

NETBANX®

Part of  OPTIMAL PAYMENTS™

Implementing 3D Secure with NETBANX

June 2011

This manual and accompanying electronic media are proprietary products of Optimal Payments plc. They are to be used only by licensed users of the product.

© 1999–2011 Optimal Payments plc. All rights reserved.

The information within this document is subject to change without notice. The software described in this document is provided under a license agreement, and may be used or copied only in accordance with this agreement. No part of this manual may be reproduced or transferred in any form or by any means without the express written consent of Optimal Payments plc.

All other names, trademarks, and registered trademarks are the property of their respective owners.

Optimal Payments plc makes no warranty, either express or implied, with respect to this product, its merchantability or fitness for a particular purpose, other than as expressly provided in the license agreement of this product. For further information, please contact Optimal Payments plc.

International Head Office

3500 de Maisonneuve W., Suite 700
Montreal, Quebec H3Z 3C1
Canada

Tel.: (514) 380-2700

Fax: (514) 380-2760

Email: info@optimalpayments.com

Technical support: support@optimalpayments.com

Web: www.optimalpayments.com

U.K. Office

Third Floor, Mount Pleasant House
Mount Pleasant
Cambridge CB3 0RN
United Kingdom

Email: info@optimalpayments.co.uk

Technical Support: support@optimalpayments.co.uk

Web: www.optimalpayments.co.uk

U.S. Office

1209 Orange Street
Wilmington, DE 19801

Gatineau Office

75 Promenade du Portage
Gatineau, Quebec J8X 2J9
Canada

Contents

Overview	1
Terminology	1
Merchant benefits	1
How 3D Secure works	2
Merchant best practices	5
Displaying 3D Secure information and logos	5
Pre-authentication message	6
Displaying the ACS URL	6
Timeout sequencing	7
Displaying messages to the customer	7
Tips	7
Important URLs	7
If you need help	7
Lookup and Authentication message response values	7
Payer Authentication Lookup response values	8
Payer Authentication Authenticate response values	8
Test cases	9
Verified by Visa test cases	9
VBV test case 1	9
VBV test case 2	10
VBV test case 3	10
VBV test case 4	11
VBV test case 5	11
VBV test case 6	12
VBV test case 7	12
VBV test case 8	12
VBV test case 9	13
VBV test case 10	13
VBV test case 11	14
MasterCard SecureCode test cases	14
MCSC test case 1	14
MCSC test case 2	15
MCSC test case 3	15
MCSC test case 4	16
MCSC test case 5	16
MCSC test case 6	17
MCSC test case 7	17
MCSC test case 8	17
MCSC test case 9	18
MCSC test case 10	18

JCB J/Secure test cases	19
J/Secure test case 1	19
J/Secure test case 2	20
J/Secure test case 3	20
J/Secure test case 4	21
J/Secure test case 5	21
J/Secure test case 6	21
J/Secure test case 7	22
J/Secure test case 8	22
J/Secure test case 9	22
J/Secure test case 10	23
J/Secure test case 11	23

Implementing 3D Secure with NETBANX

Overview

3D Secure is an online cardholder authentication program designed to make Internet purchase transactions safer by authenticating a cardholder's identity at the time of purchase, before the merchant submits an authorization request. It is currently supported by several card brands, including Visa (Verified by Visa), MasterCard (SecureCode), and JCB (J/Secure). Authorizations processed using 3D Secure are guaranteed against most common types of chargeback disputes.

If you are already integrated with the NETBANX Web Services API, then implementing the 3D Secure security feature is quite simple. All you have to do is:

1. Submit an *Enrollment Lookup* request to NETBANX to verify whether your customer's credit card is enrolled in 3D Secure.
2. NETBANX returns a PaReq and a few other values in response to your *Enrollment Lookup* request – use these values to allow your customer to authenticate their credit card.
3. Once your customer has validated their card with the Card Issuer, you receive the information you need to submit an *Authentication* request to NETBANX.

See *How 3D Secure works* on page 2 for a brief overview of the 3D Secure process.

Terminology

These are a few terms that are frequently used in the 3D Secure process.

- Merchant Authentication Processing System (MAPS) – A third-party system that verifies whether a cardholder's credit card is enrolled in the 3D Secure program.
- Access Control Server (ACS) – The Issuing Bank's server providing confirmation of card enrollment.
- Payment Authentication Request (PaReq) – A request sent to the Issuing Bank to allow the cardholder to provide a password to authenticate the credit card.
- Payment Authentication Response (PARes) – The response to the PaReq sent to NETBANX, indicating whether the cardholder has successfully authenticated the credit card.

Merchant benefits

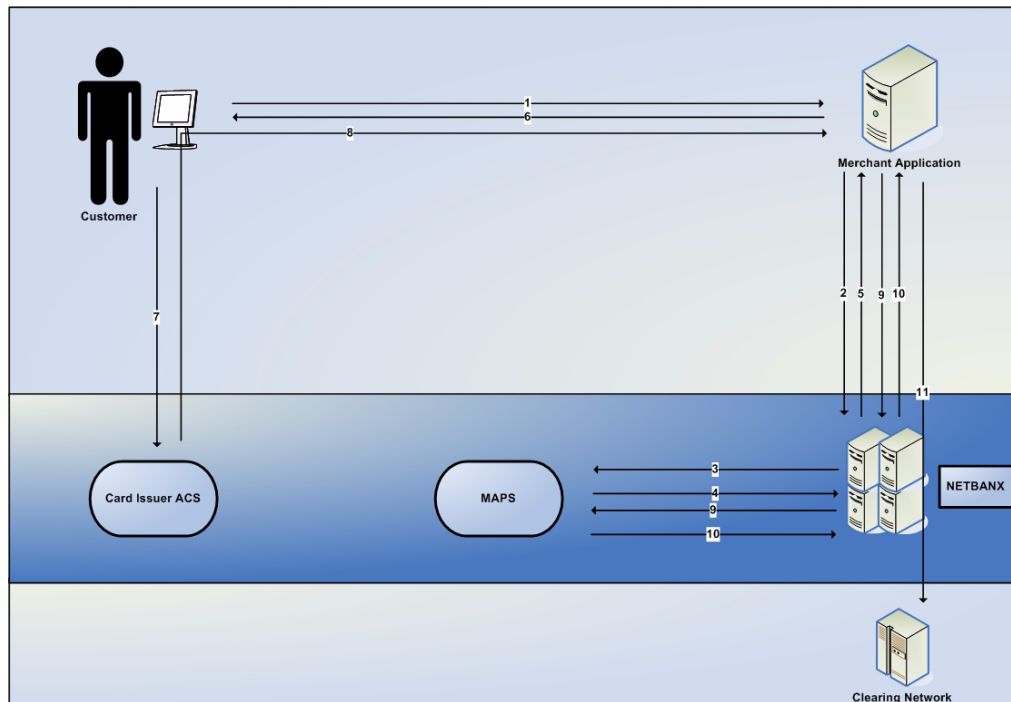
Here are a few of the benefits realized when you process transactions with 3D Secure authentication:

- By asking your customers for a password to authenticate their credit cards at your site, you increase their confidence in online purchasing, leading to increased sales volume.
- Online, real-time customer authentication reduces the risk of fraudulent transactions.
- You enjoy guaranteed payment for authenticated transactions. You receive chargeback liability protection and interchange benefits for Authorization/Purchase transactions that contain valid CAVV and the associated ECI values. These values are returned by the Issuing Bank in the Authentication Response message. See the *API Reference Guide for Web Services* for complete details on processing Authentication transactions.

- You benefit from reduced operational expenses due to fewer transaction disputes.

How 3D Secure works

Here is a typical scenario of a customer, whose credit card is enrolled in the 3D Secure program, using their credit card at your e-commerce site.



- Your customer shops online at your Web site. When they go to check out, your customer provides their payment details and clicks the Buy button.
- You submit an Enrollment Lookup request to NETBANX in order to verify that your customer's credit card is registered for 3D Secure. The request includes your merchant credentials and the credit card number. See the [API Reference Guide for Web Services](#) for complete details on processing Enrollment Lookup requests.
- NETBANX sends the enrollment lookup message to the Merchant Authentication Processing System (MAPS), to verify that your customer's credit card is in fact registered for 3D Secure.
- Assuming that the credit card is enrolled in 3D Secure, the MAPS provides an ACS URL, a Payment Authentication Request (PaReq), and an enrollment status to NETBANX.
- NETBANX passes the following values back to you in the `tdsResponse` element of the `ccTxnResponseV1`:
 - ACS URL
 - PaReq
 - Enrollment status

Here is an example:

```
<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>
```

The *ccTxnResponseV1* also contains the Confirmation Number you need to build and send a subsequent Authentication request.



Because of the existence of popup-blocking software, you must display the page in the customer's main browser window in an inline frame, and not in a popup window.

6. You redirect your customer's browser to the ACS URL, which is actually hosted by the Card Issuer. The Card Issuer form should be displayed inline within your Web page (see *Merchant best practices* on page 5). Within this redirect to the ACS URL, you must also specify the following fields:
 - A merchant-defined field (*MD*), used for your tracking purposes.
 - A return URL (*termURL*) in order to redirect your customer back to your Web site once they have submitted their password.
 - The payment request (*PaReq*), which is the response returned from the enrollment lookup.

Here is an example of an HTTP Post:

```
<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>

```

- Your customer enters their authentication data (i.e., their password) and initiates the authentication process directly with the Card Issuer.

- The Card Issuer ACS authenticates your customer and returns the result in the Payer Authentication Response (PAREs). This is returned to you via your customer's browser.

When authentication is completed, the ACS redirects your customer back to the Web site you specified in the *termURL*. Typically, this will be your own Web site.

- Once you receive the PAREs value, you initiate an Authentication request (which contains the PAREs in the *paymentResponse* element) to NETBANX. Here is an example:

```

<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>

```

See the *API Reference Guide for Web Services* for complete details on processing the Authentication request.

10. In the *tdsAuthenticateResponse* element of the *ccTxnResponseV1*, NETBANX returns the following three values you will need to include in a *ccAuthRequestV1*:
 - status (used for the *indicator* element in the *ccAuthRequestV1*)
 - cavv
 - xid
11. You submit a normal Purchase request to NETBANX, including these three values in the *authentication* element of the *ccAuthRequestV1*. Here is a snippet from a Purchase example:

```
<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>Q2prWUI2RFNBc3FOTXNlem50eWY=</xid>
  </authentication>
  ...
</ccAuthRequestV1>
```



All HTTP Posts must be URL encoded using the *application/x-www-form-urlencoded* format (see steps 9 and 11 above). Otherwise, they run the risk of failing because any reserved characters (e.g., slashes, ampersands, etc.) are stripped from requests that are not properly URL encoded.

See the [API Reference Guide for Web Services](#) for complete details on processing the *ccAuthRequestV1*.

Merchant best practices

Here are a few suggestions for displaying the 3D Secure program on your e-commerce Web site.



These suggestions are not exhaustive – for complete details, you should consult the respective Web sites of the card brands you support. For more information, see Important URLs on page 7.

Displaying 3D Secure information and logos

The logos (e.g., Verified by Visa) must at a minimum be placed on the payment details page of the checkout process, as close to the credit card entry fields as possible. The logos should link to the “learn more” URLs of the respective card brands. Ideally, these logos should be displayed prominently on any page that displays payment options.



Typically, you must agree to the Terms and Conditions of any Card Issuer before displaying their logos on your site.

Pre-authentication message

You must provide a pre-authentication message, indicating that the card holder might have to provide authentication information after they click the Buy button.

For example:

“Your card may be eligible for or enrolled in the Verified by Visa payer authentication program. After clicking the Buy button, your Card Issuer may prompt you for your payer authentication password to complete your purchase.”

Displaying the ACS URL

- Do not use popup windows to display the ACS URL – it must be displayed in frame. Visa and MasterCard forbid the use of popup windows as they could be blocked.

The screenshot shows a browser window with a blue border. At the top left is the 'Verified by VISA' logo. To its right is a box containing 'Member Name' with a small 'M' icon above it. Below the logo is the heading 'Added Protection' and the instruction 'Please submit your Verified by Visa password.' The form contains the following text: 'Merchant: merchant.com', 'Amount: \$43.28', 'Date: 01/05/2003', 'Card number: **** * 0335', and 'Personal Message: Shop securely with Verified by Visa.' Below the message is a 'Password:' label followed by a text input field. A link 'Forgot your password?' is positioned below the password field. At the bottom of the form are three buttons: 'Submit', a 'Help' button with a question mark icon, and 'Exit'.

- The frame should be a minimum of 400x400 pixels – large enough to present the entire authentication page, without scrolling, over a standard range of browser resolutions.
- The frame should also contain header text something like the following: “For your security, please fill out the form below to complete your order. Do not click the Refresh or Back button or this transaction may be interrupted or cancelled.”
- You should not display promotional messages to cardholders within the frame. It is important that cardholders have confidence in the authentication session with their card issuer.
- If you use a branded header frame (e.g., to display your merchant logo), do not use active HTML links. Below the header frame, however, you should include a link that directs the cardholder back to the checkout page in case of technical difficulties.
- If a communication is presented the following text is strongly recommended:
 - Processing your order ...
 - Do not click the Refresh or Back button or this transaction may be interrupted.
- Merchants using inline authentication windows with frames must populate the *termURL* field with an HTTPS address.

Timeout sequencing

- You should allow at least 10 seconds for the ACS to send a response to the enrollment lookup message.
- You should allow at least 10 minutes for the return of the PAREs message in response to the PaReq message.

Displaying messages to the customer

- When preparing status and error messages to display to your customers, be sure to take into account all possible outcome scenarios (e.g., timeout error, authentication failed, etc.).
- If Authentication fails, display text similar to the following:
“Your financial institution has indicated that it could not successfully authenticate this transaction. To protect against unauthorized use, this card cannot be used to complete your purchase. You may complete the purchase by selecting another form of payment.”

Tips

- Make sure the Buy button is disabled during authentication.
- Avoid passing the authentication results through hidden form fields or through the URL as query string parameters. Sensitive data passed using these techniques can be easily manipulated by the consumer.

Important URLs

Visit the following URLs for complete details and policies on implementing and advertising the branded 3D Secure program for these major Card Issuers:

- Visa – http://www.visa.ca/verified/merch_marketing.cfm
- MasterCard – http://www.mastercard.com/us/merchant/security/what_can_do/Secure-Code/index.html
- JCB – <http://www.jcb-global.com/english/solution/ec.html>

If you need help ...

If you have questions about your transaction processing, we would be happy to help. Contact Technical Support at:

- support@optimalpayments.com
- 1-888-709-8753

Lookup and Authentication message response values

Based on the Lookup and Authenticate Message response values, merchants are required to control transaction flow in a variety of ways. The following tables outline the recommended actions for the list of possible scenarios that payer authentication integrations must support. Each merchant integration is required to handle each of the following response values.

Payer Authentication Lookup response values

Table 1: Payer Authentication Lookup Response Values

Enrolled Value	Description	Recommended Action
Y	Cardholder authentication is available.	Redirect the consumer to the ACS URL to perform authentication.
N	Cardholder not enrolled in authentication program.	Complete the order as a non-authenticated transaction. Specify the proper ECI value on the authorization transaction. Visa/JCB <ul style="list-style-type: none"> • Merchant has liability protection. • ECI - 06 MasterCard <ul style="list-style-type: none"> • Merchant has no liability protection. • ECI - 01
U	Cardholder authentication is unavailable	Complete the order as a non-authenticated transaction. Specify the proper ECI value on the authorization transaction. Visa/JCB <ul style="list-style-type: none"> • Merchant has no liability protection. • ECI - 07 MasterCard <ul style="list-style-type: none"> • Merchant has no liability protection. • ECI - 01

Payer Authentication Authenticate response values

Table 2: Payer Authentication Authenticate Response Values

PAResStatus Value	Signature Verification Value	Description	Recommended Action
Y	Y	Cardholder authentication completed successfully.	Complete the order as an authenticated transaction. Visa/JCB <ul style="list-style-type: none"> • Merchant has liability protection. • ECI - 05 MasterCard <ul style="list-style-type: none"> • Merchant has liability protection. • ECI - 02
A	Y	Cardholder attempts authentication completed successfully. In the event that a MasterCard transaction results in this response value, a PAResStatus value of U will be returned in the response message.	Complete the order as an authenticated transaction. Visa/JCB <ul style="list-style-type: none"> • Merchant has liability protection. • ECI - 06 MasterCard <ul style="list-style-type: none"> • Merchant has no liability protection • ECI - 01

Table 2: Payer Authentication Authenticate Response Values

PAResStatus Value	Signature Verification Value	Description	Recommended Action
N	Y	Cardholder authentication failed.	Redirect the cardholder to payment details page. Display the recommended failed authentication message to the consumer, and prompt for another form of payment to complete the transaction.
U	Y	Cardholder was unable to be authenticated.	Complete the order as a non-authenticated transaction. Visa/JCB <ul style="list-style-type: none"> • Merchant has no liability protection. • ECI - 07 MasterCard <ul style="list-style-type: none"> • Merchant has no liability protection • ECI - 01
Y, A, N, U	N	Fraud check failure indicates that the transaction results can not be trusted.	Redirect the cardholder to payment details page. Display the recommended failed authentication message to the consumer, and prompt for another form of payment to complete the transaction.

Test cases

You can test your application by sending messages to the test environment using the card numbers provided below for various 3D Secure scenarios. Each card number will generate a unique response that your integration should be able to account for and handle properly.

Verified by Visa test cases

VBV test case 1

- Cardholder enrolled
- Successful authentication
- Successful signature verification

Table 3: VBV Test Case 1

Test Card Number	Responses	Merchant Action	Chargeback Liability
4000000000000002	<p>cmpi_lookup response</p> <ul style="list-style-type: none"> • Enrolled = Y • ACSUrl = <url> • Payload = <PAREs Payload Value> • ErrorNo = 0 • ErrorDesc = <blank> <p>cmpi_authenticate response</p> <ul style="list-style-type: none"> • PAREsStatus = Y • SignatureVerification = Y • EciFlag = 05 • Xid = <XID Value> • Cavv = <CAVV Value> • ErrorNo = 0 • ErrorDesc = <blank> 	Merchant should append the Cavv and EciFlag values to the authorization message.	None.

VBV test case 2

- Cardholder enrolled
- Successful authentication
- Unsuccessful signature verification

Table 4: VBV Test Case 2

Test Card Number	Responses	Merchant Action	Chargeback Liability
4000000000000010	<p>cmpi_lookup response</p> <ul style="list-style-type: none"> • Enrolled = Y • ACSUrl = <url> • Payload = <PAREs Payload Value> • ErrorNo = 0 • ErrorDesc = <blank> <p>cmpi_authenticate response</p> <ul style="list-style-type: none"> • PAREsStatus = Y • SignatureVerification = N • EciFlag = 05 • Xid = <XID Value> • Cavv = <CAVV Value> • ErrorNo = 0 • ErrorDesc = <blank> 	Merchant should not continue authorization, due to the failed signature verification. Merchant should prompt for another form of payment or attempt to authenticate the consumer again starting with a new cmpi_lookup message.	

VBV test case 3

- Cardholder enrolled
- Unsuccessful authentication
- Successful signature verification

Table 5: VBV Test Case 3

Test Card Number	Responses	Merchant Action	Chargeback Liability
40000000000000028	cmpt_lookup response <ul style="list-style-type: none"> Enrolled = Y ACSUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank> cmpt_authenticate response <ul style="list-style-type: none"> PAREsStatus = N SignatureVerification = Y EciFlag = 07 Xid = <XID Value> Cavv = <blank> ErrorNo = 0 ErrorDesc = <blank> 	Merchant should not continue with authorization. Merchant should prompt for another form of payment and is not permitted to submit this transaction for authorization.	

VBV test case 4

- Cardholder enrolled
- Authentication not able to complete (Authenticate message response)

Table 6: VBV Test Case 4

Test Card Number	Responses	Merchant Action	Chargeback Liability
40000000000000036	cmpt_lookup response <ul style="list-style-type: none"> Enrolled = Y ACSUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank> cmpt_authenticate response <ul style="list-style-type: none"> PAREsStatus = U SignatureVerification = Y EciFlag = 07 Xid = <XID Value> Cavv = <blank> ErrorNo = 0 ErrorDesc = <blank> 	Merchants have the option of retaining the liability and submit the transaction as nonauthenticated. An alternative action would be to prompt for another form of payment.	Merchant retains the chargeback liability.

VBV test case 5

- Timeout encountered while processing the cmpt_lookup transaction

Table 7: VBV Test Case 5

Test Card Number	Responses	Merchant Action	Chargeback Liability
4000000000000044	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = U ACUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> cmpi_authenticate message does not apply in this case. 	The cmpi_lookup transaction will simulate a timeout scenario and required 20 seconds to complete the transaction processing with the other 3-D Secure systems. Merchant integration should handle timeout processing after 10-12 seconds and proceed with the authorization message.	Merchant retains the chargeback liability.

VBV test case 6

- Cardholder not enrolled

Table 8: VBV Test Case 6

Test Card Number	Responses	Merchant Action	Chargeback Liability
4000000000000051	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = N ACUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> cmpi_authenticate message does not apply in this case. 	Merchant should submit the authorization with an ECI of 06, granting chargeback protection.	No

VBV test case 7

- Cardholder enrolled
- Authentication unavailable (Lookup message response)

Table 9: VBV Test Case 7

Test Card Number	Responses	Merchant Action	Chargeback Liability
4000000000000069	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = U ACUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> cmpi_authenticate message does not apply in this case. 	Merchant should proceed with the authorization message.	Merchant retains the chargeback liability.

VBV test case 8

- Merchant not able to execute transactions (merchant not active)

Table 10: VBV Test Case 8

Test Card Number	Responses	Merchant Action	Chargeback Liability
4000000000000077	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = <blank> ACUrl = <blank> Payload = <blank> ErrorNo = Error Number ErrorDesc = Error Description cmpi_authenticate response <ul style="list-style-type: none"> cmpi_authenticate message does not apply in this case. 	Merchant should continue with the authorization and contact technical support to investigate and resolve the issue.	Merchant retains the chargeback liability.

VBV test case 9

- Error response to cmpi_lookup message

Table 11: VBV Test Case 9

Test Card Number	Responses	Merchant Action	Chargeback Liability
4000000000000085	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = <blank> ACUrl = <blank> Payload = <blank> ErrorNo = Error Number ErrorDesc = Error Description cmpi_authenticate response <ul style="list-style-type: none"> cmpi_authenticate message does not apply in this case. 	Merchant should continue with the authorization and contact technical support to investigate and resolve the issue.	Merchant retains the chargeback liability.

VBV test case 10

- Cardholder enrolled
- Error response to cmpi_authenticate message

Table 12: VBV Test Case 10

Test Card Number	Responses	Merchant Action	Chargeback Liability
4000000000000093	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = Y ACSUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> PAREsStatus = <blank> SignatureVerification = <blank> EciFlag = <blank> Xid = <blank> Cavv = <blank> ErrorNo = Error Number ErrorDesc = Error Description 	Merchant should not continue with authorization. Merchant should prompt for another form of payment.	Merchant retains the chargeback liability.

VBV test case 11

- Cardholder enrolled
- Processing attempts performed

Table 13: VBV Test Case 11

Test Card Number	Responses	Merchant Action	Chargeback Liability
4000000000000101	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = Y ACSUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> PAREsStatus = A SignatureVerification = Y EciFlag = 06 Xid = <XID Value> Cavv = <CAVV Value> ErrorNo = 0 ErrorDesc = <blank> 	Merchant should append the Cavv and EciFlag values to the authorization message.	Merchant is granted chargeback protection.

MasterCard SecureCode test cases

MCSC test case 1

- Cardholder enrolled
- Successful authentication

- Successful signature verification.

Table 14: MCSC Test Case 1

Test Card Number	Responses	Merchant Action	Chargeback Liability
5200000000000007	cmpi_lookup response <ul style="list-style-type: none"> • Enrolled = Y • ACSUrl = <url> • Payload = <PAREs Payload Value> • ErrorNo = 0 • ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> • PAREsStatus = Y • SignatureVerification = Y • EciFlag = 02 • Xid = <XID Value> • Cavv = <CAVV Value> • ErrorNo = 0 • ErrorDesc = <blank> 	Merchant should append the Cavv and EciFlag values to the authorization message.	None.

MCSC test case 2

- Cardholder enrolled
- Successful authentication
- Unsuccessful signature verification

Table 15: MCSC Test Case 2

Test Card Number	Responses	Merchant Action	Chargeback Liability
5200000000000015	cmpi_lookup response <ul style="list-style-type: none"> • Enrolled = Y • ACSUrl = <url> • Payload = <PAREs Payload Value> • ErrorNo = 0 • ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> • PAREsStatus = Y • SignatureVerification = N • EciFlag = 02 • Xid = <XID Value> • Cavv = <CAVV Value> • ErrorNo = 0 • ErrorDesc = <blank> 	Merchant should not continue authorization, due to the failed signature verification. Merchant should prompt for another form of payment or attempt to authenticate the consumer again starting with a new cmpi_lookup message.	

MCSC test case 3

- Cardholder enrolled
- Unsuccessful authentication
- Successful signature verification

Table 16: MCSC Test Case 3

Test Card Number	Responses	Merchant Action	Chargeback Liability
5200000000000023	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = Y ACSUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> PAREsStatus = N SignatureVerification = Y EciFlag = 01 Xid = <XID Value> Cavv = <blank> ErrorNo = 0 ErrorDesc = <blank> 	Merchant should not continue with authorization. Merchant should prompt for another form of payment and is not permitted to submit this transaction for authorization.	

MCSC test case 4

- Cardholder enrolled
- Authentication not able to complete (Authenticate message response)

Table 17: MCSC Test Case 4

Test Card Number	Responses	Merchant Action	Chargeback Liability
5200000000000031	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = Y ACSUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> PAREsStatus = U SignatureVerification = Y EciFlag = 01 Xid = <XID Value> Cavv = <blank> ErrorNo = 0 ErrorDesc = <blank> 	Merchants have the option of retaining the liability and submit the transaction as nonauthenticated. An alternative action would be to prompt for another form of payment.	Merchant retains the chargeback liability.

MCSC test case 5

- Cardholder enrolled
- Authentication unavailable (Lookup message response)

Table 18: MCSC Test Case 5

Test Card Number	Responses	Merchant Action	Chargeback Liability
5200000000000049	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = U ACUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> cmpi_authenticate message does not apply in this case. 	The cmpi_lookup transaction will simulate a timeout scenario and required 20 seconds to complete the transaction processing with the other 3-D Secure systems. Merchant integration should handle timeout processing after 10-12 seconds and proceed with the authorization message.	Merchant retains the chargeback liability.

MCSC test case 6

- Cardholder not enrolled

Table 19: MCSC Test Case 6

Test Card Number	Responses	Merchant Action	Chargeback Liability
5200000000000056	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = N ACUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> cmpi_authenticate message does not apply in this case. 	Merchant should proceed with transaction.	Merchant retains the chargeback liability.

MCSC test case 7

- Cardholder enrolled
- Authentication unavailable (Lookup message response)

Table 20: MCSC Test Case 7

Test Card Number	Responses	Merchant Action	Chargeback Liability
5200000000000064	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = U ACUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> cmpi_authenticate message does not apply in this case. 	Merchant should proceed with the authorization message.	Merchant retains the chargeback liability.

MCSC test case 8

- Merchant not able to execute transactions (merchant not active)

Table 21: MCSC Test Case 8

Test Card Number	Responses	Merchant Action	Chargeback Liability
5200000000000072	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = <blank> ACSUrl = <blank> Payload = <blank> ErrorNo = Error Number ErrorDesc = Error Description cmpi_authenticate response <ul style="list-style-type: none"> cmpi_authenticate message does not apply in this case. 	Merchant should continue with the authorization and contact technical support to investigate and resolve the issue.	Merchant retains the chargeback liability.

MCSC test case 9

- Error response to cmpi_lookup message

Table 22: MCSC Test Case 9

Test Card Number	Responses	Merchant Action	Chargeback Liability
5200000000000080	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = <blank> ACSUrl = <blank> Payload = <blank> ErrorNo = Error Number ErrorDesc = Error Description cmpi_authenticate response <ul style="list-style-type: none"> cmpi_authenticate message does not apply in this case. 	Merchant should continue with the authorization and contact technical support to investigate and resolve the issue.	Merchant retains the chargeback liability.

MCSC test case 10

- Cardholder enrolled
- Error response to cmpi_authenticate message

Table 23: MCSC Test Case 10

Test Card Number	Responses	Merchant Action	Chargeback Liability
5200000000000098	Cardholder enrolled, error response to <code>cmpi_authenticate</code> message cmpi_lookup response <ul style="list-style-type: none"> Enrolled = Y ACUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> PAREsStatus = <blank> SignatureVerification = <blank> EciFlag = <blank> Xid = <blank> Cavv = <blank> ErrorNo = Error Number ErrorDesc = Error Description 	Merchant should not continue with authorization. Merchant should prompt for another form of payment.	If the transaction is submitted for authorization, liability will remain with the merchant.

JCB J/Secure test cases

J/Secure test case 1

- Cardholder enrolled
- Successful authentication
- Ssuccessful signature verification.

Table 24: J/Secure Test Case 1

Test Card Number	Responses	Merchant Action	Chargeback Liability
3000000000000004	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = Y ACUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> PAREsStatus = Y SignatureVerification = Y EciFlag = 05 Xid = <XID Value> Cavv = <CAVV Value> ErrorNo = 0 ErrorDesc = <blank> 	Merchant should append the Cavv and EciFlag values to the authorization message.	None.

J/Secure test case 2

- Cardholder enrolled
- Successful authentication
- Unsuccessful signature verification

Table 25: J/Secure Test Case 2

Test Card Number	Responses	Merchant Action	Chargeback Liability
3000000000000012	<p>cmpi_lookup response</p> <ul style="list-style-type: none"> • Enrolled = Y • ACSUrl = <url> • Payload = <PAREs Payload Value> • ErrorNo = 0 • ErrorDesc = <blank> <p>cmpi_authenticate response</p> <ul style="list-style-type: none"> • PAREsStatus = Y • SignatureVerification = N • EciFlag = 05 • Xid = <XID Value> • Cavv = <CAVV Value> • ErrorNo = 0 • ErrorDesc = <blank> 	Merchant should not continue authorization, due to the failed signature verification. Merchant should prompt for another form of payment or attempt to reauthenticate the consumer.	

J/Secure test case 3

- Cardholder enrolled
- Unsuccessful authentication
- Successful signature verification

Table 26: J/Secure Test Case 3

Test Card Number	Responses	Merchant Action	Chargeback Liability
3000000000000020	<p>cmpi_lookup response</p> <ul style="list-style-type: none"> • Enrolled = Y • ACSUrl = <url> • Payload = <PAREs Payload Value> • ErrorNo = 0 • ErrorDesc = <blank> <p>cmpi_authenticate response</p> <ul style="list-style-type: none"> • PAREsStatus = N • SignatureVerification = Y • EciFlag = 07 • Xid = <XID Value> • Cavv = <blank> • ErrorNo = 0 • ErrorDesc = <blank> 	Merchant should prompt for another form of payment and is not permitted to submit this transaction for authorization.	

J/Secure test case 4

- Cardholder enrolled
- Authentication unavailable (Authenticate message response)

Table 27: J/Secure Test Case 4

Test Card Number	Responses	Merchant Action	Chargeback Liability
3000000000000038	cmpi_lookup response <ul style="list-style-type: none"> • Enrolled = Y • ACSUrl = <url> • Payload = <PAREs Payload Value> • ErrorNo = 0 • ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> • PAREsStatus = U • SignatureVerification = Y • EciFlag = 07 • Xid = <XID Value> • Cavv = <blank> • ErrorNo = 0 • ErrorDesc = <blank> 	Merchants have the option of retaining the liability and submit the transaction as nonauthenticated. An alternative action would be to prompt for another form of payment.	

J/Secure test case 5

- Cardholder enrolled
- Authentication unavailable

Table 28: J/Secure Test Case 5

Test Card Number	Responses	Merchant Action	Chargeback Liability
213100000000027	cmpi_lookup response <ul style="list-style-type: none"> • Enrolled = U • ACSUrl = <blank> • Payload = <blank> • ErrorNo = 0 • ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> • cmpi_authenticate message does not apply in this case. 	The cmpi_lookup transaction will simulate a timeout scenario and required 20 seconds to complete the transaction processing with the other 3-D Secure systems. Merchant integration should handle timeout processing after 10-12 seconds and proceed with the authorization message. .	Merchant retains the chargeback liability

J/Secure test case 6

- Cardholder enrolled
- Authentication cancelled by user (simulating the consumer abandoning the authentication window)

Table 29: J/Secure Test Case 6

Test Card Number	Responses	Merchant Action	Chargeback Liability
213100000000019	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = Y ACSUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> cmpi_authenticate message does not apply in this case. 	No action can be taken. Transaction abandoned.	

J/Secure test case 7

- Cardholder enrolled
- Authentication unavailable

Table 30: J/Secure Test Case 7

Test Card Number	Responses	Merchant Action	Chargeback Liability
213100000000027	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = U ACSUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank> cmpi_authenticate response <ul style="list-style-type: none"> cmpi_authenticate message does not apply in this case. 	Merchant should proceed with the authorization message.	Merchant retains the chargeback liability.

J/Secure test case 8

- Merchant not able to execute transactions (merchant not active)

Table 31: J/Secure Test Case 8

Test Card Number	Responses	Merchant Action	Chargeback Liability
213100000000035	cmpi_lookup response <ul style="list-style-type: none"> Enrolled = <blank> ACSUrl = <blank> Payload = <blank> ErrorNo = Error Number ErrorDesc = Error Description cmpi_authenticate response <ul style="list-style-type: none"> cmpi_authenticate message does not apply in this case. 	Merchant should continue with the authorization and contact technical support to investigate and resolve the issue.	Merchant retains the chargeback liability.

J/Secure test case 9

- Error response to cmpi_lookup message

Table 32: J/Secure Test Case 9

Test Card Number	Responses	Merchant Action	Chargeback Liability
1800000000000002	cmpt_lookup response <ul style="list-style-type: none"> Enrolled = <blank> ACUrl = <blank> Payload = <blank> ErrorNo = Error Number ErrorDesc = Error Description cmpt_authenticate response <ul style="list-style-type: none"> cmpt_authenticate message does not apply in this case. 	Merchant should continue with the authorization and contact technical support to investigate and resolve the issue.	Merchant retains the chargeback liability.

J/Secure test case 10

- Cardholder enrolled
- Error response to cmpt_authenticate message

Table 33: J/Secure Test Case 10

Test Card Number	Responses	Merchant Action	Chargeback Liability
1800000000000010	cmpt_lookup response <ul style="list-style-type: none"> Enrolled = Y ACUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank> cmpt_authenticate response <ul style="list-style-type: none"> PAREsStatus = <blank> SignatureVerification = <blank> EciFlag = <blank> Xid = <blank> Cavv = <blank> ErrorNo = Error Number ErrorDesc = Error Description 	Merchant should not continue with authorization. Merchant should prompt for another form of payment.	If the transaction is submitted for authorization, liability will remain with the merchant.

J/Secure test case 11

- Cardholder enrolled, processing attempts performed

Table 34: J/Secure Test Case 11

Test Card Number	Responses	Merchant Action	Chargeback Liability
180000000000028	<p>cmpi_lookup response</p> <ul style="list-style-type: none"> • Enrolled = Y • ACSUrl = <url> • Payload = <PAREs Payload Value> • ErrorNo = 0 • ErrorDesc = <blank> <p>cmpi_authenticate response</p> <ul style="list-style-type: none"> • PAREsStatus = A • SignatureVerification = Y • EciFlag = 06 • Xid = <XID Value> • Cavv = <CAVV Value> • ErrorNo = 0 • ErrorDesc = <blank> 	Merchant should append the Cavv and ECI values to the authorization message.	Merchant is granted chargeback protection.