DirectLink with 3-D Secure

ingenico
ePayments

Table des matières

1. 3-D Secure v1.0

1.1 Introduction

Le protocole 3-D Secure permet au porteur de carte d'être identifié lors du processus d'achat. Le porteur de carte doit absolument être connecté à l'internet pendant le processus d'identification. Le 3-D Secure ne fonctionne donc pas pour les centres d'appels (call centers) et les paiements récurrents.
Visa a implémenté le protocole 3-D Secure sous le nom "Verified By Visa", MasterCard sous le nom "SecureCode" et JCB sous le nom "J-Secure".
Le principe même d'intégration du DirectLink avec 3-D Secure est d'initier un paiement en mode DirectLink et de le finaliser en mode e-Commerce lorsqu'une authentification du porteur de carte est requise.

1.2 Flux de Transaction 3-D via via DirectLink

Le flux de transaction inclut les étapes suivantes:

1. Vous nous envoyez une requête DirectLink pour la transaction, contenant un certain nombre de paramètres additionnels (cf. Extra request parameters).
2. Notre système reçoit le numéro de carte dans votre requête et vérifie immédiatement en ligne si la carte est enregistrée dans le repertoire VISA/MasterCard/JCB (enregistré veut dire que l'identification est possible pour le numéro de carte, par exemple la carte est une carte 3-D Secure).
3. Si le porteur de carte est enregistré, la réponse à la requête DirectLink contient un statut de paiement spécifique et du code html qui doit être retourné au client pour que ce dernier puisse entamer le processus d'identification(cf. Additional return fields). Le bloc de code html démarrera automatiquement le processus d'identification entre le porteur de carte (client) et sa banque émettrice.
4. Le porteur de carte s'identifie sur la page de sa banque émettrice.
5. Notre système reçoit la réponse d'identification de la part de l'émetteur.
6. Si l'identification est réussie, notre système soumettra la transaction financière en elle-même à l'acquéreur.
7. Vous recevez le résultat de l'identification globale et du processus d'autorisation en ligne via des canaux de feedback en mode e-Commerce.

Commentaires :

- Si le porteur n'est pas enregistré (à l'étape 3), vous recevrez la réponse XML standard en DirectLink contenant le résultat du processus d'autorisation en ligne.
- Afin de recevoir les statuts/codes d'erreur exacts des paiements (à l'étape 7), vous devez implementer le feedback post-sale en ligne (online) ou hors connexion (offline) comme décrit dans le guide d'intégration e-Commerce documentation.

1.2.1 Paramètres de requête additionnels

En dehors des paramètres standards DirectLink, vous devez également envoyer les informations suivantes:

Paramètre	Explication
FLAG3D	Valeur Fixe: 'Y'; Indique à notre système d'exécuter une identification 3-D Secure si nécessaire.
HTTP_ACCEPT	Le champ en header "Accept request" dans le navigateur du porteur de carte, utilisé pour spécifier certains médias qui sont acceptables pour la réponse. Cette valeur est utilisée par l'émetteur pour vérifier si le

Paramètre	Explication
	navigateur du porteur de carte est compatible avec le système d'identification de l'émetteur. Par exemple: Accept: */*
HTTP_USER_AGENT	Le champ en header "User-Agent request" dans le navigateur du porteur de carte, contenant des informations sur l'agent utilisateur de qui émane la requête. Cette valeur est utilisée par l'émetteur pour vérifier si le navigateur du porteur de carte est compatible avec le système d'identification de l'émetteur. Par exemple: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
WIN3DS	Manière de montrer la page d'identification au client. Valeurs possibles : • MAINW : montre la page d'identification dans la fenêtre principale (valeur par défaut). • POPUP: montre la page d'identification dans une nouvelle fenêtre venant d'apparaître (pop up) et retourne vers la fenêtre principale à la fin. • POPIX: montre la page d'identification dans une nouvelle fenêtre venant d'apparaître (pop up) et reste dans cette même fenêtre.
ACCEPTURL	URL de la page web à montrer au client lorsque le paiement est autorisé (ou en attente d'autorisation).
DECLINEURL	URL vers lequel le client est redirigé si le nombre maximal de tentatives d'autorisation échouées a été atteint (10 par défaut, mais peut être modifié dans la page d'information technique, onglet "Paramètres de transaction Globaux ", section "Tentatives de paiement multiples").
EXCEPTIONURL	URL de la page web à montrer au client lorsque le résultat du paiement est incertain.
PARAMPLUS	Champs utilisés pour les paramètres divers ainsi que leurs valeurs et qui doivent être retournés dans la requête post-sale ou la redirection finale.
COMPLUS	Champ utilisé pour soumettre un valeur qui doit être retournée dans la requête post-sale ou dans l'output.
LANGUAGE	Langue du client, par exemple: "en_US".
Optionnel	
TP	Afin de changer la disposition de la page "order_A3DS", vous pouvez envoyer un nom de template/url avec le paramètre.

Pour des details complémentaires sur ces champs, veuillez vous referrer au retour d'information sur la transaction.

1.2.2 Champs de retour additionnels

Si le porteur de carte n'est pas enregistré, la réponse <%DIRECTLINK%> habituelle est retournée. Si le porteur de carte est enregistré, les champs (additionnels) suivants seront retournés:

Paramètre	Explication
STATUS	Nouvelle valeur: "46" (en attente d'identification)
HTML_ANSWER	Code html encodé en BASE64 à ajouter à la page html retournée au client. Ce tag est ajouté comme enfant au tag XML global . Le champ HTML_Answer contient du code HTML qui doit être ajouté à la page html retournée vers le navigateur du client.

Paramètre	Explication
	Ce code chargera automatiquement la page d'identification de la banque émettrice dans une nouvelle fenêtre apparaissant dans la fenêtre principale, en fonction de la valeur du paramètre WIN3DS. Afin d'éviter toute interférence entre les tags html inclus dans le contenu du tag HTML_ANSWER XML et le reste de l'XML retourné comme réponse à la requête <%DIRECTLINK%>, le contenu du champ HTML_ANSWER est encodé en BASE64 par notre système avant que nous retournions la réponse. Par conséquent, celui-ci doit être decodé (du BASE64) avant d'être inclus dans la page html envoyée vers le porteur de carte.

1.2.3 Commentaires

Cartes de Test

Vous pouvez utiliser les cartes de test suivantes pour simuler une carte enregistrée 3-D Secure dans notre environnement de test :

Type de carte	Numéro de carte	Date d'expiration	Mot de passe
VISA	4000000000000002	N'importe quelle date dans le futur	11111
MasterCard	5300000000000006	N'importe quelle date dans le futur	11111
American Express	371449635311004	N'importe quelle date dans le futur	11111

Identification incorrecte

Si une transaction est bloquée par une identification incorrecte, le résultat de la transaction sera :

STATUS = 0

NCSTATUS = 5

NCERROR = 40001134

2. 3-D Secure v2.1 (Disponible en TEST)

2.1 Introduction

En 2013, la Commission européenne a publié une proposition de version révisée de la Directive sur les services de paiement, connue sous le nom de DSP2 (DSP2 en anglais), afin de simplifier le traitement des paiements et de créer les règles et réglementations pour les services de paiement dans l'UE. C'est pourquoi il a fallu créer une nouvelle version de 3-D Secure, la v2.1.

Le changement le plus important est qu'en tant que marchand, vous devez partager plus de données : les émetteurs sont avides de points de données pour améliorer la précision de leur décision, ce qui entraînera finalement un paiement sans problème, mais c'est vous qui collectez les données en première ligne. La méthode d'évaluation des risques de 3DS v2 est plus efficace, mais nécessite une changement de l'ensemble de l'écosystème, ce qui vous permettra de transmettre les données vers l'émetteur.

Avec l'introduction de la nouvelle directive, les principaux card schemes disposent de nouveaux logos pour la version 2 du 3DS. Comme vous avez développé votre propre page de paiement, nous vous conseillons de la mettre à jour avec ces nouveaux logos (Visa / Mastercard / JCB /...).

2.2 Flux de Transaction 3-D via DirectLink

Le flux de transaction implique les étapes suivantes :

1.Vous nous envoyez une demande DirectLink pour la transaction, qui contient un certain nombre de paramètres supplémentaires. Ces paramètres peuvent être répartis en trois groupes :

a. Paramètres obligatoires devant être saisis dans la page de paiement où le titulaire de carte entre les détails de la carte.

Paramètre	Description	Format	Obligatoire
browserAcceptHeader	Contenu exact de l'en-tête d'acceptation HTTP tel qu'il a été envoyé au marchand par le navigateur du titulaire de carte. *	Type de données : Chaîne Longueur : Variable, au maximum 2048 caractères Valeur acceptée : Si la longueur totale de l'en-tête d'acceptation envoyé par le navigateur est supérieure à 2 048 caractères, le serveur 3DS tronque la partie excédentaire.	Oui
browserColorDepth	Valeur représentant la profondeur de bits de la palette de couleurs pour l'affichage des images, en bits par pixel. Obtenue auprès du navigateur du titulaire de carte à l'aide des propriétés de profondeur des couleurs.	Type de données : Chaîne Valeurs acceptées : 1 = 1 bit 4 = 4 bits 8 = 8 bits 15 = 15 bits 16 = 16 bits 24 = 24 bits 32 = 32 bits 48 = 48 bits	Oui
browserJavaEnabled	Opérateur booléen qui représente la capacité du navigateur du titulaire de carte à exécuter Java. La valeur est fournie par les	Type de données : Opérateur booléen Valeurs acceptées : vrai	Oui

Paramètre	Description	Format	Obligatoire
	propriétés du navigateur compatible avec Java.	faux	
browserLanguage	Valeur représentant la langue du navigateur telle que définie dans le standard IETF BCP47. Fourni par les propriétés de langue du navigateur.	Type de données : Chaîne Longueur: Variable, 1 à 8 caractères	Oui
browserScreenHeight	Hauteur totale de l'écran du titulaire de carte en pixels. La valeur est fournie par les propriétés de hauteur d'écran du navigateur.	Type de données : int Contre 0 et 9999	Oui
browserScreenWidth	Largeur totale de l'écran du titulaire de carte en pixels. La valeur est fournie par les propriétés de largeur d'écran du navigateur.	Type de données : int Contre 0 et 9999	Oui
browserTimeZone	Décalage horaire entre l'heure UTC (temps universel coordonné) et l'heure locale du navigateur du titulaire de carte, en minutes.	Type de données : int Contre -720 et 840	Oui
browserUserAgent	Contenu exact de l'en-tête d'agent utilisateur HTTP. *	Longueur : Variable, au maximum 2048 caractères Type de données: Chaîne Remarque : Si la longueur totale de l'agent utilisateur envoyé par le navigateur est supérieure à 2 048 caractères, le serveur 3DS tronque la partie excédentaire.	Oui

*Il est inutile d'envoyer HTTP_ACCEPT et HTTP_USER_AGENT avec browserAcceptHeader et browserUserAgent, nous utiliserons les paramètres du navigateur.

Remarque: N'oubliez pas de calculer les paramètres dans votre signature SHA.

Veuillez trouver ci-dessous un exemple de javascript, afin de collecter ces paramètres.

```
<script type="text/javascript" language="javascript">

function createHiddenInput(form, name, value)
{
var input = document.createElement("input");
input.setAttribute("type", "hidden");
input.setAttribute("name", name);
input.setAttribute("value", value);
form.appendChild(input);
}

var myCCForms = document.getElementsByName("MyForm");
if (myCCForms != null && myCCForms.length > 0)
{
```

```
var myCCForm = myCCForms[0];
createHiddenInput(myCCForm, "browserColorDepth", screen.colorDepth);
createHiddenInput(myCCForm, "browserJavaEnabled", navigator.javaEnabled());
createHiddenInput(myCCForm, "browserLanguage", navigator.language);
createHiddenInput(myCCForm, "browserScreenHeight", screen.height);
createHiddenInput(myCCForm, "browserScreenWidth", screen.width);
createHiddenInput(myCCForm, "browserTimeZone", new Date().getTimezoneOffset());
}
</script>
```

b. Paramètres supplémentaires requis (cf. Paramètres de requête additionnels)

c. Paramètres optionnels, mais recommandés (liste de paramètres) qui, s'ils sont envoyés, auront un impact positif sur les taux de conversion des transactions. Sur la base des informations contenues dans ces paramètres, un flux d'identification sans problème potentiel peut avoir lieu. Le titulaire de carte ne devra plus s'identifier et, par conséquent, la finalisation des transactions devrait être plus rapide. Par contre, si aucun de ces paramètres n'est fourni, il sera redirigé vers l'authentification normale.

Notre système reçoît le numéro de carte dans votre requête et vérifie immédiatement en ligne si la carte est enregistrée dans le repertoire VISA/MasterCard/JCB (enregistré veut dire que l'identification est possible pour le numéro de carte, par exemple la carte est une carte 3-D Secure)

2. Sur la base de la réponse du répertoire du système, si le titulaire de carte est enregistré au 3-D Secure, deux flux potentiels sont prévus, en fonction de la fourniture ou non des paramètres supplémentaires mentionnés au point **1.c (Paramètres optionnels, mais recommandés: liste de paramètres) ci-dessus**

2.1. Un flux sans problème : Le titulaire de carte est authentifié avec succès et ne doit pas effectuer de procédure supplémentaire. L'étape 3 est donc réalisée.

2.2. Un flux avec processus d'identification : Le titulaire de carte doit s'identifier de façon plus précise.

i. La réponse à la demande DirectLink contient un statut de paiement spécifique et un code html qui a été renvoyé au client pour commencer le processus d'identification (cf. champs supplémentaires renvoyés). Le bloc de code html commencera automatiquement le processus d'identification entre le titulaire de carte (client) et sa banque émettrice.

ii. Le porteur de carte s'identifie sur la page de sa banque émettrice.

iii. Notre système reçoît la réponse d'identification de la part de l'émetteur.

iv. Si l'identification est réussie, notre système soumettra la transaction financière en elle-même à l'acquéreur.

3. Vous recevez le résultat de l'identification globale et du processus d'autorisation en ligne via des canaux de feedback en mode e-Commerce.

2.2.1 Paramètres de requête additionnels

En dehors des paramètres standards DirectLink, vous devez également envoyer les informations suivantes:

Paramètre	Explication
FLAG3D	Valeur Fixe: 'Y'; Indique à notre système d'exécuter une identification 3-D Secure si nécessaire.

Paramètre	Explication
HTTP_ACCEPT	Le champ en header “Accept request” dans le navigateur du porteur de carte, utilisé pour spécifier certains médias qui sont acceptables pour la réponse. Cette valeur est utilisée par l’émetteur pour vérifier si le navigateur du porteur de carte est compatible avec le système d’identification de l’émetteur. * Par exemple: Accept: */*
HTTP_USER_AGENT	Le champ en header “User-Agent request” dans le navigateur du porteur de carte, contenant des informations sur l’agent utilisateur de qui émane la requête. Cette valeur est utilisée par l’émetteur pour vérifier si le navigateur du porteur de carte est compatible avec le système d’identification de l’émetteur. * Par exemple: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
WIN3DS	Manière de montrer la page d’identification au client. Valeurs possibles : • MAINW : montre la page d’identification dans la fenêtre principale (valeur par défaut). • POPUP: montre la page d’identification dans une nouvelle fenêtre venant d’apparaître (pop up) et retourne vers la fenêtre principale à la fin. • POPIX: montre la page d’identification dans une nouvelle fenêtre venant d’apparaître (pop up) et reste dans cette même fenêtre.
ACCEPTURL	URL de la page web à montrer au client lorsque le paiement est autorisé (ou en attente d’autorisation).
DECLINEURL	URL vers lequel le client est redirigé si le nombre maximal de tentatives d’autorisation échouées a été atteint (10 par défaut, mais peut être modifié dans la page d’information technique, onglet "Paramètres de transaction Globaux ", section "Tentatives de paiement multiples").
EXCEPTIONURL	URL de la page web à montrer au client lorsque le résultat du paiement est incertain.
PARAMPLUS	Champs utilisés pour les paramètres divers ainsi que leurs valeurs et qui doivent être retournés dans la requête post-sale ou la redirection finale.
COMPLUS	Champ utilisé pour soumettre un valeur qui doit être retournée dans la requête post-sale ou dans l’output.
LANGUAGE	Langue du client, par exemple: “en_US”.
Optionnel	
TP	Afin de changer la disposition de la page "order_A3DS", vous pouvez envoyer un nom de template/url avec le paramètre.

*Il est inutile d'envoyer HTTP_ACCEPT et HTTP_USER_AGENT si browserAcceptHeader et browserUserAgent sont utilisés.

Pour des details complémentaires sur ces champs, veuillez vous referrer au retour d'information sur la transaction.

2.2.2 Champs de retour additionnels

Si le porteur de carte n’est pas enregistré, la réponse <%DIRECTLINK%> habituelle est retournée. Si le porteur de carte est enregistré, les champs (additionnels) suivants seront retournés:

Paramètre	Explication
STATUS	Nouvelle valeur: “46” (en attente d’identification)

Paramètre	Explication
HTML_ANSWER	Code html encodé en BASE64 à ajouter à la page html retournée au client. Ce tag est ajouté comme enfant au tag XML global . Le champ HTML_Answer contient du code HTML qui doit être ajouté à la page html retournée vers le navigateur du client. Ce code chargera automatiquement la page d'identification de la banque émettrice dans une nouvelle fenêtre apparaissant dans la fenêtre principale, en fonction de la valeur du paramètre WIN3DS. Afin d'éviter toute interférence entre les tags html inclus dans le contenu du tag HTML_ANSWER XML et le reste de l'XML retourné comme réponse à la requête <%DIRECTLINK%>, le contenu du champ HTML_ANSWER est encodé en BASE64 par notre système avant que nous retournions la réponse. Par conséquent, celui-ci doit être decodé (du BASE64) avant d'être inclus dans la page html envoyée vers le porteur de carte.

2.2.3 Commentaires

Cartes de Test

Vous pouvez utiliser la carte de test suivante pour simuler une carte enregistrée 3-D Secure dans notre environnement de test :

Flux sans problème Type de carte	Numéro de carte	Date d'expiration
VISA	4186455175836497	N'importe quelle date dans le futur
Mastercard	5137009801943438	N'importe quelle date dans le futur
American Express	375418081197346	N'importe quelle date dans le futur

Flux avec processus d'identification Type de carte	Numéro de carte	Date d'expiration
VISA	4874970686672022	N'importe quelle date dans le futur
Mastercard	5130257474533310	N'importe quelle date dans le futur
American Express	379764422997381	N'importe quelle date dans le futur

Remarque: Plus de numéros de cartes de test peuvent être téléchargés ici.

Identification incorrecte

Si une transaction est bloquée par une identification incorrecte, le résultat de la transaction sera :

STATUS = 0

NCSTATUS = 5

NCERROR = 40001134

2.3 Exclusions et exceptions pour 3DSv2

2.3.1 3DSv2 et exclusions

Avec l'introduction de 3DSv2, l'authentification du titulaire de la carte sera obligatoire, tel que défini par la Directive sur les services de paiement 2 (2015/2366 - DSP 2) de l'UE Néanmoins, certaines transactions sont exclues de cette règle si l'un des cas suivants s'applique :

- Commande mail / commande téléphonique (MOTO)
- Le PSP du marchant (aussi appelé l'acquéreur) ou le PSP de l'acheteur (aussi appelé le fournisseur de méthode de paiement de l'acheteur) est hors de la zone EEE.
- Les cartes de paiement anonymes avec une valeur maximale de 150 € (article 63)
- MIT - Transactions Initiées par le Marchant

2.3.2 Flux frictionless/avec identification pour la SCA et 3DS

Ce nouveau règlement traite notamment du concept d'authentification forte du client (soit SCA pour « Strong Customer Authentication ») . Ce processus suggère que l'émetteur (la banque du titulaire de la carte) demande au titulaire de la carte des informations supplémentaires. Dans ce cas, le processus d'authentification aboutira à un flux avec identification (exigeant que le titulaire de la carte s'authentifie de manière active) plutôt qu'un flux frictionless (n'exigeant aucune authentification de la part du titulaire de la carte).

En revanche, nous offrons à nos commerçants la possibilité d'indiquer le flux qu'ils préfèrent. À ces fins, des paramètres supplémentaires seront envoyés afin que l'émetteur puisse procéder à une évaluation des risques. En fonction de la décision de l'émetteur, un flux frictionless peut avoir lieu. Dans certains cas, le système 3DS peut même être ignoré si des exceptions particulières s'appliquent.

2.3.3 Indication du flux préféré

Pour indiquer sa préférence pour un flux frictionless au cours de la demande d'authentification, le commerçant peut envoyer le paramètre supplémentaire Mpi.threeDSRequestorChallengeIndicator. En fonction de l'évaluation du risque de fraude effectuée par le commerçant, des valeurs particulières peuvent être envoyées (soit 02 pour l'évaluation d'un risque faible et 03 pour l'évaluation d'un risque élevé).

Paramètre	Valeurs	Obligatoire/Facultatif
Mpi.threeDSRequestorChallengeIndicator	01 = aucune préférence 02 = aucun processus d'identification requis 03 = processus d'identification requis : en fonction de la préférence du marchand 04 = processus d'identification requis : Mandat	Obligatoire (si vous souhaitez un flux spécifique)

Le commerçant peut ensuite déterminer si le flux frictionless/taux de conversion est approprié en envoyant davantage de champs facultatifs.

2.3.4 Exceptions pour 3DS

Pour certaines transactions, le commerçant peut ignorer le système 3DS (aboutissant à un flux frictionless) et les autoriser directement. Ce processus est limité aux transactions qui sont exclues de la SCA (tel que décrit ci-dessus) ou qui peuvent faire l'objet d'exceptions particulières. Ces exceptions doivent stipuler dans un accord conclu entre le commerçant et son acheteur. Dans ce cas, le commerçant doit préciser qu'il souhaite ignorer le processus d'authentification en envoyant ces paramètres supplémentaires :

Paramètres	Valeurs	Obligatoire/Facultatif

FLAG3DS	N = Ignorer le processus d'authentification 3DS	Obligatoire (dans le cas où 3DS est ignoré)
3DS_EXEMPTION_INDICATOR	Justifier le choix motivant le souhait d'ignorer 3DS. Les valeurs numériques peuvent s'appliquer en fonction de la transaction 03 = ART* de l'émetteur 04 = Exception pour faible montant 05 = ART* du commerçant/de l'acheteur 06 = Liste blanche 07 = Entreprise 08 = Expédition retardée 09 = Authentification déléguée (portefeuille certifié)	Obligatoire (dans le cas où 3DS est ignoré)

* Analyse de risques de la transaction

En revanche, il appartient toujours à l'émetteur de choisir de mettre en place un processus d'authentification. Dans le cas où l'émetteur insiste pour utiliser 3DS, la transaction sera refusée.