3DS Dynamique / 3DS Sélectif

Le marchand peut configurer des règles du module antifraude pour basculer des demandes de paiement avec une demande l'authentification du consommateur 3D Secure.
Payline propose d'identifier votre moyen de paiement avec un alias Contrat_Number. Il est donc possible de configurer deux Alias sur le même contrat avec un contrat classique sans 3DS et un autre avec 3DS.
Vous pouvez également réaliser des demandes de paiement directement en 3D Secure.

Intégration

En page web, vous devez appeler le contrat (Alias) du moyen de paiement avec le service doWebPayment.
En mode direct, vous devez gérer la vérification de l'enrôlement avec le service verifyEnrollment puis réaliser la demande de paiement avec le service doAuthorization.

Le module de Lutte contre la fraude

Vous devez consulter le module de lutte contre la fraude afin de gérer les règles et les actions à mettre en place.
Il est important de bien vérifier vos taux d'acceptation en mettant en place le module antifraude et de bien ajuster les règles, plusieurs actions sont possibles pour vous aider à la mise en oeuvre de ce module.

Les valeurs ECI (Electronic Commerce Indicator)

ECI (*Electronic Commerce Indicator*) is the value returned from the Directory Server (Visa, Mastercard and JCB) to show result of authentication credit card payment from your customer on the features of 3D Secure.

1. Visa

- **ECI 05:** Card holder and issuing bank are 3D Secure. 3dSecure authentication successful. è succès
- **ECI 06:** One of card holder or issuing bank not registered as a 3D Secure. è échec
- **ECI 07:** Card holder and issuing bank not registered as a 3D Secure. è échec

2. Mastercard

- **ECI 02:** Card holder and issuing bank are 3D Secure. 3dSecure authentication successful. è succès
- **ECI 01:** One of card holder or issuing bank not registered as a 3D Secure. è échec
- **ECI 00:** Card holder and issuing bank not registered as a 3D Secure. è échec

3. JCB

- **ECI 05:** Card holder and issuing bank are 3D Secure. 3dSecure authentication successful.
- **ECI 06:** One of card holder or issuing bank not registered as a 3D Secure.
- **ECI 07:** Card holder and issuing bank not registered as a 3D Secure

Pages associées

- 3D Secure
- 3D Secure 1.0 - Authentification
- 3D Secure 1.0 - Customizing the sign name displayed during authentication
- 3D-Secure - Transfer of responsibility
- 3D-Secure - Transfert de responsabilité
- DP - 3DSecure user in direct mode V1
- DP - Utilisateur du 3DSecure en mode direct
- Messages 3D Secure