Paramètres additionnels et liste noire

Prévention de la fraude
Guide d'intégration
Version 6.2.2
15/08/2018

Table des matières

- Informations générales sur les outils de prévention de la fraude
- Paramètres additionnels sur la prévention des fraudes
  - Paramètres additionnels pour appeler la plateforme de paiement pour les cartes
- Gestion de la liste noire
  - Paramètre BlackListInfo

Historique des versions

Date	Nom	Modification
15/08/2018	Peter Posse	Version originale

Informations générales sur les outils de prévention de la fraude

La plateforme de paiement prend en charge plusieurs processus pour la prévention de la fraude. Ces processus comprennent des enquêtes auprès des agences de crédit, la surveillance du pays d'origine de la carte et les garanties de paiement pour les cartes.

La plateforme de paiement peut vérifier le pays d'origine et, dans de nombreux cas, la ville où l'adresse IP est utilisée. Si le pays d'origine ou l'adresse IP de votre acheteur n'est pas celui de vos pays de livraison, ou s'il est différent de celui de l'émetteur de la carte, la plateforme de paiement peut envoyer un avertissement par e-mail ou refuser automatiquement le paiement.

La plateforme de paiement peut vérifier l'origine de la carte : si vous entrez le pays de livraison sous forme de paramètre, la plateforme de paiement retourne le pays d'origine des cartes Visa et Mastercard, puis envoie un e-mail si le pays de livraison diffère de celui d'origine de la carte. Vous pouvez alors demander à l'acheteur pourquoi le pays d'origine de la carte est différent du pays de livraison, cela afin d'éviter les fraudes. En option, la plateforme de paiement peut également refuser d'emblée de tels paiements.

Paramètres additionnels sur la prévention des fraudes

Formats des données :

a	alphabétique
as	alphabétique avec caractères spéciaux

n	numérique
an	alphanumérique
ans	alphanumérique avec caractères spéciaux
ns	numérique avec caractères spéciaux
bool	expression booléenne (true ou false)
3	longueur fixe avec 3 chiffres/caractères
..3	longueur variable avec maximum 3 chiffres/caractères
enum	énumération de valeurs admissibles
dttm	Date et heure ISO (AAAA-MM-JJThh:mm:ss)

Abréviations :

CND	condition
M	obligatoire (mandatory en anglais)
O	optionnel
C	conditionnel

Remarque : Veuillez noter que les noms des paramètres peuvent être en majuscules ou en minuscules.

Paramètres additionnels pour appeler la plateforme de paiement pour les cartes

La prévention des fraudes via traçage IP concerne les cartes VISA et Mastercard via les interfaces de la plateforme de paiement payssl.aspx et direct.aspx.

Pour l'intégration standard et d'autres paramètres pour effectuer un paiement via les interfaces payssl.aspx et direct.aspx, veuillez consulter le manuel cartes.

Remarque : Pour des raisons de sécurité, la plateforme de paiement rejette toutes les demandes de paiement contenant des erreurs de formatage. Veuillez, par conséquent, utiliser le type de données correct pour chaque paramètre.

Le tableau ci-dessous décrit les paramètres de demandes de paiements chiffrés :

Paramètre	Format	CND	Description
IPAddr	ans..15	O	Adresse IP. Si vous transférez l'adresse IP, la plateforme de paiement peut déterminer dans quel pays et dans quelle ville votre acheteur s'est connecté à Internet (voir aussi IPZone). Format : 123.456.789.012
IPZone	ans..1100	O	Codes des pays à partir desquels vous acceptez des paiements, codes numériques à 3 chiffres selon ISO 3166-1. Séparez plusieurs pays par des virgules : **036,040,124**. Si vous transmettez des pays dans **IPZone**, la plateforme de paiement vérifie le pays d'origine de l'adresse IP de votre acheteur, s'il se trouve dans votre liste de pays et s'il correspond au pays de la carte(voir ci-dessous). La plateforme de paiement transmet également le pays de l'IP à votre boutique (voir ci-dessous). Si le pays n'est pas dans votre liste ou s'il ne correspond pas à la carte, la plateforme de paiement peut envoyer un avertissement par e-mail ou refuser automatiquement le paiement. Pour refuser des pays particuliers (liste noire) introduisez un point d'exclamation devant le code du pays : !036,!040,!124.
Zone	ans..1100	O	Codes des pays dont vous acceptez les cartes, codes numériques à 3 chiffres ou alphanumériques selon ISO 3166-1. Séparez plusieurs pays par des virgules : 036,040,124. Si vous transmettez des pays dans Zone, la plateforme de paiement peut vérifier le pays d'origine de la carte de votre acheteur (Mastercard, Visa) et s'il est repris dans votre liste de pays approuvés. La plateforme de paiement transmet également le pays de la carte à votre boutique (voir ci-dessous). Si le pays de la carte n'est pas dans votre liste ou ne correspond pas à l'adresse IP de votre acheteur, la plateforme de paiement peut envoyer un avertissement par e-mail ou refuser les paiements. Pour refuser les cartes de pays particuliers (liste noire) introduisez un point d'exclamation devant le code du pays : !036,!040,!124. Veuillez noter que la longueur maximum est limitée à 1100 caractères.

Le tableau ci-dessous contient les paramètres utilisés par la plateforme de paiement dans la réponse :

Paramètre	Format	CND	Description
Zone	a..7	O	Si des codes de pays ont été introduits dans **Zone**, la plateforme de paiement renvoie le code de pays pour la carte ou « UNKNOWN »
IPZone	a..7	O	Si des IP de pays sont transmis dans **IPZone**, dans le cas d'une demande, la plateforme de paiement renvoie le code de pays ou « UNKNOWN »
IPZoneA2	a..7	O	Si **IPZone** est soumis dans le cadre de la demande, la plateforme de paiement renvoie le code de pays à deux caractères de l'adresse IP ou « UNKNOWN » (DE=Allemagne, FR=France etc.).
IPState	a..32	O	Si **IPZone** est soumis dans le cadre de la demande, la plateforme de paiement renvoie l'état fédéral dont l'adresse IP de votre client est originaire.
IPCity	a..32	O	Si **IPZone** est soumis dans le cadre de la demande, la plateforme de paiement renvoie la ville/localité dont l'adresse IP de votre client est originaire.
IPLongitude	n..20	O	Si **IPZone** est soumis dans le cadre de la demande, la plateforme de paiement renvoie la longitude (virgule flottante, décimal) du nœud de connexion (PoP) de votre client.
IPLatitude	n..20	O	Si **IPZone** est soumis dans le cadre de la demande, la plateforme de paiement renvoie la latitude (virgule flottante, décimal) du nœud de connexion (PoP) de votre client.
fsStatus	ans..9	OC	Uniquement via direct.aspx, uniquement via EVO Payments International : ACCEPT= aucun soupçon de fraude à la carte, DENY=refus recommandé, CHALLENGE=vérification recommandée, NOSCORE=AUCUNE analyse de risque, ENETFP=Erreur exceptionnelle dans le réseau, ERROR=Erreur au centre de traitement des données, ETMOUT=Timeout
fsCode	n4	OC	Uniquement via direct.aspx, uniquement via EVO Payments International : Action recommandée : <0000> pas de résultat, <0100> accepter, <0150> toujours accepter, <0200> refuser, <0250> toujours refuser, <0300> suspect, <0330> veuillez vérifier, <0400> suspect liste noire ReD, <0500> douteux, <0600> douteux liste noire ReD, <0700> seuil dépassé, <0800> utilisation anormale, <901> erreur interne ebitGuard, <902> erreur de format

Gestion de la liste noire

Pour créer, lire, mettre à jour ou supprimer une entrée de liste noire via une connexion serveur-à-serveur, appelez l'URL suivante :

https://paymentpage.axepta.bnpparibas/BlackList.aspx

Vous avez la possibilité de bloquer les transactions grâce au BIN du client (9 chiffres)

Remarque : Pour des raisons de sécurité, la plateforme de paiement rejette toutes les demandes de paiement contenant des erreurs de formatage. Veuillez par conséquent utiliser le type de données correct pour chaque paramètre.

Le tableau ci-dessous décrit les paramètres de demande de paiement chiffrés :

Paramètre	Format	CND	Description
MerchantID	ans..30	M	ID du commerçant. Ce paramètre doit également être transféré non chiffré.
MAC	an64	M	Code d'authentification de message haché (HMAC) avec algorithme SHA-256
EventToken	enum	M	Abréviation de l'action à effectuer : <Create>, <Read>, <Update> ou <Delete>
BlackListInfo	ans...1024	M	Information relative à l'entrée de liste noire en tant que chaîne de caractères JSON au format Base64. Voir table BlackListInfo ci-dessous.

Le tableau ci-dessous contient les paramètres utilisés par la plateforme de paiement dans la réponse :

Paramètre	Format	CND	Description
MID	ans..30	M	ID du commerçant
Status	a..30	M	OK ou FAILED
Description	ans..1024	C	Détails supplémentaires, si le statut=FAILED
BlackListInfo	ans..1024	C	Information relative à l'entrée de liste noire en tant que chaîne de caractères JSON au format Base64, si statut=OK. Voir table BlackListInfo ci-dessous.

Paramètre BlackListInfo

Le tableau suivant décrit l'objet BlackListInfo pour EventToken Insert :

Paramètre	Format	CND	Description
Category	enum	M	Catégorie <EDD> pour débit direct <CC> pour carte
Number	ans..64	M	IBAN, si Category=EDD Numéro de carte, si Category=CC
BIC	ans..32	C	BIC, si Category=EDD

Le tableau suivant décrit l'objet BlackListInfo pour EventToken Insert :

Paramètre	Format	CND	Description
BlockID	an..32	M	BlockID unique
LockActive	bool	M	Définit si l'entrée doit être ou non bloquée. Bloqué : <True> Déverrouillé : <False>

Le tableau suivant décrit l'objet BlackListInfo pour EventToken Update :

Paramètre	Format	CND	Description
BlockID	an..32	M	BlockID unique

Le tableau suivant décrit l'objet BlackListInfo avec lequel la plateforme de paiement répond :

Paramètre	Format	CND	Description
BlockID	an..32	M	BlockID unique
MID	ans..30	M	ID du commerçant
Category	enum	M	Catégorie <EDD> pour prélèvement automatique, <CC> pour carte
Number	ans..64	M	IBAN, si Category=EDD Numéro de carte, si Category=CC
BIC	ans..32	C	BIC, si Category=EDD
MAC	an64	M	Code d'authentification de message haché (HMAC) avec algorithme SHA-256
LockActive	bool	M	Définit si l'entrée doit être ou non bloquée. Bloqué : <True> Déverrouillé : <False>
Created	dttm	M	Moment de la création (AAAA-MM-JJ hh:mm:ss)
Changed	dttm	M	Moment de la modification (AAAA-MM-JJ hh:mm:ss)