Authentification HMAC

Pour vous protéger de toute manipulation non autorisée de vos transactions de paiement, AXEPTA BNP Paribas vérifie si votre requête de paiement est authentique grâce à l'authentification HMAC (Hash Message Authentication Code).

Vous devrez donc transférer une valeur HMAC à la plateforme de paiement pour chaque transaction dans le paramètre MAC.

La plateforme de paiement utilise un code HMAC (Hash Message Authentication Code) pour vérifier l'authenticité de vos paiements. L'algorithme MAC SHA-256 est utilisé avec une clé de 32 chiffres (256 bits). Un mot de passe supplémentaire renforce la sécurité de la procédure HMAC.

Le tableau suivant décrit la méthode de génération des valeurs Hash pour votre paiement :

Étape	Tâche
1	Récupérer le mot de passe Hash parmi les données d'accès envoyés par l'assistance technique.
2	La valeur HMAC est calculée grâce au mot de passe et à différentes valeurs de paramétrage. Pour le calcul, les paramètres PayID (Identifiant du paiement), TransID (Identifiant de la transaction), MerchantID (Identifiant du marchand), Amount (Montant) et Currency (Devise) sont utilisés et séparés par des astérisques : PayID*TransID*MerchantID*Amount*Currency Remarque : si une transaction ne prend pas en charge tous ces paramètres, vous pouvez tout simplement omettre la valeur manquante. Par exemple, la première transaction (ci-dessous exemple 1) ne comprend pas le paramètre PayID (Identifiant de paiement). Vous n'avez donc pas à le transférer. L'identifiant du paiement (PayID) est un composant du calcul Hash dans les transactions (exemple 2 et 3): Exemple 1, sans identifiant de paiement PayID (ex. lors de l'autorisation) : *B456Ref890*YourMerchantID*9 900*EUR Exemple 2, avec identifiant de paiement PayID (ex. lors de la capture) : 1237890*B456Ref890*YourMerchantID*9 900*EUR Exemple 3, sans identifiant TransID : 1237890**YourMerchantID*9 900*EUR
3	Utilisez l'algorithme MAC SHA-256, pris en charge par la grande majorité des langages de programmation, afin de calculer la valeur Hash avec le mot de passe et les valeurs de paramétrage.
4	Utilisez le paramètre Mac pour transférer la valeur Hash avec encodage en hexadécimal à la plateforme de paiement avec chaque transaction dans le champ de données encodées.

Remarque : Si le paramètre MAC a été transféré avec la première transaction (demande d'autorisation), il est obligatoire pour toutes les transactions suivantes (ex. capture, remboursement... etc).

Important : la plateforme de paiement rejette immédiatement les transactions avec des valeurs HMAC erronées ou manquantes sans autre traitement, car il s'agit probablement d'un piratage. Par conséquent, les transactions que la plateforme de paiement rejette avec les codes d'erreur 20100044 ou 20120044 n'apparaissent pas dans le backoffice BNP Paribas.

Exemples de codes HMAC (Hash Message Authentication Code)

```
Request without PayID:
MerchantID=YourMerchantID&TransID=100000001&Amount=11&Currency=EUR&URLSuccess=htt
ps://www.shop.de/ok.html&URLFailure=https://www.shop.de/failed.html&OrderDesc=My
purchase

String for MAC generation:
*100000001*Test*11*EUR
Request with MAC:
MerchantID=YourMerchantID&TransID=100000001&Amount=11&Currency=EUR&URLSuccess=htt
ps://www.shop.de/ok.html&URLFailure=https://www.shop.de/failed.html&OrderDesc=My
purchase&MAC=A0E3A8BB9473CF4D3F91181E0859650A9AF3F4AD0AE1E839AC7B750247A2E947

Request without TransID:
MerchantID=YourMerchantID&PayID=8ee4e922c39446ac9ee66095a4a4b475&Amount=100&Curre
ncy=USD

String for MAC generation:
8ee4e922c39446ac9ee66095a4a4b475**Test*100*USD

Request with MAC:
MerchantID=YourMerchantID&PayID=8ee4e922c39446ac9ee66095a4a4b475&Amount=100&Curre
ncy=USD&MAC=F1EB4A8BB9473CF4D3F91181F0859659A9AF3F4AD0AE1E839AC7B750247A2D636
```

Le site Web du marchand doit vérifier que la notification de paiement provient réellement de BNP Paribas. En effet, un fraudeur peut initialiser une transaction et falsifier cette notification. Par conséquent, le système du marchand doit le faire automatiquement.
Actuellement, la requête de notification est uniquement chiffrée. Toutefois, ce chiffrement ne garantit pas l'authenticité d'un message. Cela garantit uniquement qu'un message ne peut pas être écouté. Il est donc impératif pour le marchand d'utiliser le paramètre de réponse MAC, basé sur le même algorithme de saisie MAC (seuls les paramètres de données seront différents).

Le schéma de données suivant s'applique ici pour la génération du code Hash :
PayID*TransID*MerchantID*Status*Code
Le paramètre MAC est uniquement retourné à l'URL Success (Réussite) ou Failure (Échec), et Notify (Notifier).