

# NETBANX®

Part of OPTIMAL PAYMENTS™

Translation Di

## Implémentation de 3D Secure avec NETBANX

Juillet 2011

Le présent manuel et le support électronique qui l'accompagne sont des produits exclusifs d'Optimal Payments, S.A.R.L. Leur usage est réservé aux utilisateurs autorisés du produit.

© 1999-2011 Optimal Payments, S.A.R.L. Tous droits réservés.

Les renseignements que contient le présent document sont susceptibles d'être modifiés sans préavis. Le logiciel décrit dans le présent document est fourni sous licence et ne peut être utilisé ou copié que conformément aux conditions du contrat de licence. Aucune partie du présent manuel ne peut être reproduite ni transférée sous quelque forme que ce soit ou par quelque moyen que ce soit sans le consentement écrit explicite d'Optimal Payments, S.A.R.L.

Les autres noms, marques de commerce et marques déposées appartiennent à leur propriétaire respectif.

Optimal Payments, S.A.R.L. n'offre aucune garantie explicite ou implicite concernant ce produit, sa qualité marchande ou son adéquation à un usage particulier autre que les garanties explicitement décrites dans le contrat de licence du produit. Pour obtenir de plus amples renseignements à ce sujet, veuillez communiquer avec Optimal Payments, S.A.R.L.

## **Siège social international**

3500, boulevard de Maisonneuve Ouest, bureau 700

Montréal (Québec) H3Z 3C1

Canada

Tél. : (514) 380-2700

Télec. : (514) 380-2760

Courriel : [info@optimalpayments.com](mailto:info@optimalpayments.com)

Soutien technique : [support@optimalpayments.com](mailto:support@optimalpayments.com)

Site Web : [www.optimalpayments.com](http://www.optimalpayments.com)

## **Bureau du Royaume-Uni**

Third Floor, Mount Pleasant House

Mount Pleasant

Cambridge CB3 0RN

Royaume-Uni

Courriel : [info@optimalpayments.co.uk](mailto:info@optimalpayments.co.uk)

Soutien technique : [support@optimalpayments.co.uk](mailto:support@optimalpayments.co.uk)

Site Web : [www.optimalpayments.co.uk](http://www.optimalpayments.co.uk)

## **Bureau des États-Unis**

1209 Orange Street

Wilmington, DE 19801

## **Bureau de Gatineau**

75, Promenade du Portage

Gatineau (Québec) J8X 2J9

Canada

Translation Draft

# Contenu

---

Aperçu . . . . .	1
Terminologie . . . . .	1
Avantages pour le marchand. . . . .	1
Fonctionnement de 3D Secure . . . . .	2
Meilleures pratiques pour les marchands . . . . .	6
Affichage de l'information et des logos de 3D Secure . . . . .	6
Message de préauthentification. . . . .	6
Affichage de l'URL de l'ACS . . . . .	7
Séquence de délai d'inactivité . . . . .	7
Affichage de messages à l'intention du client. . . . .	8
Conseils généraux. . . . .	8
Adresses URL importantes . . . . .	8
Si vous avez besoin d'aide.... . . . .	8
Valeurs de réponse aux messages d'authentification et de consultation . . . . .	8
Valeurs de réponse Consultation pour l'authentification du payeur . . . . .	9
Valeurs de réponse Authentification pour l'authentification du payeur . . . . .	9
Scénarios de test. . . . .	10
Scénarios de test Vérifié par Visa. . . . .	10
Scénario de test VPV 1 . . . . .	10
Scénario de test VPV 2 . . . . .	11
Scénario de test VPV 3 . . . . .	11
Scénario de test VPV 4 . . . . .	12
Scénario de test VPV 5 . . . . .	12
Scénario de test VPV 6 . . . . .	13
Scénario de test VPV 7 . . . . .	13
Scénario de test VPV 8 . . . . .	14
Scénario de test VPV 9 . . . . .	14
Scénario de test VPV 10 . . . . .	14
Scénario de test VPV 11 . . . . .	15
Scénarios de test MasterCard SecureCode . . . . .	15
Scénario de test MCSC 1 . . . . .	15
Scénario de test MCSC 2 . . . . .	16
Scénario de test MCSC 3 . . . . .	16
Scénario de test MCSC 4 . . . . .	17
Scénario de test MCSC 5 . . . . .	17
Scénario de test MCSC 6 . . . . .	18
Scénario de test MCSC 7 . . . . .	18
Scénario de test MCSC 8 . . . . .	19
Scénario de test MCSC 9 . . . . .	19
Scénario de test MCSC 10 . . . . .	19

Scénarios de test JCB J/Secure.....	20
Scénario de test J/Secure 1.....	20
Scénario de test J/Secure 2.....	21
Scénario de test J/Secure 3.....	21
Scénario de test J/Secure 4.....	22
Scénario de test J/Secure 5.....	22
Scénario de test J/Secure 6.....	22
Scénario de test J/Secure 7.....	23
Scénario de test J/Secure 8.....	23
Scénario de test J/Secure 9.....	24
Scénario de test J/Secure 10.....	24
Scénario de test J/Secure 11.....	24

Translation Draft

# Implémentation de 3D Secure avec NETBANX

---

## Aperçu

3D Secure est un programme d'authentification de titulaire de carte en ligne conçu pour rendre les transactions d'achat sur Internet plus sécuritaires par la confirmation de l'identité du titulaire au moment de l'achat et avant que le marchand soumette la demande d'autorisation. Le programme est actuellement compatible avec plusieurs types de cartes, notamment Visa (Vérfié par Visa), MasterCard (SecureCode) et JCB (J/Secure). Les autorisations traitées au moyen de 3D Secure sont garanties contre la plupart des types de litiges courants relativement à la rétrofacturation.

Si vous êtes déjà intégré à l'API de Services Web de NETBANX, l'implémentation de la fonction de sécurité 3D Secure est toute simple. Voici ce que vous avez à faire :

1. Envoyez une demande de *Consultation d'inscription* à NETBANX afin de vérifier si la carte de crédit de votre client est inscrite à 3D Secure.
2. NETBANX retournera une requête d'authentification de paiement (PaReq) et quelques autres valeurs en réponse à votre demande de *Consultation d'inscription*. Utilisez ces valeurs afin de permettre à votre client d'authentifier sa carte de crédit.
3. Une fois que votre client aura validé sa carte auprès de l'Émetteur de carte, vous recevrez les renseignements dont vous avez besoin afin d'envoyer une requête d'*Authentification* à NETBANX.

Consultez la rubrique *Fonctionnement de 3D Secure* à la page 2 pour obtenir un aperçu du processus 3D Secure.

## Terminologie

Voici quelques termes fréquemment utilisés en lien avec le processus 3D Secure.

- Système de traitement de l'authentification du marchand (MAPS) – un système tiers qui vérifie si le titulaire d'une carte de crédit est inscrit au programme 3D Secure.
- Système de contrôle de l'accès (ACS) – le serveur de l'institution financière émettrice fournissant la confirmation de l'inscription de la carte.
- Requête d'authentification de paiement (PaReq) – une requête envoyée à l'institution financière émettrice afin de permettre au titulaire de la carte de fournir un mot de passe pour authentifier la carte de crédit.
- Réponse d'authentification de paiement (PAREs) – la réponse à la requête PaReq envoyée à NETBANX, indiquant si le titulaire de la carte a authentifié la carte de crédit avec succès.

## Avantages pour le marchand

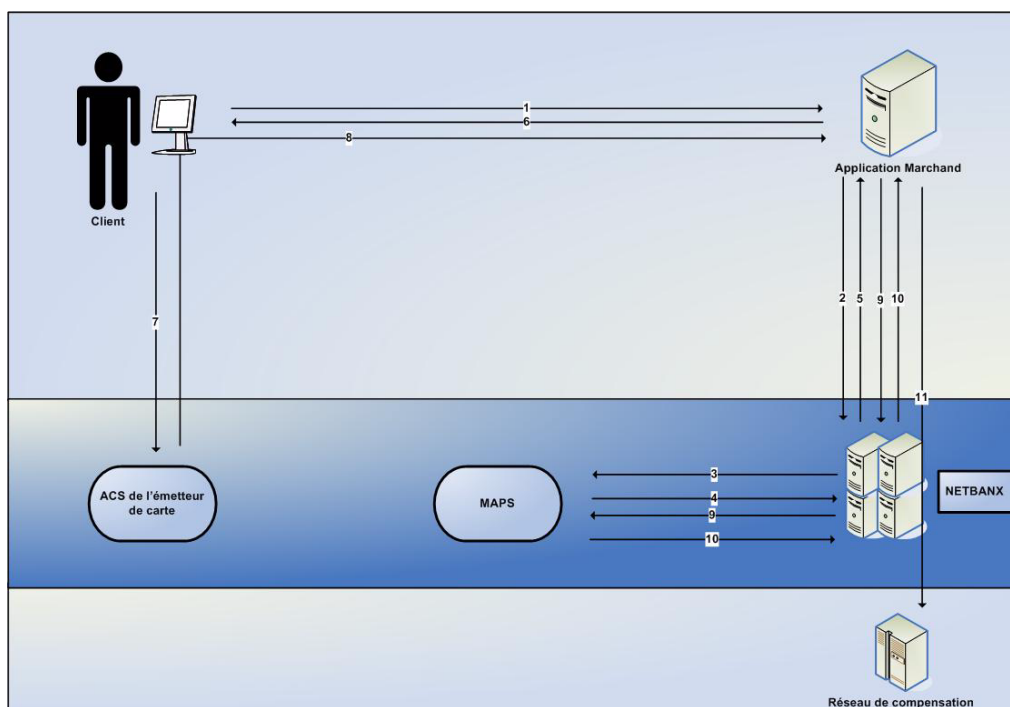
Voici quelques-uns des avantages liés au traitement des transactions au moyen de l'authentification 3D Secure :

- En demandant à vos clients de procéder à l'authentification de leurs cartes de crédit par mot de passe sur votre site, vous leur permettez d'accroître leur confiance envers les achats en ligne, ce qui contribuera à une augmentation du volume de vos ventes.
- L'authentification en ligne en temps réel par le client réduit les risques de transactions frauduleuses.

- Vous profitez d'une garantie de paiement pour les transactions avec authentification. Vous recevez une protection contre la responsabilité pour la rétrofacturation et échangez des avantages pour les transactions d'autorisation ou d'achat contenant un CAVV valide et ses valeurs ECI associées. Ces valeurs sont retournées par l'institution financière émettrice dans le message de réponse d'authentification. Consultez le *Guide de référence de l'API pour les Services Web* pour obtenir plus de détails concernant le traitement des transactions d'authentification.
- Vous profitez d'une réduction des frais d'exploitation en raison d'un plus petit nombre de litiges relatifs aux transactions.

## Fonctionnement de 3D Secure

Voici un cas typique de client dont la carte de crédit est inscrite au programme 3D Secure et qui utilise cette carte sur votre site de commerce électronique.



1. Votre client magasine en ligne sur votre site Web. Lorsqu'il passe à la caisse, votre client fournit ses renseignements de paiement, puis clique sur le bouton Acheter.
2. Vous envoyez alors une demande de Consultation d'inscription à NETBANX afin de vérifier si la carte de crédit de votre client est inscrite à 3D Secure. La demande comprend votre justificatif d'identité de marchand et le numéro de la carte de crédit. Consultez le *Guide de référence de l'API pour les Services Web* pour obtenir plus de détails concernant le traitement des demandes de Consultation d'inscription.
3. NETBANX envoie un message de consultation d'inscription au Système de traitement de l'authentification du marchand (MAPS) afin de confirmer que la carte de crédit de votre client est bien inscrite à 3D Secure.
4. Lorsque la carte est effectivement inscrite à 3D Secure, le système MAPS fournit une adresse URL d'ACS, une Requête d'authentification de paiement (PaReq) et un état d'inscription à NETBANX.

5. NETBANX vous transmet alors les valeurs suivantes sous l'élément *tdsResponse* de la fonction *ccTxnResponseV1* :

- URL d'ACS
- PaReq
- État d'inscription

En voici un exemple :

```
<ccTxnResponseV1>
<confirmationNumber>126200180</confirmationNumber>
<decision>ACCEPTED</decision>
<code>0</code>
<description>No Error</description>
-
  <detail>
<tag>InternalResponseCode</tag>
<value>0</value>
</detail>
-
  <detail>
<tag>SubErrorCode</tag>
<value>0</value>
</detail>
-
  <detail>
<tag>InternalResponseDescription</tag>
<value>no_error</value>
</detail>
<txnTime>2008-07-30T14:46:07.859-04:00</txnTime>
<duplicateFound>>false</duplicateFound>
-
  <tdsResponse>
-
    <acsURL>
https://testcustomer34.Cardinalcommerce.com/V3DSStart?osb=visa-3&VAA=B
</acsURL>
<paymentRequest>Response String Returned from Lookup Service</paymentRequest>
<enrollmentStatus>Y</enrollmentStatus>
</tdsResponse>
</ccTxnResponseV1>
```

La fonction *ccTxnResponseV1* contient également le numéro de confirmation dont vous avez besoin pour créer et envoyer une requête d'authentification subséquente.



*Afin de contourner les logiciels bloqueurs de fenêtres contextuelles, vous devez afficher la page dans la fenêtre principale du navigateur du client, à l'intérieur d'un cadre avec bordure, et non dans une fenêtre contextuelle.*

6. Vous redirigez ensuite le navigateur de votre client vers l'adresse URL d'ACS, laquelle est en réalité hébergée par l'émetteur de la carte. Le formulaire de l'émetteur de carte devrait aussi s'afficher à l'intérieur d'un cadre sur votre page Web (voir *Meilleures pratiques pour les marchands* à la page 6). La redirection vers l'adresse URL d'ACS doit aussi préciser le contenu des champs suivants :

- Un champ défini par le marchand (*MD*), utilisé aux fins de suivi.

- Une adresse URL de retour (*termURL*) afin de rediriger votre client de nouveau vers votre site Web après avoir saisi leur mot de passe.
- La requête de paiement (*PaReq*), c'est-à-dire la réponse retournée par la consultation d'inscription.

Voici un exemple de publication HTTP :

```
<HTML>
<BODY onload="document.frmLaunch.submit();">
<FORM name="frmLaunch" method="POST" action="ACSUrl Value">
<input type="hidden" name="PaReq" value="Response String Returned from Lookup
Service">
<input type="hidden" name="TermUrl" value="Fully Qualified URL">
<input type="hidden" name="MD" value="Session Tracking Value">
</FORM>
</BODY>
</HTML>
```

7. Votre client saisit ses données d'authentification (c.-à-d., son mot de passe) et lance le processus d'authentification directement auprès de l'émetteur de la carte.

The screenshot shows a web form for Verified by Visa authentication. At the top left is the 'Verified by VISA' logo. To the right is a 'Member Name' field with a small 'M' icon. Below this is the heading 'Added Protection' and the instruction 'Please submit your Verified by Visa password.' The transaction details are listed: Merchant: merchant.com, Amount: \$43.28, Date: 01/05/2003, and Card number: \*\*\*\* \* 0335. A 'Personal Message' section says 'Shop securely with Verified by Visa.' Below that is a 'Password:' label followed by a text input field and a 'Forgot your password?' link. At the bottom, there is a 'Submit' button, a 'Help' button with a question mark icon, and an 'Exit' button.

8. Le système ACS de l'émetteur de la carte effectue l'authentification de votre client, puis retourne le résultat sous forme de Réponse d'authentification du payeur (PARes). Ces données vous sont transférées par le navigateur de votre client.

Une fois le processus d'authentification terminé, le système ACS redirige votre client vers le site Web défini sous l'élément *termURL*. Normalement, il devrait s'agir de votre propre site Web.

9. Après avoir reçu la valeur de la requête PAREs, vous lancez une requête d'authentification (laquelle contient la requête PAREs sous l'élément *paymentResponse*) auprès de NETBANX. En voici un exemple :

```
<ccAuthenticateRequestV1
xmlns="http://www.optimalpayments.com/creditcard/xmlschema/v1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.optimalpayments.com/creditcard/xmlschema/v1">
<merchantAccount>
<accountNum>1000022246</accountNum>
<storeID>test</storeID>
<storePwd>test</storePwd>
</merchantAccount>
<confirmationNumber>125774665</confirmationNumber>
<paymentResponse>Response String Returned to the Term URL from the Card Issuer
</paymentResponse>
</ccAuthenticateRequestV1>
```

Consultez le [Guide de référence de l'API pour les Services Web](#) pour obtenir plus de détails concernant le traitement des requêtes d'authentification.

10. L'élément *tdsAuthenticateResponse* de la fonction *ccTxnResponseV1* NETBANX renvoie les trois valeurs suivantes que vous devrez inclure dans une fonction *ccAuthRequestV1* :

- état (utilisé pour l'élément *indicator* de la fonction *ccAuthRequestV1*)
- cavv
- xid

11. Vous envoyez ensuite une requête d'Achat normale à NETBANX, comprenant ces trois valeurs sous l'élément *authentication* de la fonction *ccAuthRequestV1*. Voici un exemple de bout de code d'une fonction d'Achat :

```
<ccAuthRequestV1 xmlns="http://www.optimalpayments.com/creditcard/xmlschema/v1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.optimalpayments.com/creditcard/xmlschema/v1">
  <merchantAccount>
    <accountNum>12345678</accountNum>
    <storeID>myStoreID</storeID>
    <storePwd>myStorePWD</storePwd>
  </merchantAccount>
  ...
  <authentication>
    <indicator>05</indicator>
    <cavv>AAABB4WZ1QAAAAAAcJmVENiWiV+=</cavv>
    <xid>Q2prWUI2RFNBc3FOTXN1em50eWY=</xid>
  </authentication>
  ...
</ccAuthRequestV1>
```



**Toutes les publications HTTP doivent être codées par URL à l'aide du format *application/x-www-form-urlencoded* (voir les étapes 9 et 11 ci-dessus). Autrement, il y a un risque d'échec puisque les caractères réservés (p. ex., barre oblique, perluète, etc.) seront retirés des requêtes qui ne sont pas correctement codées par URL.**

Consultez le [Guide de référence de l'API pour les Services Web](#) pour obtenir plus de détails concernant le traitement des fonctions *ccAuthRequestV1*.

## Meilleures pratiques pour les marchands

Voici quelques conseils pour l'affichage du programme 3D Secure sur votre site Web de commerce électronique.



*Ces conseils ne sont que des suggestions sommaires. Pour obtenir des instructions plus détaillées, nous vous recommandons de consulter les sites Web respectifs des cartes de crédit que vous acceptez. Pour obtenir plus de détails, consultez la rubrique Adresses URL importantes à la page 8.*

### Affichage de l'information et des logos de 3D Secure

Les logos (par ex., Vérifié par Visa) doivent au minimum être affichés sur la page des détails de la transaction pendant le processus de paiement, le plus près possible des zones de saisie des renseignements de carte de crédit. Ces logos devraient s'afficher comme des liens vers les adresses URL des sections « en savoir davantage » des sites des cartes de crédit respectives. Idéalement, ces logos devraient apparaître en évidence sur toutes les pages contenant des options de paiement.



*De manière générale, vous devez d'abord accepter certaines Conditions de l'émetteur de la carte avant d'utiliser ses logos sur votre site.*

### Message de préauthentification

Vous devez fournir un message de préauthentification, indiquant notamment que le titulaire de la carte de crédit pourrait devoir fournir des renseignements d'authentification après avoir cliqué sur le bouton Acheter.

Par exemple :

« Votre carte peut être admissible à l'inscription ou être déjà inscrite au programme d'authentification du payeur Vérifié par Visa. Après avoir cliqué sur le bouton Acheter, l'émetteur de votre carte peut vous demander votre mot de passe d'authentification du payeur afin d'effectuer votre achat. »

## Affichage de l'URL de l'ACS

- N'utilisez pas de fenêtre contextuelle pour afficher l'URL de l'ACS, mais affichez plutôt cette page dans un cadre. Visa et MasterCard interdisent l'utilisation de fenêtres contextuelles, car celles-ci peuvent être bloquées par le navigateur.

- Le cadre à afficher devrait avoir une taille minimale de 400x400 pixels, soit suffisamment large pour afficher la totalité de la page d'authentification sans barres de défilement pour la gamme normale de résolution d'affichage des navigateurs.
- Le cadre devrait aussi avoir un texte d'en-tête comme celui-ci :  
« Pour des raisons de sécurité, veuillez remplir le formulaire ci-dessous afin d'exécuter votre commande. Ne cliquez pas sur les boutons Actualiser ou Précédent afin de ne pas interrompre ou annuler la transaction. »
- Vous ne devriez pas afficher de messages promotionnels à l'intention des titulaires de carte à l'intérieur de ce cadre. Il est primordial que les titulaires soient en confiance relativement à la session d'authentification auprès de l'émetteur de leur carte.
- Si vous utilisez un cadre avec un en-tête de marque (par ex., pour afficher votre logo de marchand), n'utilisez pas de liens HTML actifs. Cependant, sous le cadre d'en-tête, vous devriez inclure un lien vers la page de paiement, en cas de difficultés techniques.
- Si vous devez afficher des messages de communication, l'utilisation du texte suivant est fortement recommandée :
  - Traitement de votre commande en cours...
  - Ne cliquez pas sur les boutons Actualiser ou Précédent afin de ne pas interrompre ou annuler la transaction.
- Les marchands faisant appel à des fenêtres d'authentification incrustée avec cadres doivent insérer une adresse HTTPS à l'intérieur du champ *termURL*.

## Séquence de délai d'inactivité

- Prévoyez un minimum de 10 secondes pour l'envoi d'une réponse par le système ACS au message de consultation d'inscription.
- Prévoyez un minimum de 10 minutes pour l'obtention d'une réponse PARES au message PaReq.

## Affichage de messages à l'intention du client

- Lorsque vous créez des messages d'état ou d'erreur à l'intention de vos clients, assurez-vous de considérer tous les scénarios possibles (par ex., erreur de délai d'inactivité, échec d'authentification, etc.).
- En cas d'échec de l'authentification, vous pouvez afficher un message semblable à celui-ci :  
« Votre institution financière nous indique que le processus d'authentification de cette transaction a échoué. Afin de vous protéger contre une utilisation non autorisée, cette carte ne peut pas être utilisée afin d'effectuer votre achat. Vous devez choisir un autre mode de paiement afin d'effectuer cet achat. »

## Conseils généraux

- Assurez-vous que le bouton Acheter est désactivé pendant l'authentification.
- Évitez de transmettre les résultats du processus d'authentification à l'intérieur de champs de formulaire cachés ou par l'URL sous forme de paramètres de chaîne de requête. Les données sensibles transmises de cette manière pourraient être facilement manipulées par le consommateur.

## Adresses URL importantes

Consultez les URL suivantes pour connaître les détails et politiques d'implémentation et de promotion du programme de marque 3D Secure pour ces émetteurs de carte importants :

- Visa – [http://www.visa.ca/verified/merch\\_marketing.cfm](http://www.visa.ca/verified/merch_marketing.cfm)
- MasterCard – [http://www.mastercard.com/us/merchant/security/what\\_can\\_do/SecureCode/index.html](http://www.mastercard.com/us/merchant/security/what_can_do/SecureCode/index.html)
- JCB – <http://www.jcb-global.com/english/solution/ec.html>

## Si vous avez besoin d'aide...

Si vous avez des questions à propos du traitement de vos transactions, nous serons heureux d'y répondre. Communiquez avec le soutien technique par courriel ou par téléphone :

- [support@optimalpayments.com](mailto:support@optimalpayments.com)
- 1 888 709-8753

## Valeurs de réponse aux messages d'authentification et de consultation

Selon les valeurs de réponse aux messages d'authentification et de consultation, les marchands doivent contrôler le flux des transactions de différentes façons. Les tableaux suivants contiennent les actions recommandées pour les scénarios possibles que doivent prendre en charge les intégrations de processus d'authentification du payeur. Chaque intégration de marchand doit gérer chacune des valeurs de réponses suivantes.

## Valeurs de réponse Consultation pour l'authentification du payeur

**Tableau 1 : Valeurs de réponse Consultation pour l'authentification du payeur**

Valeur d'inscription	Description	Action recommandée
Y	L'authentification du titulaire de la carte est disponible.	Rediriger le client vers l'URL de l'ACS pour effectuer l'authentification.
N	Le titulaire de la carte n'est pas inscrit au programme d'authentification.	Exécuter la commande en tant que transaction sans authentification. La bonne valeur ECI doit être définie pour la transaction d'autorisation. <b>Visa/JCB</b> <ul style="list-style-type: none"> <li>Le marchand a une protection de responsabilité.</li> <li>ECI – 06</li> </ul> <b>MasterCard</b> <ul style="list-style-type: none"> <li>Le marchand n'a pas de protection de responsabilité.</li> <li>ECI – 01</li> </ul>
U	L'authentification du titulaire de la carte n'est pas disponible.	Exécuter la commande en tant que transaction sans authentification. La bonne valeur ECI doit être définie pour la transaction d'autorisation. <b>Visa/JCB</b> <ul style="list-style-type: none"> <li>Le marchand n'a pas de protection de responsabilité.</li> <li>ECI – 07</li> </ul> <b>MasterCard</b> <ul style="list-style-type: none"> <li>Le marchand n'a pas de protection de responsabilité.</li> <li>ECI – 01</li> </ul>

## Valeurs de réponse Authentification pour l'authentification du payeur

**Tableau 2 : Valeurs de réponse Authentification pour l'authentification du payeur**

Valeur PAResStatus	Valeur de Vérification de signature	Description	Action recommandée
Y	Y	Authentification du titulaire de la carte effectuée avec succès.	Exécuter la commande en tant que transaction avec authentification. <b>Visa/JCB</b> <ul style="list-style-type: none"> <li>Le marchand a une protection de responsabilité.</li> <li>ECI – 05</li> </ul> <b>MasterCard</b> <ul style="list-style-type: none"> <li>Le marchand a une protection de responsabilité.</li> <li>ECI – 02</li> </ul>

**Tableau 2 : Valeurs de réponse Authentification pour l'authentification du payeur**

Valeur PResStatus	Valeur de Vérification de signature	Description	Action recommandée
A	Y	Tentative d'authentification du titulaire de la carte effectuée avec succès. Si une transaction MasterCard retourne cette valeur de réponse, une valeur PResStatus correspondant à U sera retournée dans le message de réponse.	Exécuter la commande en tant que transaction avec authentification. <b>Visa/JCB</b> <ul style="list-style-type: none"> <li>Le marchand a une protection de responsabilité.</li> <li>ECI – 06</li> </ul> <b>MasterCard</b> <ul style="list-style-type: none"> <li>Le marchand n'a pas de protection de responsabilité.</li> <li>ECI – 01</li> </ul>
N	Y	Échec de l'authentification du titulaire de la carte.	Rediriger le titulaire de la carte vers la page des détails de la transaction. Afficher le message d'échec d'authentification recommandé à l'intention du consommateur, invitant ce dernier à utiliser un autre mode de paiement pour effectuer la transaction.
U	Y	Impossible d'effectuer l'authentification du titulaire de la carte.	Exécuter la commande en tant que transaction sans authentification. <b>Visa/JCB</b> <ul style="list-style-type: none"> <li>Le marchand n'a pas de protection de responsabilité.</li> <li>ECI – 07</li> </ul> <b>MasterCard</b> <ul style="list-style-type: none"> <li>Le marchand n'a pas de protection de responsabilité.</li> <li>ECI – 01</li> </ul>
Y, A, N, U	N	L'échec de la vérification contre la fraude indique que les résultats de la transaction constituent un risque.	Rediriger le titulaire de la carte vers la page des détails de la transaction. Afficher le message d'échec d'authentification recommandé à l'intention du consommateur, invitant ce dernier à utiliser un autre mode de paiement pour effectuer la transaction.

## Scénarios de test

Vous pouvez tester votre application en transmettant des messages à l'environnement de test au moyen des numéros de carte fournis ci-dessous reliés à divers scénarios avec 3D Secure. Chaque numéro de carte générera une réponse unique que votre intégration devrait pouvoir reconnaître et gérer correctement.

### Scénarios de test Vérifié par Visa

#### Scénario de test VPV 1

- Titulaire de la carte inscrit
- Authentification réussie
- Vérification de signature réussie

**Tableau 3 : Scénario de test VPV 1**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
4000000000000002	<b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PAREs Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>• PAREsStatus = Y</li> <li>• SignatureVerification = Y</li> <li>• EciFlag = 05</li> <li>• Xid = &lt;XID Value&gt;</li> <li>• Cavv = &lt;CAVV Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul>	Le marchand doit ajouter les valeurs Cavv et EciFlag au message d'autorisation.	Aucune

*Scénario de test VPV 2*

- Titulaire de la carte inscrit
- Authentification réussie
- Vérification de signature non réussie

**Tableau 4 : Scénario de test VPV 2**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
4000000000000010	<b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PAREs Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>• PAREsStatus = Y</li> <li>• SignatureVerification = N</li> <li>• EciFlag = 05</li> <li>• Xid = &lt;XID Value&gt;</li> <li>• Cavv = &lt;CAVV Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul>	Le marchand <b>ne doit pas</b> poursuivre l'autorisation en raison de l'échec de la vérification de la signature. Le marchand doit inviter le consommateur à utiliser un autre mode de paiement ou tenter de procéder à l'authentification du consommateur de nouveau en commençant par un nouveau message cmpi_lookup.	

*Scénario de test VPV 3*

- Titulaire de la carte inscrit
- Authentification non réussie
- Vérification de signature réussie

**Tableau 5 : Scénario de test VPV 3**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
4000000000000028	<p><b>cmapi_lookup réponse</b></p> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PARes Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmapi_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>• PAResStatus = N</li> <li>• SignatureVerification = Y</li> <li>• EciFlag = 07</li> <li>• Xid = &lt;XID Value&gt;</li> <li>• Cavv = &lt;vide&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul>	<p>Le marchand <b>ne doit pas</b> poursuivre l'autorisation. Le marchand doit inviter le consommateur à utiliser un autre mode de paiement et n'est pas autorisé à demander une autorisation pour cette transaction.</p>	

*Scénario de test VPV 4*

- Titulaire de la carte inscrit
- Authentification impossible à effectuer (réponse au message d'authentification)

**Tableau 6 : Scénario de test VPV 4**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
4000000000000036	<p><b>cmapi_lookup réponse</b></p> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PARes Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmapi_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>• PAResStatus = U</li> <li>• SignatureVerification = Y</li> <li>• EciFlag = 07</li> <li>• Xid = &lt;XID Value&gt;</li> <li>• Cavv = &lt;vide&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul>	<p>Le marchand peut conserver la responsabilité et soumettre la transaction à titre de transaction non authentifiée. Le marchand peut aussi inviter le consommateur à utiliser un autre mode de paiement.</p>	<p>Le marchand conserve la responsabilité pour la rétrofacturation.</p>

*Scénario de test VPV 5*

- Délai d'inactivité atteint lors du traitement de la transaction cmapi\_lookup

**Tableau 7 : Scénario de test VPV 5**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
4000000000000044	<b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>Enrolled = U</li> <li>ACSUrl = &lt;vide&gt;</li> <li>Payload = &lt;vide&gt;</li> <li>ErrorNo = 0</li> <li>ErrorDesc = &lt;vide&gt;</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>Le message cmpi_authenticate ne s'applique pas dans ce cas.</li> </ul>	La transaction cmpi_lookup simulera un scénario d'expiration du délai d'inactivité et les 20 secondes requises pour effectuer le traitement de la transaction avec les autres systèmes 3-D Secure. L'intégration du marchand doit procéder au traitement de l'expiration du délai d'inactivité au bout d'un délai de 10 à 12 secondes et poursuivre en donnant le message d'autorisation.	Le marchand conserve la responsabilité pour la rétrofacturation.

*Scénario de test VPV 6*

- Titulaire de la carte non inscrit

**Tableau 8 : Scénario de test VPV 6**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
4000000000000051	<b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>Enrolled = N</li> <li>ACSUrl = &lt;vide&gt;</li> <li>Payload = &lt;vide&gt;</li> <li>ErrorNo = 0</li> <li>ErrorDesc = &lt;vide&gt;</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>Le message cmpi_authenticate ne s'applique pas dans ce cas.</li> </ul>	Le marchand doit envoyer la demande d'autorisation avec une valeur ECI de 06, accordant la protection en cas de rétrofacturation.	Non

*Scénario de test VPV 7*

- Titulaire de la carte inscrit
- Authentification non disponible (réponse au message de consultation)

**Tableau 9 : Scénario de test VPV 7**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
4000000000000069	<b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>Enrolled = U</li> <li>ACSUrl = &lt;vide&gt;</li> <li>Payload = &lt;vide&gt;</li> <li>ErrorNo = 0</li> <li>ErrorDesc = &lt;vide&gt;</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>Le message cmpi_authenticate ne s'applique pas dans ce cas.</li> </ul>	Le marchand doit poursuivre et passer au message d'autorisation.	Le marchand conserve la responsabilité pour la rétrofacturation.

Scénario de test VPV 8

- Le marchand ne peut exécuter les transactions (marchand non actif)

**Tableau 10 : Scénario de test VPV 8**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
4000000000000077	<b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>• Enrolled = &lt;vide&gt;</li> <li>• ACSUrl = &lt;vide&gt;</li> <li>• Payload = &lt;vide&gt;</li> <li>• ErrorNo = Numéro de l'erreur</li> <li>• ErrorDesc = Description de l'erreur</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>• Le message cmpi_authenticate ne s'applique pas dans ce cas.</li> </ul>	Le marchand doit poursuivre l'autorisation et communiquer avec le soutien technique pour examiner et résoudre le problème.	Le marchand conserve la responsabilité pour la rétrofacturation.

Scénario de test VPV 9

- Erreur en réponse au message cmpi\_lookup

**Tableau 11 : Scénario de test VPV 9**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
4000000000000085	<b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>• Enrolled = &lt;vide&gt;</li> <li>• ACSUrl = &lt;vide&gt;</li> <li>• Payload = &lt;vide&gt;</li> <li>• ErrorNo = Numéro de l'erreur</li> <li>• ErrorDesc = Description de l'erreur</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>• Le message cmpi_authenticate ne s'applique pas dans ce cas.</li> </ul>	Le marchand doit poursuivre l'autorisation et communiquer avec le soutien technique pour examiner et résoudre le problème.	Le marchand conserve la responsabilité pour la rétrofacturation.

Scénario de test VPV 10

- Titulaire de la carte inscrit
- Erreur en réponse au message cmpi\_authenticate

**Tableau 12 : Scénario de test VPV 10**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
4000000000000093	<p><b>cmpi_lookup réponse</b></p> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PAREs Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmpi_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>• PAREsStatus = &lt;vide&gt;</li> <li>• SignatureVerification = &lt;vide&gt;</li> <li>• EciFlag = &lt;vide&gt;</li> <li>• Xid = &lt;vide&gt;</li> <li>• Cavv = &lt;vide&gt;</li> <li>• ErrorNo = Numéro de l'erreur</li> <li>• ErrorDesc = Description de l'erreur</li> </ul>	Le marchand <b>ne doit pas</b> poursuivre l'autorisation. Le marchand doit inviter le consommateur à utiliser un autre mode de paiement.	Le marchand conserve la responsabilité pour la rétrofacturation.

*Scénario de test VPV 11*

- Titulaire de la carte inscrit
- Tentatives de traitement exécutées

**Tableau 13 : Scénario de test VPV 11**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
4000000000000101	<p><b>cmpi_lookup réponse</b></p> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PAREs Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmpi_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>• PAREsStatus = A</li> <li>• SignatureVerification = Y</li> <li>• EciFlag = 06</li> <li>• Xid = &lt;XID Value&gt;</li> <li>• Cavv = &lt;CAVV Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul>	Le marchand doit ajouter les valeurs Cavv et EciFlag au message d'autorisation.	Le marchand a droit à la protection en cas de rétrofacturation.

Scénarios de test MasterCard SecureCode

*Scénario de test MCSC 1*

- Titulaire de la carte inscrit
- Authentification réussie
- Vérification de signature réussie.

**Tableau 14 : Scénario de test MCSC 1**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
5200000000000007	<p><b>cmpi_lookup réponse</b></p> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PAREs Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmpi_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>• PAREsStatus = Y</li> <li>• SignatureVerification = Y</li> <li>• EciFlag = 02</li> <li>• Xid = &lt;XID Value&gt;</li> <li>• Cavv = &lt;CAVV Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul>	Le marchand doit ajouter les valeurs Cavv et EciFlag au message d'autorisation.	Aucune

*Scénario de test MCSC 2*

- Titulaire de la carte inscrit
- Authentification réussie
- Vérification de signature non réussie

**Tableau 15 : Scénario de test MCSC 2**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
52000000000000015	<p><b>cmpi_lookup réponse</b></p> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PAREs Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmpi_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>• PAREsStatus = Y</li> <li>• SignatureVerification = N</li> <li>• EciFlag = 02</li> <li>• Xid = &lt;XID Value&gt;</li> <li>• Cavv = &lt;CAVV Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul>	Le marchand <b>ne doit pas</b> poursuivre l'autorisation en raison de l'échec de la vérification de la signature. Le marchand doit inviter le consommateur à utiliser un autre mode de paiement ou tenter de procéder à l'authentification du consommateur de nouveau en commençant par un nouveau message cmpi_lookup.	

*Scénario de test MCSC 3*

- Titulaire de la carte inscrit
- Authentification non réussie
- Vérification de signature réussie

**Tableau 16 : Scénario de test MCSC 3**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
5200000000000023	<p><b>cmpi_lookup réponse</b></p> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PAREs Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmpi_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>• PAREsStatus = N</li> <li>• SignatureVerification = Y</li> <li>• EciFlag = 01</li> <li>• Xid = &lt;XID Value&gt;</li> <li>• Cavv = &lt;vide&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul>	<p>Le marchand <b>ne doit pas</b> poursuivre l'autorisation. Le marchand doit inviter le consommateur à utiliser un autre mode de paiement et n'est pas autorisé à demander une autorisation pour cette transaction.</p>	

*Scénario de test MCSC 4*

- Titulaire de la carte inscrit
- Authentification impossible à effectuer (réponse au message d'authentification)

**Tableau 17 : Scénario de test MCSC 4**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
5200000000000031	<p><b>cmpi_lookup réponse</b></p> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PAREs Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmpi_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>• PAREsStatus = U</li> <li>• SignatureVerification = Y</li> <li>• EciFlag = 01</li> <li>• Xid = &lt;XID Value&gt;</li> <li>• Cavv = &lt;vide&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul>	<p>Le marchand peut conserver la responsabilité et soumettre la transaction à titre de transaction non authentifiée. Le marchand peut aussi inviter le consommateur à utiliser un autre mode de paiement.</p>	<p>Le marchand conserve la responsabilité pour la rétrofacturation.</p>

*Scénario de test MCSC 5*

- Titulaire de la carte inscrit
- Authentification non disponible (réponse au message de consultation)

**Tableau 18 : Scénario de test MCSC 5**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
5200000000000049	<p><b>cmpi_lookup réponse</b></p> <ul style="list-style-type: none"> <li>Enrolled = U</li> <li>ACSUrl = &lt;vide&gt;</li> <li>Payload = &lt;vide&gt;</li> <li>ErrorNo = 0</li> <li>ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmpi_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>Le message cmpi_authenticate ne s'applique pas dans ce cas.</li> </ul>	<p>La transaction cmpi_lookup simulera un scénario d'expiration du délai d'inactivité et les 20 secondes requises pour effectuer le traitement de la transaction avec les autres systèmes 3-D Secure.</p> <p>L'intégration du marchand doit procéder au traitement de l'expiration du délai d'inactivité au bout d'un délai de 10 à 12 secondes et poursuivre en donnant le message d'autorisation.</p>	<p>Le marchand conserve la responsabilité pour la rétrofacturation.</p>

*Scénario de test MCSC 6*

- Titulaire de la carte non inscrit

**Tableau 19 : Scénario de test MCSC 6**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
5200000000000056	<p><b>cmpi_lookup réponse</b></p> <ul style="list-style-type: none"> <li>Enrolled = N</li> <li>ACSUrl = &lt;vide&gt;</li> <li>Payload = &lt;vide&gt;</li> <li>ErrorNo = 0</li> <li>ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmpi_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>Le message cmpi_authenticate ne s'applique pas dans ce cas.</li> </ul>	<p>Le marchand doit poursuivre le traitement de la transaction.</p>	<p>Le marchand conserve la responsabilité pour la rétrofacturation.</p>

*Scénario de test MCSC 7*

- Titulaire de la carte inscrit
- Authentification non disponible (réponse au message de consultation)

**Tableau 20 : Scénario de test MCSC 7**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
5200000000000064	<p><b>cmpi_lookup réponse</b></p> <ul style="list-style-type: none"> <li>Enrolled = U</li> <li>ACSUrl = &lt;vide&gt;</li> <li>Payload = &lt;vide&gt;</li> <li>ErrorNo = 0</li> <li>ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmpi_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>Le message cmpi_authenticate ne s'applique pas dans ce cas.</li> </ul>	<p>Le marchand doit poursuivre et passer au message d'autorisation.</p>	<p>Le marchand conserve la responsabilité pour la rétrofacturation.</p>

*Scénario de test MCSC 8*

- Le marchand ne peut exécuter les transactions (marchand non actif)

**Tableau 21 : Scénario de test MCSC 8**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
5200000000000072	<b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>• Enrolled = &lt;vide&gt;</li> <li>• ACSUrl = &lt;vide&gt;</li> <li>• Payload = &lt;vide&gt;</li> <li>• ErrorNo = Numéro de l'erreur</li> <li>• ErrorDesc = Description de l'erreur</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>• Le message cmpi_authenticate ne s'applique pas dans ce cas.</li> </ul>	Le marchand doit poursuivre l'autorisation et communiquer avec le soutien technique pour examiner et résoudre le problème.	Le marchand conserve la responsabilité pour la rétrofacturation.

*Scénario de test MCSC 9*

- Erreur en réponse au message cmpi\_lookup

**Tableau 22 : Scénario de test MCSC 9**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
5200000000000080	<b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>• Enrolled = &lt;vide&gt;</li> <li>• ACSUrl = &lt;vide&gt;</li> <li>• Payload = &lt;vide&gt;</li> <li>• ErrorNo = Numéro de l'erreur</li> <li>• ErrorDesc = Description de l'erreur</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>• Le message cmpi_authenticate ne s'applique pas dans ce cas.</li> </ul>	Le marchand doit poursuivre l'autorisation et communiquer avec le soutien technique pour examiner et résoudre le problème.	Le marchand conserve la responsabilité pour la rétrofacturation.

*Scénario de test MCSC 10*

- Titulaire de la carte inscrit
- Erreur en réponse au message cmpi\_authenticate

**Tableau 23 : Scénario de test MCSC 10**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
5200000000000098	Titulaire de la carte inscrit, erreur en réponse au message cmpi_authenticate <b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PAREs Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>• PAREsStatus = &lt;vide&gt;</li> <li>• SignatureVerification = &lt;vide&gt;</li> <li>• EciFlag = &lt;vide&gt;</li> <li>• Xid = &lt;vide&gt;</li> <li>• Cavv = &lt;vide&gt;</li> <li>• ErrorNo = Numéro de l'erreur</li> <li>• ErrorDesc = Description de l'erreur</li> </ul>	Le marchand <b>ne doit pas</b> poursuivre l'autorisation. Le marchand doit inviter le consommateur à utiliser un autre mode de paiement.	Si la demande d'autorisation de la transaction est effectuée, le marchand conserve la responsabilité pour la rétrofacturation.

### Scénarios de test JCB J/Secure

*Scénario de test J/Secure 1*

- Titulaire de la carte inscrit
- Authentification réussie
- Vérification de signature réussie.

**Tableau 24 : Scénario de test J/Secure 1**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
3000000000000004	<b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PAREs Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>• PAREsStatus = Y</li> <li>• SignatureVerification = Y</li> <li>• EciFlag = 05</li> <li>• Xid = &lt;XID Value&gt;</li> <li>• Cavv = &lt;CAVV Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul>	Le marchand doit ajouter les valeurs Cavv et EciFlag au message d'autorisation.	Aucune

*Scénario de test J/Secure 2*

- Titulaire de la carte inscrit
- Authentification réussie
- Vérification de signature non réussie

**Tableau 25 : Scénario de test J/Secure 2**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
3000000000000012	<p><b>cmpi_lookup réponse</b></p> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PAREs Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmpi_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>• PAREsStatus = Y</li> <li>• SignatureVerification = N</li> <li>• EciFlag = 05</li> <li>• Xid = &lt;XID Value&gt;</li> <li>• Cavv = &lt;CAVV Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul>	<p>Le marchand <b>ne doit pas</b> poursuivre l'autorisation en raison de l'échec de la vérification de la signature. Le marchand doit inviter le consommateur à utiliser un autre mode de paiement ou tenter de procéder de nouveau à l'authentification du consommateur.</p>	

*Scénario de test J/Secure 3*

- Titulaire de la carte inscrit
- Authentification non réussie
- Vérification de signature réussie

**Tableau 26 : Scénario de test J/Secure 3**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
3000000000000020	<p><b>cmpi_lookup réponse</b></p> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PAREs Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmpi_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>• PAREsStatus = N</li> <li>• SignatureVerification = Y</li> <li>• EciFlag = 07</li> <li>• Xid = &lt;XID Value&gt;</li> <li>• Cavv = &lt;vide&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul>	<p>Le marchand doit inviter le consommateur à utiliser un autre mode de paiement et n'est pas autorisé à demander une autorisation pour cette transaction.</p>	

*Scénario de test J/Secure 4*

- Titulaire de la carte inscrit
- Authentification non disponible (réponse au message d'authentification)

**Tableau 27 : Scénario de test J/Secure 4**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
3000000000000038	<p><b>cmpi_lookup réponse</b></p> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PAREs Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmpi_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>• PAREsStatus = U</li> <li>• SignatureVerification = Y</li> <li>• EciFlag = 07</li> <li>• Xid = &lt;XID Value&gt;</li> <li>• Cavv = &lt;vide&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul>	Le marchand peut conserver la responsabilité et soumettre la transaction à titre de transaction non authentifiée. Le marchand peut aussi inviter le consommateur à utiliser un autre mode de paiement.	

*Scénario de test J/Secure 5*

- Titulaire de la carte inscrit
- Authentification non disponible

**Tableau 28 : Scénario de test J/Secure 5**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
213100000000027	<p><b>cmpi_lookup réponse</b></p> <ul style="list-style-type: none"> <li>• Enrolled = U</li> <li>• ACSUrl = &lt;vide&gt;</li> <li>• Payload = &lt;vide&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmpi_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>• Le message cmpi_authenticate ne s'applique pas dans ce cas.</li> </ul>	La transaction cmpi_lookup simulera un scénario d'expiration du délai d'inactivité et les 20 secondes requises pour effectuer le traitement de la transaction avec les autres systèmes 3-D Secure. L'intégration du marchand doit procéder au traitement de l'expiration du délai d'inactivité au bout d'un délai de 10 à 12 secondes et poursuivre en donnant le message d'autorisation.	Le marchand conserve la responsabilité pour la rétrofacturation.

*Scénario de test J/Secure 6*

- Titulaire de la carte inscrit
- Authentification annulée par l'utilisateur (simulation de l'abandon de la fenêtre d'authentification par le consommateur)

**Tableau 29 : Scénario de test J/Secure 6**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
213100000000019	<b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PARes Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>• Le message cmpi_authenticate ne s'applique pas dans ce cas.</li> </ul>	Aucune action n'est possible. Transaction abandonnée.	

*Scénario de test J/Secure 7*

- Titulaire de la carte inscrit
- Authentification non disponible

**Tableau 30 : Scénario de test J/Secure 7**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
213100000000027	<b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>• Enrolled = U</li> <li>• ACSUrl = &lt;vide&gt;</li> <li>• Payload = &lt;vide&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>• Le message cmpi_authenticate ne s'applique pas dans ce cas.</li> </ul>	Le marchand doit poursuivre et passer au message d'autorisation.	Le marchand conserve la responsabilité pour la rétrofacturation.

*Scénario de test J/Secure 8*

- Le marchand ne peut exécuter les transactions (marchand non actif)

**Tableau 31 : Scénario de test J/Secure 8**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
213100000000035	<b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>• Enrolled = &lt;vide&gt;</li> <li>• ACSUrl = &lt;vide&gt;</li> <li>• Payload = &lt;vide&gt;</li> <li>• ErrorNo = Numéro de l'erreur</li> <li>• ErrorDesc = Description de l'erreur</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>• Le message cmpi_authenticate ne s'applique pas dans ce cas.</li> </ul>	Le marchand doit poursuivre l'autorisation et communiquer avec le soutien technique pour examiner et résoudre le problème.	Le marchand conserve la responsabilité pour la rétrofacturation.

Scénario de test J/Secure 9

- Erreur en réponse au message cmpi\_lookup

**Tableau 32 : Scénario de test J/Secure 9**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
180000000000002	<b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>• Enrolled = &lt;vide&gt;</li> <li>• ACSUrl = &lt;vide&gt;</li> <li>• Payload = &lt;vide&gt;</li> <li>• ErrorNo = Numéro de l'erreur</li> <li>• ErrorDesc = Description de l'erreur</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>• Le message cmpi_authenticate ne s'applique pas dans ce cas.</li> </ul>	Le marchand doit poursuivre l'autorisation et communiquer avec le soutien technique pour examiner et résoudre le problème.	Le marchand conserve la responsabilité pour la rétrofacturation.

Scénario de test J/Secure 10

- Titulaire de la carte inscrit
- Erreur en réponse au message cmpi\_authenticate

**Tableau 33 : Scénario de test J/Secure 10**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
180000000000010	<b>cmpi_lookup réponse</b> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PARes Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <b>cmpi_authenticate réponse</b> <ul style="list-style-type: none"> <li>• PAResStatus = &lt;vide&gt;</li> <li>• SignatureVerification = &lt;vide&gt;</li> <li>• EciFlag = &lt;vide&gt;</li> <li>• Xid = &lt;vide&gt;</li> <li>• Cavv = &lt;vide&gt;</li> <li>• ErrorNo = Numéro de l'erreur</li> <li>• ErrorDesc = Description de l'erreur</li> </ul>	Le marchand ne doit pas poursuivre l'autorisation. Le marchand doit inviter le consommateur à utiliser un autre mode de paiement.	Si la demande d'autorisation de la transaction est effectuée, le marchand conserve la responsabilité pour la rétrofacturation.

Scénario de test J/Secure 11

- Titulaire de la carte inscrit, tentatives de traitement effectuées

**Tableau 34 : Scénario de test J/Secure 11**

Numéro de la carte de test	Réponses	Action du marchand	Responsabilité pour la rétrofacturation
180000000000028	<p><b>cmpt_lookup réponse</b></p> <ul style="list-style-type: none"> <li>• Enrolled = Y</li> <li>• ACSUrl = &lt;url&gt;</li> <li>• Payload = &lt;PAREs Payload Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul> <p><b>cmpt_authenticate réponse</b></p> <ul style="list-style-type: none"> <li>• PAREsStatus = A</li> <li>• SignatureVerification = Y</li> <li>• EciFlag = 06</li> <li>• Xid = &lt;XID Value&gt;</li> <li>• Cavv = &lt;CAVV Value&gt;</li> <li>• ErrorNo = 0</li> <li>• ErrorDesc = &lt;vide&gt;</li> </ul>	Le marchand doit ajouter les valeurs Cavv et ECI au message d'autorisation.	Le marchand a droit à la protection en cas de rétrofacturation.

Translation Draft

Translation Draft