

Message **cmpi_lookup**

This message is used to verify if the issuer and cardholder participates in an Authentication program by utilizing the PAN value passed in the message to determine the proper Payment Initiative (PI). Using the version value, the message will process according to the PI under its primary message version as defined by the system.

Field Name	Description	Required
MsgType	cmpi_lookup	Y
Version	Application message version identifier. (Should be 1.4 for new development)	Y
ProcessorId	Application processor identifier.	Y
MerchantId	Application defined merchant identification code.	Y
Password	Required only when processing certain Visa Regions. Used to facilitate Merchant Authentication File (MAF) authentication processing.	N
OrderNumber	Order Number from the merchant commerce website.	Y
PurchaseAmount	Formatted Total Sale amount for the transaction (E.g. \$123.67).	N
RawAmount	Total sale amount without any decimalization (E.g. 12367).	Y
PurchaseCurrency	3 digit numeric, ISO 4217 currency code for the sale amount.	Y
PAN	Credit Card number used for the transaction.	Y
PANExpr	Credit Card expiration date, formatted YYMM.	Y
OrderDesc	Brief description of items purchased, limited to 125 characters.	N
UserAgent	The exact content of the HTTP user-agent header.	N

Field Name	Description	Required
BrowserHeader	The exact content of the HTTP accept header.	N
Recurring	Flag to specify if the Merchant and cardholder have agreed to recurring payments. (Y/N)	N
RecurringFrequency	Integer value indicating the minimum number of days between authorizations. A frequency of monthly is indicated by the value 28. Required if recurring = Y.	N
RecurringEnd	The date after which no further recurring authorizations should be preformed. Format YYYYMMDD. Required if recurring = Y.	N
Installment	An integer value greater than 1 indicating the maximum number of permitted authorizations for installment payments. Must be included if the merchant and cardholder have agreed to installment payments.	N

Sample Message

```

<CardinalMPI>
  <MsgType>cmpi_lookup</MsgType>
  <Version>1.4</Version>
  <ProcessorId>100</ProcessorId>
  <MerchantId>123456</MerchantId>
  <Password></Password>
  <OrderNumber>182397541265</OrderNumber>
  <PurchaseAmount>$123.45</PurchaseAmount>
  <RawAmount>12345</RawAmount>
  <PurchaseCurrency>840</PurchaseCurrency>
  <PAN>4111111111111111</PAN>
  <PANExpr>0501</PANExpr>
  <OrderDesc>Order #182397541265</OrderDesc>
  <UserAgent>Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)</UserAgent>
  <BrowserHeader>*/*</BrowserHeader>
  <Recurring>Y</Recurring>
  <RecurringFrequency>28</RecurringFrequency>
  <RecurringEnd>20050101</RecurringEnd>
  <Installment>2</Installment>
</CardinalMPI>

```

Response to cmpi_lookup

This message is generated as a response to the cmpi_lookup message.

Field Name	Description	Required
ErrorDesc	Application error description for the associated error number.	Y
ErrorNo	Application error number. A non zero value represents the error encountered while attempting the process the message request.	Y
TransactionId	Transaction Id. This value is required to be passed on the cmpi_authenticate message to link the cmpi_lookup and cmpi_authenticate message together.	Y
Payload	Contains the encoded PAREq generated by MAPS. Available if Enrolled = Y.	N
SPAHiddenFields	Contains the SPA hidden form fields. This value is only available during MasterCard transactions.	N
Enrolled	Cardholder enrollment status. (Y = Cardholder Enrolled, N = Not Enrolled, or U = Cardholder Enrolled but Authentication Unavailable)	Y
ACSUrl	Contains the fully qualified URL of the Issuer ACS. This is used by the merchant to redirect the cardholder. Returned if Enrolled = Y.	N

Sample Message

```
<CardinalMPI>
  <ErrorDesc></ErrorDesc>
  <ErrorNo>0</ErrorNo>
  <TransactionId>75f986t76f6</TransactionId>
  <Payload>eNpVUK1TwjAQ/SsM402nSUuKwGwzq1QUFUXhoMeQ7rR12rSkLSC/3gSoH5PLvreb7svg
  VWiEcMlykYjhzlWYixk0ZB97DLA//2lflidPWUDedr+kqSzzDRj0XQ5bAYv+GGwxZ1lRaKuw51PCAtNEpaJ
  kLVHITc3MyeeY/ZA+QMIUc9C7nbY36fMeb7JnWiQkC+UToKFUi67RCQI48yKJRtf7iA0aBtAAanfGkrssRlB
  vdzpHn27LJjahExwRABGQ38kWjY0ql7pPI74u44frhzy+nRzuVo+XHxuxfHdV+oRkFgCxFRCJGrlHaY8O
  Pdbx3BH1Rnanlw8it9PwC/eq5/WdgW92PTFQ2kbjE3BN0ub+cmDc16hku1WLAPdlodBUGGt/Yoiwknw
  p8jLDzouOUDuOY4awLJDfpSb31nxZW5vvBTppj9+bbaf26lUi8tZHMZBYJ/JWGA7pcZlyig7trlAiJUG55c
  m589hon+f5hv738Di</Payload>
  <SPAHiddenFields></SPAHiddenFields>
  <Enrolled>Y</Enrolled>
  <ACSUrl>https://www.issuingbank.com/acs</ACSUrl>
</CardinalMPI>
```

Message **cmpi_authenticate**

This message is used to communicate the Payer Authentication Response (PAREs) generated by the Issuer ACS software to the MAPS. The MAPS will verify the digital signature within the PAREs to validate that the PAREs was generated by legitimate Issuer ACS software. The MAPS will extract the transaction status, Xid, CAVV/AAV and the ECI flag and provide the data elements to the Merchant.

Field Name	Description	Required
MsgType	cmpi_authenticate	Y
Version	Application message version identifier. (Should be 1.4 for new development)	Y
TransactionId	Transaction Id. This value is required to be passed on the cmpi_authenticate message to link the cmpi_lookup and cmpi_authenticate message together.	Y
ProcessorId	Application processor identifier.	Y
MerchantId	Application defined merchant identification code.	Y
PAREsPayload	PAREs generated by the issuer ACS.	Y

Sample Message<CardinalMPI>

```
<Version>1.4</Version>
<MsgType>cmpi_authenticate</MsgType>
<TransactionId>75f986t76f6</TransactionId>
<ProcessorId>100</ProcessorId>
<MerchantId>123456</MerchantId>
<PAREsPayload>***** PAREs Message *****</PAREsPayload>
</CardinalMPI>
```

Response to cmpi_authenticate

This message is generated as a response to the cmpi_authenticate message.

Field Name	Description	Required
ErrorDesc	Application error description for the associated error number.	Y
ErrorNo	Application error number. A non zero value represents the error encountered while attempting the process the message request.	Y
Cavv	Transaction Stain from PAREs. (28 character, Base 64 encoded). This value should be appended to the authorization message signifying that the transaction has been successfully authenticated.	Y
SignatureVerification	Status of the Signature Verification of the PAREs message (Y or N). Y indicates that the signature of the xml message has been validated successfully and the message contents can be trusted. N indicates that for a variety of reason, tampering, certificate expiration, etc. the message could not be validated, and the result should not be trusted.	Y
Xid	Transaction Xid from PAREs. This value should be appended to the authorization message signifying that the transaction has been successfully authenticated.	Y
EciFlag	E-Commerce Indicator (ECI) from PAREs. This value should be appended to the authorization message signifying that the transaction has been successfully authenticated.	Y
PAResStatus	Transaction status from PAREs (Y, N, U, or A)	Y

Sample Message

```
CardinalMPI>  
  <ErrorDesc></ErrorDesc>  
  <ErrorNo>0</ErrorNo>  
  <Cavv>AAAAAAAAAAAAAAAAAAAAAAAAAAAA=</Cavv>  
  <SignatureVerification>Y</SignatureVerification>  
  <Xid>64E775ftff67f7R7Fr7</Xid>  
  <EciFlag>05</EciFlag>  
  <PAResStatus>Y</PAResStatus>  
</CardinalMPI>
```

USING THE RESPONSE VALUES

To get the full benefit from the Visa (VbV) and MasterCard (SecureCode) payment authentication programs, Merchants must not only make changes to their web site to incorporate the authentication process itself, but must also slightly alter the authorization process.

New authentication data elements have been introduced in support of both VbV and SecureCode programs. As of April 5, 2003, these new data elements (eCommerce Indicator (ECI) and Cardholder Authentication Verification Value/Universal Cardholder Authentication Field (CAVV/UCAF)) must be passed as part of the authorization process to achieve the full benefit of authentication and qualify for chargeback protection for Visa reason codes 23, 61, 75 and 83 and MasterCard reason code 37.

Another important note, Access Control Servers (Card Issuer side of authentication) are not required to return ECI values in any case other than a successful execution, although some may always return an ECI, regardless of the outcome. If the ECI is not present, the Merchant must place the value presented below in the ECI field of the authorization message before forwarding the request.

Decision Matrices

Merchant web site interaction is carried out through two message types, `cmpi_lookup` and `cmpi_authenticate`. The matrices following show the possible response values from each of the messages with the related description and the suggested action the Merchant should take when the response is presented. Please remember that not every case is clear-cut and risk based decisions will still need to be made.

Lookup Response (cmpi_lookup message)

Response Values	Description	Action
Y	Card is eligible for authentication processing	Merchant forwards Payer Authentication Request to Access Control Server.
N	<p>Visa: Card is eligible for attempts liability, but attempts proof is not available. This response value will not be used by Issuers in the U.S.; however, it will be used by those in other countries.</p> <p>MasterCard: Card is not eligible or enrolled in SecureCode program. Merchant retains liability.</p>	<p>Visa: Merchant proceeds with purchase, submitting an ECI of 6 in the Authorization Request and leaves the CAVV blank.</p> <p>The Issuer may not submit a chargeback if the cardholder later disputes this purchase. The Merchant gets chargeback protection.</p> <p>MasterCard: Merchant proceeds with purchase, submitting an ECI of 1 in the Authorization Request and leaves the CAVV blank.</p> <p>The Merchant retains the liability if the cardholder later disputes making this purchase.</p>
U	Unable to process or card is not eligible for attempts processing (e.g., Commercial and anonymous Prepaid Cards)	<p>Merchant proceeds with purchase as non-authenticated and submits authorization with ECI of 7 (Visa) or 1 (MasterCard).</p> <p>The Merchant retains the liability if the cardholder later disputes making this purchase.</p>
Blank	An enrollment response was not returned from the MAPS server.	<p>Merchant should resubmit enrollment request. After retry processing is complete,, processing should continue without authentication.</p> <p>Incident should be reported to technical support using the error number returned with the cmpi_lookup response.</p> <p>The Merchant retains the liability if the cardholder later disputes making this purchase.</p>
Error	The MAPS server encountered an error while processing.	<p>Submit the authorization request. Verify the cmpi_lookup message format and contact Technical Support.</p> <p>The Merchant retains the liability and should contact Technical Support to research this issue.</p>

Authenticate Response (cmpi_authenticate message)

Response Values	Description	Action
Y	Authentication approved. The Issuer has authenticated the cardholder by verifying the identity information or password.	The ACS returns a CAVV and an ECI of 5 (Visa) or 2 (MasterCard) in the Payer Authentication Response. The Issuer may not submit a chargeback if the cardholder later disputes this purchase. The Merchant gets chargeback protection.
A	Authentication attempted. The Cardholder is not enrolled and the Merchant has attempted authentication. Note: MasterCard SecureCode does not support attempts processing.	The ACS returns a CAVV and an ECI of 6 (Visa) or 1 (MasterCard) in the Payer Authentication Response. The Issuer may not submit a chargeback if the cardholder later disputes this purchase. The Merchant gets chargeback protection.
N	Authentication failed. The Issuer is not able to authenticate the cardholder. The ACS does not return CAVV or ECI values in the Payer Authentication Response.	Merchants are not permitted to submit these transactions for authorization processing. The Merchant should prompt the cardholder for another form of payment to complete the transaction.
U	Unable to authenticate. The Issuer ACS is not able to complete the authentication request and does not return a CAVV or an ECI value.	Merchants proceed with these purchases as non-authenticated. The Merchant retains the liability if the cardholder later disputes this purchase.
Blank	An Authentication Response was not returned from the Issuer ACS. Possible reasons include: - User closed the popup window. - The user is running pop-up blocking software that prevents the pop-up from appearing. - The Merchant's site did not correctly open the popup window.	Merchants proceed with these purchases as non-authenticated. Merchant retains liability if the cardholder later disputes making this purchase.
Error	The MAPS server encountered an error within the PAREs generated by the Issuer ACS server.	Errors are more susceptible to malicious activity. It is in the Merchant's best interest to attempt to re-authenticate the cardholder or ask for another form of payment. The Merchant retains the liability if the transaction is sent for authorization without re-authenticating.

Testing Environment

To assist your integration efforts, the Testing Facility is available to perform various predefined integration tests. Once you have completed integration with your site, testing can begin by sending messages to the testing facility using the following test case PAN numbers. Each PAN will generate a unique response that your integration should be able to account for and handle properly.

To support end to end certification requirements of ecommerce systems the Test environment support the various test case outcomes to be invoked thru either the PAN or PAN expiration values. In those cases where gateways or processors required specific card numbers to be used the defined PAN expiration values can be used to invoke and test the various 3-D Secure authentication responses thru the test system. Note that the test case PAN values take precedence over the PAN expiration values within the test system. These PAN expiration values can be used with any of the supported card types, however depending on operating guidelines some outcomes may not apply.

PAN Value	Test Case Description
0701	Cardholder Enrolled (Y), Successful Authentication (Y), Successful Signature Verification (Y)
0702	Cardholder Enrolled (Y), Successful Authentication (Y), Unsuccessful Signature Verification (N)
0703	Cardholder Enrolled (Y), Unsuccessful Authentication (N), Successful Signature Verification (Y)
0704	Cardholder Enrolled (Y), Attempts Authentication (A), Successful Signature Verification (Y)
0705	Cardholder Enrolled (Y), Authentication Unavailable (U)
0706	Cardholder Enrolled (Y), Authentication Abandoned
0707	Cardholder Not Enrolled (N)
0708	Authentication Unavailable (U)
0709	Merchant Not able to execute transactions (Merchant not Active)
0710	Error Response to <code>cmpi_lookup</code>
0711	Cardholder Enrolled (Y), Error Response to <code>cmpi_authenticate</code>

To use the testing facility, the following must be used with the post command to send the messages into the testing facility:

<https://centineltest.cardinalcommerce.com/maps/txns.asp>

In addition to the test PANs listed below, other data elements are required to be passed within the messages. Refer to the API section of the installation guide for the particular web application. It is extremely important to note that these values are validated based solely on their format, not on the correctness of the content of the information.

It is recommended that you use your production Merchant Id and Processor Id values. During testing, if you do not have your Merchant Id or Processor Id information, you can specify and use any value as long as the value meets the data requirements. To assist with any potential support issues, it is recommended that you provide your Merchant name within the order description field of the cmpi_lookup request.

Verified by Visa (VbV) Test Cases

Test Case 1

Test PAN	Scenario
4000000000000002	Successful Authentication. Cardholder enrolled, successful authentication, successful signature verification.
	cmpi_lookup response
	Enrolled = Y ACUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	PAREsStatus = Y SignatureVerification = Y ECiFlag = 05 Xid = <XID Value> Cavv = <CAVV Value> ErrorNo = 0 ErrorDesc = <blank>
	Merchant Action
Merchant should append the CAVV and ECiFlag values to the authorization message.	

Test Case 2

Test PAN	Scenario
4000000000000010	Cardholder enrolled, successful authentication, unsuccessful signature verification
	cmpi_lookup response
	Enrolled = Y ACUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	PAREsStatus = Y SignatureVerification = N EciFlag = 05 Xid = <XID Value> Cavv = <CAVV Value> ErrorNo = 0 ErrorDesc = <blank>
	Merchant Action
	Merchant should NOT continue authorization, due to the failed signature verification. Merchant should prompt for another form of payment or attempt to re-authenticate the consumer.

Test PAN	Scenario
4000000000000028	Cardholder enrolled, unsuccessful authentication, successful signature verification
	cmpi_lookup response
	Enrolled = Y ACUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	PAREsStatus = N SignatureVerification = Y EciFlag = 07 Xid = <XID Value> Cavv = <blank> ErrorNo = 0 ErrorDesc = <blank>
	Merchant Action
	Merchant should not continue with authorization. Merchant should prompt for another form of payment and is not permitted to submit this transaction for authorization.

Test Case 3

Test Case 4

Test PAN	Scenario
4000000000000036	Cardholder enrolled, Authentication not able to complete (PAREs)
	cmpi_lookup response
	Enrolled = Y ACUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	PAREsStatus = U SignatureVerification = Y EciFlag = 07 Xid = <XID Value> Cavv = <blank> ErrorNo = 0 ErrorDesc = <blank>
	Merchant Action
Merchants have the option of retaining the liability and submit the transaction as non-authenticated. An alternative action would be to prompt for another form of payment.	

Test Case 5

Test PAN	Scenario
4000000000000044	Cardholder enrolled, Authentication cancelled by user (simulating the consumer abandoning the authentication window)
	cmpi_lookup response
	Enrolled = Y ACUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	cmpi_authenticate message does not apply in this case.
	Merchant Action
Merchants have the option of proceeding with the transaction and retaining liability, or prompt for another form of payment.	

Test Case 6

Test PAN	Scenario
4000000000000051	Cardholder not enrolled
	cmpi_lookup response
	Enrolled = N ACUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	cmpi_authenticate message does not apply in this case.
	Merchant Action
	Merchant should submit the authorization with an ECI of 06, granting chargeback protection.

Test Case 7

Test PAN	Scenario
4000000000000069	Cardholder enrolled, Authentication unavailable (VERes)
	cmpi_lookup response
	Enrolled = U ACUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	cmpi_authenticate message does not apply in this case.
	Merchant Action
	Merchant should proceed with the authorization message. merchant retains the chargeback liability.

Test Case 8

Test PAN	Scenario
4000000000000077	Merchant not able to execute transactions (merchant not active)
	cmpi_lookup response
	Enrolled = <blank> ACUrl = <blank> Payload = <blank> ErrorNo = Error Number ErrorDesc = Error Description
	cmpi_authenticate response
	cmpi_authenticate message does not apply in this case.
	Merchant Action
Merchant should continue with the authorization and contact technical support to investigate and resolve the issue. Merchant retains chargeback liability.	

Test Case 9

Test PAN	Scenario
4000000000000085	Error response to cmpi_lookup message
	cmpi_lookup response
	Enrolled = <blank> ACUrl = <blank> Payload = <blank> ErrorNo = Error Number ErrorDesc = Error Description
	cmpi_authenticate response
	cmpi_authenticate message does not apply in this case.
	Merchant Action
Merchant should continue with the authorization and contact technical support to investigate and resolve the issue. Merchant retains chargeback liability.	

Test Case 10

Test PAN	Scenario
4000000000000093	Cardholder enrolled, error response to cmpi_authenticate message
	cmpi_lookup response
	Enrolled = Y ACUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	PAREsStatus = <blank> SignatureVerification = <blank> EciFlag = <blank> Xid = <blank> Cavv = <blank> ErrorNo = Error Number ErrorDesc = Error Description
	Merchant Action
Merchant should continue with the authorization and contact technical support to investigate and resolve the issue. Merchant retains chargeback liability.	

Test Case 11

Test PAN	Scenario
4000000000000101	Cardholder enrolled, processing attempts performed
	cmpi_lookup response
	Enrolled = Y ACUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	PAREsStatus = A SignatureVerification = Y EciFlag = 06 Xid = <XID Value> Cavv = <CAVV Value> ErrorNo = 0 ErrorDesc = <blank>
	Merchant Action
Merchant should append the Cavv and ECI values to the authorization message. Merchant is granted chargeback protection.	

MasterCard SecureCode Test Cases

Test Case 1

Test PAN	Scenario
5200000000000007	Successful Authentication. Cardholder enrolled, successful authentication, successful signature verification.
	cmpi_lookup response
	Enrolled = Y ACUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	PAREsStatus = Y SignatureVerification = Y EciFlag = 02 Xid = <XID Value> Cavv = <CAVV Value> ErrorNo = 0 ErrorDesc = <blank>
	Merchant Action
	Merchant should append the CAVV and EciFlag values to the authorization message.

Test Case 2

Test PAN	Scenario
52000000000000015	Cardholder enrolled, successful authentication, unsuccessful signature verification
	cmpi_lookup response
	Enrolled = Y ACUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	PAREsStatus = Y SignatureVerification = N EciFlag = 02 Xid = <XID Value> Cavv = <CAVV Value> ErrorNo = 0 ErrorDesc = <blank>
	Merchant Action
	Merchant should NOT continue authorization, due to the failed signature verification. Merchant should prompt for another form of payment or attempt to re-authenticate the consumer.

Test Case 3

Test PAN	Scenario
5200000000000023	Cardholder enrolled, unsuccessful authentication, successful signature verification
	cmpi_lookup response
	Enrolled = Y ACSUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	PAREsStatus = N SignatureVerification = Y EciFlag = 01 Xid = <XID Value> Cavv = <blank> ErrorNo = 0 ErrorDesc = <blank>
	<p style="text-align: center;">Merchant Action</p> <p>Merchant should not continue with authorization. Merchant should prompt for another form of payment and is not permitted to submit this transaction for authorization.</p>

Test Case 4

Test PAN	Scenario
5200000000000031	Cardholder enrolled, Authentication not able to complete (PAREs)
	cmpi_lookup response
	Enrolled = Y ACSUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	PAREsStatus = U SignatureVerification = Y EciFlag = 01 Xid = <XID Value> Cavv = <blank> ErrorNo = 0 ErrorDesc = <blank>
	<p style="text-align: center;">Merchant Action</p> <p>Merchants have the option of retaining the liability and submit the transaction as non-authenticated. An alternative action would be to prompt for another form of payment.</p>

Test Case 5

Test PAN	Scenario
5200000000000049	Cardholder enrolled, Authentication cancelled by user (simulating the consumer abandoning the authentication window)
	cmpi_lookup response
	Enrolled = Y ACUrl = <url> Payload = <PARES Payload Value> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	cmpi_authenticate message does not apply in this case.
	Merchant Action Merchants have the option of proceeding with the transaction and retaining liability, or prompt for another form of payment.

Test Case 6

Test PAN	Scenario
5200000000000056	Cardholder not enrolled
	cmpi_lookup response
	Enrolled = N ACUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	cmpi_authenticate message does not apply in this case.
	Merchant Action Merchant should proceed with transaction while retaining chargeback liability.

Test Case 7

Test PAN	Scenario
5200000000000064	Cardholder enrolled, Authentication unavailable (VERes)
	cmpi_lookup response
	Enrolled = U ACUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	cmpi_authenticate message does not apply in this case.
	Merchant Action
	Merchant should proceed with the authorization message. merchant retains the chargeback liability.

Test Case 8

Test PAN	Scenario
5200000000000072	Merchant not able to execute transactions (merchant not active)
	cmpi_lookup response
	Enrolled = <blank> ACUrl = <blank> Payload = <blank> ErrorNo = Error Number ErrorDesc = Error Description
	cmpi_authenticate response
	cmpi_authenticate message does not apply in this case.
	Merchant Action
	Merchant should continue with the authorization and contact technical support to investigate and resolve the issue. Merchant retains chargeback liability.

Test Case 9

Test PAN	Scenario
5200000000000080	Error response to cmpi_lookup message
	cmpi_lookup response
	Enrolled = <blank> ACUrl = <blank> Payload = <blank> ErrorNo = Error Number ErrorDesc = Error Description
	cmpi_authenticate response
	cmpi_authenticate message does not apply in this case.
	Merchant Action
	Merchant should continue with the authorization and contact technical support to investigate and resolve the issue. Merchant retains chargeback liability.

Test Case 10

Test PAN	Scenario
5200000000000098	Cardholder enrolled, error response to cmpi_authenticate message
	cmpi_lookup response
	Enrolled = Y ACUrl = <url> Payload = <PARES Payload Value> ErrorNo = 0 ErrorDesc = <blank>
	cmpi_authenticate response
	PARESStatus = <blank> SignatureVerification = <blank> EciFlag = <blank> Xid = <blank> Cavv = <blank> ErrorNo = Error Number ErrorDesc = Error Description
	Merchant Action
	Merchant should continue with the authorization and contact technical support to investigate and resolve the issue. Merchant retains chargeback liability.

ERROR HANDLING

The following list of MAPS error codes, descriptions and explanations are provided to assist merchants with error code handling during integration. When an error is returned by the `cmpi_lookup` or `cmpi_authenticate` messages, the simplest approach is to retry the authentication process. If an error is received on the `cmpi_authenticate`, the `cmpi_authenticate` should not be resubmitted. The entire authentication must be retried starting with a new `cmpi_lookup` message being sent. For those merchants integrating with a more enhanced error handling model, all error codes are provided with a suggested merchant action. It is possible for multiple error codes to be returned. These will be in a comma-separated form, and merchant decisions only need to be based on the first error code in the list.

Common MAPS Errors

Error Code	Error Description	Explanation	Merchant Action
112	Invalid Message Context	The Message-Context header value does not appear on the message header. This error only occurs when the MAPS Server has not been configured properly.	Complete transaction without authentication, contact technical support.
2001	Unsupported Message Type	The <code>MsgType</code> element value within the message does not meet the API requirements.	Complete transaction without authentication, contact technical support.
2003	Internal Error: Unable to handle message type at this time	The message could not be handled properly by the MAPS server. This error only occurs when the MAPS Server has not been configured properly.	Complete transaction without authentication, contact technical support.
2006	Unsupported Message Version	The <code>Version</code> element value within the message does not meet the API requirements. The value specified in <code>Version</code> is either not recognized or not supported.	Complete transaction without authentication, check message values.
2007	Message Group Disabled	Transaction messages have been disabled. If they should be enabled, contact technical support.	Complete transaction without authentication, contact technical support.
2009	Invalid Request Format: Invalid XML	Transaction message was not valid XML.	Complete transaction without authentication, check message values.
2010	Invalid Request Format: Empty Request	Transaction message was empty.	Complete transaction without authentication, check message values.

Transaction - cmpi_lookup

Error Code	Error Description	Explanation	Merchant Action
350	Unable to locate Merchant Configuration Information Within System	The Merchant Id, Processor Id data pair could not be located within the system. Commonly the merchant account is not configured within the system or invalid Merchant Id or Processor Id data elements were sent on the request message.	Complete transaction without authentication, check message values. Confirm the values passed on the message match the values configured within your account profile.
351	Payment Initiative Configuration Is Not Available, Unable To Process Transaction	The merchant's payment initiative configuration information is not properly configured. Most likely the merchant's configuration does not have any configuration information defined.	Complete transaction without authentication, check merchant configuration.
455	Acquirer Information Not Available	The merchant's acquirer configuration is incomplete preventing the processing of the request.	Complete transaction without authentication, check merchant configuration.
1001	Error Processing Message Request	Common Error Code returned when a processing error was encountered during the processing of a 3-D Secure message.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
1010	Error Processing VEReq	Common Error Code returned when a processing error was encountered. A detailed error code is also returned with this error code.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
1036	Unsupported Cardholder Enrolled Value	Value within the VERes message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
1070	Error processing VERes	Value within the VERes message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
1075	Encountered Empty VERes	Value within the VERes message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
1085	Error processing PAREq, Display Amount Could Not Be Determined	The amount could not be determined based on the raw amount formatting or the purchase amount.	Complete transaction without authentication, check message values.

Transaction - cmpi_lookup (cont.)

Error Code	Error Description	Explanation	Merchant Action
1090	Unsupported PAREq Version requested by ACS	Value within the VERes message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
1110	Error Persisting Verification Information	Unforeseen error occurred while persisting Verification Information.	Complete transaction without authentication, contact technical support.
1120	Error Persisting Authentication Information	Unforeseen error occurred while persisting Authentication Information.	Complete transaction without authentication, contact technical support.
1125	Error Persisting Transaction_Lookup Information, possibly duplicate Order Number	Unforeseen error occurred while persisting transaction information. Commonly encountered when multiple messages were sent using the same order number.	Retry transaction, restart payer authentication.
1126	Error UpdatingTransaction_Lookup Information	Unforeseen error occurred while persisting transaction information.	Retry transaction, restart payer authentication.
1130	Error Persisting VERes Information	Unforeseen error occurred while persisting transaction information.	Retry transaction, restart payer authentication.
1150	Error Persisting PAREq Information	Unforeseen error occurred while persisting transaction information.	Retry transaction, restart payer authentication.
1160	Error Persisting VEReq Information	Unforeseen error occurred while persisting transaction information.	Retry transaction, restart payer authentication.
1360	Payment Initiative Not Supported	The PAN element value within the request message doesn't map to a supported payment initiative. The PAN was not a Visa or, MasterCard type.	Complete transaction without authentication, check message values.

Transaction - cmpi_lookup (cont.)

Error Code	Error Description	Explanation	Merchant Action
1380	Payment Initiative Not Supported Under Specified Message Version	The Version and PAN element values within the message request correspond to a payment initiative that is not supported.	Complete transaction without authentication, check message values.
1400	Message Version Not Supported	The Version element value within the message does not meet the API requirements. The value specified is not a supported message version.	Complete transaction without authentication, check message values.
4000	Error Validating Processor Id Value	The Processor Id element value within the message does not meet the API requirements. The value was empty or not supplied in the request.	Complete transaction without authentication, check message values.
4020	Error Validating Merchant Id Value	The Merchant Id element value within the message does not meet the API requirements. The value was empty or not supplied in the request	Complete transaction without authentication, check message values.
4030	Error Validating PAN Value	The PAN element value within the message request does not meet the API requirements. The value is required to be numeric, 13 to 19 digits.	Complete transaction without authentication, check message values.
4040	Error Validating 3-D Secure Version Value	Value within the VERes message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4050	Error Validating Merchant Password	The Password element value within the message does not meet the API requirements. The value was not 8 characters in length.	Complete transaction without authentication, check message values.
4090	Error Validating Credit Card Expiration Information	The PAN Expiration element value within the message does not meet the API requirements. The value is empty, currently past the date supplied, or not supplied in the required (yyMM) format.	Complete transaction without authentication, check message values.
4140	Error Validating ACS URL	Value within the VERes message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.

Transaction - cmpi_lookup (cont.)

Error Code	Error Description	Explanation	Merchant Action
4150	Error Validating Payment Protocol	Value within the VERes message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4240	Merchant unable to process transactions, not active	The merchant account not active within system.	Complete transaction without authentication, check merchant configuration.
4245	Merchant unable to process transactions, Payment Initiative not active	The payment initiative configuration is not active for merchant. This configuration attribute is controlled by the MSP, they should be contacted regarding this issue.	Complete transaction without authentication, check merchant configuration.
4260	Error Validating Order Number	The Order Number element value within the message does not meet the API requirements. The value was empty or not supplied in the request.	Retry transaction, restart payer authentication.
4270	Error Validating Raw Amount	The Raw Amount element value within the message does not meet the API requirements. The value was empty, not supplied, or contained a non numeric value.	Retry transaction, restart payer authentication.
4295	Error Validating Order Description, Greater Than Allowed Size	The Order Description element value within the message does not meet the API requirements. The supplied value was greater than allowed size of 125 characters.	Retry transaction, restart payer authentication.
4310	Error parsing VERes Message Elements	Value within the VERes message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4330	Error Validating Enrollment Response	Value within the VERes message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4340	Error Validating iReq Code	Value within the VERes message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.

Transaction - cmpi_lookup (cont.)

Error Code	Error Description	Explanation	Merchant Action
4350	Error Validating Message Extension	Value within the VERes message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4360	Error Validating Critical Message Extensions	Value within the VERes message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4370	Error Validating Msgld Within VERes and VERes Messages	Value within the VERes message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4380	Error Validating Recurring Frequency Value	The Recurring Frequency element value within the message request does not meet the API requirements. When Recurring flag is Y, the Recurring Frequency value is required to be a numeric value.	Retry transaction, restart payer authentication.
4390	Error Validating Recurring Frequency End Date	The Recurring Frequency End Date element value within the message request does not meet the API requirements. When Recurring flag was Y, Recurring Frequency Date supplied in request was empty or not in required format (YYYYMMDD) .	Retry transaction, restart payer authentication.
4460	Error Validating Message Id	Value within the VERes message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4490	Error Validating ISO Currency Code	The Purchase Currency element value within the message request does not meet the API requirements. The value was empty or contained an unsupported value. The value is required to be an ISO 4271 numeric currency code.	Retry transaction, restart payer authentication.
4520	Error Validating Installment Value	The Installment element value within the message request does not meet the API requirements. The value was non numeric.	Retry transaction, restart payer authentication.
4530	Error Validating Installment Value, Must Be Greater Than 1	The Installment element value within the message request does not meet the API requirements. The value was not greater than 1	Retry transaction, restart payer authentication.

Transaction - cmpi_authenticate

Error Code	Error Description	Explanation	Merchant Action
350	Unable to locate Merchant Configuration Information Within System	The Merchant Id, Processor Id data pair could not be located within the system. Commonly the merchant account is not configured within the system or invalid Merchant Id or Processor Id data elements were sent on the request message.	Complete transaction without authentication, check merchant configuration.
351	Payment Initiative Configuration Is Not Available, Unable To Process Transaction	The merchant's payment initiative configuration information is not properly configured. Most likely the merchant's configuration does not have any configuration information defined.	Complete transaction without authentication, check merchant configuration.
455	Acquirer Information Not Available	The merchant's acquirer configuration is incomplete preventing the processing of the request.	Complete transaction without authentication, check merchant configuration.
1050	Error Processing PAREs	Common Error Code returned when a processing error was encountered during the processing of a 3-D Secure message.	Retry transaction, restart payer authentication.
1051	Error Processing PAREs, Error Response Returned By ACS	Common Error Code, the Card Issuer ACS server encountered an error processing the payer authentication transaction.	Retry transaction, restart payer authentication.
1055	Error Deserializing PAREs	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, restart payer authentication.
1060	Missing or Invalid PAREs	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, restart payer authentication.
1120	Error Persisting Authentication Information	Unforeseen error occurred while persisting Authentication Information.	Retry transaction, restart payer authentication.
1140	Error Persisting PAREs Information	Unforeseen error occurred while persisting PAREs Information	Retry transaction, restart payer authentication.

Transaction - cmpi_authenticate (cont.)

Error Code	Error Description	Explanation	Merchant Action
1350	Transaction Lookup Not Successful, Check Order Number	The Order Number element value within the message does not correspond to an Order Number that was processed by the cmpi_lookup message. The order number value is used to link the cmpi_authenticate message to a cmpi_lookup message.	Retry transaction, restart payer authentication.
1355	Transaction Lookup Not Successful, Check Transaction Id	The Transaction Id element value within the message does not correspond to an Transaction Id value that resulted from the processing of a cmpi_lookup message. The Transaction Id value is used to link the cmpi_authenticate message to a cmpi_lookup message.	Retry transaction, restart payer authentication.
1360	Payment Initiative Not Supported	The values provided within the message correspond to a Payment Initiative that is no longer supported by the system.	Retry transaction, restart payer authentication.
4010	Error Validating Acquirer Bin Value	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4020	Error Validating Merchant Id Value	The Merchant Id element value within the message does not meet the API requirements. The value was empty or not supplied in the request.	Complete transaction without authentication, check message values.
4030	Error Validating PAN Value	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4040	Error Validating 3-D Secure Version Value	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4160	Error Validating Purchase.date	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4170	Error Validating Purchase.xid	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.

Transaction - cmpi_authenticate (cont.)

Error Code	Error Description	Explanation	Merchant Action
4180	Error Validating Purchase.purchAmount	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4240	Merchant unable to process transactions, not active	The merchant account not active within system.	Complete transaction without authentication, check merchant configuration.
4245	Merchant unable to process transactions, Payment Initiative not active	The payment initiative configuration is not active for merchant. This configuration attribute is controlled by the MSP, they should be contacted regarding this issue.	Complete transaction without authentication, check merchant configuration.
4250	Error Validating Processor Id Value	The Processor Id element value within the message does not meet the API requirements. The value was empty or not supplied in the request.	Complete transaction without authentication, check message values.
4267	Error Validating Message, Order Number is Empty	The Order Number element value within the message does not meet the API requirements. The value was empty or not supplied in the request.	Retry transaction, restart payer authentication.
4268	Error Validating Message, Transaction Id is Empty	The Transaction Id element value within the message does not meet the API requirements. The value was empty or not supplied in the request.	Retry transaction, restart payer authentication.
4331	Error Validating Authentication Status	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, restart payer authentication.
4340	Error Validating iRe Code	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4350	Error Validating Message Extension	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4360	Error Validating Critical Message Extensions	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.

Transaction - cmpi_authenticate (cont.)

Error Code	Error Description	Explanation	Merchant Action
4400	Error Parsing PARES Message Elements	Value within the PARES message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4410	Error Validating Vendor Code	Value within the PARES message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4420	Error Validating PAN Value, Should Not Contain Zeros	Value within the PARES message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4430	Error Validating TX.cavv Value, Should Not Be Present	Value within the PARES message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4435	Error Validating TX.cavv Value	Value within the PARES message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4440	Error Validating TX.eci Value, Should Not Be Present	Value within the PARES message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4445	Error Validating TX.eci Value	Value within the PARES message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4450	Error Validating TX.cavvAlgorithm Value, Should Not Be Present	Value within the PARES message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4455	Error Validating TX.cavvAlgorithm Value	Value within the PARES message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.

Transaction - cmpi_authenticate (cont.)

Error Code	Error Description	Explanation	Merchant Action
4460	Error Validating Message Id	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4470	Error Validating (MsgId, Xid, Purchase.currency, Purchase.exponent, Purchase.purchAmount) Within PAREq and PAREs Messages	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4480	Error Validating PAREs Id	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4490	Error Validating ISO Currency Code	The Purchase Currency element value within the message request does not meet the API requirements. The value was empty or contained an unsupported value. The value is required to be an ISO 4271 numeric currency code.	Retry transaction, restart payer authentication.
4500	Error Validating ISO Currency Exponent	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4510	Error Validating TX.time	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4540	Error Validating PAREs Id and Reference URI	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4550	Error Validating PAREs, Invalid Message.Signature.Canonicalization Method xmlns attribute	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4560	Error Validating PAREs, Invalid Message.Signature.SignatureMethod xmlns attribute	Value within the PAREs message does not meet the requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.

Transaction - cmpi_authenticate (cont.)

Error Code	Error Description	Explanation	Merchant Action
4570	Error Validating PAREs, Invalid Message.Signature.SignedInfo xmlns attribute	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4580	Error Validating PAREs, Invalid Message.Signature xmlns attribute	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.
4590	Error Validating PAREs, Invalid Digital Signature Value	Value within the PAREs message does not meet the format requirements defined by 3-D Secure protocol.	Retry transaction, a component within the 3-D Secure infrastructure responded incorrectly.