

Return codes - 3DS (03) - Additional Information

Restitution du "Cardholder Information Text" : Enrichissement des messages de refus 3D Secure

Dorénavant, les émetteurs et les serveurs d'authentification (ACS) peuvent éventuellement fournir des informations au titulaire de la carte lors d'un refus dans le traitement d'authentification 3D Secure.

Par exemple, "Une authentification supplémentaire est nécessaire pour cette transaction, veuillez contacter XXXX à XXX" avec le nom et le téléphone. Cette information sera affichée et elle ne sera pas enregistrée. Monext Online complète le longMessage existant en rajoutant l'information cardHolderMsg fourni.

Le message sera affiché sur le "ticket de non paiement" en cas de refus.

En mode direct : le web service [verifyEnrollmentResponse](#) peut être complété lors d'un refus d'authentification.

```
<obj:code>03009</obj:code>
<obj:shortMessage>ERROR</obj:shortMessage>
<obj:longMessage>3DS technical error - Your card does not have a password setup in our system. Please contact your customer service.`</obj:longMessage>
```

En mode web : le service [getWebPaymentDetailsResponse](#) peut être complété lors d'un refus d'authentification.

```
<obj:code>03022</obj:code>
<obj:shortMessage>CANCELLED</obj:shortMessage>
<obj:longMessage>Authentication verification failed - Your card does not have a password setup in our system. Please contact your customer service.`</obj:longMessage>
```

Ces codes concernant le traitement du 3D-Secure.

Code retour	Plus d'informations
03000	Ce code est reçu en réponse d'une authentification EnrollmentRequest() avec données 3DS acceptées (transStatus='Y').
03003	Lors d'une demande EnrollmentRequest(initial), ce code est retourné lors d'une authentification de type Challenge. Code indique : • soit le contrat n'est pas correctement enrôlé 3D-Secure, • soit les cartes ne sont pas enrôlées 3D-Secure V2.
03004	Lors de l'authentification 3DS, une redirection vers le serveur d'authentification de l'ACS de la banque de l'acheteur reste sans réponse : un refus est donc émis.
03009	Les opérations avec un enrôlement 3DS en échec avec ce code retour et avec un transStatus à X indique une indisponibilité sur l'ACS de la banque.
03010	Problème technique : en générale le champ avec l'erreur est retournée dans le message. Il est souvent lié à un problème de format ou de longueur. Exemple : Invalid input: Length of TDS2.merchantName is too long (40 lt 54)
03011	Il est restitué en réponse des appels webService (verifyEnrollement, doWebPayment, doAuthorisation, doImmediateWalletPayment...) lorsque dans les données 3DS récupérées du MPI le CAVV est masqué, c'est à dire quand le traitement a mis trop de temps pour les récupérer ou qu'elles ont déjà été récupérées. L'authentification/le paiement sera refusé. Le commerçant doit demander de réaliser un nouveau paiement afin de réaliser une nouvelle authentification.
03012	Le service bancaire d'authentification (ACS/DS) est indisponible.
03021	Ce code indique un problème d'enrôlement 3DS et il est lié à une mauvaise saisie des données de paiements.

03022	Ce code indique que l'authentification de l'acheteur a échoué. Le système bancaire demande une vérification sur le téléphone mobile de l'acheteur et il doit s'authentifier avec l'application de sa banque. Cette demande d'authentification est une obligation d'une directive européenne sur les services de paiement en vigueur dans l'union européenne. La transaction n'a jamais abouti et l'acheteur n'a jamais été débité. Vous pouvez consulter la valeur retournée dans le détail de la transaction dans le bloc 3D Secure : le champ Authentifié (Authenticated) • Y - Authentification ou vérification réalisée avec succès. • N - Pas d'authentification ou de vérification . La transaction est refusée. => l'acheteur n'a pas réussi à s'authentifier. • U - Authentification ou vérification n'a pas pu être réalisée. Problème technique. • A - Authentification ou vérification a été réalisé sans succès. • C - Demande d'authentification obligatoire. • R - Authentification ou vérification du compte rejeté par la banque de l'acheteur. => la banque de l'acheteur a refusé l'authentification. • X - Délai d'authentification dépassée. • I - Transaction authentifiée suite à une exemption de la banque du commerçant (TRA). Vous pouvez également consulter la valeur du champ trans Status Reason qui vous apportera des informations supplémentaires : Codes - transStatusReason Sur l'environnement de test, il se peut que le simulateur ACS soit indisponible. Généralement, l'acheteur réalise un nouveau paiement de sa commande pour que l'authentification soit réalisée avec succès.
03102	Authentification acceptée en Frictionless (authentification sans interaction). La demande d'autorisation est doit être réalisée.
03104	Challenge accepté lors d'une demande d'authentification avec le SDK Mobile du commerçant : Monext Online intègre les informations dans la demande d'autorisation.