



Cardinal Centinel™ *for Merchants*



Thin Client Integration Guide Payer Authentication

For Centinel Version 8.0

Acknowledgements

CardinalCommerce Corporation acknowledges with gratitude the contribution of its associates who developed the Cardinal Payment Authentication Platform.

© 2007 by CardinalCommerce Corporation. All rights reserved.

Trademark Information

CardinalCommerce, Cardinal Centinel Authentication Software for Merchants, and Centinel are trademarks of CardinalCommerce Corporation.

Cardinal Centinel is protected under U.S. Patent No. 7,051,002 B2 - "Universal merchant platform for payment authentication".

Microsoft is a registered trademark of Microsoft Corporation. Microsoft Internet Explorer is a trademark of the Microsoft Corporation.

Visa is a registered trademark of Visa. Verified by Visa and VbV are trademarks of Visa.

Mastercard is a registered trademark of Mastercard International Incorporated. Mastercard SecureCode and SecureCode are registered trademarks of Mastercard International Incorporated.

All other trademarks are the properties of their respective owners.

This manual may not, in whole or in part, be copied, photocopied, reproduced, translated, or converted to any electronic or machine readable form without prior written consent of CardinalCommerce Corporation.

Contact Information

CardinalCommerce Corporation
6119 Heisley Rd.
Mentor, OH 44060
USA
www.cardinalcommerce.com

TABLE OF CONTENTS

1 Overview.....	5
2 The Payer Authentication Transaction.....	6
3 Implementation Checklist.....	8
4 Thin Client.....	9
4.1 Thin Client Architecture.....	11
5 Thin Client Integration.....	13
5.1 Message Versions.....	13
5.2 Lookup Message Integration.....	13
5.2.1 cmpi_lookup.....	14
5.2.2 Processing the Lookup Response.....	18
5.3 Authenticate Message Integration.....	19
5.3.1 cmpi_authenticate.....	20
5.4 Auth-Bridge Message Integration.....	23
5.4.1 cmpi_ab_lookup.....	23
5.5 Payer Authentication Flow Diagram.....	26
5.6 Payer Authentication Decision Table.....	26
6 Integration Notes.....	30
6.1 Logo Placement.....	30
6.2 Payer Authentication Integration Messaging.....	30
6.2.1 Pre-Authentication Messaging.....	30
6.2.2 Framed Inline Authentication Window.....	31
6.2.3 Authentication Result Messaging.....	32
6.3 Implementation Considerations.....	33
6.3.1 Disable the Submit Button.....	33
6.3.2 Atomic Actions.....	33
6.3.3 Browser Back Button.....	33
6.3.4 Authorization Integration.....	33
7 Integration Testing.....	35
7.1 Verified by Visa Test Cases.....	37
7.2 MasterCard SecureCode Test Cases.....	48
7.3 JCB J/Secure Test Cases.....	59
8 Integration Error Handling.....	71
8.1 Common Centinel MAPS Errors.....	71
8.2 cmpi_ab_lookup.....	71
8.3 cmpi_authenticate.....	72
8.4 cmpi_lookup.....	74
9 Frequently Asked Questions.....	77

10 Appendix A - ISO Codes..... 80
10.1 ISO 4217 Currency Codes..... 80
10.2 ISO 3166 Country Codes..... 86

1 Overview

This guide provides an overview of the Cardinal Centinel Thin Client technology. General integration, testing and usage instructions for the Cardinal Centinel Thin Client are outlined in this document. API information required to integrate specific web applications with the Centinel Thin Client can be found within this document.

Integrating the Thin Client will enable participation in the Verified by Visa, MasterCard SecureCode and JCB J/Secure Payer Authentication programs.

This document assumes you have familiarity with your website and payment processing procedures as well as a proficiency using the technologies and programming languages used by your e-commerce website.

Note: The Cardinal Thin Client version number does not correspond to the Cardinal Centinel Authentication Software for Merchants version number. The Thin Client versions available for download will always be the most current version of the Thin Client software.

2 The Payer Authentication Transaction

The Verified by Visa, MasterCard SecureCode and JCB J/Secure Payer Authentication programs are based off the 3-D Secure Protocol. The Payer Authentication transaction is divided into the follow 3-D Secure domains.

Issuer Domain: Systems and functions of Card Issuers and Cardholders

Card Issuers enroll and activate cardholder accounts to participate in the payer authentication programs. The Card Issuer is responsible for authenticating the card holder during the checkout process.

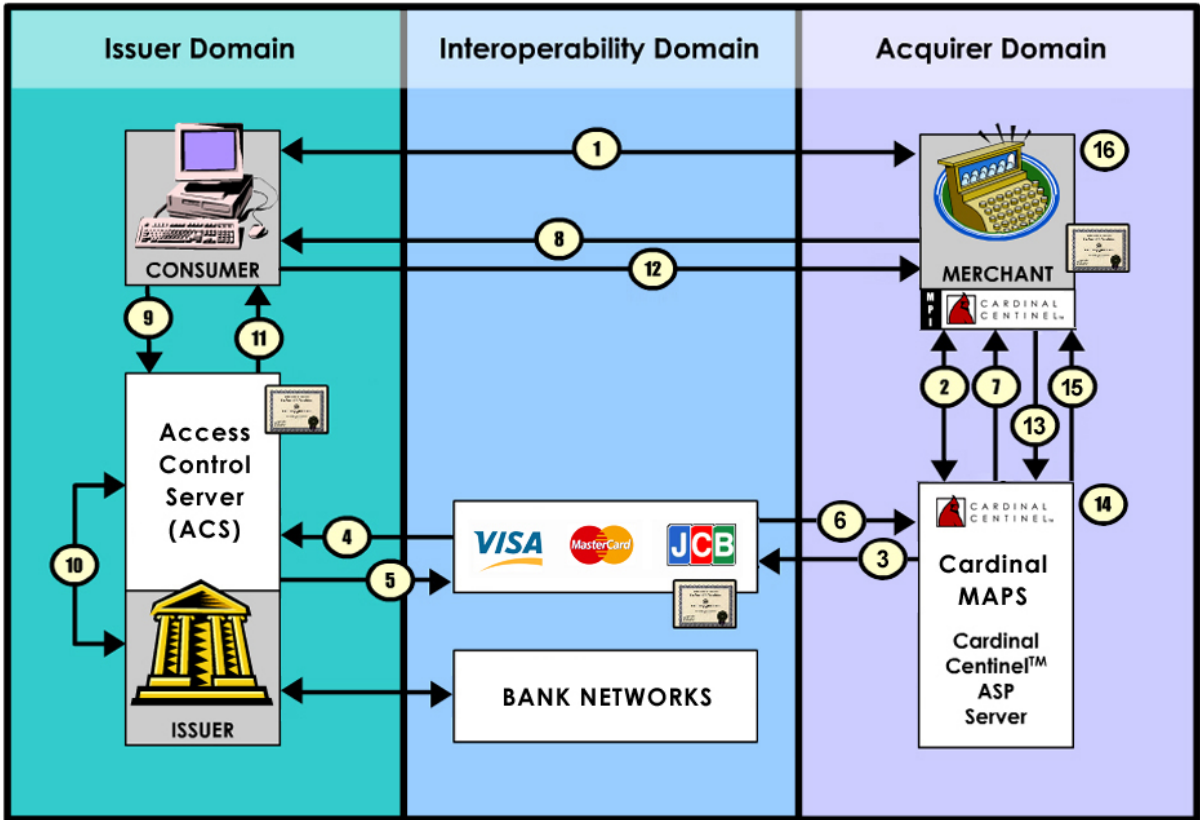
Acquirer Domain: Systems and functions of Acquirers and Merchants

Merchants communicate with Centinel to initiate the authentication process. Once authentication is completed, the authentication data is appended to the financial transaction that is sent to the gateway or processor.

Interoperability Domain: Systems and functions allowing the Issuer Domain to interoperate with the Acquirer Domain

Centinel communicates with the various directory servers to facilitate the communication between the cardholder and their Card Issuer. Once the cardholder is redirected to their Card Issuer, the cardholder will be prompted for their authentication credentials.

Below is a graphic representation of the payer authentication message flow specific to Cardinal Centinel. A detailed description of each of the steps within this diagram follows the graphic.



1. Consumer shops online at Merchant website. At the point of checkout, the cardholder fills out the checkout form including the payment details and clicks the 'Buy' button.
2. Based on the payment information, the Merchant, via the Thin Client, passes a Lookup message to Centinel Merchant Authentication Processing System (MAPS). This message contains all the required information provided by the cardholder in order to check the enrollment of the cardholder.
3. Based on the card number range stored within Centinel MAPS (pulled from the Directory Server daily), a Verify Enrollment Request (VEReq) message will be sent to the Enrollment Directory server.
4. The Enrollment Directory Server will send the VEReq to the Cardholder's Issuing Bank Access Control Server (ACS) to determine the enrollment status.
5. The Verify Enrollment Response (VERes) is returned to the Directory Server with the corresponding ACS URL, if applicable.
6. Centinel receives the response from the directory server, interprets the response and conditionally creates the Payment Authentication Request (PAREq) based on the enrollment status.
7. The Lookup response is returned to the Thin Client with an Enrolled status and conditionally with the PAREq for further authentication processing.
8. Based on the Enrolled value returned on the Lookup response, the Merchant will either redirect the cardholder's browser to the corresponding Issuing Bank ACS (ACSUrl) or process the authorization transaction as a non-authenticated order. Within the redirect to the ACSUrl, the Merchant specifies a return url location for the Consumer to be redirected to after authentication completes (TermUrl).
9. The Card Issuer displays the authentication form to the cardholder. The cardholder enters their authentication data and initiates the authentication process directly with the ACS.
10. The Issuing Bank ACS authenticates the cardholder. The authentication result is represented by the Payer Authentication Response (PAREs) generated by the Card Issuer ACS.
11. Once authentication is completed, the ACS redirects the Consumer back to the Merchant website (TermUrl).
12. The PAREs is returned to the merchant through the Consumers web browser.
13. The Merchant receives the PAREs value and initiates the Authenticate message, via the Thin Client, which is sent to the Centinel MAPS for processing.
14. Centinel decrypts the authentication result (PAREs), validates the message format, verifies the digital signatures of the transaction, and stores the transaction details within the Centinel reporting system.
15. Centinel formats the Authenticate response message and sends the ECI and Cavv/UCAF data elements on the response back to the merchant.
16. The Merchant processes the Authenticate response message, extracts the ECI and Cavv/UCAF data values, and processes the real time authorization transaction. Note that batch authorization processing is also permitted.

3 Implementation Checklist

Payer Authentication Implementation Checklist	
1.	<p>Install the Thin Client on your test and production servers.</p> <p>See the <i>Thin Client Installation Guide</i> included with the Thin Client download for additional information.</p>
2.	<p>Integrate the Thin Client into the eCommerce website to perform the Lookup Message transactions.</p> <p>See section 5.2 of the <i>Payer Authentication Integration Guide</i> for additional information.</p>
3.	<p>Integrate the authentication window using a framed inline frameset to allow for consistent site branding during the authentication process. Text surrounding the authentication window guide the cardholder during the authentication process.</p> <p>See the integration samples included with the Thin Client for a complete, working sample Authentication window implementation.</p>
4.	<p>Modify the Order Management System to ensure that all authorization transactions to the Gateway or Processor include the Authentication data elements (Cavv, Xid, ECI). Without these data elements, the Merchant will not receive the benefits of the Authentication programs.</p> <p>See the <i>Gateway Integration Guide</i> for additional information or directly review the gateway documentation.</p>
5.	<p>Display the Visa, MasterCard and JCB "Learn More" logos on the home and checkout pages of your website. These logos alert the Consumer to your participation in the Payer Authentication programs.</p> <p>See the integration samples included with the Thin Client for logo placement and Javascript code references.</p>
6.	<p>Provide messaging to the cardholder prior to payer authentication. This involves the logo placement and messaging on the checkout page that collects payment information. Instruct the Consumer that they may be required to provide their authentication password to complete the order.</p> <p>See the integration samples included with the Thin Client for sample Pre-Authentication messaging.</p>
7.	<p>Ensure that the website properly notifies the Consumer of the various outcomes of the Authentication transactions. Verify that the Consumer experience is handled properly.</p> <p>See the integration samples included with the Thin Client for sample Result messaging.</p>
8.	<p>Educate the customer support staff on the Payer Authentication programs using the <i>Customer Support Guide</i>.</p>

4 Thin Client

To assist merchants with the integration of our services with their eCommerce website, the Thin Client technology is available to minimize any custom development required by the Merchant. The Thin Client integration enables merchants to quickly communicate with the CardinalCommerce Application Service Provider (ASP) platform. This communication allows all the changing business rules and configuration information to be managed centrally within the ASP platform. As business rules or payment initiative programs evolve, these modifications are made centrally and do not effect the Merchant's eCommerce website directly. The hosted services minimizes any ongoing maintenance, further allowing Merchants to focus on their business objectives instead of maintaining software.

The following Centinel Thin Clients are currently available:

Cold Fusion
COM
Java
Microsoft .NET
Perl
PHP

Included with the Thin Client technology are integration samples. These samples can be used as templates for integration and provide code samples for processing the API messages with the hosted service. The code samples include comments which highlight error handling and general usage examples.

Note: If one of the available Thin Clients does not meet your system requirements a direct XML integration solution is available. A XML Integration Guide is available for Merchants who wish to explore this option.

In addition to the Thin Client offerings, we work closely with Shopping Cart vendors and Order Management System vendors to develop cartridges which handle all Thin Client integration requirements. If you happen to use a product that can be Centinel enabled through one of these cartridges, then your technical development requirements are minimized. Typically, enabling the Centinel service using a cartridge requires a simple configuration within the product's administration console.

Note: The available cartridges only support Verified by Visa and MasterCard Secure Code transaction processing.

The following Centinel Cartridges are currently available:

AbleCommerce .Net
AbleCommerce Cold Fusion
Apple Cart
ASPDotNetStoreFront
BVCommerce
Candy Press
Cart 32
cf_ezcart
Devix

ITeTools
LaGarde StoreFront
Lite Commerce
Miva Merchant
osCommerce
Product Cart
Sales Cart
X-Cart

4.1 Thin Client Architecture

The Thin Client has a common API for message handling. Each Thin Client exposes methods for request message creation, the sending and receiving of transaction data, and response message interpretation.

Note: Detailed API information is available for each Thin Client in the Thin Client installation guides.

Request Object

Method	Description
Add	<p>Adds name-value pairs used to construct the XML Messages.</p> <p>Usage : void Add(String name, String value)</p> <p>Parameters : name - name of the parameter value - value of the parameter</p> <p>Returns : void</p>
SendHTTP	<p>Sends the request message to the Centinel MAPS. MAPS returns a response message. The response message is deserialized into name-value pairs and returned from the method in the form of a Thin Client response object.</p> <p>Usage : ResponseObject SendHTTP(String transactionURL)</p> <p>Parameters : transactionURL - fully qualified transaction URL</p> <p>Returns : ResponseObject</p> <p>Note: The various platform versions of the Thin Client may overload this method and allow you to specify optional timeout parameters for the MAPS message communication.</p>

Response Object

Method	Description
GetValue	<p>Returns the value for a named element returned on the response message.</p> <p>Usage : String GetValue(String name)</p> <p>Parameters : name - name of the parameter</p> <p>Returns : String value of the name parameter</p>

5 Thin Client Integration

The Thin Client provides a communication shell that accepts name-value pairs. The name-value pairs are serialized to an XML message and communicated to the Centinel Merchant Authentication Processing System (MAPS). The Centinel MAPS communicates the response message to the Thin Client which makes the message elements available to the Merchant as name-value pairs.

The core transaction involves implementation of two messages, the Lookup Message (cmpi_lookup) and the Authenticate Message (cmpi_authenticate). Each message requires the Merchant to collect data from the Consumer, construct the message using the Thin Client, and send the request message to the Centinel platform for processing. Merchants must utilize the response values to control the flow of the Consumer's transaction.

Included with each of the Thin Clients are integration samples and marketing materials needed to complete the Payer Authentication and alternative payment integrations. Included within the code samples are additional comments on how to construct and process the required API messages.

Payer Authentication also requires a modification to the authorization processing. In addition to the authentication of the Consumer at checkout it is also required that the data elements resulting from the authentication processing be passed along to the gateway on the authorization and settlement transactions. Each Gateway API supports the passing of these data elements in slightly different ways. API details for passing the authentication data elements are available within the Centinel Gateway Integration Guide or contact your gateway provider directly for details.

5.1 Message Versions

The following message versions are currently supported:

Message Version	Payment Initiative
1.7	Verified by Visa
1.7	MasterCard SecureCode
1.7	JCB J/Secure

5.2 Lookup Message Integration

The Lookup Message is responsible for initiating the Payer Authentication. The integration point for the Lookup Message is immediately following the capture of the payment information, including the final order amount and the credit card information.

Note: Authentication is REQUIRED to take place prior to authorization. Data resulting from the authentication process MUST be represented on the authorization transaction to ensure the merchant will be provided the benefits from the program.

The Lookup Message is constructed and sent to the Centinel MAPS for processing. The

Lookup Message requires transaction specific data elements to be formatted on the request message. Please refer to the Message API section for the complete list of required message elements.

The response message is returned from the Centinel MAPS, and the merchant invokes the Thin Client API to reference the response values. In the event that the `Enrolled` value is `Y` the `ACSUrl` element will contain a fully qualified URL that the consumer should be redirected to for authentication with the Card Issuer.

5.2.1 cmpi_lookup

The `cmpi_lookup` is the first transaction of the Lookup/Authenticate pair that is used to process the payer authentication transaction. The `TransactionType` value represented on the transaction request will dictate how the transaction will be processed.

The `CardNumber` value dictates the program that will be used in processing the transaction. Currently Verified by Visa, MasterCard SecureCode and JCB J/Secure are supported by Centinel.

Request Message

Field Name	Description	Required
MsgType	cmpi_lookup	Y
Version	Application message version identifier. Current Version - 1.7	Y
ProcessorId	Merchant processor identification code. This value is assigned to the Merchant.	Y
MerchantId	Merchant identification code. This value is assigned to the Merchant.	Y
TransactionPwd	A password to secure and verify the transaction originated from merchant represented by the transaction details. The password value is configured through the merchant profile. Limit 50 characters	Y
TransactionType	Identifies the Transaction Type used for processing. [C] C Credit Card / Debit Card Authentication	Y
Amount	Unformatted total transaction amount without any decimalization. For example, \$100.00 = 10000, \$123.67 = 12367, \$.99 = 99	Y
CurrencyCode	3 digit numeric, ISO 4217 currency code for the sale amount. For example, USD - 840, EUR - 978, JPY - 392, CAD - 124, GBP - 826	Y
CardNumber	Credit card number, up to 19 digits in length.	Y
CardExpMonth	Card Number Expiration Month, 2 digits in length, formatted MM.	Y
CardExpYear	Card Number Expiration Year, 4 digits in length, formatted YYYY.	Y

OrderNumber	Order Number or transaction identifier from the Merchant eCommerce website. Limit 50 characters.	Y
OrderDescription	Brief description of items purchased. Limit 125 characters.	N
UserAgent	The exact content of the HTTP user-agent header. Limit 256 characters.	N
BrowserHeader	The exact content of the HTTP accept header. Limit 256 characters.	N
Recurring	Flag to specify if the Merchant and Consumer have agreed to recurring payments. [Y, N]	N
RecurringFrequency	Integer value indicating the minimum number of days between recurring 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 performed. 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
AcquirerPassword	Required only when processing within certain Visa Regions. The value is used to facilitate Merchant Authentication File (MAF) authentication processing. Note that if this value is passed it will override the password value configured on the Merchant's payment initiative configuration.	N
EMail	Consumer's email address. Limit 255 characters.	N
IPAddress	The IP Address of the Consumer. Format NNN.NNN.NNN.NNN	N
BillingFirstName	Consumer's first name. Limit 50 characters.	N
BillingMiddleName	Consumer's middle name. Limit 50 characters.	N
BillingLastName	Consumer's last name. Limit 50 characters.	N
BillingAddress1	Address Information. Limit 50 characters.	N
BillingAddress2	Address Information. Limit 50 characters.	N
BillingCity	Consumer's city of the billing address. Limit 50 characters.	N
BillingState	Consumer's state or province of the billing address. Limit 50 characters.	N
BillingPostalCode	Address postal code. Limit 10 characters.	N
BillingCountryCode	Consumer's country code of the billing address. Alpha ISO 3166, for example US - United States, ZA - South Africa. Complete list of ISO 3166 values is included in the Appendix. Limit 3 characters.	N
BillingPhone	Phone number for billing address. Unformatted billing phone without hyphens. Limit 20 characters. For example, 555-555-5555 = 5555555555	N

BillingAltPhone	<p>Alternate Phone number for billing address.</p> <p>Unformatted billing phone without hyphens. Limit 20 characters.</p> <p>For example, 555-555-5555 = 5555555555</p>	N
ShippingFirstName	Consumer's first name. Limit 50 characters.	N
ShippingMiddleName	Consumer's middle name. Limit 50 characters.	N
ShippingLastName	Consumer's last name. Limit 50 characters.	N
ShippingAddress1	Address Information. Limit 50 characters.	N
ShippingAddress2	Address Information. Limit 50 characters.	N
ShippingCity	Consumer's city of the shipping address. Limit 50 characters.	N
ShippingState	Consumer's state or province of the shipping address. Limit 50 characters.	N
ShippingPostalCode	Address postal code. Limit 10 characters.	N
ShippingCountryCode	Consumer's country code of the shipping address. Alpha ISO 3166, for example US - United States, ZA - South Africa. Complete list of ISO 3166 values is included in the Appendix. Limit 3 characters.	N
ShippingPhone	<p>Phone number for shipping address.</p> <p>Unformatted billing phone without hyphens. Limit 20 characters.</p> <p>For example, 555-555-5555 = 5555555555</p>	N
ShippingAltPhone	<p>Alternate Phone number for shipping address.</p> <p>Unformatted billing phone without hyphens. Limit 20 characters.</p> <p>For example, 555-555-5555 = 5555555555</p>	N
Item_Name_X	Name of item purchased. Limit 128 characters.	N
Item_Desc_X	Brief description of item.Limit 256 characters.	N
Item_Price_X	<p>Unformatted price of item X transaction amount without any decimalization. Limit 20 characters.</p> <p>For example, \$100.00 = 10000, \$123.67 = 12367, \$.99 = 99</p>	N
Item_Quantity_X	Number of items purchased.Limit 20 characters.	N
Item_SKU_X	Item SKU number. Limit 20 characters.	N

Sample Message

```

<CardinalMPI>
  <MsgType>cmpi_lookup</MsgType>
  <Version>1.7</Version>
  <ProcessorId>100</ProcessorId>
  <MerchantId>123456</MerchantId>
  <TransactionPwd>passw0rd</TransactionPwd>
  <TransactionType>C</TransactionType>
  <OrderNumber>182397541265</OrderNumber>
  <Amount>12345</Amount>
  <CurrencyCode>840</CurrencyCode>
  <CardNumber>4111111111111111</CardNumber>
  <CardExpMonth>02</CardExpMonth>
  <CardExpYear>2009</CardExpYear>
  <OrderDescription>Order #182397541265</OrderDescription>
  <UserAgent>Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)</UserAgent>
  <BrowserHeader>*/*</BrowserHeader>
  <EMail>buyer@cardinalcommerce.com</EMail>
  <IPAddress>207.48.141.20</IPAddress>
  <BillingFirstName>Mary</BillingFirstName>
  <BillingLastName>Smith</BillingLastName>
  <BillingAddress1>6362 Main Street</BillingAddress1>
  <BillingAddress2></BillingAddress2>
  <BillingCity>Cleveland</BillingCity>
  <BillingState>OH</BillingState>
  <BillingPostalCode>44124</BillingPostalCode>
  <BillingCountryCode>US</BillingCountryCode>
  <ShippingFirstName>Mary</ShippingFirstName>
  <ShippingLastName>Smith</ShippingLastName>
  <ShippingAddress1>6362 Main Street</ShippingAddress1>
  <ShippingAddress2></ShippingAddress2>
  <ShippingCity>Cleveland</ShippingCity>
  <ShippingState>OH</ShippingState>
  <ShippingPostalCode>44124</ShippingPostalCode>
  <ShippingCountryCode>US</ShippingCountryCode>
  <Item_Name_1>2GB MP3 Player</Item_Name_1>
  <Item_Desc_1>The simple MP3 player</Item_Desc_1>
  <Item_Quantity_1>1</Item_Quantity_1>
  <Item_Tax_Selector_1>Ventura County</Item_Tax_Selector_1>
  <Item_SKU_1>112233</Item_SKU_1>
  <Item_Name_2>100GB Hard Drive</Item_Name_2>
  <Item_Desc_2>The New 100GB Hard Drive</Item_Desc_2>
  <Item_Quantity_2>1</Item_Quantity_2>
  <Item_SKU_2>444555666</Item_SKU_2>
</CardinalMPI>

```

Response Message

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

Field Name	Description	Required
ErrorNo	Application error number(s). A non-zero value represents the error encountered while attempting to process the message request.	Y
ErrorDesc	Application error description for the associated error number(s).	Y
TransactionId	Centinel transaction identifier. This value identifies the transaction within the	Y

	Centinel system. To complete the transaction, the value is required to be passed on the Authenticate message to link the Lookup and Authenticate message together.	
Enrolled	Status of authentication eligibility. If the Enrolled value is NOT Y, then the Consumer is NOT eligible for authentication. Y - Cardholder Enrolled N - Not Enrolled U - Cardholder Authentication Unavailable	Y
ACSUrl	The fully qualified URL to redirect the Consumer to complete the payer authentication transaction. Available if Enrolled = Y.	N
Payload	The encoded payment request generated by MAPS. Available if Enrolled = Y.	N
EciFlag	Electronic Commerce Indicator (ECI). The ECI value represented by this element should be passed on the authorization transaction to the gateway/processor. MasterCard 01 - Indicates Merchant Liability 02 - Indicates Card Issuer Liability Visa 05 - Indicates Card Issuer Liability 06 - Indicates Card Issuer Liability 07 - Indicates Merchant Liability JCB 05 - Indicates Card Issuer Liability 06 - Indicates Card Issuer Liability 07 - Indicates Merchant Liability	Y

Sample Message

```
<CardinalMPI>
  <ErrorNo>0</ErrorNo>
  <ErrorDesc></ErrorDesc>
  <TransactionId>75f986t76f6</TransactionId>
  <Payload>eNpVUk1TwjAQ/SsM402nSUuKwSC/3gSoH5PL</Payload>
  <Enrolled>Y</Enrolled>
  <ACSUrl>https://www.somewebsite.com/acs</ACSUrl>
  <EciFlag>07</EciFlag>
</CardinalMPI>
```

5.2.2 Processing the Lookup Response

Verify that the transaction is eligible for Authentication by evaluating the `Enrolled` element on the `cmpi_lookup` response message. In the event that the `Enrolled` element contains a `Y` value, Authentication is available and the Consumer should be redirected to the `ACSUrl` to

complete the transaction. The `ACSUrl` element contains the fully qualified URL to the Card Issuer Authentication system. It is required that the Consumer authenticate themselves directly with the Card Issuer. If the Enrolled value is NOT Y, then the Consumer is NOT eligible for Authentication. The ECI value represented on the Lookup response should be passed on the authorization transaction to the gateway/processor.

Redirect the Consumer to the ACSUrl via a HTTP Form POST. Construct the following form populated with the values returned on the `cmpi_lookup` response message.

Note: The form field names are case sensitive.

Form Field Descriptions

Field Name	Description
ACSUrl	The fully qualified URL to redirect the Consumer to complete authentication. Value should be retrieved from the <code>ACSUrl</code> field within the <code>cmpi_lookup</code> response message and inserted into the form.
PaReq	The encoded authentication request generated by MAPS. Value should be retrieved from the <code>Payload</code> field within the <code>cmpi_lookup</code> response message and inserted into the form.
TermUrl	The fully qualified URL of the Merchant webpage configured to receive the Consumer returning from completing authentication or PayPal payment. This URL will represent the webpage that will process the <code>cmpi_authenticate</code> message.
MD	Merchant session tracking identifier. The value will be returned to the <code>TermUrl</code> when the Consumer is returned after completing authentication or PayPal payment. The field is available if necessary. If not needed, simply pass an empty value on the form. Note: This field must contain only ASCII characters in the range 0x20 to 0x7E; if other data is needed, the field must be Base64 encoded. The size of the field (after Base64 encoding, if applicable) is limited to 1024 bytes.

5.3 Authenticate Message Integration

The Authenticate Message is responsible for returning the Payer Authentication outcome to the merchant. The message will return the status of the Authentication to the merchant, enabling the merchant to handle the order/authorization processing according to the outcome.

Once Authentication is completed, the consumer will be redirected back to the `TermUrl` representing a webpage on the Merchant website. The merchant is required to receive this form POST, and construct the Authenticate message to complete the transaction and determine the status of the Authentication. Centinel will receive the Authenticate message, decrypt the Authentication data and perform data validation checks on the Authentication result. Centinel will return a response indicating the status of the Authentication transaction.

In the event that a non zero `ErrorNo` value is returned or the `SignatureVerification` element indicates that a fraud check failed verification, the transaction should not be authorized, and the consumer should be prompted for another method of payment.

In the event that the `ErrorNo` element is 0 (zero) and the `SignatureVerification` element is `Y`, indicating all fraud checks were satisfied, then the `PAResStatus` value will define how the transaction should be processed. Based on the transaction outcome the Merchant's order management system should be updated and the appropriate message should be displayed to the consumer.

5.3.1 `cmpi_authenticate`

Second message of the Lookup/Authenticate pair used in processing Payer Authentication transactions. The `PARes` values are posted to the `TermURL` from the external systems involved in processing the transactions. The webpage represented by the `TermURL` should retrieve the `PARes` value from the HTTP Request object for use in creating this message.

The message is used to communicate the `PARes` generated by the Issuer ACS software to the Centinel. Centinel will verify the digital signature within the `PARes` to validate that the authentication results were properly generated and not altered. The authentication data values including the transaction status, `Xid`, `Cavv/AAV` and the `ECI` are extracted from the `PARes` and returned to the merchant on the response message.

Request Message

Field Name	Description	Required
<code>MsgType</code>	<code>cmpi_authenticate</code>	Y
<code>Version</code>	Application message version identifier. Current Version - 1.7	Y
<code>ProcessorId</code>	Merchant processor identification code. This value is assigned to the Merchant.	Y
<code>MerchantId</code>	Merchant identification code. This value is assigned to the Merchant.	Y
<code>TransactionType</code>	Identifies the Transaction Type used for processing. [C] C Credit Card / Debit Card Authentication	Y
<code>TransactionPwd</code>	A password to secure and verify the transaction originated from merchant represented by the transaction details. The password value is configured through the merchant profile. Limit 50 characters	Y
<code>TransactionId</code>	Centinel generated transaction identifier. Value links the request message to the <code>cmpi_lookup</code> message.	Y
<code>PAResPayload</code>	<code>PARes</code> generated by the external system that processed the authentication with the Consumer.	Y

Sample Message

```
<CardinalMPI>
  <Version>1.7</Version>
```

```

<MsgType>cmpi_authenticate</MsgType>
<ProcessorId>100</ProcessorId>
<MerchantId>123456</MerchantId>
<TransactionType>C</TransactionType>
<TransactionPwd>Passw0rd</TransactionPwd>
<TransactionId>7fDSaySnCmDGCjPglzqX</TransactionId>
<PAREsPayload>***** Payload Message *****</PAREsPayload>
</CardinalMPI>

```

Response Message

This message is generated in response to the cmpi_authenticate request 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 to process the message request.	Y
PAREsStatus	Transaction status result identifier. [Y, N, U, A] Y - Successful Authentication (Merchant Protected) N - Failed Authentication (No Protection) U - Unable to Complete Authentication (No Protection) A - Successful Attempts Transaction (Merchant Protected)	Y
SignatureVerification	Transaction Signature status identifier [Y, N]. Y - Indicates that the signature of the PAREs has been validated successfully and the message contents can be trusted. N - Indicates that for a variety of reasons; tampering, certificate expiration, etc. the PAREs could not be validated, and the result should not be trusted.	Y
Cavv	Cardholder Authentication Verification Value (Cavv), Authentication Verification Value (AVV), or Universal Cardholder Authentication Field (UCAF). This value should be appended to the authorization message signifying that the transaction has been successfully authenticated. This value will be encoded according to the merchant's configuration in either Base64 encoding or Hex encoding. A Base64 encoding merchant configuration will produce values of 28 or 32 characters. A Hex encoding merchant configuration will produce values of 40 or 48 characters. The value when decoded will either be 20 bytes for Cavv or 20 or 24 bytes if it is a AAV (MasterCard UCAF).	N
EciFlag	Electronic Commerce Indicator (ECI). The ECI value represented by this element should be passed on the authorization transaction to the gateway/processor. MasterCard 01 - Indicates Merchant Liability 02 - Indicates Card Issuer Liability Visa	Y

	<p>05 - Indicates Card Issuer Liability 06 - Indicates Card Issuer Liability 07 - Indicates Merchant Liability</p> <p>JCB</p> <p>05 - Indicates Card Issuer Liability 06 - Indicates Card Issuer Liability 07 - Indicates Merchant Liability</p>	
Xid	<p>Transaction identifier resulting from authentication processing.</p> <p>Gateway/Processor API specification may require this value to be appended to the authorization message. This value will be encoded according to the merchant's configuration in either Base64 encoding or Hex encoding. A Base64 encoding merchant configuration will produce values of 28 characters. A Hex encoding merchant configuration will produce values of 40 characters.</p>	N

Sample Message

```

<CardinalMPI>
  <ErrorDesc></ErrorDesc>
  <ErrorNo>0</ErrorNo>
  <PAREsStatus>Y</PAREsStatus>
  <SignatureVerification>Y</SignatureVerification>
  <Cavv>AAAAAAAAAAAAAAAAAAAAAAAAA= </Cavv>
  <EciFlag>05</EciFlag>
  <Xid>k4Vf36ijnJX54kwHQNqUr8/ruvs= </Xid>
</CardinalMPI>

```

5.4 Auth-Bridge Message Integration

This message is used to locate Payer Authentication data elements (Cavv, ECI, Xid) allowing merchants to retrieve the data values needed to populate the authorization to the gateway or processor. Certain order management systems and other middleware products do not support the passing of the Payer Authentication data elements through the platform. Using this message, merchants have the ability to bridge these systems, and alter the authorization transactions with the Payer Authentication details.

To ensure that the original transaction is located, the `TransactionId` value returned on the `cmpi_lookup` response should be used on the request message. If for some reason the `TransactionId` is not available, the transaction can be located through the use of the other data elements. In this case, all the other data elements (`Amount`, `CurrencyCode`, `CardNumber`) must match with the transaction occurring between the `FromDt` and `ToDt` values.

Note: Either the `TransactionId` or (`Amount`, `CurrencyCode`, `CardNumber`, `FromDt`, `ToDt`) data elements must be used to process the transaction.

5.4.1 cmpi_ab_lookup

Request Message

Field Name	Description	Required
MsgType	cmpi_ab_lookup	Y
Version	Application message version identifier. Current Version - 1.7	Y
ProcessorId	Merchant processor identification code. This value is assigned to the Merchant.	Y
MerchantId	Merchant identification code. This value is assigned to the Merchant.	Y
TransactionPwd	A password to secure and verify the transaction originated from merchant represented by the transaction details. The password value is configured through the merchant profile. Limit 50 characters	Y
TransactionId	The Centinel generated <code>TransactionId</code> value from the original Lookup/ Authenticate message pair. This value specifies the exact transaction that is being requested by the request message.	N
Amount	Value represents the transaction amount without any decimalization or punctuation. Examples \$123.67 - 12367, \$1,500.00 - 150000	N

CurrencyCode	3 digit numeric, ISO 4217 currency code for the sale amount. Complete list of ISO 4217 values is included in the Appendix.	N
CardNumber	Credit Card number used for the transaction.	N
FromDt	Beginning of period to search for payer authentication, formatted MM/dd/yyyy HH:mm:ss . Only the date portion is required. If the time is not specified, the beginning of the date is used. Not required if TransactionId is provided.	N
ToDt	End of period to search for payer authentication, formatted MM/dd/yyyy HH:mm:ss . Only the date portion is required. If the time is not specified, the beginning of the date is used. Not required if TransactionId is provided.	N

Sample Message

```
<CardinalMPI>
  <MsgType>cmpi_ab_lookup</MsgType>
  <Version>1.7</Version>
  <ProcessorId>100</ProcessorId>
  <MerchantId>123456</MerchantId>
  <TransactionPwd>Passw0rd</TransactionPwd>
  <TransactionType>C</TransactionType>
  <Amount>34920</Amount>
  <CurrencyCode>840</CurrencyCode>
  <CardNumber>4012001011000770</CardNumber>
  <FromDt>01/01/2005 00:00:00</FromDt>
  <ToDt>01/02/2005 00:00:00</ToDt>
</CardinalMPI>
```

Response Message

This message is generated as a response to the cmpi_ab_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
Cavv	<p>Cardholder Authentication Verification Value (Cavv), Authentication Verification Value (AVV), or Universal Cardholder Authentication Field (UCAF).</p> <p>This value should be appended to the authorization message signifying that the transaction has been successfully authenticated. This value will be encoded according to the merchant's configuration in either Base64 encoding or Hex encoding. A Base64 encoding merchant configuration will produce values of 28 or 32 characters. A Hex encoding merchant configuration will produce values of 40 or 48 characters. The value when decoded will either be 20 bytes for Cavv or 20 or 24 bytes if it is a AAV (MasterCard UCAF).</p>	Y
Xid	<p>Transaction Xid from 3-D Secure Authentication. Gateway/Processor API specification may require this value to be appended to the authorization message.</p> <p>This value will be encoded according to the merchant's configuration in either Base64 encoding or Hex encoding. A Base64 encoding merchant configuration will produce values of 28 characters. A Hex encoding merchant configuration will produce values of 40 characters.</p>	Y

EciFlag	<p>Electronic Commerce Indicator (ECI) [01, 02, 05, 06, 07]. Based on the Transaction Status, the corresponding ECI value will be required to be appended to the authorization message.</p> <p>MasterCard</p> <p>01 - Indicates Merchant Liability 02 - Indicates Card Issuer Liability</p> <p>Visa</p> <p>05 - Indicates Card Issuer Liability 06 - Indicates Card Issuer Liability 07 - Indicates Merchant Liability</p> <p>JCB</p> <p>05 - Indicates Card Issuer Liability 06 - Indicates Card Issuer Liability 07 - Indicates Merchant Liability</p>	Y
Enrolled	<p>Status of availability. [Y, N, U]</p> <p>Y - Cardholder Enrolled N - Not Enrolled U - Cardholder Enrolled but Authentication Unavailable</p>	Y
PAResStatus	<p>Transaction status result identifier. [Y, N, U, A]</p> <p>Y Success Transaction N Failed Transaction U Unable to Complete Transaction A Successful Attempts Transaction</p>	Y
SignatureVerification	<p>Transaction Signature status identifier. [Y, N]</p> <p>Y - Indicates that the signature of the PARes has been validated successfully and the message contents can be trusted.</p> <p>N - Indicates that for a variety of reasons; tampering, certificate expiration, etc. the PARes could not be validated, and the result should not be trusted.</p>	Y

Sample Message

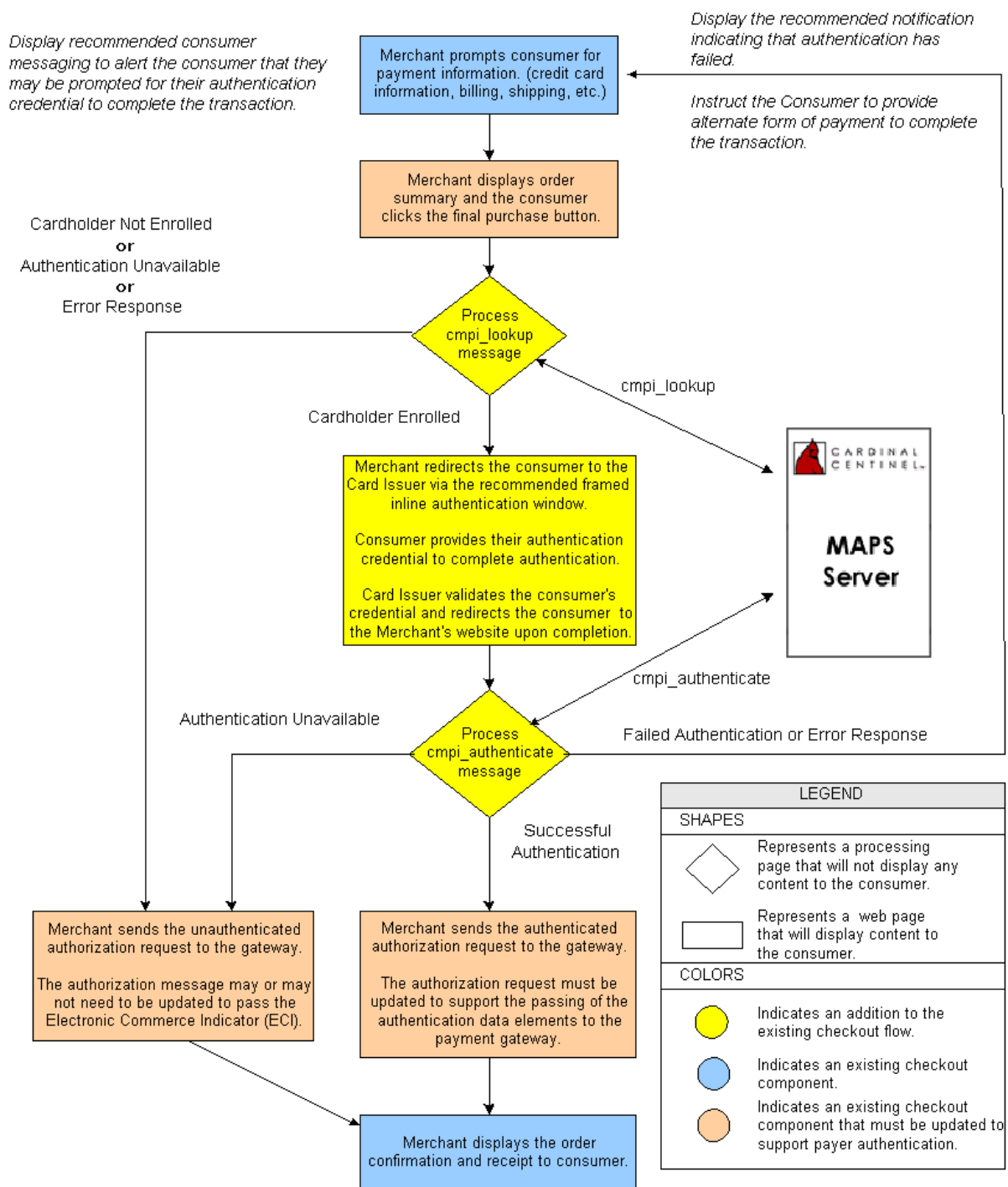
```

<CardinalMPI>
  <ErrorDesc></ErrorDesc>
  <ErrorNo>0</ErrorNo>
  <Cavv>AAAAAAAAAAAAAAAAAAAAAAAAA= </Cavv>
  <Xid>k4Vf36ijnJX54kwHQNqUr8/ruvs= </Xid>
  <EciFlag>05</EciFlag>
  <Enrolled>Y</Enrolled>
  <PAResStatus>Y</PAResStatus>
  <SignatureVerification>Y</SignatureVerification>
</CardinalMPI>

```

5.5 Payer Authentication Flow Diagram

The following flow diagram is intended to highlight the possible transaction paths that must be supported by a merchant integration.



5.6 Payer Authentication Decision Table

Based on the Lookup and Authenticate Message response values Merchants are required to control transaction flow in a variety of ways. The following decision table outlines 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.

Note: The Decision Table covers only those transaction responses that contain a zero `ErrorNo` value.

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.	<p>Complete the order as a non-authenticated transaction. Specify the proper ECI value on the authorization transaction.</p> <p>Visa / JCB</p> <p>Merchant has liability protection.</p> <p>ECI - 06</p> <p>MasterCard</p> <p>Merchant has no liability protection.</p> <p>ECI - 01</p>
U	Cardholder authentication is unavailable.	<p>Complete the order as a non-authenticated transaction. Specify the proper ECI value on the authorization transaction.</p> <p>Visa / JCB</p> <p>Merchant has no liability protection.</p> <p>ECI - 07</p> <p>MasterCard</p> <p>Merchant has no liability protection.</p> <p>ECI - 01</p>

Payer Authentication Authenticate Response Values

PResStatus Value	SignatureVerification Value	Description	Recommended Action

Y	Y	Cardholder Authentication completed successfully.	<p>Complete the order as an authenticated transaction.</p> <p>Visa / JCB</p> <p>Merchant has liability protection.</p> <p>ECI - 05</p> <p>MasterCard</p> <p>Merchant has liability protection.</p> <p>ECI - 02</p>
A	Y	<p>Cardholder attempts authentication completed successfully.</p> <p>In the event that a MasterCard transaction results in this response value, Centinel will return a <code>PAResStatus</code> value of <code>U</code> on the response message.</p>	<p>Complete the order as an authenticated transaction.</p> <p>Visa / JCB</p> <p>Merchant has liability protection.</p> <p>ECI - 06</p> <p>MasterCard</p> <p>Merchant has no liability protection</p> <p>ECI - 01</p>
N	Y	Cardholder failed authentication.	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.	<p>Complete the order as a non-authenticated transaction.</p> <p>Visa / JCB</p> <p>Merchant has no liability protection.</p> <p>ECI - 07</p> <p>MasterCard</p> <p>Merchant has no liability protection</p> <p>ECI - 01</p>

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.
------------	---	--	---

6 Integration Notes

In addition to the API integration to facilitate the Payer Authentication process, the Merchant must also make some important enhancements to the website to support the Payer Authentication transaction.

6.1 Logo Placement

The Payer Authentication program "Learn More" logos are required to be placed on the payment details page of the checkout process. The usage guidelines require that each of these logos link to their respective websites to enable the consumer to learn more about each of the programs.

The usage guidelines and "Learn More" links are outlined within the Visa, MasterCard and JCB Merchant Toolkits that are available for download within the Centinel Merchant Administration portal.



These logos should be linked to the html pages provided in the samples. These pages should be hosted by the Merchant.

6.2 Payer Authentication Integration Messaging

In support of the payer authentication usage guidelines, Merchants must provide a brief message regarding payer authentication to cardholders on the checkout page. The intention of the messaging is to notify the cardholder that they may be prompted either to provide their authentication password or possibly be prompted to activate their card in the authentication program. The pre-authentication message is most effective and most likely to be read by cardholders when placed immediately next to the final order button.

6.2.1 Pre-Authentication Messaging

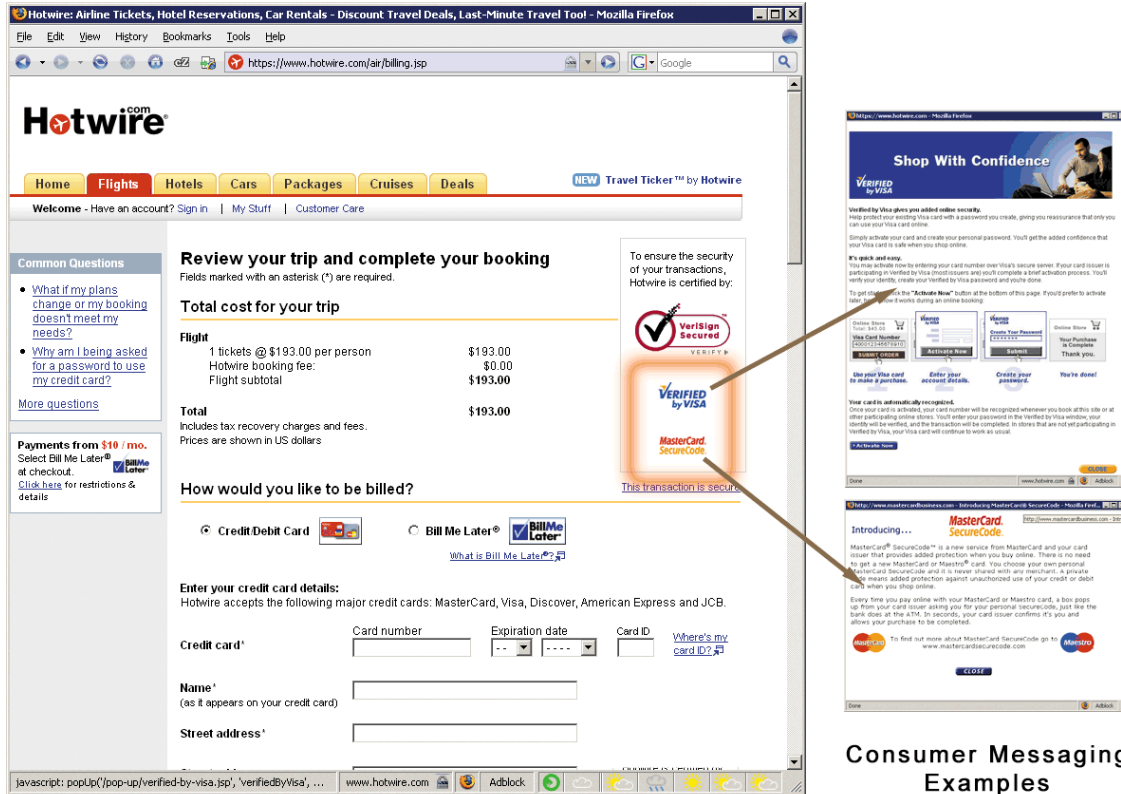
The messaging is also intended to provide a further reminder and reassurance to the cardholder, beyond the presence of the "Learn More" logos, that the Merchant participates in the respective authentication programs. **However, any messaging must not state affirmatively that the cardholder will have an authentication experience, and the Merchant must not indicate that the Merchant requires the cardholder to authenticate himself or herself.**

Sample Pre-Authentication Message

Your card may be eligible or enrolled in Verified by Visa, MasterCard SecureCode or JCB J/Secure payer authentication programs. After clicking the 'Submit Order' button, your Card Issuer may prompt you for your payer authentication password to complete your purchase.

Note: The Pre-Authentication message should be adjusted to only reference those programs integrated by the Merchant.

The following graphic highlights pre-authentication messaging and logo placement on an e-commerce checkout page.



Consumer Messaging Examples

6.2.2 Framed Inline Authentication Window

The framed inline presentation of the Card Issuer's authentication form, within an HTML 'frameset' or iFrame allows the Merchant to maintain site branding and provide a consistent look and feel through the authentication process. The inline approach does **NOT** pop up a new browser window, therefore the authentication process is not impacted by pop-up blocking software.

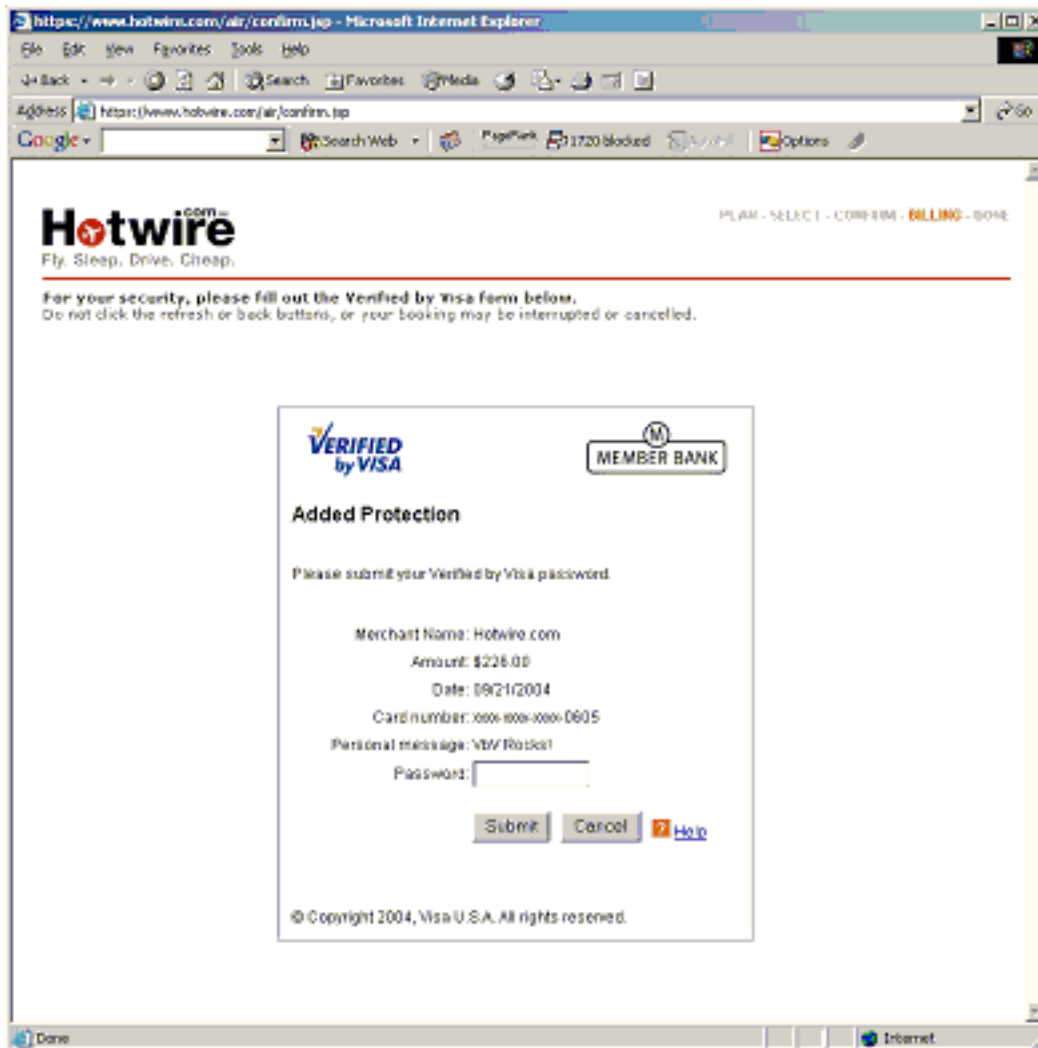
The header portion of the frameset should contain text similar to the following:

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.

The portion of the frameset that displays the Card Issuer authentication form must be large enough to display the entire form without scrolling (400 X 400 pixels). Verify the frameset size is large enough while testing with the Centinel Test system.

Note: In some regions with dual-language requirements (e.g. Quebec, Canada) it will not be possible to display the entire authentication form without scrolling. In this case it will be necessary to

ensure that the framed authentication is scrollable.



6.2.3 Authentication Result Messaging

Merchants must ensure that they account for all possible response scenarios and verify the user experience is handled properly in all cases. These scenarios include, successful authentication, failed authentications, signature verification failures, not enrolled cards as well as others. Each of these possible scenarios are outlined within the testing section of this guide.

Authentication Failure Messaging

When Merchants receive a failed authentication response value, Merchants must immediately display a message or page to advise the cardholder that the purchase will not be completed with the credit card information provided. The recommended wording for the failed authentication message is:

Authentication Failed

Your financial institution has indicated that it could not successfully authentic-

ate 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.

6.3 Implementation Considerations

During the integration process, be sure to address the following items to increase the success of your integration efforts. It is also highly recommended that Merchants review these tasks in the event that any significant changes are made to the checkout process within their website.

6.3.1 Disable the Submit Button

It is highly recommended that the final "Buy" button is disabled using Javascript to limit the impact that a double submit of the purchase form has on the authentication process. Instances may arise where a double submit may have a negative impact on the session management within the ecommerce system and prevent authentication from completing successfully.

6.3.2 Atomic Actions

Security solutions are only as secure as the weakest link the transaction chain. The transaction processing sequences are designed with transaction signature and fraud checks to ensure that the transaction results have not been manipulated. It is important to carry over these strict processing techniques over to the Merchant website to ensure that once the data is returned to the Merchant it is interpreted and used properly.

Implementing atomic actions within the transaction processing pages will ensure that the results of the authentication and payment processing are handled properly. Be sure to process the Lookup and Authenticate messages and immediately perform the recommended action using the response values. Avoid passing the authentication results through hidden form fields or through the URL as query string parameters. Passing sensitive data using these techniques can be easily manipulated by the consumer.

6.3.3 Browser Back Button

Ensure that your integration handles unexpected user behaviours gracefully, specifically back button activity. The use of session checks at various points throughout the authentication flow can prevent an authenticated transaction from being re entering the authentication processing flow subsequent times. Testing and handling these cases will lead to a optimal checkout experience for your consumers.

6.3.4 Authorization Integration

The Payer Authentication process generates additional data elements (CAVV, ECI, XID) that **MUST** be sent to the gateway or processor on the authorization request (CAVV, ECI and, optionally XID). For some gateways and processors the settlement request may also require the ECI value to be appended to the settlement transaction. The presence of these values on the authorization and settlement transactions will determine the protection or benefit that will be provided to the merchant. Additional information regarding how to pass the authentication data elements to various gateways are provided in the *Gateway Integration Guide*. If your gateway is not listed in the document or you have any further questions regarding the passing of the data elements on the authorization transaction, please refer to your vendor's documentation for additional information. It is highly recommended that each merchant confirm that their gateway or processor are properly receiving these data elements once integra-

7 Integration Testing

To assist your activation efforts, the Centinel Testing Facility is available to perform various predefined activation tests. Once you have completed activation with your site, testing can begin by sending messages to the testing facility using defined test cases. Each test case will generate a unique response that your activation should be able to account for and handle properly. The recommended actions are also included within the test case.

By default your username/password credential to login to the test system is your assigned MerchantId value and the password "changeit". Go to the Centinel Test Website (<https://centineltest.cardinalcommerce.com>) and login to your test Merchant account.



Note: The Centinel Test system requires merchants to use their assigned ProcessorId and MerchantId values for transaction processing.

Test Case Hierarchy

To support end-to-end certification requirements of eCommerce systems the Centinel Test environment supports the various test case outcomes using the following values:

1. Test Name (e.g. "Test01" in the First or Last name fields and/or the Order Description field)
2. Expiration Date (`CardExpMonth` and `CardExpYear`)
3. PAN (`CardNumber`)

The above values are listed in order of precedence. Using the test case name (e.g. "Test01") in either of the name fields and/or order description fields will invoke that test case and takes precedence over any other values present. The results generated should match the results of the test case as shown in the tables in this section.

If the test name or order description are not present, then the expiration date will be used, if present. The expiration values take precedence over the PAN and can be used with any cardnumber (for cases where gateways or processors required specific card numbers to be used) to invoke and test the various Payer Authentication responses through the test system.

Note: Although these expiration values can be used with any of the supported card types, depending on operating guidelines of the Payer Authentication program, some outcomes may not apply.

If there are no test names, order descriptions or expiration dates present, the test cases can be invoked by PAN (`CardNumber`). In addition to the test values listed in the tables, other data elements are required to be passed within the messages. Refer to the API section for complete API details. 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.

7.1 Verified by Visa Test Cases

Test Case 1

Test Case 01	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	Cardholder enrolled, successful authentication, successful signature verification.	Merchant should append the Cavv and EciFlag values to the authorization message.
	"Test01"	<any>	<any>	cmapi_lookup response	
	<any>	01/2007 or 01/2008	<any>	Enrolled = Y ACSUrl = <url> Payload = <value> ErrorNo = 0 ErrorDesc = <blank>	
	<any>	01/2009 (and later)	4000000000000002	cmapi_authenticate response PAResStatus = Y SignatureVerification = Y EciFlag = 05 Xid = <Xid Value> Cavv = <Cavv Value> ErrorNo = 0 ErrorDesc = <blank>	

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test01" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 01/2007 or 01/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 01/2009 or later (02/2009, 03/2010, etc)

Use pan 4000000000000002

Test Case 2

Test Case 02	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	<p>Cardholder enrolled, successful authentication, unsuccessful signature verification</p> <p>cmapi_lookup response</p> <p>Enrolled = Y ACSUrl = <url> Payload = <value> ErrorNo = 0 ErrorDesc = <blank></p> <p>cmapi_authenticate response</p> <p>PAResStatus = Y SignatureVerification = N EciFlag = 05 Xid = <Xid Value> Cavv = <Cavv Value> ErrorNo = 0 ErrorDesc = <blank></p>	<p>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 cmapi_lookup message.</p>
	"Test02"	<any>	<any>		
	<any>	02/2007 or 02/2008	<any>		
	<any>	02/2009 (and later)	4000000000000010		

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test02" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 02/2007 or 02/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 2/2009 or later (3/2009, 4/2009, etc)

Use pan 4000000000000010

Test Case 3

Test Case 03	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	Cardholder enrolled, unsuccessful authentication, successful signature verification	Merchant should NOT continue with authorization. Merchant should prompt for another form of payment and is not permitted to submit this transaction for authorization.
	"Test03"	<any>	<any>	cmapi_lookup response	
	<any>	03/2007 or 03/2008	<any>	Enrolled = Y ACSUrl = <url> Payload = <value> ErrorNo = 0 ErrorDesc = <blank>	
	<any>	03/2009 (and later)	4000000000000028	cmapi_authenticate response	
				PAResStatus = N SignatureVerification = Y EciFlag = 07 Xid = <Xid Value> Cavv = <blank> ErrorNo = 0 ErrorDesc = <blank>	

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test03" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 03/2007 or 03/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 3/2009 or later (4/2009, 5/2009, etc)

Use pan 4000000000000010

Test Case 4

Test Case 04	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	Cardholder enrolled, processing attempts performed	Merchant should append the Cavv and EciFlag values to the authorization message. Merchant is granted chargeback protection.
	"Test04"	<any>	<any>	cmpt_lookup response	
	<any>	04/2007 or 04/2008	<any>	Enrolled = Y ACSUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank>	
	<any>	04/2009 (and later)	4000000000000101	cmpt_authenticate response	
				PAREsStatus = A SignatureVerification = Y EciFlag = 06 Xid = <Xid Value> Cavv = <Cavv Value> ErrorNo = 0 ErrorDesc = <blank>	

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test04" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 04/2007 or 04/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 4/2009 or later (5/2009, 6/2009, etc)

Use pan 4000000000000101

Test Case 5

Test Case 05	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	Cardholder enrolled, Authentication not able to complete (Authenticate message response)	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.
	"Test05"	<any>	<any>	cmpt_lookup response	
	<any>	05/2007 or 05/2008	<any>	Enrolled = Y ACSUrl = <url> Payload = <value> ErrorNo = 0 ErrorDesc = <blank>	
	<any>	05/2009 (and later)	4000000000000036	cmpt_authenticate response	
				PAResStatus = U SignatureVerification = Y EciFlag = 07 Xid = <Xid Value> Cavv = <blank> ErrorNo = 0 ErrorDesc = <blank>	

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test05" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 05/2007 or 05/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 5/2009 or later (6/2009, 7/2009, etc)

Use pan 4000000000000036

Test Case 6

Test Case 06	Use one and only one Name, Expiration, and PAN from a row.	Scenario / Expected Results	Merchant Action												
	<table border="1"> <thead> <tr> <th>Name</th> <th>Expiration</th> <th>PAN</th> </tr> </thead> <tbody> <tr> <td>"Test06"</td> <td><any></td> <td><any></td> </tr> <tr> <td><any></td> <td>06/2007 or 06/2008</td> <td><any></td> </tr> <tr> <td><any></td> <td>06/2009 (and later)</td> <td>4000000000000044</td> </tr> </tbody> </table>	Name	Expiration	PAN	"Test06"	<any>	<any>	<any>	06/2007 or 06/2008	<any>	<any>	06/2009 (and later)	4000000000000044	<p>Timeout Encountered while processing the cmpi_lookup transaction</p> <p>cmpi_lookup response</p> <p>Enrolled = <blank> ACSUrl = <blank> Payload = <blank> ErrorNo = Timeout number ErrorDesc = Error communicating with MPI server.</p> <p>cmpi_authenticate response</p> <p>cmpi_authenticate message does not apply in this case.</p>	<p>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.</p>
Name	Expiration	PAN													
"Test06"	<any>	<any>													
<any>	06/2007 or 06/2008	<any>													
<any>	06/2009 (and later)	4000000000000044													

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test06" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 06/2007 or 06/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 6/2009 or later (7/2009, 8/2009, etc)

Use pan 4000000000000044

Test Case 7

Test Case 07	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	Cardholder not enrolled cmapi_lookup response	Merchant should submit the authorization with an ECI of 06, granting chargeback protection.
	"Test07"	<any>	<any>	Enrolled = N ACSUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank>	
	<any>	07/2007 or 07/2008	<any>	cmapi_authenticate response	
	<any>	07/2009 (and later)	4000000000000051	cmapi_authenticate message does not apply in this case.	

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test07" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 07/2007 or 07/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 7/2009 or later (8/2009, 9/2009, etc)

Use pan 4000000000000051

Test Case 8

Test Case 08	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	<p>Cardholder enrolled, Authentication unavailable (Lookup message response)</p> <p>cmpi_lookup response</p> <p>Enrolled = U ACSUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank></p> <p>cmpi_authenticate response</p> <p>cmpi_authenticate message does not apply in this case.</p>	<p>Merchant should proceed with the authorization message. Merchant retains the chargeback liability.</p>
	"Test08"	<any>	<any>		
	<any>	08/2007 or 08/2008	<any>		
	<any>	08/2009 (and later)	4000000000000069		

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test08" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 08/2007 or 08/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 8/2009 or later (9/2009, 10/2009, etc)

Use pan 4000000000000069

Test Case 9

Test Case 09	Use one and only one Name, Expiration, and PAN from a row.	Scenario / Expected Results	Merchant Action															
	<table border="1"> <thead> <tr> <th>Name</th> <th>Expiration</th> <th>PAN</th> </tr> </thead> <tbody> <tr> <td>"Test09"</td> <td><any></td> <td><any></td> </tr> <tr> <td><any></td> <td>09/2007 or 09/2008</td> <td><any></td> </tr> <tr> <td><any></td> <td>09/2009 (and later)</td> <td>4000000000000077</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Name	Expiration	PAN	"Test09"	<any>	<any>	<any>	09/2007 or 09/2008	<any>	<any>	09/2009 (and later)	4000000000000077				<p>Merchant not able to execute transactions (merchant not active)</p> <p>cmapi_lookup response</p> <p>Enrolled = U ACSUrl = <blank> Payload = <blank> ErrorNo = 1001 ErrorDesc = Error processing message request</p> <p>cmapi_authenticate response</p> <p>cmapi_authenticate message does not apply in this case.</p>	<p>Merchant should continue with the authorization and contact technical support to investigate and resolve the issue. Merchant retains chargeback liability.</p>
Name	Expiration	PAN																
"Test09"	<any>	<any>																
<any>	09/2007 or 09/2008	<any>																
<any>	09/2009 (and later)	4000000000000077																

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test09" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 09/2007 or 09/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 9/2009 or later (10/2009, 11/2009, etc)

Use pan 4000000000000077

Test Case 10

Test Case 10	Use one and only one Name, Expiration, and PAN from a row.	Scenario / Expected Results	Merchant Action															
	<table border="1"> <thead> <tr> <th>Name</th> <th>Expiration</th> <th>PAN</th> </tr> </thead> <tbody> <tr> <td>"Test10"</td> <td><any></td> <td><any></td> </tr> <tr> <td><any></td> <td>10/2007 or 10/2008</td> <td><any></td> </tr> <tr> <td><any></td> <td>10/2009 (and later)</td> <td>4000000000000085</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Name	Expiration	PAN	"Test10"	<any>	<any>	<any>	10/2007 or 10/2008	<any>	<any>	10/2009 (and later)	4000000000000085				<p>Error response to <code>cmapi_lookup</code> message</p> <p>cmapi_lookup response</p> <p>Enrolled = U ACSUrl = <blank> Payload = <blank> ErrorNo = 1001 ErrorDesc = Error processing message request.</p> <p>cmapi_authenticate response</p> <p><code>cmapi_authenticate</code> message does not apply in this case.</p>	<p>Merchant should continue with the authorization and contact technical support to investigate and resolve the issue. Merchant retains chargeback liability.</p>
Name	Expiration	PAN																
"Test10"	<any>	<any>																
<any>	10/2007 or 10/2008	<any>																
<any>	10/2009 (and later)	4000000000000085																

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test10" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 10/2007 or 10/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 10/2009 or later (11/2009, 12/2009, etc)

Use pan 4000000000000085

Test Case 11

Test Case 11	Use one and only one Name, Expiration, and PAN from a row.	Scenario / Expected Results	Merchant Action												
	<table border="1"> <thead> <tr> <th>Name</th> <th>Expiration</th> <th>PAN</th> </tr> </thead> <tbody> <tr> <td>"Test11"</td> <td><any></td> <td><any></td> </tr> <tr> <td><any></td> <td>11/2007 or 11/2008</td> <td><any></td> </tr> <tr> <td><any></td> <td>11/2009 (and later)</td> <td>4000000000000093</td> </tr> </tbody> </table>	Name	Expiration	PAN	"Test11"	<any>	<any>	<any>	11/2007 or 11/2008	<any>	<any>	11/2009 (and later)	4000000000000093	<p>Cardholder enrolled, error response to cmpi_authenticate message</p> <p>cmpi_lookup response</p> <p>Enrolled = Y ACSUrl = <url> Payload = <value> ErrorNo = 0 ErrorDesc = <blank></p> <p>cmpi_authenticate response</p> <p>PAResStatus = <blank> SignatureVerification = <blank> EciFlag = 07 Xid = <blank> Cavv = <blank> ErrorNo = 1050 ErrorDesc = Error processing PARes.</p>	<p>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.</p>
Name	Expiration	PAN													
"Test11"	<any>	<any>													
<any>	11/2007 or 11/2008	<any>													
<any>	11/2009 (and later)	4000000000000093													

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test11" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 11/2007 or 11/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 11/2009 or later (12/2009, 01/2010, etc)

Use pan 4000000000000093

7.2 MasterCard SecureCode Test Cases

Test Case 1

Test Case 01	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	Cardholder enrolled, error response to <code>cmpi_authenticate</code> message	Merchant should append the Cavv and EciFlag values to the authorization message.
	"Test01"	<any>	<any>	cmpi_lookup response	
	<any>	01/2007 or 01/2008	<any>	Enrolled = Y ACUrl = <url> Payload = <value> ErrorNo = 0 ErrorDesc = <blank>	
	<any>	01/2009 (and later)	5200000000000007	cmpi_authenticate response	
				PAResStatus = Y SignatureVerification = Y EciFlag = 02 Xid = <Xid Value> Cavv = <Cavv Value> ErrorNo = 0 ErrorDesc = <blank>	

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test01" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 01/2007 or 01/2008

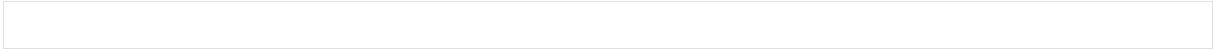
Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 01/2009 or later (02/2009, 02/2010, etc)

Use pan 5200000000000007



Test Case 2

Test Case 02	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	Cardholder enrolled, successful authentication, unsuccessful signature verification	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.
	"Test02"	<any>	<any>	cmpi_lookup response	
	<any>	02/2007 or 02/2008	<any>	Enrolled = Y ACSUrl = <url> Payload = <PAREs Payload Value> ErrorNo = 0 ErrorDesc = <blank>	
	<any>	02/2009 (and later)	5200000000000015	cmpi_authenticate response	
				PAREsStatus = Y SignatureVerification = N EciFlag = 02 Xid = <Xid Value> Cavv = <Cavv Value> ErrorNo = 0 ErrorDesc = <blank>	

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test02" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 02/2007 or 02/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 02/2009 or later (03/2009, 04/2010, etc)

Use pan 5200000000000015

Test Case 3

Test Case 03	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	<p>Cardholder enrolled, unsuccessful authentication, successful signature verification</p> <p>cmapi_lookup response</p> <p>Enrolled = Y ACSUrl = <url> Payload = <value> ErrorNo = 0 ErrorDesc = <blank></p> <p>cmapi_authenticate response</p> <p>PAResStatus = N SignatureVerification = Y EciFlag = 01 Xid = <Xid Value> Cavv = <blank> ErrorNo = 0 ErrorDesc = <blank></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>
	"Test03"	<any>	<any>		
	<any>	03/2007 or 03/2008	<any>		
	<any>	03/2009 (and later)	5200000000000023		

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test03" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 03/2007 or 03/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 03/2009 or later (04/2009, 05/2010, etc)

Use pan 5200000000000023

Test Case 4

Test Case 04	Use one and only one Name, Expiration, and PAN from a row.	Scenario / Expected Results	Merchant Action												
	<table border="1"> <thead> <tr> <th>Name</th> <th>Expiration</th> <th>PAN</th> </tr> </thead> <tbody> <tr> <td>"Test04"</td> <td><any></td> <td><any></td> </tr> <tr> <td><any></td> <td>05/2007 or 05/2008</td> <td><any></td> </tr> <tr> <td><any></td> <td>05/2009 (and later)</td> <td>5200000000000031</td> </tr> </tbody> </table>	Name	Expiration	PAN	"Test04"	<any>	<any>	<any>	05/2007 or 05/2008	<any>	<any>	05/2009 (and later)	5200000000000031	<p>Cardholder enrolled, Authentication not able to complete (Authenticate message response)</p> <p>cmpt_lookup response</p> <p>Enrolled = Y ACSUrl = <url> Payload = <value> ErrorNo = 0 ErrorDesc = <blank></p> <p>cmpt_authenticate response</p> <p>PAResStatus = U SignatureVerification = Y EciFlag = 01 Xid = <Xid Value> Cavv = <blank> ErrorNo = 0 ErrorDesc = <blank></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>
Name	Expiration	PAN													
"Test04"	<any>	<any>													
<any>	05/2007 or 05/2008	<any>													
<any>	05/2009 (and later)	5200000000000031													

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test04" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 05/2007 or 05/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 04/2009 or later (05/2009, 06/2010, etc)

Use pan 5200000000000031

Test Case 5

Test Case 05	Use one and only one Name, Expiration, and PAN from a row.	Scenario / Expected Results	Merchant Action												
	<table border="1"> <thead> <tr> <th>Name</th> <th>Expiration</th> <th>PAN</th> </tr> </thead> <tbody> <tr> <td>"Test05"</td> <td><any></td> <td><any></td> </tr> <tr> <td><any></td> <td>06/2007 or 06/2008</td> <td><any></td> </tr> <tr> <td><any></td> <td>06/2009 (and later)</td> <td>5200000000000049</td> </tr> </tbody> </table>	Name	Expiration	PAN	"Test05"	<any>	<any>	<any>	06/2007 or 06/2008	<any>	<any>	06/2009 (and later)	5200000000000049	<p>Timeout Encountered while processing the <code>cmapi_lookup</code> transaction.</p> <p>cmapi_lookup response</p> <p>Enrolled = <blank> ACSUrl = <blank> Payload = <blank> ErrorNo = Timeout number ErrorDesc = Error communicating with MPI Server</p> <p>cmapi_authenticate response</p> <p><code>cmapi_authenticate</code> message does not apply in this case.</p>	<p>The <code>cmapi_lookup</code> 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.</p>
Name	Expiration	PAN													
"Test05"	<any>	<any>													
<any>	06/2007 or 06/2008	<any>													
<any>	06/2009 (and later)	5200000000000049													

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test05" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 05/2007 or 05/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 05/2009 or later (06/2009, 07/2010, etc)

Use pan 5200000000000049

Test Case 6

Test Case 06	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	Cardholder not enrolled	Merchant should proceed with transaction. Merchant retains the chargeback liability.
	"Test06"	<any>	<any>	cmpi_lookup response	
	<any>	07/2007 or 07/2008	<any>	Enrolled = N ACSUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank>	
	<any>	07/2009 (and later)	5200000000000056	cmpi_authenticate response cmpi_authenticate message does not apply in this case.	

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test06" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 07/2007 or 07/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 07/2009 or later (08/2009, 09/2010, etc)

Use pan 5200000000000056

Test Case 7

Test Case 07	Use one and only one Name, Expiration, and PAN from a row.	Scenario / Expected Results	Merchant Action												
	<table border="1"> <thead> <tr> <th>Name</th> <th>Expiration</th> <th>PAN</th> </tr> </thead> <tbody> <tr> <td>"Test07"</td> <td><any></td> <td><any></td> </tr> <tr> <td><any></td> <td>08/2007 or 08/2008</td> <td><any></td> </tr> <tr> <td><any></td> <td>08/2009 (and later)</td> <td>5200000000000064</td> </tr> </tbody> </table>	Name	Expiration	PAN	"Test07"	<any>	<any>	<any>	08/2007 or 08/2008	<any>	<any>	08/2009 (and later)	5200000000000064	<p>Cardholder enrolled, Authentication Unavailable (Lookup message response)</p> <p>cmpi_lookup response</p> <p>Enrolled = U ACSUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank></p> <p>cmpi_authenticate response</p> <p>cmpi_authenticate message does not apply in this case.</p>	<p>Merchant should proceed with the authorization message. Merchant retains the chargeback liability.</p>
Name	Expiration	PAN													
"Test07"	<any>	<any>													
<any>	08/2007 or 08/2008	<any>													
<any>	08/2009 (and later)	5200000000000064													

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test07" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 08/2007 or 08/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 08/2009 or later (09/2009, 10/2010, etc)

Use pan 5200000000000064

Test Case 8

Test Case 08	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	<p>Merchant not able to execute transactions (merchant not active)</p> <p>cmapi_lookup response</p> <p>Enrolled = U ACSUrl = <blank> Payload = <blank> ErrorNo = 1001 ErrorDesc = Error processing message request</p> <p>cmapi_authenticate response</p> <p>cmapi_authenticate message does not apply in this case.</p>	<p>Merchant should continue with the authorization and contact technical support to investigate and resolve the issue. Merchant retains chargeback liability.</p>
	"Test08"	<any>	<any>		
	<any>	09/2007 or 09/2008	<any>		
	<any>	09/2009 (and later)	5200000000000072		

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test08" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 09/2007 or 09/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 09/2009 or later (10/2009, 11/2009, etc)

Use pan 5200000000000072

Test Case 9

Test Case 09	Use one and only one Name, Expiration, and PAN from a row.	Scenario / Expected Results	Merchant Action												
	<table border="1"> <thead> <tr> <th>Name</th> <th>Expiration</th> <th>PAN</th> </tr> </thead> <tbody> <tr> <td>"Test09"</td> <td><any></td> <td><any></td> </tr> <tr> <td><any></td> <td>10/2007 or 10/2008</td> <td><any></td> </tr> <tr> <td><any></td> <td>10/2009 (and later)</td> <td>5200000000000080</td> </tr> </tbody> </table>	Name	Expiration	PAN	"Test09"	<any>	<any>	<any>	10/2007 or 10/2008	<any>	<any>	10/2009 (and later)	5200000000000080	<p>Error response to <code>cmapi_lookup</code> message</p> <p>cmapi_lookup response</p> <p>Enrolled = U ACSUrl = <blank> Payload = <blank> ErrorNo = 1001 ErrorDesc = Error processing message request</p> <p>cmapi_authenticate response</p> <p><code>cmapi_authenticate</code> message does not apply in this case.</p>	<p>Merchant should continue with the authorization and contact technical support to investigate and resolve the issue. Merchant retains chargeback liability.</p>
Name	Expiration	PAN													
"Test09"	<any>	<any>													
<any>	10/2007 or 10/2008	<any>													
<any>	10/2009 (and later)	5200000000000080													

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test09" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 10/2007 or 10/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 10/2009 or later (11/2009, 12/2009, etc)

Use pan 5200000000000080

Test Case 10

Test Case 10	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	Cardholder enrolled, error response to cmpi_authenticate message	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.
	"Test10"	<any>	<any>	cmpi_lookup response	
	<any>	11/2007 or 11/2008	<any>	Enrolled = Y ACUrl = <url> Payload = <value> ErrorNo = 0 ErrorDesc = <blank>	
	<any>	11/2009 (and later)	5200000000000098	cmpi_authenticate response	
				PAResStatus = <blank> SignatureVerification = <blank> EciFlag = 01 Xid = <blank> Cavv = <blank> ErrorNo = 1050 ErrorDesc = Error processing PARes	

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test10" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 11/2007 or 11/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 11/2009 or later (12/2009, 01/2010, etc)

Use pan 5200000000000098

7.3 JCB J/Secure Test Cases

Test Case 1

Test Case 01	Use one and only one Name, Expiration, and PAN from a row.	Scenario / Expected Results	Merchant Action												
	<table border="1"> <thead> <tr> <th>Name</th> <th>Expiration</th> <th>PAN</th> </tr> </thead> <tbody> <tr> <td>"Test01"</td> <td><any></td> <td><any></td> </tr> <tr> <td><any></td> <td>01/2007 or 01/2008</td> <td><any></td> </tr> <tr> <td><any></td> <td>01/2009 (and later)</td> <td>3000000000000004</td> </tr> </tbody> </table>	Name	Expiration	PAN	"Test01"	<any>	<any>	<any>	01/2007 or 01/2008	<any>	<any>	01/2009 (and later)	3000000000000004	<p>Cardholder enrolled, successful authentication, successful signature verification.</p> <p>cmpi_lookup response</p> <p>Enrolled = Y ACSUrl = <url> Payload = <value> ErrorNo = 0 ErrorDesc = <blank></p> <p>cmpi_authenticate response</p> <p>PAResStatus = Y SignatureVerification = Y EciFlag = 05 Xid = <Xid Value> Cavv = <Cavv Value> ErrorNo = 0 ErrorDesc = <blank></p>	<p>Merchant should append the Cavv and EciFlag values to the authorization message.</p>
Name	Expiration	PAN													
"Test01"	<any>	<any>													
<any>	01/2007 or 01/2008	<any>													
<any>	01/2009 (and later)	3000000000000004													

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test01" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 01/2007 or 01/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 01/2009 or later (02/2009, 03/2009, etc)

Use pan 3000000000000004

Test Case 2

Test Case 02	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	Cardholder enrolled, successful authentication, unsuccessful signature verification.	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.
	"Test02"	<any>	<any>	cmapi_lookup response	
	<any>	02/2007 or 02/2008	<any>	Enrolled = Y ACSUrl = <url> Payload = <value> ErrorNo = 0 ErrorDesc = <blank>	
	<any>	02/2009 (and later)	3000000000000012	cmapi_authenticate response	
				PAResStatus = Y SignatureVerification = N EciFlag = 05 Xid = <Xid Value> Cavv = <Cavv Value> ErrorNo = 0 ErrorDesc = <blank>	

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test02" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 02/2007 or 02/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 02/2009 or later (03/2009, 04/2009, etc)

Use pan 3000000000000012

Test Case 3

Test Case 03	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	<p>Cardholder enrolled, unsuccessful authentication, successful signature verification</p> <p>cmpt_lookup response</p> <p>Enrolled = Y ACSUrl = <url> Payload = <value> ErrorNo = 0 ErrorDesc = <blank></p> <p>cmpt_authenticate response</p> <p>PAResStatus = N SignatureVerification = Y EciFlag = 07 Xid = <Xid Value> Cavv = <blank> ErrorNo = 0 ErrorDesc = <blank></p>	<p>Merchant should prompt for another form of payment and is not permitted to submit this transaction for authorization.</p>
	"Test03"	<any>	<any>		
	<any>	03/2007 or 03/2008	<any>		
	<any>	03/2009 (and later)	3000000000000020		

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test03" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 03/2007 or 03/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 03/2009 or later (04/2009, 05/2009, etc)

Use pan 3000000000000020

Test Case 4

Test Case 04	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	<p>Cardholder enrolled, Authentication Unavailable (Authenticate message response)</p> <p>cmapi_lookup response</p> <p>Enrolled = Y ACSUrl = <url> Payload = <value> ErrorNo = 0 ErrorDesc = <blank></p> <p>cmapi_authenticate response</p> <p>PAResStatus = U SignatureVerification = Y EciFlag = 07 Xid = <Xid Value> Cavv = <blank> ErrorNo = 0 ErrorDesc = <blank></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>
	"Test04"	<any>	<any>		
	<any>	05/2007 or 05/2008	<any>		
	<any>	05/2009 (and later)	3000000000000038		

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test04" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 05/2007 or 05/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 05/2009 or later (06/2009, 07/2009, etc)

Use pan 3000000000000038

Test Case 5

Test Case 05	Use one and only one Name, Expiration, and PAN from a row.	Scenario / Expected Results	Merchant Action												
	<table border="1"> <thead> <tr> <th>Name</th> <th>Expiration</th> <th>PAN</th> </tr> </thead> <tbody> <tr> <td>"Test05"</td> <td><any></td> <td><any></td> </tr> <tr> <td><any></td> <td>06/2007 or 06/2008</td> <td><any></td> </tr> <tr> <td><any></td> <td>06/2009 (and later)</td> <td>213100000000001</td> </tr> </tbody> </table>	Name	Expiration	PAN	"Test05"	<any>	<any>	<any>	06/2007 or 06/2008	<any>	<any>	06/2009 (and later)	213100000000001	<p>Timeout encountered while processing the <code>cmapi_lookup</code> transaction</p> <p>cmapi_lookup response</p> <p>Enrolled = <blank> ACSUrl = <blank> Payload = <blank> ErrorNo = Timeout number ErrorDesc = Error communicating with MPI Server</p> <p>cmapi_authenticate response</p> <p>cmapi_authenticate message does not apply in this case.</p>	<p>The <code>cmapi_lookup</code> 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.</p>
Name	Expiration	PAN													
"Test05"	<any>	<any>													
<any>	06/2007 or 06/2008	<any>													
<any>	06/2009 (and later)	213100000000001													

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test05" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 06/2007 or 06/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 06/2009 or later (07/2009, 08/2009, etc)

Use pan 213100000000001

Test Case 6

Test Case 06	Use one and only one Name, Expiration, and PAN from a row.	Scenario / Expected Results	Merchant Action															
	<table border="1"> <thead> <tr> <th>Name</th> <th>Expiration</th> <th>PAN</th> </tr> </thead> <tbody> <tr> <td>"Test06"</td> <td><any></td> <td><any></td> </tr> <tr> <td><any></td> <td>07/2007 or 07/2008</td> <td><any></td> </tr> <tr> <td><any></td> <td>07/2009 (and later)</td> <td>213100000000019</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Name	Expiration	PAN	"Test06"	<any>	<any>	<any>	07/2007 or 07/2008	<any>	<any>	07/2009 (and later)	213100000000019				<p>Cardholder not enrolled</p> <p>cmpi_lookup response</p> <p>Enrolled = N ACSUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank></p> <p>cmpi_authenticate response</p> <p>cmpi_authenticate message does not apply in this case.</p>	<p>Merchant should proceed with transaction. Merchant retains the chargeback liability.</p>
Name	Expiration	PAN																
"Test06"	<any>	<any>																
<any>	07/2007 or 07/2008	<any>																
<any>	07/2009 (and later)	213100000000019																

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test06" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 07/2007 or 08/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 07/2009 or later (08/2009, 09/2009, etc)

Use pan 213100000000019

Test Case 7

Test Case 07	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	Cardholder enrolled, Authentication Unavailable	Merchant should proceed with the authorization message. Merchant retains the chargeback liability.
	"Test07"	<any>	<any>	cmpi_lookup response	
	<any>	08/2007 or 08/2008	<any>	Enrolled = U ACUrl = <blank> Payload = <blank> ErrorNo = 0 ErrorDesc = <blank>	
	<any>	08/2009 (and later)	213100000000027	cmpi_authenticate response cmpi_authenticate message does not apply in this case.	

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test07" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 08/2007 or 08/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 08/2009 or later (09/2009, 10/2009, etc)

Use pan 213100000000027

Test Case 8

Test Case 08	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	<p>Merchant not able to execute transactions (merchant not active)</p> <p>cmapi_lookup response</p> <p>Enrolled = U ACSUrl = <blank> Payload = <blank> ErrorNo = 1001 ErrorDesc = Error processing message request</p> <p>cmapi_authenticate response</p> <p>cmapi_authenticate message does not apply in this case.</p>	<p>Merchant should continue with the authorization and contact technical support to investigate and resolve the issue. Merchant retains chargeback liability.</p>
	"Test08"	<any>	<any>		
	<any>	09/2007 or 09/2008	<any>		
	<any>	09/2009 (and later)	213100000000035		

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test08" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 09/2007 or 09/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 09/2009 or later (10/2009, 11/2009, etc)

Use pan 213100000000035

Test Case 9

Test Case 09	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	<p>Error response to <code>cmapi_lookup</code> message</p> <p>cmapi_lookup response</p> <p>Enrolled = U ACSUrl = <blank> Payload = <blank> ErrorNo = 1001 ErrorDesc = Error processing message request</p> <p>cmapi_authenticate response</p> <p><code>cmapi_authenticate</code> message does not apply in this case.</p>	<p>Merchant should continue with the authorization and contact technical support to investigate and resolve the issue. Merchant retains chargeback liability.</p>
	"Test09"	<any>	<any>		
	<any>	10/2007 or 10/2008	<any>		
	<any>	10/2009 (and later)	180000000000002		

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test09" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 10/2007 or 10/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 10/2009 or later (11/2009, 12/2009, etc)

Use pan 180000000000002

Test Case 10

Test Case 10	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	Cardholder enrolled, error response to cmpi_authenticate message	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.
	"Test10"	<any>	<any>	cmpi_lookup response	
	<any>	11/2007 or 11/2008	<any>	Enrolled = Y ACSUrl = <url> Payload = <value> ErrorNo = 1050 ErrorDesc = Error processing PAREs	
	<any>	11/2009 (and later)	180000000000010	cmpi_authenticate response	
				PAREsStatus = <blank> SignatureVerification = <blank> EciFlag = 07 Xid = <blank> Cavv = <blank> ErrorNo = Error Number ErrorDesc = Error Description	

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test10" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 11/2007 or 11/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 11/2009 or later (12/2009, 01/2010, etc)

Use pan 180000000000010

Test Case 11

Test Case 11	Use one and only one Name, Expiration, and PAN from a row.			Scenario / Expected Results	Merchant Action
	Name	Expiration	PAN	Cardholder enrolled, processing attempts performed cmapi_lookup response Enrolled = Y ACSUrl = <url> Payload = <value> ErrorNo = 0 ErrorDesc = <blank>	Merchant should append the Cavv and ECI values to the authorization message. Merchant is granted chargeback protection.
	"Test11"	<any>	<any>		
	<any>	04/2007 or 04/2008	<any>	cmapi_authenticate response PAREsStatus = A SignatureVerification = Y EciFlag = 06 Xid = <Xid Value> Cavv = <Cavv Value> ErrorNo = 0 ErrorDesc = <blank>	
	<any>	04/2009 (and later)	180000000000028		

Notes:

Use one and only one method (Name, Expiration, Pan) for this test case

Name method:

Set the name (first name, last name, or order description) as "test11" (any Capitalization)

Any expiration and any pan may be used.

Expiration method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 04/2007 or 04/2008

Use any pan

Pan method:

The name (first name, last name, or order description) must NOT have "test".

Use expiration 04/2009 or later (05/2009, 06/2009, etc)

Use pan 180000000000028

8 Integration Error Handling

The following list of Centinel 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.

8.1 Common Centinel MAPS Errors

Error Code	Error Description	Explanation	Merchant Action
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 Centinel MAPS server. This error only occurs when the Centinel 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.

8.2 `cmpi_ab_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.
950	Invalid Date Format or Range Specified	The transaction dates passed on the request message do not meet the format requirements.	Verify the dates and retry the transaction.
2002	Invalid Merchant Id or Processor Id	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.	Verify the information within your merchant profile.
2020	Invalid Transaction Password	The transaction password provided on the request message was incorrect.	Verify the transaction password within your merchant profile.
2021	Merchant Profile is not configured with a Transaction Password	The transaction password provided on the request message was incorrect.	Verify the transaction password within your merchant profile.
4000	Error Validating Processor Id Value	Unable to validate the Processor Id value passed on the request.	Complete transaction without authentication.
4020	Error Validating Merchant Id Value	Configuration Issue	Complete transaction without authentication, check merchant configuration.
4025	Error Validating Transaction Type	Configuration Issue	Complete transaction without authentication, check merchant configuration.
4900	Error Processing Authentication Lookup Request	General error encountered while processing the request.	Complete transaction without authentication, check merchant configuration.
4910	Authentication Data Not Available	System was unable to locate the transaction details by the values on the request message.	Verify the transaction details and retry.

8.3 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.	Contact technical support.
1001	Error Processing Message Request	General error encountered.	Complete transaction without authentication.
1051	Error Processing PAREs, Error Response Returned By ACS	General Protocol error encountered.	Complete transaction without authentication.
1055	Error Deserializing PAREs	General transaction error encountered.	Complete transaction without authentication.
1060	Missing or Invalid PAREs	General transaction error encountered.	Complete transaction without authentication.
1120	Error Persisting Authentication Information	General transaction error encountered.	Complete transaction without authentication.
1140	Error Persisting PAREs Information	General transaction error encountered.	Complete transaction without authentication.
1355	Transaction Lookup Not Successful, Check Transaction Id	General transaction error encountered.	Complete transaction without authentication.
1360	Payment Initiative Not Supported	General transaction error encountered.	Complete transaction without authentication.
1390	Card Type and Message Type Mismatch	General transaction error encountered.	Complete transaction without authentication.
1752	Error Processing SECURE-eBill Complete Transaction	General transaction error encountered.	Complete transaction without authentication.
1755	Unable to complete SECURE-eBill Transaction	General transaction error encountered.	Complete transaction without authentication.
1789	Error Communicating with SECURE-eBill	General transaction error encountered.	Complete transaction without authentication.
4000	Error Validating Processor Id Value	Unable to validate the Processor Id value passed on the request.	Complete transaction without authentication.
4020	Error Validating Merchant Id Value	Configuration Issue	Complete transaction without authentication, check merchant configuration.
4240	Merchant unable to process transactions, not active	Configuration Issue	Complete transaction without authentication, check merchant configuration.

4243	Merchant unable to process transactions, Payment Initiative configuration not found.	Configuration Issue	Complete transaction without authentication, check merchant configuration.
4245	Merchant unable to process transactions, Payment Initiative not active	Configuration Issue	Complete transaction without authentication, check merchant configuration.
4268	Error Validating Message, Transaction Id is Empty	General transaction error encountered.	Complete transaction without authentication.
4400	Error Parsing PAREs Message Elements	General transaction error encountered.	Complete transaction without authentication.
4770	Error Validating AAV Control byte	General transaction error encountered.	Complete transaction without authentication.
4780	Error Validating AAV Sale Amount	General transaction error encountered.	Complete transaction without authentication.
4790	Error Validating AAV Sale Amount Truncation Value	General transaction error encountered.	Complete transaction without authentication.
4800	Error Validating AAV Transaction Currency Code	General transaction error encountered.	Complete transaction without authentication.
4810	Error Validating Merchant Name Hash	General transaction error encountered.	Complete transaction without authentication.
4820	Error Validating Merchant Transaction Stamp	General transaction error encountered.	Complete transaction without authentication.
4963	Error Locating Express Checkout Data For Processing, Check TransactionId	General transaction error encountered.	Complete transaction without authentication.
4965	Error Locating Transaction Results, Check TransactionId	General transaction error encountered.	Complete transaction without authentication.

8.4 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.
789	Error Communicating with PayP-	General processing error.	Verify information, retry transac-

	al		tion. If problem continues contact technical support.
798	Merchant PayPal Configuration Not Found in System	System configuration error.	Contact technical support.
826	Error Retrieving Processor In System	System configuration error.	Contact technical support.
870	Error Retrieving Credential From System	System configuration error.	Contact technical support.
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.
1002	Error Processing Lookup Request Message	General error encountered.	Complete transaction without authentication.
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.
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.
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.
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.
1130	Error Persisting VERes Information	General transaction error encountered.	Complete transaction without authentication.

1150	Error Persisting PAREq Information	General transaction error encountered.	Complete transaction without authentication.
1160	Error Persisting VEReq Information	General transaction error encountered.	Complete transaction without authentication.
1360	Payment Initiative Not Supported	General transaction error encountered.	Complete transaction without authentication.
1380	Payment Initiative Not Supported Under Specified Message Version	General transaction error encountered.	Complete transaction without authentication.
1390	Card Type and Message Type Mismatch	General transaction error encountered.	Complete transaction without authentication.
1400	Message Version Not Supported	General transaction error encountered.	Complete transaction without authentication.
1710	SECURE-eBill Configuration Not Available, Please Contact Support	General transaction error encountered.	Complete transaction without authentication.
2107	Unable to Insert BML Application Data	General transaction error encountered, unable to complete transaction	Verify profile configuration, and retry transactions.
2112	Unable to Locate BML Application Configuration Data	Configuration Issue	Contact technical support.
2401	Unable to Complete NetCash Transaction	Configuration Issue	Contact technical support.
4000	Error Validating Processor Id Value	Unable to validate the Processor Id value passed on the request.	Complete transaction without authentication.
4020	Error Validating Merchant Id Value	Configuration Issue	Complete transaction without authentication, check merchant configuration.
4240	Merchant unable to process transactions, not active	Configuration Issue	Complete transaction without authentication, check merchant configuration.
4243	Merchant unable to process transactions, Payment Initiative configuration not found.	Configuration Issue	Complete transaction without authentication, check merchant configuration.
4245	Merchant unable to process transactions, Payment Initiative not active	Configuration Issue	Complete transaction without authentication, check merchant configuration.
4310	Error parsing VERes Message Elements	General transaction error encountered.	Complete transaction without authentication.
4375	Error Validating Recurring Value	General transaction error encountered.	Complete transaction without authentication.
4930	Error Processing PayPal Ex-	General transaction error en-	Complete transaction without au-

	press Checkout	countered.	thentication.
4951	Error Processing PayPal Transaction, Merchant Pull not activated	General transaction error encountered.	Complete transaction without authentication.
4955	System PayPal Configuration Not Available, Please Contact Support	General transaction error encountered, unable to complete PayPal payment	Verify profile configuration, and retry transactions.
4960	Error Persisting PayPal Transaction Information	General transaction error encountered.	Retry Transaction
5960	Error Persisting SECURE-eBill Transaction Information	General transaction error encountered.	Retry Transaction

9 Frequently Asked Questions

This sections contains frequently asked questions regarding Merchant Integration in general and the Centinel Thin Client technology.

Q: How do I check for card enrollment?

A: The purpose of the `cmpi_lookup` message is to verify enrollment of the card number. Please refer to the documentation regarding the required elements of the `cmpi_lookup` message

Q: How do I post values to the ACS Url ?

A: Posting the values to the ACS Url are done via a HTML form with specific form values. A Microsoft .NET example form is as follows:

```
<form name="frmLaunch" method="POST" action="<% Response.Write( strACUrl ) %>">
<input type="hidden" name="PaReq" value="<% Response.Write( strPaReqPayload )
%>"/>
<input type="hidden" name="TermUrl" value="<% Response.Write( strWebsiteTermUrl )
%>"/>
<input type="hidden" name="MD" value="<% Response.Write( strSessionTrackingId )
%>"/>
```

Note: Note that the form field names are `case sensitive`.

The Form action value is the ACSUrl value returned on the `cmpi_lookup` response.

The PaReq value is returned on the `cmpi_lookup` response, there should be no manipulation done on the value.

The TermUrl is the location on the Merchant's site that the results of the payer authentication will be posted by the ACS Server.

The MD or Merchant Data field is required on the form and is used by the Merchant to retain session information during the payer authentication transaction. If not needed by the Merchant, an empty value can be specified on the form.

Q: What are Attempts Authentication Transactions?

A: Attempts Authentication is signified by receiving an Authentication Status of 'A' from an authentication transaction. From a Merchant standpoint it is the same as a card holder authenticating successfully, and receiving an Authentication Status of 'Y'. Merchant has liability protection for these transaction.

It indicates that Verified by Visa or JCB J/Secure payer authentication was attempted for the transaction. It occurs when the Card Issuer does not yet have the ability to provide the Authentication Service. Therefore, there is nothing available to prompt for the card holders VbV password. In these cases, an 'A' is passed as the result of the authentication attempt.

Note: MasterCard SecureCode does not support Attempts Authentication, therefore you will not see any 'A' responses for that transaction type.

Q: Which Integration option should I choose, PopUp or Inline?

A: Merchants are required to integrate with an inline mode. A PopUp integration approach is susceptible to pop up blocking software, and may have a negative impact on the user experience. An inline mode utilizing frames is the recommended integration option. The only requirement of a framed approach relates to a 400 pixel by 400 pixel minimum display frame for the Card Issuer's authentication form.

Q: Once installed, how will I know if a transaction has gone through or not?

A: Once the integration is complete, and you have completed transaction testing against the CentinelTest environment, you are ready for production. Once transactions have been processed through the production systems you can run the Transaction Reports to view activity. These reports are available through the Merchant Administration portal.

You will also be able to assert that transactions were processed due to the additional ECI and Cavv/AAV values that you will have for the authorization message. These values will be available on the `cmpi_authenticate` response.

Q: What will I need to pass on the authorization message to my gateway to get the chargeback liability protection and interchange benefits?

A: Merchants are given chargeback liability protection and interchange benefits for those authorization messages that contain valid Cavv/AAV and the associated ECI values on the authorization request. These values are returned by the `cmpi_authenticate` response message.

Note: Gateways and Processors will validate the Cavv/AAV values presented on the authorization transactions are valid for the transaction details.

Q: Where can I get the Verified by Visa and MasterCard SecureCode program logos and marketing material for use on my website?

A: Program logos and marketing material is available within the Centinel Merchant Administration website. Login using your Merchant account, then from the main menu, the Payment Initiative and Marketing Materials link will take you to the information.

Q: If your server goes down, how does that affect us? Will our checkout process still function?

A: If Centinel Server becomes unavailable, the thin client request will return an error on the response. It is critical that when checking for the Centinel values within the response messages that your integration always check for the `ErrorNo` and `ErrorDesc` values. If an Error is encountered it is recommended that the message request is retried. If the second request results in an error, then normal non-authenticated checkout processing should take effect.

Q: How can I process payer authentication using multiple currency codes?

A: Our `cmpi_lookup` message allows you to pass the currency code to be used for the specific transaction enrollment lookup and authenticate. The 3 digit numeric, ISO 4217 currency code, represented by the `purchase_currency` element of the `cmpi_lookup` will be used on the payer authentication transaction. Centinel will validate the currency codes passed, to ensure they are valid according to the ISO 4217 specification.

Q: Does the Thin Client Cold Fusion require a separate `Application.CFM` file?

A: The Cold Fusion sample applications each include a simple `Application.CFM` file. The following code shows the entire file:

```
<cfapplication name="Thin Client Cold Fusion"
               sessionmanagement="Yes"
               clientmanagement="Yes"
               setclientcookies="Yes"
               sessiontimeout="#CREATETIMESPAN(0,0,20,0)#">
</cfsilent>
```

SessionManagement and ClientManagement have been turned on as well as the Application Name being set. The `Application.CFM` file was deliberately kept to a bare minimum so that no changes would be required in existing applications that would create conflicts.

Q: What changes need to be made to the Cold Fusion Administrator?

A: None. The development environment was the "default, out of the box" settings from the in-

10 Appendix A - ISO Codes

Appendix lists all ISO standard codes used by the Centinel systems.

10.1 ISO 4217 Currency Codes

Alpha Code	Country	Currency Name
ADP	020	Andorran Peseta
AED	784	UAE Dirham
AFA	004	Afghani
ALL	008	Lek
AMD	051	Armenian Dram
ANG	532	Netherlands Antillian Guilder
AON	024	Kwanza
ARS	032	Argentine Peso
ATS	040	Austrian Schilling
AUD	036	Australian Dollar
AWG	533	Aruban Guilder
AZM	031	Azerbaijani Manat
BAM	977	Convertible Marks
BBD	052	Barbados Dollar
BDT	050	Bangladesh Taka
BEF	056	Belgium Franc
BGL	100	Bulgarian Lev
BHD	048	Belgium Franc
BIF	108	Burundi Franc
BMD	060	Bermudian Dollar
BND	096	Brunei Dollar
BOB	068	Boliviano
BRL	986	Brazilian Real

BSD	986	Brazilian Real
BTN	064	Ngultrum
BWP	072	Botswana Pula
BYR	974	Belarussian Rouble
BZD	084	Belize Dollar
CAD	124	Canadian Dollar
CDF	976	Franc Congolais
CHF	756	Swiss Franc
CLP	152	Chilean Peso
CNY	156	Chinese Renminbi Yuan
COP	170	Colombian Peso
CRC	188	Costa Rican Colon
CUP	192	Cuban Peso
CVE	132	Cape Verde Escudo
CYP	196	Cyprus Pound
CZK	203	Czech Koruna
DEM	276	Deutsche Mark
DJF	262	Djibouti Franc
DKK	208	Danish Krone
DOP	214	Dominican Peso
DZD	012	Algerian Dinar
EEK	233	Kroon
EGP	818	Egyptian Pound
ERN	232	Nakfa
ETB	230	Ethiopian Birr
EUR	978	EURO
FIM	246	Finnish Markka
FJD	242	Fiji Dollar
FKP	238	Falkland Islands Pound

FRF	250	French Franc
GBP	826	Sterling
GEL	981	Lari
GHC	288	Ghana Cedi
GIP	292	Gibraltar Pound
GMD	270	Dalasi
GNF	324	Guinea Franc
GTQ	320	Quetzal
GWP	624	Guinea-Bissau Peso
GYP	328	Guyana Dollar
HKD	344	Hong Kong Dollar
HNL	340	Lempira
HRK	191	Croatian Kuna
HTG	332	Gourde
HUF	348	Hungary Forint
IDR	360	Rupiah
IEP	372	Irish Punt
ILS	376	New Israeli Sheqel
INR	356	Indian Ruppe
IQD	368	Iraqi Dinar
IRR	364	Iranian Rial
ISK	352	Iceland Krona
ITL	380	Italian Lira
JMD	388	Jamaican Dollar
JOD	400	Jordanian Dinar
JPY	392	Japanese Yen
KES	404	Kenyan Shilling
KGS	417	Som
KHR	116	Riel

KMF	174	Comoro Franc
KPW	408	North Korean Won
KRW	410	South Korean Won
KWD	414	Kuwaiti Dinar
KYD	136	Cayman Islands Dollar
KZT	398	Tenge
LAK	418	Kip
LBP	422	Lebanese Pound
LKR	144	Sri Lanka Rupee
LRD	430	Liberian Dollar
LSL	426	Loti
LTL	440	Lithuanian Litus
LUF	442	Luxembourg Franc
LVL	428	Latvian Lats
LYD	434	Libyan Dinar
MAD	504	Moroccan Dirham
MDL	498	Moldovan Leu
MGF	450	Malagasy Franc
MKD	807	Denar
MMK	104	Kyat
MNT	496	Tugrik
MOP	446	Pataca
MRO	478	Ouguiya
MTL	470	Maltese Lira
MUR	480	Mauritius Rupee
MVR	462	Rufiyaa
MWK	454	Kwacha
MXN	484	Mexican Peso
MYR	458	Malaysian Ringgit

MZM	508	Mozambique Metical
NAD	516	Namibia Dollar
NGN	566	Naira
NIO	558	Cordoba Oro
NLG	528	Dutch Guilder
NOK	578	Norwegian Krone
NPR	524	Nepalese Rupee
NZD	554	New Zealand Dollar
OMR	512	Rial Omani
PAB	590	Balboa
PEN	604	Nuevo Sol
PGK	598	Kina
PHP	608	Philippine Peso
PKR	586	Pakistan Rupee
PLN	985	Zloty
PTE	620	Portuguese Escudo
PYG	600	Guarani
QAR	634	Qatari Rial
ROL	642	Leu
RUB	643	Russian Ruble
RUR	810	Russian Ruble
RWF	646	Rwanda Franc
SAR	682	Saudi Riyal
SBD	90	Solomon Islands Dollar
SCR	690	Seychelles Rupee
SDD	736	Sudanese Dinar
SEK	752	Swedish Krona
SGD	702	Singapore Dollar
SHP	654	Saint Helena Pound

SIT	705	Tolar
SKK	703	Slovak Koruna
SLL	694	Leone
SOS	706	Somali Shilling
SRG	740	Suriname Guilder
STD	678	Dobra
SVC	222	El Salvador Colon
SYP	760	Syrian Pound
SZL	748	Lilangeni
THB	764	Thailand Baht
TJS	972	Somoni
TMM	795	Manat
TND	788	Tunisian Dinar
TOP	776	Pa'anga
TPE	626	Timor Escudo
TRL	792	Turkish Lira
TTD	780	Trinidad and Tobago Dollar
TWD	901	New Taiwan Dollar
TZS	834	Tanzanian Shilling
UAH	980	Hryvnia
UGX	800	Uganda Shilling
USD	840	US Dollar
UYU	858	Peso Uruguayo
UZS	860	Tanzanian Shilling
VEB	862	Bolivar
VND	704	Dong
VUV	548	Vatu
WST	882	Tala
XAF	950	CFA Franc BEAC

XCD	951	East Caribbean Dollar
XOF	952	CFA Franc BCEAO
XPF	953	CFP Franc
YER	886	Yemeni Rial
YUM	891	Yugoslavian Dinar
ZAR	710	South Africa Rand
ZMK	894	Kwacha
ZWD	716	Zimbabwe Dollar

10.2 ISO 3166 Country Codes

Alpha Code	Country
AD	Andorra
AE	United Arab Emirates
AF	Afghanistan
AG	Antigua & Barbuda
AI	Anguilla
AL	Albania
AM	Armenia
AN	Netherlands Antilles
AO	Angola
AQ	Antarctica
AR	Argentina
AS	American Samoa
AT	Austria
AU	Australia
AW	Aruba
AZ	Azerbaijan

BA	Bosnia and Herzegovina
BB	Barbados
BD	Bangladesh
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BH	Bahrain
BI	Burundi
BJ	Benin
BM	Bermuda
BN	Brunei Darussalam
BO	Bolivia
BR	Brazil
BS	Bahama
BT	Bhutan
BU	Burma (no longer exists)
BV	Bouvet Island
BW	Botswana
BY	Belarus
BZ	Belize
CA	Canada
CC	Cocos (Keeling) Islands
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Cote D'ivoire (Ivory Coast)
CK	Cook Islands
CL	Chile
CM	Cameroon

CN	China
CO	Colombia
CR	Costa Rica
CS	Czechoslovakia (no longer exists)
CU	Cuba
CV	Cape Verde
CX	Christmas Island
CY	Cyprus
CZ	Czech Republic
DD	German Democratic Republic (no longer exists)
DE	Germany
DJ	Djibouti
DK	Denmark
DM	Dominica
DO	Dominican Republic
DZ	Algeria
EC	Ecuador
EE	Estonia
EG	Egypt
EH	Western Sahara
ER	Eritrea
ES	Spain
ET	Ethiopia
FI	Finland
FJ	Fiji
FK	Falkland Islands (Malvinas)
FM	Micronesia
FO	Faroe Islands
FR	France

FX	France, Metropolitan
GA	Gabon
GB	United Kingdom (Great Britain)
GD	Grenada
GE	Georgia
GF	French Guiana
GH	Ghana
GI	Gibraltar
GL	Greenland
GM	Gambia
GN	Guinea
GP	Guadeloupe
GQ	Equatorial Guinea
GR	Greece
GS	South Georgia and the South Sandwich Islands
GT	Guatemala
GU	Guam
GW	Guinea-Bissau
GY	Guyana
HK	Hong Kong
HM	Heard & McDonald Islands
HN	Honduras
HR	Croatia
HT	Haiti
HU	Hungary
ID	Indonesia
IE	Ireland
IL	Israel
IN	India

IO	British Indian Ocean Territory
IQ	Iraq
IR	Islamic Republic of Iran
IS	Iceland
IT	Italy
JM	Jamaica
JO	Jordan
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KH	Cambodia
KI	Kiribati
KM	Comoros
KN	St. Kitts and Nevis
KP	Korea, Democratic People's Republic of
KR	Korea, Republic of
KW	Kuwait
KY	Cayman Islands
KZ	Kazakhstan
LA	Lao People's Democratic Republic
LB	Lebanon
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia

LY	Libyan Arab Jamahiriya
MA	Morocco
MC	Monaco
MD	Moldova, Republic of
MG	Madagascar
MH	Marshall Islands
ML	Mali
MN	Mongolia
MM	Myanmar
MO	Macau
MP	Northern Mariana Islands
MQ	Martinique
MR	Mauritania
MS	Montserrat
MT	Malta
MU	Mauritius
MV	Maldives
MW	Malawi
MX	Mexico
MY	Malaysia
MZ	Mozambique
NA	Nambia
NC	New Caledonia
NE	Niger
NF	Norfolk Island
NG	Nigeria
NI	Nicaragua
NL	Netherlands
NO	Norway

NP	Nepal
NR	Nauru
NT	Neutral Zone (no longer exists)
NU	Niue
NZ	New Zealand
OM	Oman
PA	Panama
PE	Peru
PF	French Polynesia
PG	Papua New Guinea
PH	Philippines
PK	Pakistan
PL	Poland
PM	St. Pierre & Miquelon
PN	Pitcairn
PR	Puerto Rico
PT	Portugal
PW	Palau
PY	Paraguay
QA	Qatar
RE	Reunion
RO	Romania
RU	Russian Federation
RW	Rwanda
SA	Saudi Arabia
SB	Solomon Islands
SC	Seychelles
SD	Sudan
SE	Sweden

SG	Singapore
SH	St. Helena
SI	Slovenia
SJ	Svalbard & Jan Mayen Islands
SK	Slovakia
SL	Sierra Leone
SM	San Marino
SN	Senegal
SO	Somalia
SR	Suriname
ST	Sao Tome & Principe
SU	Union of Soviet Socialist Republics (no longer exists)
SV	El Salvador
SY	Syrian Arab Republic
SZ	Swaziland
TC	Turks & Caicos Islands
TD	Chad
TF	French Southern Territories
TG	Togo
TH	Thailand
TJ	Tajikistan
TK	Tokelau
TM	Turkmenistan
TN	Tunisia
TO	Tonga
TP	East Timor
TR	Turkey
TT	Trinidad & Tobago
TV	Tuvalu

TW	Taiwan, Province of China
TZ	Tanzania, United Republic of
UA	Ukraine
UG	Uganda
UM	United States Minor Outlying Islands
US	United States of America
UY	Uruguay
UZ	Uzbekistan
VA	Vatican City State (Holy See)
VC	St. Vincent & the Grenadines
VE	Venezuela
VG	British Virgin Islands
VI	United States Virgin Islands
VN	Viet Nam
VU	Vanuatu
WF	Wallis & Futuna Islands
WS	Samoa
YD	Democratic Yemen (no longer exists)
YE	Yemen
YT	Mayotte
YU	Yugoslavia
ZA	South Africa
ZM	Zambia
ZR	Zaire
ZW	Zimbabwe
ZZ	Unknown or unspecified country