DP - Utilisateur du 3DSecure en mode direct

Contenu

Cette intégration n'est plus conforme à la nouvelle directive européenne. Veuillez vous reporter la documentation 3DSV2.

Introduction

Pré-requis bancaire et de connexion 3DSecure

Ce traitement repose sur la mise en place d'un contrôle supplémentaire lors d'un achat en ligne : en complément des données bancaires, l'acheteur validera son paiement en saisissant une donnée secrète que lui aura fourni sa banque.
Ce dispositif s'accompagne d'une évolution réglementaire appelée "liability shift" ou "transfert de responsabilité" dont le principe est de faire supporter le risque d'impayé émis pour contestation du porteur à la banque du porteur et non plus au commerçant, si le porteur a validé son paiement en renseignant les données 3D Secure et que le commerçant a respecté les mesures de sécurité énoncées dans les conditions générales de vente de son contrat de commerce électronique souscrit auprès de sa banque.

La solution de paiement Payline a déroulé une certification 3DSecure avec les banques, ainsi qu'avec Visa et MCI.

Souscription

Le commerçant doit souscrire auprès de sa banque à un contrat VADS (VAD type 3D Secure).
Le commerçant informe Payline qu'il a souscrit à un contrat VADS avec 3DSecure.
L'équipe Payline, doit procéder à l'enregistrement du commerçant auprès de Visa et MCI, « un délai de 10 jours est nécessaire ».
Dès confirmation des réseaux Visa et MCI, l'équipe Payline informe le commerçant qu'il va procéder à l'activation du contrat VADS.
Dès activation du contrat VADS, tous les flux transitant sur ce contrat seront des transactions 3DS.

Pré-requis d'utilisation de la solution de paiement Payline

La solution 3D Secure en mode interface Direct assure le transfert sécurisé des données sensibles, traite les demandes d'authentification et d'autorisation.

Les points d'intégration :

- *verifyEnrollment* est nécessaire pour assurer l'authentification et *doAuthorization* pour réaliser l'autorisation ;
- récupérer le résultat de la transaction avec *gettransactionDetails*.

Vous devez vérifier la clé d'accès des services et configuration le paramétrage SOAP UI.

3D-Secure en mode interface direct avec un paiement

Les étapes suivantes présentents les deux web services verifyEnrollment et doAuthorization permettant de reéaliser une transaction 3DSecure en utilisant le mode interface direct de la solution de paiement Payline.

Etape 1 : verifyEnrollment

Ce premier appel web service permet de vérifier l'éligibilité du porteur au dispositif 3DSecure, et donc de savoir si le porteur de la carte est bien enregistré auprès d'un Directory Server VISA ou Mastercard.

Voici un exemple de requête / réponse pour le web services verifyEnrollment :

verifyEnrollmentRequest	verifyEnrollmentResponse
<impl:verifyEnrollmentRequest> <impl:card> <obj:number>**4970100000325734**</obj:number> <obj:type>**CB**</obj:type> <obj:expirationDate>**0912**</obj:expirationDate> <obj:cvx>**123**</obj:cvx> </impl:card> <impl:payment> <obj:amount>**4050**</obj:amount> <obj:currency>**978**</obj:currency> <obj:action>**100**</obj:action> <obj:mode>**CPT**</obj:mode> <obj:contractNumber>**CB3DS**</obj:contractNumber> </impl:payment> <impl:orderRef>**REF0923847**</impl:orderRef> </impl:verifyEnrollmentRequest>	<verifyEnrollmentResponse> <result> <code>**03000**</code> <shortMessage>**ACCEPTED**</shortMessage> <longMessage>**Operation Successfull**</longMessage> </result> <actionUrl>**https://acs.banque.com/mdpayacs/pareq**</actionUrl> <actionMethod>**POST**</actionMethod> <pareqFieldName>**PaReq**</pareqFieldName> <pareqFieldValue> **eJxVkdtuwjAMhl+l4gGaA21ZkcnEOGhIYzAYQ9rNFFoPKq** **ClScvh7ZeUMrbcxJ9jx/ZveN8oxP4co1KhgDFqLdfoJHGnw** **XgrpM2QNQRMuzPMBRxR6SRLBXOpy4Hc0GSpaCPTQoCM** **8qfRq2C86fkBkBphj2rUF+x6gFwRUrlH0e1NnRiPQCqCKCv** **TQl0E9ymQG0CpdmJTFIc2lafTyV1n2XqH7rciGqUp/Zh3TM** **TXKiuLJC9RA7EJQO59TUtraVPgnMRivPgMJkt/uNoO5Xzrl** **5OBz5eDj5fZ8K0DxEZALAsUnJp2KQ8cGrY5a3tmosoPcm8** **7E4PFzPGoa1utPXCwhbpX8Kh9+esBo7LCNLqIsPVg5rsR4** **PmQpWgijKy/NsSoIzNGfd1n6D1bpaPCiNiklIdBJXXF9qfES** **MY4DauvLACxGaTeIqmXbKx/y/8Ba4usNQ==** </pareqFieldValue> <termUrlName>**TermUrl**</termUrlName> <termUrlValue> </termUrlValue> <mdFieldName>**MD**</mdFieldName> <mdFieldValue>**1Fz9nEnAZJNn8NvXEKDT**</mdFieldValue> </verifyEnrollmentResponse>

Une fois le verifyEnrollment réalisé, l'authentification auprès du serveur ACS doit être effectuée. Pour cela, il est nécessaire d'envoyer les informations du verifyEnrollment sur le serveur d'authentification.

Envoi des informations

Pour envoyer ces informations :

- en POST alors créer un formulaire HTML.
- en GET alors constuire.

POST : Les informations seront envoyées au serveur d'authentification à travers le formulaire ci-dessous.
Les noms des champs et des valeurs sont récupérés dynamiquement du verifyEnrollmentResponse :

- Suivi de la session :
  - mdFieldName = **MD**
  - mdFieldValue = **1Fz9nEnAZJNn8NvXEKDT**

- Valeur de la requête d'authentification :
  - pareqFieldName = **PaReq**
  - pareqFieldValue = **eJxVkdtuwjAMhl+l4gGaA...**

- Adresse su rlaquelle l'acheteur est redirigé al a fin de l'authentification. Le Pares sera rajouté a la fin de cette URL :
  - termUrlName = **TermUrl**
    termUrlValue = **http://demoShop/3DSecure/receive_form.php**

- Adresse du serveur d'authentification : cette adresse doit récupérer un formulaire envoyé en POST.
  - actionUrl = **https://acs.banque.com/mdpayacs/pareq**

Exemple de formulaire HTML pour réaliser un test sur votre serveur :

Formulaire HTML

```
<form name="downloadForm" action="https://acs.banque.com/mdpayacs/pareq" method="POST">

<input type="hidden" name="TermUrl" value="http://demoShop/3DSecure/receive_form.php">
PAREQ : <input type="text" name="PaReq">
<br />
MD : <input type="text" name="MD">
<br />
<input type="submit" name="submit" value="Submit">
</form>
```

Réception des informations retournées lors de l'authentification

Le serveur d'authentification envoi son message sur l'URL renseignée dans le paramètre TermURL (envoyé dans le formulaire précédent). Dans le formulaire de réponse, deux champs doivent être récupérés pour poursuivre la transaction en mode 3DSecure :

- Le champ **MD** : toujours le même champ permettant le suivi de la session
- le champ **PaRes** (Payer Authentication Response) : chaine de caractères cryptée contenant la réponse du serveur d'authentification. La valeur du champ PaRes va permettre de valider ou non la transaction comme une transaction 3DSecure.

Ces deux champs sont récupérés et permettent de compléter le doAuthorizationRequest en mode 3DSecure.

Exemple de script (ici écrit en PHP) permettant de récupérer la réponse à l'authentification :

Script PHP : receive_form.php

```
<?php
$pares = $_POST['PaRes'];
$md = $_POST['MD'];

echo "MD : ".$md."<br />PARES :
".$pares;
?>
```

Remarque : ce script doit être placé sur un serveur web démarré et dans un dossier correspondant à l'adresse envoyé via le champ TermURL.

Exemple : si le serveur est en local il est tout à fait possible de mettre comme valeur :
TermURL = *http://127.0.0.1/3DSecure/receive_form.php*

Etape 2 : doAuthorizathion avec les paramètres 3D Secure

L'appel web service de la méthode doAuthorization permet d'effectuer directement la transaction avec les paramètres 3DSecure.
Les paramètres renseignés : md / pares permettent de vérifier l'authentification et donc l'identité de l'utilisateur avant d'effectuer la transaction.

Si les paramètres sont corrects, la transaction est alors directement effectuée comme pour le doAuthorization classique.

doAuthorizationRequest	doAuthorizationResponse

```
<impl:doAuthorizationRequest>
<impl:payment>
<obj:amount>4150</obj:amount>
<obj:currency>978</obj:currency>
<obj:action>100</obj:action>
<obj:mode>CPT</obj:mode>
<obj:contractNumber>CB3DS</obj:contractNumber>
</impl:payment>
<impl:card>
<obj:number>4970105512345674</obj:number>
<obj:type>CB</obj:type>
<obj:expirationDate>0912</obj:expirationDate>
<obj:cvx>123</obj:cvx>
</impl:card>
<impl:order>
<obj:ref>REF023493</obj:ref>
<obj:country>FR</obj:country>
<obj:taxes>100</obj:taxes>
<obj:amount>1400</obj:amount>
<obj:currency>978</obj:currency>
<obj:date>28/01/2009 09:32</obj:date>
</impl:order>
<impl:buyer>
<obj:lastName>Dupond</obj:lastName>
<obj:firstName>Wilfried</obj:firstName>
<obj:email>wilfried.dupond@yahoo.fr</obj:email>
</impl:buyer>
<impl:authentication3DSecure>
<obj:md>xRtMifcy975D2EB3Zs8e</obj:md>
<obj:pares>
eJzFV2mTokoW/Ssd/T4a3ewKHZQq8LT8uWh9v0X8C9X
9dnSvZpwiZxtkQnR4/vcxQo0vM1a4/lI9R/BFjkEQryXL4
NU12Tb4MZVE1L1+PbVv/QJC+77/3xPfzNUWmgFEEZZ
k6R9fX0cle6U6nJcsH1bnKovDIruH7bTYMGmP5/2X9wl
2H14xxBT5b5PbbzFGVt8eCEo8aYT83umHcP/OLJ8Dvzb
YYYo8JPjlasmZySB7LnHxxTOXl6x8fSC1kadK0/86Mb7N
Dmzw2LW7JsXdOgDbKqGt0MWzXUzHgfeTiJHYyXt3GvIi

LP+N9W4D2XV0MrIQkUn+/iOLJrhOdX5t6je0MVLvrO6/
+UWyynOS9H7sYGAZ5U3lbmDcT3ZMMEcjDfJb20VXhTw

bWgWEOt2Ix04i1tmBAuFHx2aEgzgEtcaJzH8TLbsXbpj4r

.....
</obj:pares>
<obj:xid/>
<obj:eci/>
<obj:cavv/>
<obj:cavvAlgorithm/>
<obj:vadsResult/>
</impl:authentication3DSecure>
</impl:doAuthorizationRequest>
```

```
<doAuthorizationResponse>
<result>
<code>00000</code>
<shortMessage>ACCEPTED</shortMessage>
<longMessage>Transaction approved<
/longMessage>
</result>
<transaction>
<id>90217095220928</id>
<date>17/02/09 09:52</date>
<isDuplicated>0</isDuplicated>
<isPossibleFraud>0</isPossibleFraud>
<fraudResult/>
<explanation/>
<threeDSecure>Y</threeDSecure>
<score/>
</transaction>
<authorization>
<number>A55A</number>
<date>17/02/09 09:52</date>
</authorization>
</doAuthorizationResponse>
```


Centre administration

Menu 'Suivi technique des appels webservice' pour retrouver l'appel du web service verifyEnrollment permet de voir le détail du verifyEnrollment.

Le résultat de la transaction 3DSecure est alors visible dans le centre d'administration Payline : sur les résultats d'une recherche et dans le détail de la transaction onglet 3DSecure : écran recherche des transactions et Détail de la transaction 3DSecure.

Résultats de la recherche

Rappel des critères : Transactions d'aujourd'hui - ID commerçant : 35505904577638 (AFONE PAIEMENT) - Transactions acceptées - Transactions refusées - Carte 3DSecure

Total : 3/3 transaction(s)

ID	Ref cmd	Date trans	Montant	Type transaction	Retour	MdP	Point de Vente	Donnée porteur	3D
11204170250382	33812-00942	04/12/2012 17:02:50	1,00 EUR	Autorisation+Validation	00000	VISA	DEMO PAYLINE	497762XXXXXX3465	Oui
11204165852891	33812-00928	04/12/2012 16:58:52	5,00 EUR	Autorisation+Validation	00000	MASTERCARD	DEMO PAYLINE	513742XXXXXX8079	Oui
11204161425640	33812-00907	04/12/2012 16:14:25	1,00 EUR	Autorisation+Validation	00000	MASTERCARD	DEMO PAYLINE	513742XXXXXX8079	Oui

3DSecure

Transaction 3DSecure	**Oui (Commercant + Acheteur)**
Enrôlé	**Oui (Y)**
Authentifié	**Oui (Y)**
md	**juqFzcMSxrmCZkHuW7aJ**
xid	**anVxRnpjTVN4cm1DWmtIdVc3YUo=**
cryptogramme	**AAABA5eFhQAAAAACN4WFAAAAAAA=**
algo crypto	**2**
eci	**05**

Schéma du paiement 3D Secure

1. Le consommateur valide son panier afin que le marchand prépare la page web où seront renseignés les données de paiement.
   Un message « VEReq » (Verification enrollment request) permet l'accès au Directory Serveur afin de vérifier l'inscription de la carte dans l' annuaire contenant les cartes déclarées « enrôlées » 3-D Secure et de fournir l'URL de l'ACS correspondants.
   La réponse « VERes » (Verification enrollment response) contenant le résultat de l'authentification sera retourné au Merchand Plug-in (MPI) pour gérer le dialogue avec le Directory et l'ACS en vue de permettre à l'acheteur de s'authentifier.
2. Le commerçant redirige le consommateur sur l'URL de l'ACS pour l'authentification.
   La demande « PAReq » (Payer authentification request) permet l'accès à l'ACS de la banque du porteur pour déclencher la phase d' authentification.
   La réponse « PARes »(Payer authentification response), contenant le résultat de l'authentification du porteur de la carte sera transmis au commerçant.
3. Le commerçant peut déclencher une demande d'autorisation et de validation de paiement en appelant le service doAuthorizationRequest.
4. Le commerçant récupère les détails de la transaction en appelant le service getTransactionDetails.