

CyberSource Payer Authentication

Using the Simple Order API

February 2017



CyberSource Contact Information

For general information about our company, products, and services, go to <http://www.cybersource.com>.

For sales questions about any CyberSource Service, email sales@cybersource.com or call 650-432-7350 or 888-330-2300 (toll free in the United States).

For support information about any CyberSource Service, visit the Support Center at <http://www.cybersource.com/support>.

Copyright

© 2017 CyberSource Corporation. All rights reserved. CyberSource Corporation ("CyberSource") furnishes this document and the software described in this document under the applicable agreement between the reader of this document ("You") and CyberSource ("Agreement"). You may use this document and/or software only in accordance with the terms of the Agreement. Except as expressly set forth in the Agreement, the information contained in this document is subject to change without notice and therefore should not be interpreted in any way as a guarantee or warranty by CyberSource. CyberSource assumes no responsibility or liability for any errors that may appear in this document. The copyrighted software that accompanies this document is licensed to You for use only in strict accordance with the Agreement. You should read the Agreement carefully before using the software. Except as permitted by the Agreement, You may not reproduce any part of this document, store this document in a retrieval system, or transmit this document, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written consent of CyberSource.

Restricted Rights Legends

For Government or defense agencies. Use, duplication, or disclosure by the Government or defense agencies is subject to restrictions as set forth the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and in similar clauses in the FAR and NASA FAR Supplement.

For civilian agencies. Use, reproduction, or disclosure is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer Software Restricted Rights clause at 52.227-19 and the limitations set forth in CyberSource Corporation's standard commercial agreement for this software. Unpublished rights reserved under the copyright laws of the United States.

Trademarks

Authorize.Net, eCheck.Net, and The Power of Payment are registered trademarks of CyberSource Corporation.

CyberSource, CyberSource Payment Manager, CyberSource Risk Manager, CyberSource Decision Manager, and CyberSource Connect are trademarks and/or service marks of CyberSource Corporation.

All other brands and product names are trademarks or registered trademarks of their respective owners.

Contents

Recent Revisions to This Document 7

About This Guide 8

Audience 8

Purpose 8

Scope 8

Conventions 9

 Note and Important Statements 9

 Text and Command Conventions 9

Related Documents 10

Customer Support 10

Chapter 1 **Introducing Payer Authentication** 11

Payer Authentication Overview 11

 Overview of Chargeback Protection 13

Prerequisites for Implementing Payer Authentication 13

 Required Merchant Information 14

 Joint e-Commerce Framework Testing (JEF Tests) 14

Payer Authentication Process 15

 Enrollment and Authentication 15

 Validate Authentication 17

Chapter 2 **Integrating Payer Authentication into Your Business** 18

Process Overview 19

 Phase 1: Prerequisites 19

 Phase 2: Implementation 20

 Phase 3: Formal Testing 21

 Phase 4: Code Deployment to Production Environment 22

Implementing Payer Authentication Services	23
Step 1: Checking Enrollment	24
A. Requesting the Check Enrollment Service	24
B. Interpreting the Reply	25
Step 2: Authenticating Enrolled Cards	26
A. Creating the HTTP POST Form	26
B. Creating the HTML Frame for Authentication	26
C. Receiving the PARES Message from the Card-Issuing Bank	27
Step 3: Validating Authentication	28
A. Requesting the Validation Service	28
B. Interpreting the Reply	30
C. Redirecting Customers to Pass or Fail Message Page	30

Chapter 3 **Testing Payer Authentication Services** 31

Testing Process	31
Enrollment Check	31
Authentication Validation	34
Expected Results	35
Test Cases	37
Verified by Visa	37
Mastercard SecureCode	46
Maestro SecureCode	55
American Express SafeKey	60
JCB J/Secure	66
Diners Club ProtectBuy	72

Appendix A **API Fields** 78

Formatting Restrictions	78
Data Type Definitions	78
Request Fields	79

Appendix B **Reason Codes** 95

Appendix C **Request and Reply Examples** 96

Check Enrollment Example	96
Transaction Reply for Visa with Verified by Visa	97
Transaction Reply for Mastercard with SecureCode	98
Transaction Reply for JCB with J/Secure	99

Validate Authentication	100
Transaction Reply for Visa with Verified by Visa	100
Transaction Reply for Mastercard with SecureCode	101
Transaction Reply for JCB with J/Secure	101
ProofXML	102

Appendix D Web Site Modification Reference 103

Web Site Modification Checklist	103
3D Secure Services Logos	104
Informational Message Examples	105

Appendix E Payer Authentication Transaction Details in the Business Center 106

Searching for Payer Authentication Details	106
Enrolled Card	106
Enrollment Check	106
Authentication Validation	112
Card Not Enrolled	113
Payer Authentication Details	113
Transaction Details	115
Payer Authentication Search	116
Storing Payer Authentication Data	117

Appendix F Payer Authentication Reports 118

Payer Authentication Summary Report	118
Downloading the Report	119
Matching the Report to the Transaction Search Results	120
Interpreting the Report	121
Comparing Payer Authentication and Payment Reports	122
Payer Authentication Detail Report	123
Report	124
<Result>	124
<PayerAuthDetail>	124
<ProofXML>	126
<VEReq>	127
<VERes>	128
<PAREq>	129
<PAREs>	130
<AuthInfo>	132

Examples	133
Failed Enrollment Check	133
Successful Authentication	134

Appendix G Rules-Based Payer Authentication 135

Available Rules	135
API Replies	136
Bypassed Authentication Transactions	136
Risk-Based Bank Transactions	137

Glossary 138

Index 145

Recent Revisions to This Document

Release	Changes
February 2017	<ul style="list-style-type: none"> Added collection indicator of 1 to Test Case 18, Mastercard SecureCode Card Enrolled: Attempts Processing. See "Test Cases," page 37. Corrected the returned collection indicator and e-commerce indicator for Test Case 26, Mastercard SecureCode Enrollment Check Error, and Test Case 39, Maestro SecureCode Enrollment Check Error. The collection indicator value has been corrected from 1 to 0; the e-commerce indicator value has been corrected from spa to internet. See "Test Cases," page 37. Added possible values for American Express SafeKey reply fields. See "American Express SafeKey," page 60.
September 2016	Added API request fields as optional for enrollment service and required for American Express SafeKey processing in the United States (domestic only). See "Request Fields," page 79 .
June 2016	<ul style="list-style-type: none"> Added note that all white spaces must be removed from PaRes field in the validation request. See "Step 3: Validating Authentication," page 28. Updated Mastercard and Maestro SecureCode Card Not Enrolled test cases. See "Test Cases," page 37. Updated payerAuthEnrollReply_ucafCollectionIndicator reply field to include value of 0. See "API Fields," page 78.
March 2016	<ul style="list-style-type: none"> Added information about implementing Payer Authentication with Visa Checkout. See "Implementing Payer Authentication Services," page 23. Added support for Diners Club and Elo cards, including new test cases, and updated API fields. See "Diners Club ProtectBuy," page 72, and "Reply Fields," page 85. Updated the reports chapter to include American Express, Diners Club, and Elo cards. See "Interpreting the Report," page 121.
September 2015	Updated URL for testing. See "Phase 2: Implementation," page 20 .
August 2015	<ul style="list-style-type: none"> Added new Visa and Mastercard test cases for passive authentication (RIBA_PASS) and risk-based bank authentication (RIBA). See "Test Cases," page 37. Added the Authentication Type to test cases. See "Test Cases," page 37. Updated the Mastercard reply fields. See "Mastercard SecureCode," page 46. Added information about the rules-based Payer Authentication feature. See "Rules-Based Payer Authentication," page 135.

About This Guide

Audience

This guide is written for application developers who want to use the CyberSource Simple Order API to integrate Payer Authentication services into their order management system.

Implementing CyberSource Payer Authentication services requires software development skills. You must write code that uses the API request and reply fields to integrate Payer Authentication services into your existing order management system.

Purpose

This guide describes tasks you must complete to integrate Payer Authentication Services into your existing order management system.

Scope

This guide describes how to use the Simple Order API to integrate Payer Authentication services with your order management system. It does not describe how to get started using the Simple Order API nor does it explain how to use CyberSource services other than Payer Authentication. For that information, see ["Related Documents," page 10](#).

Conventions

Note and Important Statements



Note

A *Note* contains helpful suggestions or references to material not contained in this document.



Important

An *Important* statement contains information essential to successfully completing a task or learning a concept.

Text and Command Conventions

Convention	Usage
bold	<ul style="list-style-type: none"> Field and service names in text. For example: Include the ics_applications field. Items that you are instructed to act upon. For example: Click Save.
<i>italic</i>	<ul style="list-style-type: none"> Filenames and pathnames. For example: Add the filter definition and mapping to your <i>web.xml</i> file. Placeholder variables for which you supply particular values.
monospace	<ul style="list-style-type: none"> XML elements. Code examples and samples. Text that you enter in an API environment. For example: Set the davService_run field to <code>true</code>.

Related Documents

- *Getting Started with CyberSource Advanced for the Simple Order API* describes how to get started using the Simple Order API. ([PDF](#) | [HTML](#))
- *Decision Manager Developer Guide Using the Simple Order API* describes how to integrate Decision Manager, a fraud detection service, with your order management system. ([PDF](#) | [HTML](#))
- *Credit Card Services Using the Simple Order API* describes how to integrate CyberSource payment processing services into your business. ([PDF](#) | [HTML](#))
- *Secure Acceptance Web/Mobile Configuration Guide* describes how to create Secure Acceptance Web/Mobile profiles, which enable you to integrate your order management system with the Secure Acceptance Web/Mobile checkout. ([PDF](#) | [HTML](#))
- *Secure Acceptance Silent Order POST Development Guide* describes how to create Secure Acceptance Silent Order POST profiles, which enable you to integrate your order management system with a web site to process transactions. ([PDF](#) | [HTML](#))
- *Reporting Developer Guide* describes how to view and configure Business Center reports. ([PDF](#) | [HTML](#))

Refer to the Support Center for complete CyberSource technical documentation:

http://www.cybersource.com/support_center/support_documentation

Customer Support

For support information about any CyberSource service, visit the Support Center:

<http://www.cybersource.com/support>

Introducing Payer Authentication

CyberSource Payer Authentication services enable you to add support to your web store for card authentication services, including Visa Verified by VisaSM, Mastercard[®] and Maestro[®] SecureCode[™] (UK Domestic and international), American Express SafeKeySM, JCB J/Secure[™], and Diners Club ProtectBuy.

These card authentication services deter unauthorized card use and protect you from fraudulent chargeback activity referred to as *liability shift*. However, Payer Authentication is not a fraud management service, such as Decision Manager with Advanced Fraud Screen. CyberSource recommends that you implement a comprehensive fraud management program in addition to Payer Authentication services.

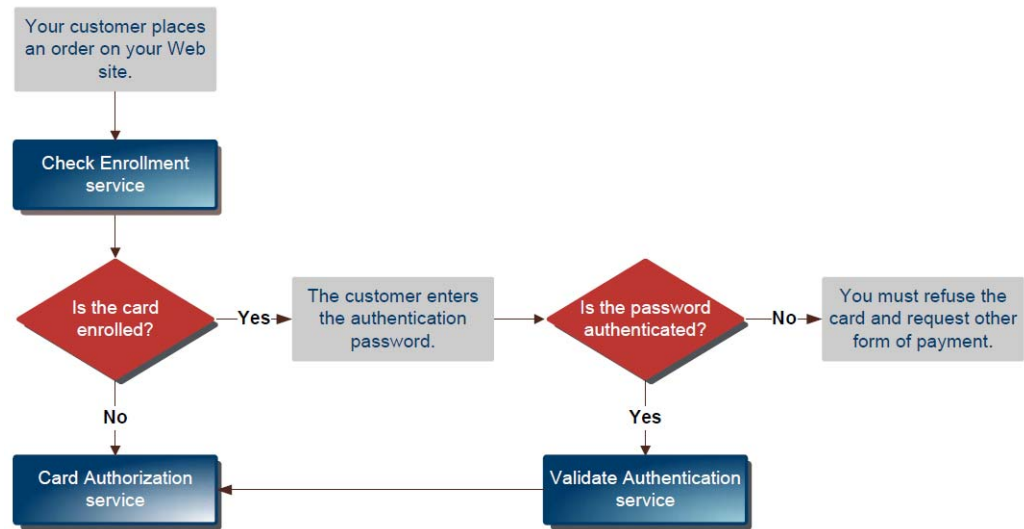
You can use Payer Authentication services with specific payment processors. To find out if your payment processor supports this feature, see the “Payer Authentication” section in *Credit Card Services Using the Simple Order API* ([PDF](#) | [HTML](#)).

Payer Authentication Overview

Payer Authentication provides the following services:

- Check Enrollment: Determines whether the customer is enrolled in one of the card authentication programs.
- Validate Authentication: Ensures that the authentication that you receive from the issuing bank is valid.

[Figure 1](#) shows the Payer Authentication process after a customer places an order on your web site. CyberSource provides the Check Enrollment, Card Authorization, and the Validate Authentication services.

Figure 1 Payer Authentication Process Overview

The Check Enrollment service determines whether the customer is enrolled in one of the card authentication services:

■ **No**

If the card is not enrolled, you can process the authorization immediately.

■ **Yes**

If the card is enrolled, the customer's browser displays a window where the customer can enter the password associated with the card. This is how the customer authenticates their card with the issuing bank.

- If the password matches the password stored by the bank, you need to verify that the information is valid with the Validate Authentication service. If the identity of the sender is verified, you can process the payment with the Card Authorization service.
- If the password does not match the password stored by the bank, the customer may be fraudulent. You must refuse the card and can request another form of payment.

Overview of Chargeback Protection

Visa, Mastercard, Maestro, American Express, JCB, and Diners Club may offer chargeback protection if merchants participate in [3D Secure](#) card authentication programs, such as Verified by Visa or Mastercard SecureCode.

Chargebacks occur after a transaction is processed, and how they are handled varies according to the region that issued the card. Payment card company rules might vary over time and across geographical regions. CyberSource recommends that you contact your merchant account provider to find out exactly how to interpret chargeback requirements and which chargeback protections are offered.

Prerequisites for Implementing Payer Authentication

To use the Payer Authentication services, you and your developers must be able to complete these tasks:

- Write code to enable a connection to the issuing bank.
- Add specific data to your API requests to CyberSource.
- Validate the necessary data.
- Provide the additional data to the authorization request.
- Modify your web site to help the customer understand the process.

Required Merchant Information

Before using CyberSource Payer Authentication services in production, you must contact Customer Support to provide information about your company and your acquiring bank so that CyberSource can configure your account to implement these services.

You must provide the information listed in [Table 1](#) to CyberSource before Payer Authentication services can be enabled:

Table 1 Merchant Information Required for Payer Authentication Services

Information	Description
About your company	<ul style="list-style-type: none"> Your CyberSource merchant ID. URL of your company's web site, for example: http://www.example.com Two-character ISO code for your country.
Bank Information	<ul style="list-style-type: none"> Name of your bank acquirer. Complete name and address of your bank contact, including email address.
Visa, Mastercard, Maestro, American Express, JCB, and Diners Club Information	Information provided by your bank acquirer about each payment card company for which you are configured:
Acquirer merchant ID	<ul style="list-style-type: none"> 6-digit BIN numbers. Acquirer merchant ID: merchant ID assigned by your acquirer. All currencies that you are set up to process.

Joint e-Commerce Framework Testing (JEF Tests)

This section applies to the following card types: Visa, Mastercard, Maestro, American Express, and JCB.

JEF is a set of payment integration tests that simulates realistic scenarios that would have an impact on your business in a production environment. Each test is designed to ensure that your implementation of Payer Authentication services processes the data correctly. CyberSource provides you with a test plan that describes expected results. After your implementation is ready to deploy to your production environment, you must notify your CyberSource contact to schedule the formal testing.

For more information, see ["Phase 3: Formal Testing," page 21](#).

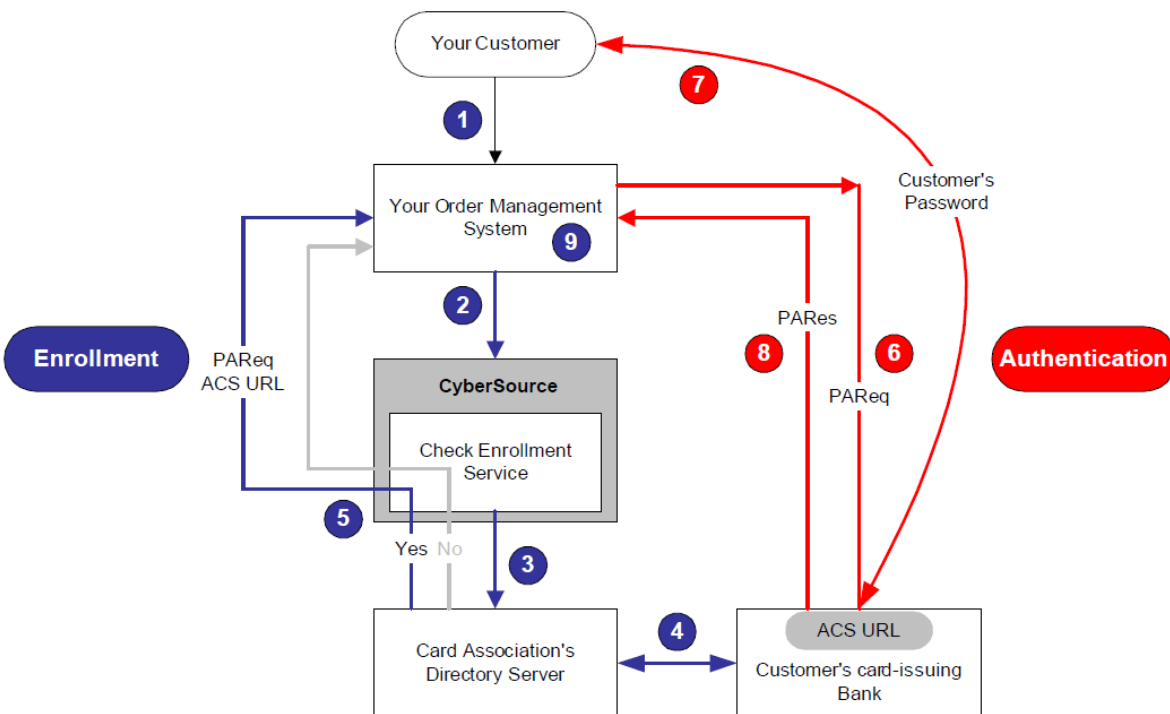
Payer Authentication Process

This section describes the Payer Authentication process. [Figure 2](#) describes the enrollment and authentication process. [Figure 3](#) describes the steps for validating card authentication.

Enrollment and Authentication

The goal is to verify that the customer is enrolled in a card authentication program and to create the authentication request message (PAReq) for enrolled cards. The enrollment check is shown in Steps 2 to 5; the authentication is shown in Steps 6 to 8.

Figure 2 Enrollment and Authentication Process



- 1** When the customer places an order on your web site, your order management system extracts the purchase information from the POST of the final page of the order.
- 2** To verify that the customer is enrolled in one of the card authentication programs, you request the Enrollment Check service.
- 3** CyberSource contacts the appropriate [Directory Server](#) for the card type.
- 4** The Directory Server verifies with the bank that issued the card that the card is enrolled. If the card is enrolled, the directory server receives the URL of the [Access Control Server](#) (ACS) where the customer can be authenticated.

- 5 The Directory Server replies to CyberSource and to your Order Management System as follows:
 - If the customer is enrolled, you receive this information:
 - A payer authentication request (PAReq) message, which contains a unique transaction ID (XID).
 - The ACS URL of the issuing bank where you need to send the PAReq message.
 - If the card is not enrolled, authentication and validation are omitted and the process proceeds with card authorization.
- 6 If the card is enrolled, you send the PAReq message to the ACS URL of the card-issuing bank to request authentication.
- 7 The customer's web browser displays the card-issuing bank's authentication dialog box where the customer enters their password for the card.
- 8 The card-issuing bank replies to your order management system with a PAREs message that contains the results of the authentication.
- 9 You verify that the signature in the PAREs is the same as that in the PAReq.

This final check verifies that the enrollment and validation checks are for the same transaction. The rest of the process is described in the following "Validate Authentication" section.

Validate Authentication

The Validate Authentication service verifies and interprets the payment authentication response message returned by the card-issuing bank.

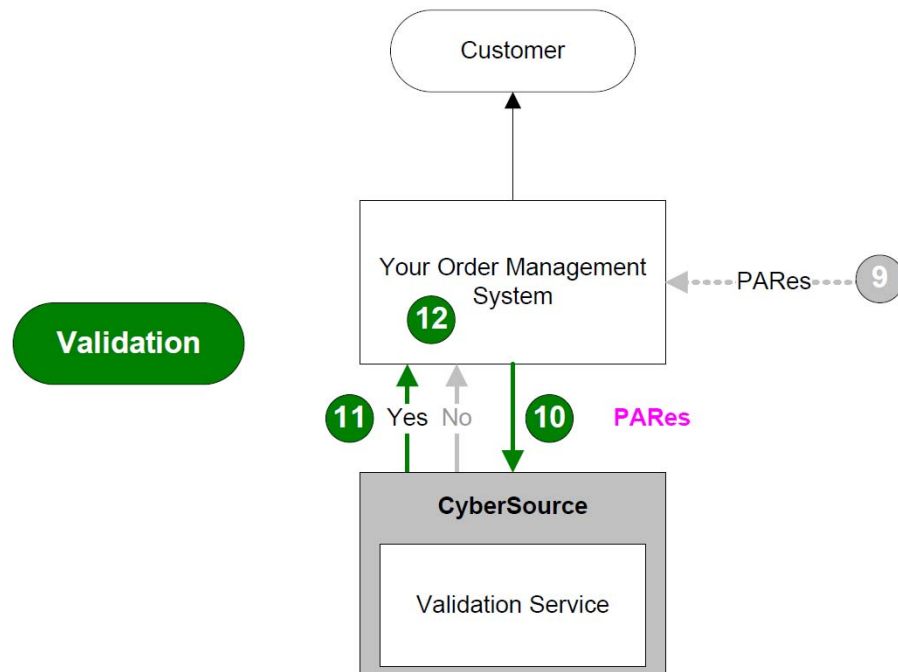


Important

If the authentication fails, Visa, American Express, JCB, and Diners Club require that you do not accept the card. Instead, you must ask the customer to use another payment method.

The steps in the following figure resume the process started in the ["Enrollment and Authentication Process,"](#) page 15.

Figure 3 Validate Authentication Process



- 1 You extract the [PAREs](#) message from the form and request the CyberSource Validate Authentication service, which uses the message's digital signature to verify the sender's identity.
- 2 You receive a reply with the authentication result.
- 3 You verify that the [XID](#) in the PAREs is the same as that in the [PAREq](#).

This final check verifies that the enrollment and validation checks are for the same transaction.

Integrating Payer Authentication into Your Business

The integration process takes approximately 10 weeks from the initial stages of contacting your [acquirer](#) until you can use Payer Authentication in your production environment.



Add 1 week for each Joint e-Commerce Framework (JEF) testing attempt. For example, if your Payer Authentication implementation passes the JEF test on the first attempt, the Payer Authentication process should take approximately 10 weeks to complete. However, if your implementation fails during the first test attempt, expect to add an additional week to the schedule, and expect integration to take approximately 11 weeks. For more information about JEF testing, see "[Joint e-Commerce Framework Testing \(JEF Tests\)](#)," [page 14](#).

Process Overview

The following tables summarize the process of integrating Payer Authentication services into your existing business processes.

Phase 1: Prerequisites

Before implementing Payer Authentication services, your business team must contact your acquirer and CyberSource to begin setting up the service. Your software development team should become familiar with the API fields and technical details of this service.

Table 2 Prerequisite Tasks (Approximate Time to Complete is Two Weeks)

Project Manager Tasks	Developer Tasks
1 Contact your acquirer about using 3D Secure Services (Verified by Visa, Mastercard SecureCode, American Express SafeKey, JCB J/Secure, and Diners Club ProtectBuy). Discuss liability shift to understand the protections offered for your region.	1 Review Credit Card Services Using the Simple Order API .
2 Go to www.cybersource.com/register to create a CyberSource merchant ID that you will use for testing your Payer Authentication implementation.	2 Review CyberSource Payer Authentication Using the Simple Order API .
3 Notify your CyberSource account representative that you want to implement Payer Authentication (3D Secure). Give them the CyberSource merchant ID you created in Step 2 that you will use for testing. For more information, see "Required Merchant Information," page 14.	
Note Set up for testing can take up to 3 business days.	

Phase 2: Implementation

Implementation includes modifying your web site front end and developing the software code to integrate with Payer Authentication services. For a detailed discussion of the steps in this phase, see this chapter's sections starting with ["Implementing Payer Authentication Services,"](#) page 23.

Table 3 Implementation Tasks (Approximate Time to Complete is Four Weeks)

Project Manager Tasks	Developer Tasks
	1 Develop code to modify your web site checkout page appearance. For information about requirements for modifying your web site checkout page, see Appendix D, "Web Site Modification Reference," on page 103.
	2 Develop code to send a request (VEReq) to verify card enrollments. See "A. Requesting the Check Enrollment Service," page 24.
	3 If required, enable API logging for debugging purposes.
	4 Display the Access Control Server URL (ACS URL) correctly, and capture the return data for the PAREq . See "B. Interpreting the Reply," page 25.
	5 Add code to the HTTP POST request to send the required data, including the PAREq , to the ACS URL.
	6 Develop code to send a validate request to CyberSource and include the correct data sent to the TermURL from the ACS URL. See "A. Requesting the Validation Service," page 28.
	7 Where applicable, develop code to pass appropriate data into the authorization requests. See "B. Interpreting the Reply," page 30.
	8 Use the test cases in Chapter 3, "Testing Payer Authentication Services," on page 31 to test your preliminary code and make the appropriate changes. For test transactions, send requests to the test URL: <code>https://ics2wstesta.ic3.com/commerce/1.x/transactionProcessor</code>
	9 If not activated previously, enable API logging for the formal testing phase.
1 After code complete has been confirmed, contact your CyberSource account representative to arrange a time to begin formal testing with the CyberSource technical team.	10 Confirm with your business contact or project manager that the code is complete (written and tested).

Phase 3: Formal Testing

To ensure that your implementation of Payer Authentication services is coded correctly, CyberSource recommends that you complete [Joint e-Commerce Framework Testing](#) for the following card types: Visa, Mastercard, Maestro, American Express, and JCB. Ensure that you run only accreditation tests during formal testing.

Table 4 Formal Testing Tasks (Approximate Time to Complete is One Week)

CyberSource Technical Team Tasks	Project Manager Tasks	Developer Tasks
1 Provide to the merchant's developer team a test document that describes the accreditation tests and the expected test results.		1 During the scheduled test time, run the accreditation tests in the exact sequence as described in the testing document provided by CyberSource.
		2 Record the test results as described in the testing document, and send the completed tests to the CyberSource technical team. Important Only send your test results when they match the required results as described in the testing document. Send API logs for each test run.
2 Mark and review the test results, which takes up to 3 working days. If your testing does not meet the criteria for successful Payer Authentication processing, CyberSource provides a list of improvements.		3 Repeat Steps 1 and 2 until successful completion of JEF testing.

Note Each additional formal test run attempt requires approximately 1 additional week.

Phase 4: Code Deployment to Production Environment

Table 5 Code Deployment Tasks (Approximate Time to Complete is Three Weeks)

CyberSource Tasks	Project Manager Tasks	Developer Tasks
	<p>1 Provide banking information to CyberSource so your account can be created on the production Directory Servers.</p> <p>Note Account creation on the production Directory Servers takes 2 weeks. Provide your banking information as soon as possible to avoid delays.</p> <p>Barclays Barclays performs this step on your behalf. Notify them in advance to avoid delays. When they provide the following information, send it to your CyberSource account representative:</p> <ul style="list-style-type: none"> • Visa Login ID • Visa password • Mastercard Merchant ID 	
1 CyberSource primary support team asks your acquiring bank to upload data to the Directory Servers.	2 Request that CyberSource enable your production account for Payer Authentication services.	
2 After the CyberSource team receives confirmation that the data has been uploaded to the Directory Servers, the team loads the data on to the Merchant Plugin (MPI) for processing.		1 Verify logging capabilities in production. Some acquiring banks require that you maintain a log of the response fields (for example ProofXML , PAREq , PAREs , CAVV , and ECI). Typically this data must be presented in decompressed, decoded form to dispute chargebacks.
<p>3 When the third parties notify CyberSource of successful activation, Payer Authentication services are turned on for your account.</p> <p>Note This step takes approximately 3 days.</p>		

Implementing Payer Authentication Services



Warning

Do not use Payer Authentication services for subscription payments because you cannot receive chargeback protection for these transactions.

To reduce your development time, CyberSource recommends that you request both payer authentication and the card authorization services at the same time. When you do so, CyberSource automatically sends the correct information to your payment processor. For example, CyberSource converts the values of these fields, which are in base64, to the proper format required by your payment processor:

- **CAVV:** `payerAuthValidateReply_cavv`
- **AAV:** `payerAuthValidateReply_ucafAuthenticationData`
- **XID:** `payerAuthEnrollReply_xid` and `payerAuthValidateReply_xid`

If you request the services separately, you need to include the value of these fields, not the field name, in the subsequent card authorization service request.

In most cases, you request card authorization only once for each purchase. However, you need to send multiple authorization requests if the original authorization expires before it is captured, which can occur when order fulfillment is split or delayed.

- *Single authorizations:* For most purchases, you request authorization only once with either one or both Payer Authentication services:
 - With Check Enrollment: the authorization is processed only if the customer is not enrolled in a card authentication program. If the customer is enrolled, you must validate the authentication before the card can be authorized.
 - With Validate Authentication: the authorization is processed only if the customer's authentication is valid.
- *Multiple Authorizations:* In these cases, you need to include in subsequent authorization requests the same payer authentication data contained in the original request so that your acquiring bank can track all related requests if a dispute occurs.



Important

If you are using Visa Checkout, you must include the payer authentication enroll service and the credit card authorization service in the same request message in order to decrypt the primary account number (PAN) and complete the rest of the payer authentication flow. When you submit a separate request message for each service, the payer authentication enroll service request fails.

Step 1: Checking Enrollment

When the customer places an order on your web site, your order management system processes the purchase information from the POST of the final page of the order. The goal is to verify that the card is enrolled and to authenticate the results if it is enrolled. To do so, you request the Enrollment Check service ([VEReq](#)), and then proceed as follows:

- If the card is enrolled, the [VERes](#) reply field indicates enrollment. The reply also contains the [URL of the Access Control Server](#) and the [PAREq](#).
- If the card is not enrolled, proceed directly to card authorization.

A. Requesting the Check Enrollment Service



Important

Before requesting **payerAuthEnrollService**, check the first digit of the card number to verify the card type. The first digit for Visa is 4; the first digit for Mastercard is 5; Maestro can start with 5 or 6; Diners Club can start with 3 or 5; and the first digit for American Express and JCB is 3. Specifying the card type is required for all Payer Authentication services.

Use the Check Enrollment service to verify that the card is enrolled in a card authentication program. For a list of the fields used when requesting the service, see ["Request Fields," page 79](#). You can use the enrollment check and card authorization services in the same request or in separate requests:

- *Same request:* CyberSource attempts to authorize the card if your customer is not enrolled in a payer authentication program (reason code 100 is returned). In this case, the field values that are required to prove you attempted to check enrollment are passed automatically to the authorization service.
- *Separate requests:* You must manually include the enrollment check result values (Enrollment Check Reply Fields) in the authorization service request (Card Authorization Request Fields). The following table lists these fields:

Identifiers	Enrollment Check Reply Fields	Card Authorization Request Fields
E-commerce indicator	payerAuthEnrollReply_commerceIndicator	ccAuthService_commerceIndicator
Collection indicator (Mastercard only)	payerAuthEnrollReply_ucafCollectionIndicator	ucaf_collectionIndicator
Result of the enrollment check for Asia, Middle East, and Africa Gateway	payerAuthEnrollReply_veresEnrolled	ccAuthService_veresEnrolled

B. Interpreting the Reply

The replies are similar for all card types. See [Appendix C, "Request and Reply Examples,"](#) on page 96 for examples of enrollment replies.

Enrolled Cards

You receive reason code 475 if the customer's card is enrolled in a payer authentication program:

```
decision=REJECT  
  
reasonCode=475  
  
payerAuthEnrollReply_reasonCode=475
```

If you receive this reply, you can proceed to validate authentication.

Cards Not Enrolled

You receive reason code 100 in the following cases:

- If the account number is not enrolled in a payer authentication program. The other services in your request are processed normally.
- If payer authentication is not supported by the card type, such as Discover.

```
decision=Accept  
  
reasonCode=100  
  
payerAuthEnrollReply_reasonCode=100
```

If you receive this reply, you can proceed to card authorization.

Step 2: Authenticating Enrolled Cards

When you have verified that a customer's card is enrolled in a card authentication program, you must redirect the customer to the URL of the card-issuing bank's [Access Control Server](#) (ACS URL) by using an [HTTP POST request](#) web form that contains the [PAReq](#) data, the [Termination URL](#) (TermURL), and [merchant data](#) (MD).

A. Creating the HTTP POST Form

Example POST Form

```

if card is enrolled == TRUE Then
    variable acsURL = <acsURL reply field>
    variable paReq = <paReq reply field>

    <body onload="document.PAEnrollForm.submit ();">
    <form id="PAEnrollForm" name="PAEnrollForm" action="acsURL value"
    method="post" target="paInlineFrame">
        <input type="hidden" name="PaReq" value="paReq value"
        <input type="hidden" name="TermUrl" value="http://
        myPAValidationPage.ext" /
        <input type="hidden" name="MD" value="<xid value>" />
    </form>
else

/* If the card is not enrolled, do not submit the form. Instead, skip the
authentication and validation processes. Proceed directly to card
authorization. */

```

The page typically includes JavaScript that automatically posts the form. This code provides the following:

- A page that receives the reply fields for the enrollment check service.
- A form that contains the required data for the card-issuing bank.

B. Creating the HTML Frame for Authentication

When your customers are redirected to the [ACS URL](#), their browsers display the frame that contains the card-issuing bank's password authentication dialog box or the option to sign up for the program (activation form).

On the page that contains the in-line frame for the ACS URL, add the following:

- HTML frame large enough to accommodate the card-issuer's authentication form or the activation form, and text that describes the process to customers.

- Outside the HTML frame, you must provide a brief message that guides customers through the process. For example, *“Please wait while we process your request. Do not click the Back button or refresh the page. Otherwise, this transaction may be interrupted.”*

Payment card companies provide guidance on their web sites about using their logos and accommodating their authentication/activation forms. For information about downloading this information, see [Appendix D, “3D Secure Services Logos,” on page 104](#). When testing your integration, verify that the frames you use are large enough.

C. Receiving the PAREs Message from the Card-Issuing Bank

The card-issuing bank sends a [PAREs](#) message to your [TermURL](#) in response to the [PAREq](#) data that you sent with the web form. The PAREs message is sent by using an HTTP POST request and contains the result of the authentication you requested:

```
variable paRes = <signedPAREs reply field>
```

The signed PAREs field contains a [base64](#)-encoded string that contains the following information:

- PaRes

Digitally signed payer authentication response message that contains the authentication result.



The field name has a lowercase “a” (PaRes), but the message name has an uppercase “A” (PAREs).

- MD

Merchant data, which is included only if you provided it in the outgoing page when you sent the enrollment authentication request (PAREq).



For card types that accept attempts processing in addition to card enrollment in a 3D Secure program, you might receive a response message that is identical to a successful authentication message except that the status in the authentication result field indicates a successful *attempt* instead of a successful *authentication*.

Step 3: Validating Authentication

For enrolled cards, the next step is to request the validation service to verify the authentication message (PAREs) returned by the card-issuing bank.

A. Requesting the Validation Service

When you make the validation request, you must:

- Extract the PAREs message from the form received from the card-issuing bank.
- Remove all white spaces created by tabs, spaces, or line breaks from the PaRes field. Do not modify any other part of the PaRes field.

**Note**

You must remove all white space characters or the validation service request will fail.

- Send the PaRes to CyberSource in the signed PaRes field of the validation service. The reply that you receive contains the validation result.

You can use the validation and card authorization services in the same request or in separate requests:

- *Same request:* CyberSource automatically attempts to authorize your customer's card if validation succeeds. The values of the required fields are added automatically to the authorization service. If you use this method, do not pass into your request any fields that CyberSource derives from the PAREs because that data could be overwritten.

**Note**

If the **businessRules_ignoreValidateResult** request field is set to *yes* and you request the validation and card authorization services together, the authorization service attempts to authorize the customer's card even if validation fails. Therefore, CyberSource recommends that you use this request field only when using other services and fraud tools.

- *Separate requests:* You must manually include the validation result values (Payer Authentication Reply Fields) in the authorization service request (Card Authorization Request Fields), which are listed in the following table:

Identifiers	Payer Authentication Reply Fields	Card Authorization Request Fields
Result of the validation check (For the Asia, Middle East, and African Gateway and ATOS only)	payerAuthValidateReply_paresStatus	ccAuthService_paresStatus
XID	payerAuthValidateReply_xid	ccAuthService_xid
E-commerce indicator	payerAuthValidateReply_commerceIndicator	ccAuthService_commerceIndicator
ECI raw	PayerAuthValidateReply_eciRaw	ccAuthService_eciRaw
CAVV (Visa and American Express only)	PayerAuthValidateReply_cavv	ccAuthService_cavv
CAVV algorithm (ATOS only)	payerAuthValidateReply_cavvAlgorithm	ccAuthService_cavvAlgorithm
AAV (Mastercard only. Known as UCAF)	payerAuthValidateReply_ucafAuthenticationData	ucaf_authenticationData
Collection indicator (Mastercard only)	payerAuthValidateReply_ucafCollectionIndicator	ucaf_collectionIndicator

**Important**

To increase the likelihood that you will receive liability shift protection, you must ensure that you pass all the pertinent data for the card type and processor into your request. Failure to do so may invalidate your liability shift for that transaction. Include the electronic commerce indicator (ECI), the transaction ID (XID), and the following card-specific information in your authorization request:

- For Visa, American Express, JCB, and Diners Club, include the CAVV (cardholder authentication verification value).
- For Mastercard, include the UCAF (universal cardholder authentication field) and the collection indicator.

B. Interpreting the Reply



Important

If the authentication fails, Visa, American Express, JCB, and Diners Club require that you do not accept the card. Instead, you must ask the customer to use another payment method.

Proceed with the order according to the validation response that you receive. The replies are similar for all card types:

- *Success:*

You receive the reason code 100, and other service requests, including authorization, are processed normally.

- *Failure:*

You receive reason code 476 indicating that the authentication failed, so the other services in your request are not processed. If you want to process the other services or fraud tools despite the failure, set the request field **businessRules_ignoreValidateResult** to `true`.

- *Error:*

If you receive an error from the payment card company, process the order according to your business rules. If the error occurs frequently, report it to [Customer Support](#). If you receive a CyberSource system error, determine the cause, and proceed with card authorization only if appropriate.

To verify that the enrollment and validation checks are for the same transaction, ensure that the XID in the enrollment check and validation replies are identical.

C. Redirecting Customers to Pass or Fail Message Page

After authentication is completed, redirect the customer to a page containing a success or failure message. You must ensure that all messages that display to customers are accurate, complete, and that they address all possible scenarios for enrolled and nonenrolled cards. For example, if the authentication fails, a message such as the following should be displayed to the customer:

Authentication Failed

Your card issuer cannot authenticate this card. Please select another card or form of payment to complete your purchase.

Testing Payer Authentication Services

After you have completed the necessary changes to your Web and API integration, verify that all components are working correctly by performing all the tests for the cards that you support. Each test contains the specific input data and the most important results fields that you receive in the API reply.

Testing Process

Use the card number specified in the test with the card's expiration date set as follows: the month of December and the current year plus two. For example, for 2015, use 2017. You also need the minimum required fields for an order.

Enrollment Check

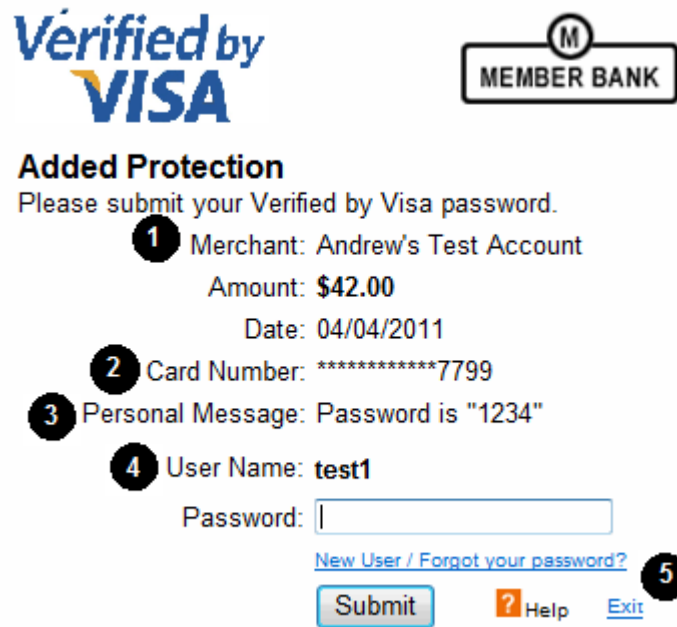
For some of the enrolled cards, an authentication window appears after the enrollment check completes. [Figure 4](#) shows an authentication window for Verified by Visa. The window for Mastercard is similar.

**Note**

To see the authentication window, you must enable your browser to display popup windows.

The test password is always 1234.

Figure 4 Verified by Visa Authentication Window



The image shows a 'Verified by Visa' authentication window. At the top left is the 'Verified by VISA' logo. At the top right is a 'MEMBER BANK' logo with an 'M' in a circle. Below the logos, the text 'Added Protection' is followed by 'Please submit your Verified by Visa password.' The form contains several fields and links, each marked with a numbered circle:

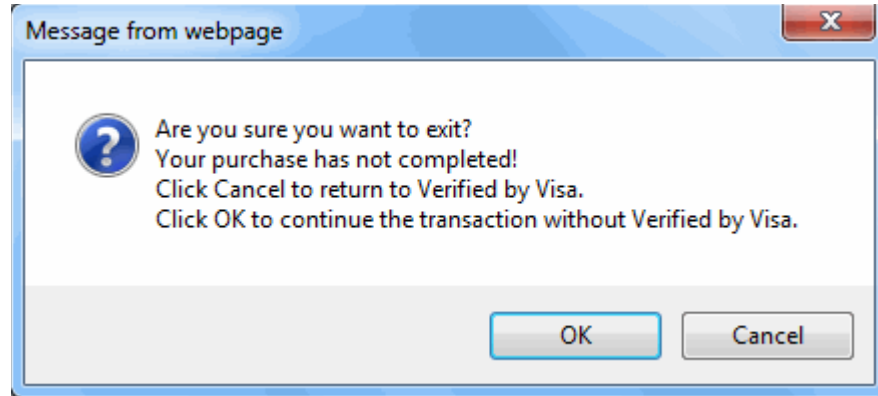
- 1** Merchant: Andrew's Test Account
Amount: \$42.00
Date: 04/04/2011
- 2** Card Number: *****7799
- 3** Personal Message: Password is "1234"
- 4** User Name: test1
Password:
- [New User / Forgot your password?](#)
-
- [? Help](#)
- [Exit](#) **5**

- 1 Your merchant ID.
- 2 Last four digits of the card number.
- 3 Password to enter in the text box below.
- 4 Default username for all tests.
- 5 This Exit link enables the customer to prevent the authentication process.

Depending on the user's action, two results are possible:

- If the user submits the password for the enrolled card, you receive the URL of the [Access Control Server](#) (ACS) where the customer can be authenticated.
- If the user clicks the Exit link and clicks OK in the verification window ([Figure 5](#)), authentication does not occur.

Figure 5 Verified by Visa Verification Window



[Table 6](#) lists the reply fields used in the test cases.

Table 6 Reply Fields Used in the Enrollment Check Test Cases

Names Used in Test Cases	API Field
ACS URL	payerAuthEnrollReply_acsURL
E-commerce indicator	payerAuthEnrollReply_commerceIndicator
ECI	payerAuthEnrollReply_eci
PAReq	payerAuthEnrollReply_paReq
proofXML	payerAuthEnrollReply_proofXML
Reason code	payerAuthEnrollReply_reasonCode
VERes enrolled	payerAuthEnrollReply_veresEnrolled
XID	payerAuthEnrollReply_xid

Authentication Validation

Table 7 lists only the reply fields used in the test cases.

Table 7 Reply Fields Used in the Authentication Validation Test Cases

Names Used in Test Cases	API Field
Authentication result	payerAuthValidateReply_authenticationResult
E-commerce indicator	payerAuthValidateReply_commerceIndicator
AAV (Mastercard only)	payerAuthValidateReply_ucafAuthenticationData
CAVV (Visa only)	payerAuthValidateReply_cavv
Collection indicator	payerAuthValidateReply_ucafCollectionIndicator
ECI	payerAuthValidateReply_eci
PARes status	payerAuthValidateReply_authenticationStatusMessage
Reason code	payerAuthValidateReply_reasonCode
XID	payerAuthValidateReply_xid

Expected Results

These flowcharts provide an overview of the payer authentication process based on the enrollment status of the card and the subsequent customer experience with the authentication path.

Use this information with the test cases to determine how to process orders.

Figure 6 Authentication Path for Visa, American Express, JCB, and Diners Club

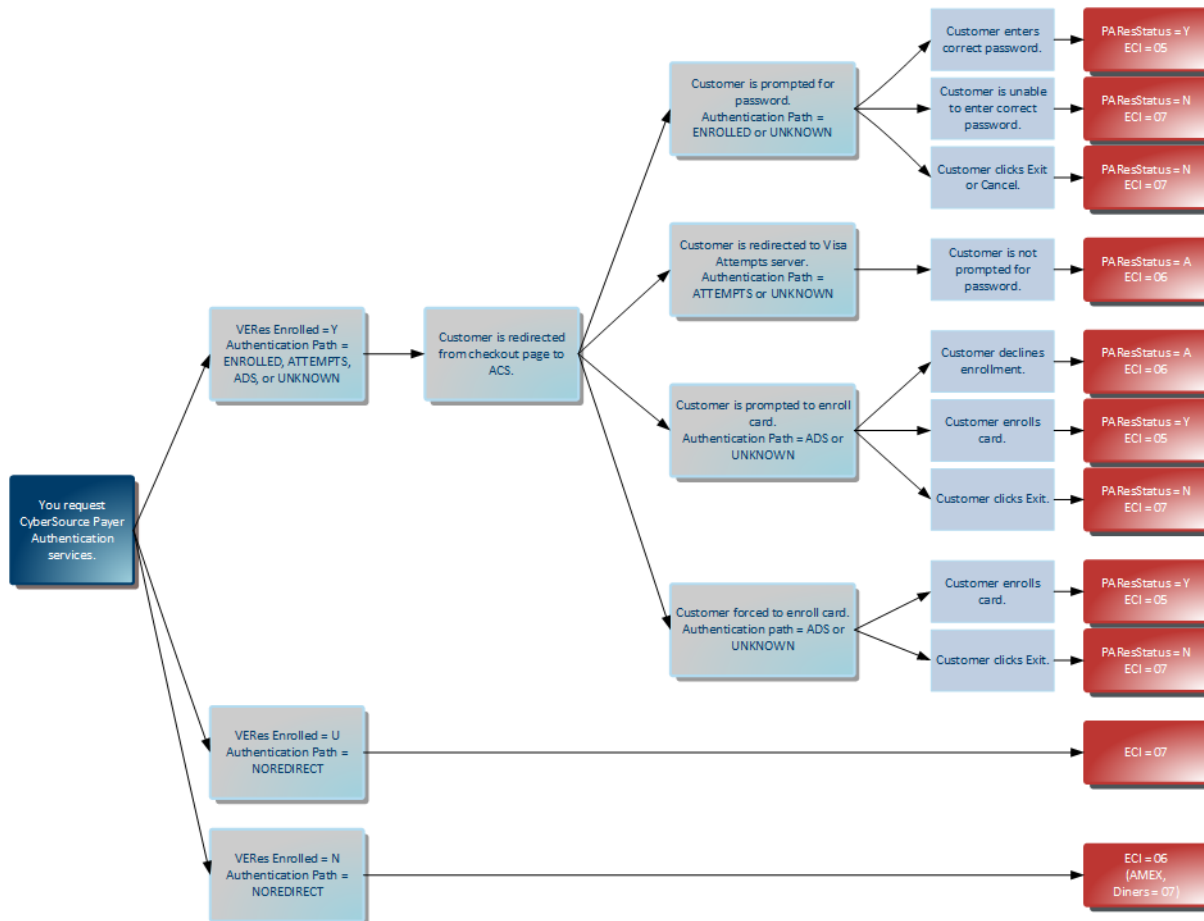
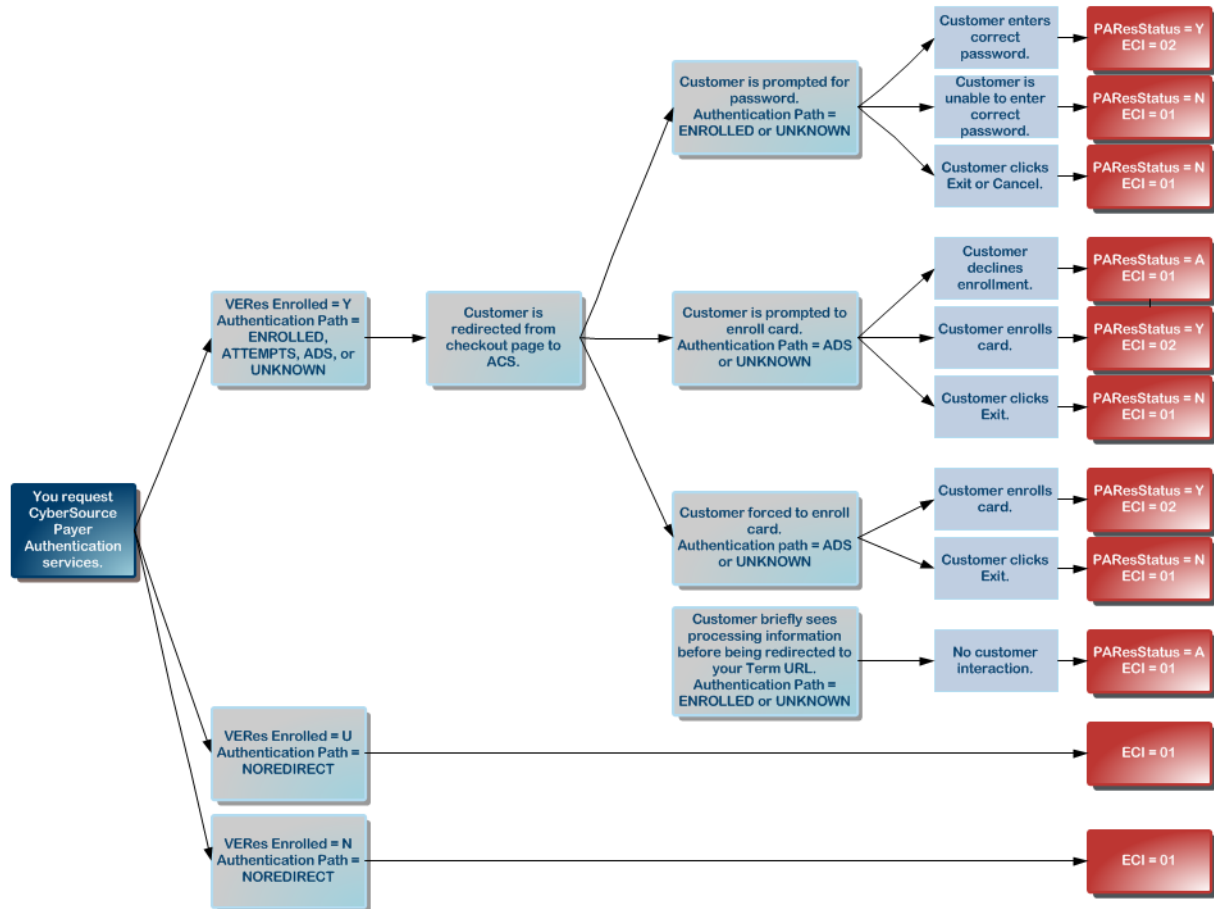


Figure 7 Authentication Path for Mastercard and Maestro



Test Cases

Verified by Visa

You can use Payer Authentication services with 16- and 19-digit Visa cards if these are supported by your processor.

Table 8 Possible Values for Verified by Visa Reply Fields

Result and Interpretation		Validate Authentication Reply			
		Authentication Result	ECI	Commerce Indicator	Reason Code
Success	Successful authentication.	0	05	vbv	100
	Recorded attempt to authenticate.	1	06	vbv_ attempted	100
Failure (Customer not responsible)	System error that prevents the completion of authentication: you can proceed with authorization, but there is no liability shift.	6	^a	— ^b	100
	Issuer unable to perform authentication.	6	07	internet	100
	No response from the Directory Servers or Issuer because of a problem.		07	internet vbv_failure (processors: AIBMS, Barclays, Streamline, or FDC Germany)	
	Invalid PAREs.	-1	—	—	476
Failure (Customer responsible)	Authentication failed or cardholder did not complete authentication. If the authentication fails, Visa requires that you do not accept the card. You must ask the customer to use another payment method.	9	—	—	476

^a The ECI value can vary depending on the reason for the failure.

^b A dash (—) indicates that the field is blank or absent.


Test Case 1: Verified by Visa Card Enrolled: Successful Authentication

Card Number	4000000000000002 With authentication window	
	4000000000000000022	
	40000000000000119 Without authentication window	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
	Reason code 475	Reason code 100
Summary	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	
	ics_pa_validate service was successful.	
	ACS URL URL	Authentication result 0
	PAReq PAReq value	CAVV CAVV value
	proofXML proofXML value	E-commerce indicator vbv
	VERes enrolled Y	ECI 05
	XID XID value	PARes status Y
		XID XID value
Action	1 Add the signed PARes to the Validate Authentication request. 2 Ensure that the XID from the enrollment check matches that from the authentication validation. 3 Add the CAVV and ECI values to your authorization request.	

Test Case 2: Verified by Visa Card Enrolled: Successful Authentication but Invalid PARes

Card Number	4000000000000010 With authentication window	
	4000000000000000071	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
	Reason code 475	Reason code 476
Summary	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	
	We encountered a Payer Authentication problem: PARes signature digest value mismatch. PARes message has been modified.	
	ACS URL URL value	Authentication result -1
	PAReq PAReq value	XID XID value
	proofXML proofXML value	
	VERes enrolled Y	
	XID XID value	
Action	Do not proceed with authorization. Instead, ask the customer for another form of payment.	

Test Case 3: Verified by Visa Card Enrolled: Attempts Processing

Card Number	4000000000000101	Without authentication window
	400000000000000063	With authentication window
	40000000000000127	Card enrollment option during purchase process
Auth. Type	Activation during shopping	
Results	Check Enrollment	Validate Authentication
	Summary	
	Reason code 475	Reason code 100
	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	ics_pa_validate service was successful.
	Details	
	ACS URL URL value	Authentication result 1
	PAReq PAReq value	CAVV CAVV value
	proofXML proofXML value	E-commerce indicator vbv_attempted
	VERes enrolled Y	ECI 06
	XID XID value	PARes status A
		XID XID value
Action	<p>If you request Validate Authentication and authorization services separately, follow these steps:</p> <ol style="list-style-type: none"> 1 Add the signed PARes to the Validate Authentication request. 2 Ensure that the XID from the enrollment check matches that from the authentication validation. 3 Add the CAVV and ECI values to your authorization request. <p>If you request the Validate Authentication and authorization services together, the process described above occurs automatically. Test card 4000000000000127 enables you to reproduce the process by which the customer enrolls the card during the purchase. If the card is not enrolled, a card enrollment option windows appears in the customer's browser after the enrollment check. The customer can activate the card at that time or later. In both cases, the card is authenticated, and validation is successful.</p> 	

Test Case 4: Verified by Visa Card Enrolled: Incomplete Authentication

Card Number	40000000000000036 400000000000000055	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 100
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	<ul style="list-style-type: none"> ■ Issuer unable to perform authentication. ■ ics_pa_validate service was successful.
	ACS URL URL value	Authentication result 6
	PAReq PAReq value	E-commerce indicator internet
	proofXML proofXML value	ECI 07
	VERes enrolled Y	PARes status U
	XID XID value	XID XID value
Action	Ask the customer for another form of payment, or submit the transaction. No liability shift.	

Test Case 5: Verified by Visa Card Enrolled: Unsuccessful Authentication

Card Number	40000000000000028 With authentication window 400000000000000048	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	<ul style="list-style-type: none"> ■ User failed authentication. ■ Payer cannot be authenticated.
	ACS URL URL value	Authentication result 9
	PAReq PAReq value	PARes status N
	proofXML proofXML value	XID XID value
	VERes enrolled Y	
	XID XID value	
Action	You are not permitted to submit this transaction for authorization. Instead ask the customer for another form of payment.	

Test Case 6: Verified by Visa Card Enrolled: Unsuccessful Authentication (Customer Exited)

Card Number	4000008531947799		
Auth. Type	Active authentication		
Results	Check Enrollment	Validate Authentication	
Summary	Reason code	475	Reason code 476
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.		<ul style="list-style-type: none"> Customer prevents authentication. ics_pa_validate service was successful.
	ACS URL	URL value	Authentication result 9
	PAReq	PAReq value	PARes status N
	proofXML	proofXML value	XID XID value
	VERes enrolled	Y	
	XID	XID value	
Action	You are not permitted to submit this transaction for authorization. Instead ask the customer for another form of payment.		

Test Case 7: Verified by Visa Card Enrolled: Unavailable Authentication

Card Number	40000000000000069 4000000000000000014		
Auth. Type	Active authentication		
Results	Check Enrollment	Validate Authentication	
Summary	Reason code	100	
Details	ics_pa_enroll service was successful.		
	E-commerce indicator	internet	
	proofXML	proofXML value	
	VERes enrolled	U	
Action	Submit your authorization request. No liability shift.		

Test Case 8: Verified by Visa Card Enrolled: Authentication Error

Card Number	4000000000000093 40000000000000006	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	We encountered a Payer Authentication problem: Error Processing PAREs.
Details	ACS URL URL value	E-commerce indicator internet
	PAReq PAReq value	ECI 07
	proofXML proofXML value	
	VERes enrolled Y	
	XID XID value	
Action	Ask the customer for another form of payment. No liability shift.	

Test Case 9: Verified by Visa Card Not Enrolled

Card Number	4000000000000051 40000000000000030	
Auth. Type	Non-participating bank	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
	ics_pa_enroll service was successful.	
Details	E-commerce indicator vbv_attempted	
	ECI 06	
	proofXML proofXML value	
	VERes enrolled N	
Action	Submit your authorization request. Liability shift.	

Test Case 10: Verified by Visa Enrollment Check: Time-Out

Card Number	4000000000000044	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code	100
	ics_pa_enroll service was successful.	
Details	E-commerce indicator	internet
	proofXML	proofXML value
Action	After 10–12 seconds, proceed with the authorization request. No liability shift.	

Test Case 11: Verified by Visa Enrollment Check Error

Card Number	4000000000000085	Error response
	4000000000000077	Incorrect Configuration: Unable to Authenticate
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code	100
	ics_pa_enroll service was successful.	
Details	E-commerce indicator	internet
	proofXML	proofXML value
	VERes enrolled	U
Action	Proceed with the authorization request, and contact your support representative to resolve the issue. No liability shift. If you requested payer authentication and authorization together, the authorization is processed automatically.	

Test Case 12: Verified by Visa Enrollment RIBA_PASS

Card Number	4000180000000002	
Auth. Type	Passive authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 100
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	ics_pa_validate service was successful.
	ACS URL URL	Authentication result 0
	PAReq PAReq value	CAVV CAVV value
	proofXML proofXML value	E-commerce indicator vbv
	VERes enrolled Y	ECI 05
	XID XID value	PARes status Y
		XID XID value
Action	1 Add the signed PARes to the Validate Authentication request. 2 Ensure that the XID from the enrollment check matches that from the authentication validation. 3 Add the CAVV and ECI values to your authorization request.	

Test Case 13: Verified by Visa Enrollment RIBA_PASS: Unsuccessful Authentication

Card Number	4000180000000028	
Auth. Type	Passive authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	<ul style="list-style-type: none"> ■ User failed authentication. ■ Payer cannot be authenticated.
	ACS URL URL value	Authentication result 9
	PAReq PAReq value	PARes status N
	proofXML proofXML value	XID XID value
	VERes enrolled Y	
	XID XID value	
Action	You are not permitted to submit this transaction for authorization. Instead ask the customer for another form of payment.	

Test Case 14: Verified by Visa Enrollment RIBA

Card Number	4000260000000002 With authentication window	
Auth. Type	Risk-based bank	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 100
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	ics_pa_validate service was successful.
	ACS URL URL	Authentication result 0
	PAReq PAReq value	CAVV CAVV value
	proofXML proofXML value	E-commerce indicator vbv
	VERes enrolled Y	ECI 05
	XID XID value	PARes status Y
		XID XID value
Action	1 Add the signed PARes to the Validate Authentication request. 2 Ensure that the XID from the enrollment check matches that from the authentication validation. 3 Add the CAVV and ECI values to your authorization request.	

Test Case 15: Verified by Visa Enrollment RIBA: Unsuccessful Authentication

Card Number	40002600000000028 With authentication window	
Auth. Type	Risk-based bank	
Results	Reason code 475	Reason code 476
Summary	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	<ul style="list-style-type: none"> ■ User failed authentication. ■ Payer cannot be authenticated.
Details	ACS URL URL value	Authentication result 9
	PAReq PAReq value	PARes status N
	proofXML proofXML value	XID XID value
	VERes enrolled Y	
	XID XID value	
Action	You are not permitted to submit this transaction for authorization. Instead ask the customer for another form of payment.	

Mastercard SecureCode

Table 9 Possible Values for Mastercard and Maestro SecureCode Reply Fields

Result and Interpretation		payerAuthValidateReply_			
		authentication Result	ucafCollection Indicator	commerce Indicator	reason Code
Success	Successful authentication.	0	2	spa	100
	Authentication not completed.	1	1	spa	100
Failure (Customer not responsible)	System error (Issuer unable to perform authentication): you cannot authorize this card; no liability shift.	6	1	spa	100
	Invalid PAREs.	-1	0		476
Failure (Customer responsible)	Authentication failed or cardholder did not complete authentication.	9	1	–	476

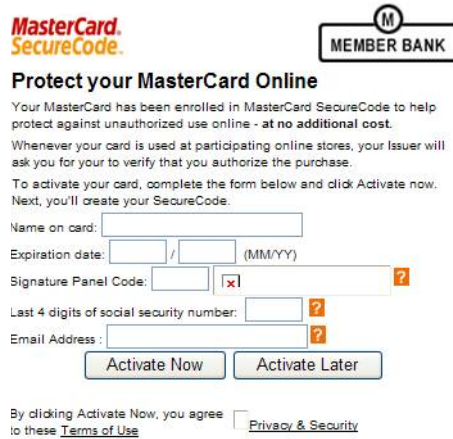
Test Case 16: Mastercard SecureCode Card Enrolled: Successful Authentication

Card Number	5200000000000007	With authentication window
	52000000000000114	Without authentication window
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
	Reason code 475	Reason code 100
Summary	The card is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	
	ics_pa_validate service was successful.	
	ACS URL URL	Authentication result 0
	PAReq PAReq value	AAV AAV value
	proofXML proofXML value	Collection indicator 2
	VERes enrolled Y	E-commerce indicator spa
	XID XID value	PARes status Y
		XID XID value
Action	1 Add the signed PAREs to the Validate Authentication request. 2 Ensure that the XID from the enrollment check matches that from the authentication validation. 3 Add the required payer authentication values to your authorization request.	

Test Case 17: Mastercard SecureCode Card Enrolled: Successful Authentication but Invalid PAREs

Card Number	5200000000000015 With authentication window	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	Payer Authentication problem: PAREs signature digest value mismatch. PAREs message has been modified.
	ACS URL URL	Authentication result -1
	PARReq PARReq value	XID XID value
	proofXML proofXML value	
	VERes enrolled Y	
	XID XID value	
Action	Do not process the authorization request. Instead ask the customer for another form of payment.	

Test Case 18: Mastercard SecureCode Card Enrolled: Attempts Processing

Card Number	5200000000000122 Card enrollment option during purchase process 5200000000000106	
Auth. Type	Activation during shopping	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 100
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	
	ACS URL URL	Authentication result 1
	PAReq PAReq value	AAV AAV value
	proofXML proofXML value	Collection indicator 1
	VERes enrolled Y	E-commerce indicator spa
	XID XID value	PARes status A
		XID XID value
Action	<p>This test card enables you to reproduce the process by which the customer enrolls the card during the purchase. If the card is not enrolled, a card enrollment option windows appears in the customer's browser after the enrollment check. The customer can activate the card at that time or later. In both cases, the card is authenticated, and validation is successful.</p> <ol style="list-style-type: none"> 1 Add the signed PARes to the validation request. 2 In the reply, ensure that the XID from the enrollment check matches that from the validation. 3 Add the required payer authentication values to your authorization request. 	

Test Case 19: Mastercard SecureCode Card Enrolled: Incomplete Authentication

Card Number	5200000000000031 Without authentication window	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 100
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	<ul style="list-style-type: none"> ■ ics_pa_validate service was successful. ■ Issuer unable to perform authentication.
	ACS URL URL value	Authentication result 6
	PAReq PAReq value	Collection indicator 1
	proofXML proofXML value	E-commerce indicator spa
	VERes enrolled Y	PARes status U
	XID XID value	XID XID value
Action	Ask the customer for another form of payment, or submit the transaction. Liability shift.	

Test Case 20: Mastercard SecureCode Card Enrolled: Unsuccessful Authentication

Card Number	5200000000000023 With authentication window	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	<ul style="list-style-type: none"> ■ User failed authentication ■ Payer could not be authenticated.
	ACS URL URL value	Authentication result 9
	PAReq PAReq value	PARes status N
	proofXML proofXML value	
	VERes enrolled Y	XID XID value
	XID XID value	
Action	You are not permitted to submit this transaction for authorization. Instead ask the customer for another form of payment.	

Test Case 21: Mastercard SecureCode Card Enrolled: Unsuccessful Authentication (Customer Exited)

Card Number	5641821000010028	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	<ul style="list-style-type: none"> Customer prevents authentication. ics_pa_validate service was successful.
	ACS URL URL value	Authentication result 9
	PAReq PAReq value	PARes status N
	proofXML proofXML value	XID XID value
	VERes enrolled Y	
	XID XID value	
Action	You are not permitted to submit this transaction for authorization. Instead ask the customer for another form of payment.	

Test Case 22: Mastercard SecureCode Card Enrolled: Unavailable Authentication

Card Number	5200000000000064	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
Details	ics_pa_enroll service was successful.	
	Collection indicator 1	
	E-commerce indicator spa	
	proofXML proofXML value	
	VERes enrolled U	
Action	Submit the transaction. No liability shift.	

Test Case 23: Mastercard SecureCode Card Enrolled: Authentication Error

Card Number	5200000000000098 Without authentication window	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	We encountered a Payer Authentication problem: Error Processing PAREs.
Details	ACS URL URL value	Collection indicator 1
	PARReq PARReq value	E-commerce indicator internet
	proofXML proofXML value	
	VERes enrolled Y	
	XID XID value	
Action	Ask the customer for another form of payment. No liability shift.	

Test Case 24: Mastercard SecureCode Card Not Enrolled

Card Number	5200000000000056	
Auth. Type	Non-participating bank	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
	ics_pa_enroll service was successful.	
Details	Collection indicator 0	
	E-commerce indicator spa	
	proofXML proofXML value	
	VERes enrolled N	
Action	Submit the transaction.	

Test Case 25: Mastercard SecureCode Enrollment Check Time-Out

Card Number	5200000000000049	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
	ics_pa_enroll service was successful.	
Details	Collection indicator 1	
	E-commerce indicator spa	
	proofXML proofXML value	
Action	After 10–12 seconds, proceed with the authorization message. No liability shift.	

Test Case 26: Mastercard SecureCode Enrollment Check Error

Card Number	5200000000000080	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
	ics_pa_enroll service was successful.	
Details	Collection indicator 0	
	E-commerce indicator internet	
	proofXML proofXML value	
	VERes enrolled U	
Action	Proceed with the authorization request, and contact your support representative to resolve the issue. No liability shift. If you requested payer authentication and authorization together, the authorization is processed automatically.	

Test Case 27: Mastercard SecureCode RIBA_PASS

Card Number	5200180000000007	
Auth. Type	Passive authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 100
	The card is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	ics_pa_validate service was successful.
Details	ACS URL URL	Authentication result 0
	PAReq PAReq value	AAV AAV value
	proofXML proofXML value	Collection indicator 2
	VERes enrolled Y	E-commerce indicator spa
	XID XID value	PARes status Y
		XID XID value
Action	1 Add the signed PARes to the Validate Authentication request. 2 Ensure that the XID from the enrollment check matches that from the authentication validation. 3 Add the required payer authentication values to your authorization request.	

Test Case 28: Mastercard SecureCode RIBA_PASS: Unsuccessful Authentication

Card Number	5200180000000023	
Auth. Type	Passive authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	■ User failed authentication ■ Payer could not be authenticated.
Details	ACS URL URL value	Authentication result 9
	PAReq PAReq value	PARes status N
	proofXML proofXML value	
	VERes enrolled Y	XID XID value
	XID XID value	
Action	You are not permitted to submit this transaction for authorization. Instead ask the customer for another form of payment.	

Test Case 29: Mastercard SecureCode RIBA

Card Number	5200260000000007 With authentication window	
Auth. Type	Risk-based bank	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 100
	The card is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	ics_pa_validate service was successful.
Details	ACS URL URL	Authentication result 0
	PAReq PAReq value	AAV AAV value
	proofXML proofXML value	Collection indicator 2
	VERes enrolled Y	E-commerce indicator spa
	XID XID value	PARes status Y
		XID XID value
Action	1 Add the signed PARes to the Validate Authentication request. 2 Ensure that the XID from the enrollment check matches that from the authentication validation. 3 Add the required payer authentication values to your authorization request.	

Test Case 30: Mastercard SecureCode RIBA: Unsuccessful Authentication

Card Number	52002600000000023 With authentication window	
Auth. Type	Risk-based bank	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	■ User failed authentication ■ Payer could not be authenticated.
Details	ACS URL URL value	Authentication result 9
	PAReq PAReq value	PARes status N
	proofXML proofXML value	
	VERes enrolled Y	XID XID value
	XID XID value	
Action	You are not permitted to submit this transaction for authorization. Instead ask the customer for another form of payment.	

Maestro SecureCode


Test Case 31: Maestro SecureCode Card Enrolled: Successful Authentication

Card Number	6759411100000008	Without authentication window
	6759410000006404	With authentication window
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
	Reason code 475	Reason code 100
Summary	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	
	ics_pa_validate service was successful.	
	ACS URL URL	Authentication result 0
	PAReq PAReq value	AAV AAV value
	proofXML proofXML value	Collection indicator 2
	VERes enrolled Y	E-commerce indicator spa
	XID XID value	PARes status Y
		XID XID value
Action	<ol style="list-style-type: none"> 1 Add the signed PARes to the validation request. 2 In the reply, ensure that the XID from the enrollment check matches that from the validation. 3 Add the required payer authentication values to your authorization request. 	

Test Case 32: Maestro SecureCode Card Enrolled: Successful Authentication but Invalid PARes

Card Number	6331101234567892	Without authentication window
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
	Reason code 475	Reason code 476
Summary	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	
	Payer Authentication problem: PARes signature digest value mismatch. PARes message has been modified.	
	ACS URL URL	Authentication result -1
	PAReq PAReq value	XID XID value
	proofXML proofXML value	
	VERes enrolled Y	
	XID XID value	
Action	Do not process the authorization request. Instead ask the customer for another form of payment.	

Test Case 33: Maestro SecureCode Card Enrolled: Attempts Processing

Card Number	560000000000000193 Card enrollment option during purchase process	
Auth. Type	Activation during shopping	
Results	Check Enrollment	Validate Authentication
	Summary Reason code 475	Reason code 100
	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	ics_pa_validate service was successful.
	Details ACS URL URL	Authentication result 1
	PAReq PAReq value	AAV AAV value
	proofXML proofXML value	E-commerce indicator spa
	VERes enrolled Y	PARes status A
	XID XID value	XID XID value
Action	<p>This test card enables you to reproduce the process by which the customer enrolls the card during the purchase. If the card is not enrolled, a card enrollment option windows appears in the customer's browser after the enrollment check. The customer can activate the card at that time or later. In both cases, the card is authenticated, and validation is successful.</p> <ol style="list-style-type: none"> 1 Add the signed PARes to the Validate Authentication request. 2 Ensure that the XID from the enrollment check matches that from the authentication validation. 3 Add the required payer authentication values to your authorization request. 	

Test Case 34: Maestro SecureCode Card Enrolled: Incomplete Authentication

Card Number	6331101250353227 Without authentication window	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 100
	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	Issuer unable to perform authentication.
Details	ACS URL URL value	Authentication result 6
	PAReq PAReq value	Collection indicator 1
	proofXML proofXML value	E-commerce indicator spa
	VERes enrolled Y	PARes status U
	XID XID value	XID XID value
Action	Ask the customer for another form of payment, or submit the transaction. No liability shift.	

Test Case 35: Maestro SecureCode Card Enrolled: Unsuccessful Authentication

Card Number	6331100610194313 Without authentication window	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	User failed authentication
Details	ACS URL URL value	Authentication result 9
	PAReq PAReq value	PARes status N
	proofXML proofXML value	XID XID value
	VERes enrolled Y	
	XID XID value	
Action	You are not permitted to submit this transaction for authorization. Instead ask the customer for another form of payment.	

Test Case 36: Maestro SecureCode Card Enrolled: Unavailable Authentication (Time-out)

Card Number	6331100266977839	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
	ics_pa_enroll service was successful.	
Details	Collection indicator 1	
	E-commerce indicator spa	
	proofXML proofXML value	
Action	Submit the transaction. No liability shift.	

Test Case 37: Maestro SecureCode Card Enrolled: Authentication Error

Card Number	560000511607577094 Without authentication window	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	We encountered a Payer Authentication problem: Error Processing PAREs.
Details	ACS URL URL value	Collection indicator 1
	PAReq PAReq value	E-commerce indicator internet
	proofXML proofXML value	
	VERes enrolled Y	
	XID XID value	
Action	Do not request authorization. Instead ask the customer for another form of payment. No liability shift.	

Test Case 38: Maestro SecureCode Card Not Enrolled

Card Number	560000227571480302	
Auth. Type	Non-participating bank	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
	ics_pa_enroll service was successful.	
Details	Collection indicator 0	
	E-commerce indicator spa	
	proofXML proofXML value	
	VERes enrolled N	
Action	Submit the transaction.	

Test Case 39: Maestro SecureCode Enrollment Check Error

Card Number	560000841211092515	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
	ics_pa_enroll service was successful.	
Details	Collection indicator 0	
	E-commerce indicator internet	
	proofXML proofXML value	
	VERes enrolled U	
Action	Proceed with the authorization request, and contact your support representative to resolve the issue. No liability shift. If you requested payer authentication and authorization together, the authorization is processed automatically.	

American Express SafeKey

Table 10 Possible Values for American Express SafeKey Reply Fields

Result and Interpretation		Validate Authentication Reply			
		Authentication Result	ECI	Commerce Indicator	Reason Code
Success	Successful authentication.	0	05	aesk	100
	Recorded attempt to authenticate.	1	06	aesk_ attempted	100
Failure (Customer not responsible)	System error that prevents the completion of authentication: you can proceed with authorization, but there is no liability shift.	6	a	— ^b	100
	Issuer unable to perform authentication.	6	07	internet	100
	Incomplete or unavailable authentication.		07	internet	
	Invalid PAREs.	-1	—	—	476
Failure (Customer responsible)	Authentication failed or cardholder did not complete authentication. If the authentication fails, Visa requires that you do not accept the card. You must ask the customer to use another payment method.	9	—	—	476

a The ECI value can vary depending on the reason for the failure.

b A dash (—) indicates that the field is blank or absent.

Test Case 40: American Express SafeKey Card Enrolled: Successful Authentication

Card Number	340000000003961	Without authentication window	
	371449111020228	With authentication window	
Auth. Type	Active authentication		
Results	Check Enrollment		Validate Authentication
	Reason code	475	Reason code 100
	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.		ics_pa_validate service was successful.
	ACS URL	URL value	Authentication result 0
	PAReq	PAReq value	CAVV CAVV value
	proofXML	proofXML value	E-commerce indicator aesk
	VERes enrolled	Y	ECI 05
	XID	XID value	PARes status Y
			XID XID value
Action	1 Add the signed PARes to the Validate Authentication request. 2 Ensure that the XID from the enrollment check matches that from the authentication validation. 3 Add the CAVV and ECI values to your authorization request.		

Test Case 41: American Express SafeKey Card Enrolled: Successful Authentication but Invalid PARes

Card Number	340000000006022		
Auth. Type	Active authentication		
Results	Check Enrollment		Validate Authentication
	Reason code 475		Reason code 476
Summary	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.		We encountered a Payer Authentication problem: PARes signature digest value mismatch. PARes message has been modified.
	ACS URL	URL value	Authentication result -1
	PAReq	PAReq value	XID XID value
	proofXML	proofXML value	
	VERes enrolled	Y	
	XID	XID value	
Action	Do not proceed with authorization. Instead, ask the customer for another form of payment.		

Test Case 42: American Express SafeKey Card Enrolled: Attempts Processing

Card Number	340000000003391	Without authentication window	
	344400000000569	Card enrollment option during purchase process	
Auth. Type	Activation during shopping		
Results	Check Enrollment		Validate Authentication
	Summary	Reason code 475	Reason code 100
		The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	
	Details	ACS URL URL value	Authentication result 1
		PAReq PAReq value	CAVV CAVV value
		proofXML proofXML value	E-commerce indicator aesk_attempted
		VERes enrolled Y	ECI 06
		XID XID value	PARes status A
			XID XID value
Action	If you request Validate Authentication and authorization services separately, follow these steps: 1 Add the signed PARes to the Validate Authentication request. 2 Ensure that the XID from the enrollment check matches that from the authentication validation. 3 Add the CAVV and ECI values to your authorization request. If you request the validation and authorization services together, the process described above occurs automatically.		

Test Case 43: American Express SafeKey Card Enrolled: Incomplete Authentication

Card Number	340000000002302	Without authentication window	
Auth. Type	Active authentication		
Results	Check Enrollment		Validate Authentication
	Reason code	475	Reason code 100
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.		ics_pa_validate service was successful.
	ACS URL	URL value	Authentication result 6
	PAReq	PAReq value	E-commerce indicator internet
	proofXML	proofXML value	ECI 07
	VERes enrolled	Y	PARes status U
	XID	XID value	XID XID value
	Ask the customer for another form of payment, or submit the transaction. No liability shift.		

Test Case 44: American Express SafeKey Card Enrolled: Unsuccessful Authentication

Card Number	340000000000033 Without authentication window	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	<ul style="list-style-type: none"> ■ User failed authentication. ■ Payer cannot be authenticated.
	ACS URL URL value	Authentication result 9
	PAReq PAReq value	PARes status N
	proofXML proofXML value	ECI 07
	VERes enrolled Y	XID XID value
	XID XID value	
Action	You are not permitted to submit this transaction for authorization. Instead ask the customer for another form of payment.	

Test Case 45: American Express SafeKey Card Enrolled: Unavailable Authentication

Card Number	3400000000007780	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
Details	ics_pa_enroll service was successful.	
	E-commerce indicator internet	
	proofXML proofXML value	
	VERes enrolled U	
Action	Submit your authorization request. No liability shift.	

Test Case 46: American Express SafeKey Card Enrolled: Authentication Error

Card Number	340000000009299	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	We encountered a Payer Authentication problem: Error Processing PAREs.
Details	ACS URL URL value	ECI 07
	PAReq PAReq value	E-commerce Indicator internet
	proofXML proofXML value	
	VERes enrolled Y	
	XID XID value	
Action	Ask the customer for another form of payment. No liability shift.	

Test Case 47: American Express SafeKey Card Not Enrolled

Card Number	340000000008135	
Auth. Type	Non-participating bank	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
	ics_pa_enroll service was successful.	
Details	E-commerce indicator internet	
	ECI 07	
	proofXML proofXML value	
	VERes enrolled N	
Action	Submit the transaction.	

Test Case 48: American Express SafeKey Enrollment Check: Time-Out

Card Number	340000000008309	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
	ics_pa_enroll service was successful.	
Details	E-commerce indicator internet	
	ECI 07	
	proofXML proofXML value	
Action	After 10–12 seconds, proceed with the authorization request. No liability shift.	

Test Case 49: American Express SafeKey Enrollment Check Error

Card Number	340000000007244	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
	ics_pa_enroll service was successful.	
Details	E-commerce indicator internet	
	proofXML proofXML value	
	VERes enrolled U	
Action	Proceed with the authorization request, and contact your support representative to resolve the issue. If you requested payer authentication and authorization together, the authorization is processed automatically. No liability shift.	

JCB J/Secure

Table 11 Possible Values for JCB J/Secure Reply Fields

Result and Interpretation		payerAuthValidateReply_			
		authentication Result	eci	commerceIndicator	reasonCode
Success	Successful authentication.	0	05	js	100
	Recorded attempt to authenticate	1	06	js_attempted	100
Failure (Customer not responsible)	System error that prevents the completion of authentication: you can proceed with authorization, but no liability shift.	6	a	__b	
	Issuer unable to perform authentication	6	07	internet	100
	Incomplete or unavailable authentication.		07	internet js_failure	
	Invalid PAREs.	-1	00		476
Failure (Customer responsible)	Authentication failed or cardholder did not complete authentication. If the authentication fails, Visa requires that you do not accept the card. You must ask the customer to use another payment method.	9	—	—	476

a The ECI value can vary depending on the reason for the failure.

b A dash (—) indicates that the field is blank or absent.

Test Case 50: JCB J/Secure Card Enrolled: Successful Authentication

Card Number	3569990010083722 Without authentication window	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 100
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	ics_pa_validate service was successful.
	ACS URL URL	Authentication result 0
	PAReq PAReq value	CAVV CAVV value
	proofXML proofXML value	E-commerce indicator js
	VERes enrolled Y	ECI 05
	XID XID value	PARes status Y
		XID XID value
Action	1 Add the signed PARes to the Validate Authentication request. 2 Ensure that the XID from the enrollment check matches that from the authentication validation. 3 Add the CAVV and ECI values to your authorization request.	

Test Case 51: JCB J/Secure Card Enrolled: Successful Authentication but Invalid PARes (Signature Failure)

Card Number	3569990010083748	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	We encountered a Payer Authentication problem: PARes signature digest value mismatch. PARes message has been modified.
	ACS URL URL value	Authentication result -1
	PAReq PAReq value	XID XID value
	VERes enrolled Y	
Action	Do not proceed with authorization. Instead ask the customer for another form of payment.	

Test Case 52: JCB J/Secure Card Enrolled: Attempted Authentication

Card Number	3569960010083758		
Auth. Type	Activation during shopping		
Results	Check Enrollment	Validate Authentication	
Summary	Reason code	475	Reason code 100
	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.		ics_pa_validate service was successful.
Details	ACS URL	URL value	Authentication result 1
	PAReq	PAReq value	CAVV CAVV value
	proofXML	proofXML value	E-commerce indicator js_attempted
	VERes enrolled	Y	ECI 06
	XID	XID value	PARes status A
			XID XID value
Action	<p>If you request Validate Authentication and authorization services separately, follow these steps:</p> <ol style="list-style-type: none"> 1 Add the signed PARes to the validation request. 2 In the reply, ensure that the XID from the enrollment check matches that from the validation. 3 Add the CAVV and ECI values to your authorization request. <p>If you request the Validate Authentication and authorization services together, the steps described above occurs automatically.</p>		

Test Case 53: JCB J/Secure Card Enrolled: Incomplete Authentication (Unavailable)

Card Number	3541599998103643	Without authentication window	
Auth. Type	Active authentication		
Results Summary	Check Enrollment		Validate Authentication
	Reason code	475	Reason code 100
	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.		<div><div>■ Issuer unable to perform authentication.</div><div>■ ics_pa_validate service was successful.</div></div>
Details	ACS URL	URL value	Authentication result 6
	PAReq	PAReq value	E-commerce indicator internet
	proofXML	proofXML value	ECI 07
	VERes enrolled	Y	PARes status U
	XID	XID value	XID XID value
Action	Ask the customer for another form of payment, or submit the transaction. No liability shift.		

Test Case 54: JCB J/Secure Card Enrolled: Failed Authentication

Card Number	3569990110083721 Without authentication window	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	<ul style="list-style-type: none"> ■ User failed authentication. ■ Payer cannot be authenticated.
	ACS URL URL value	Authentication result 9
	PAReq PAReq value	PARes status N
	proofXML proofXML value	XID XID value
	VERes enrolled Y	
	XID XID value	
Action	You are not permitted to submit this transaction for authorization. Instead ask the customer for another form of payment.	

Test Case 55: JCB J/Secure Card Enrolled: Unavailable Authentication

Card Number	3541599999103865	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
Details	ics_pa_enroll service was successful.	
	E-commerce indicator internet	
	proofXML proofXML value	
	VERes enrolled U	
Action	Submit your authorization request. No liability shift.	

Test Case 56: JCB J/Secure Card Enrolled: Authentication Error Processing PAREs

Card Number	3541599999103881	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	We encountered a Payer Authentication problem: Error Processing PAREs.
	ACS URL URL value	ECI 07
	PARReq PARReq value	E-commerce indicator internet
	proofXML proofXML value	
	VERes enrolled Y	
	XID XID value	
Action	Ask the customer for another form of payment. No liability shift.	

Test Case 57: JCB J/Secure Card Not Enrolled

Card Number	3569970010083724	
Auth. Type	Non-participating bank	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
Details	ics_pa_enroll service was successful.	
	E-commerce indicator js_attempted	
	ECI 06	
	proofXML proofXML value	
	VERes enrolled N	
Action	Submit your authorization request. Liability shift.	

Test Case 58: JCB J/Secure Enrollment Check: Time-Out

Card Number	3569980010083723	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
	ics_pa_enroll service was successful.	
Details	E-commerce indicator internet	
	proofXML proofXML value	
Action	After 10–12 seconds, proceed with the authorization request. No liability shift.	

Test Case 59: JCB J/Secure Enrollment Check: Lookup Error Processing Message Request

Card Number	3541599969103614	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
	ics_pa_enroll service was successful.	
Details	E-commerce indicator internet	
	proofXML proofXML value	
	VERes enrolled U	
Action	Proceed with the authorization request, and contact your support representative to resolve the issue. No liability shift. If you requested payer authentication and authorization together, the authorization is processed automatically.	

Diners Club ProtectBuy

Table 12 Possible Values for Diners Club ProtectBuy Reply Fields

Result and Interpretation		Validate Authentication Reply			
		Authentication Result	ECI	Commerce Indicator	Reason Code
Success	Successful authentication.	0	05	pb	100
	Recorded attempt to authenticate.	1	06	pb_attempted	100
Failure (Customer not responsible)	System error that prevents the completion of authentication: you can proceed with authorization, but there is no liability shift.	6	a	— ^b	100
	Issuer unable to perform authentication.	6	07	internet	100
	Incomplete or unavailable authentication.		07	internet	
	Invalid PAREs.	-1	—	—	476
Failure (Customer responsible)	Authentication failed or cardholder did not complete authentication. If the authentication fails, Visa requires that you do not accept the card. You must ask the customer to use another payment method.	9	—	—	476

a The ECI value can vary depending on the reason for the failure.

b A dash (—) indicates that the field is blank or absent.

Test Case 60: Diners Club ProtectBuy Card Enrolled: Successful Authentication

Card Number	3005000000006246	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 100
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	ics_pa_validate service was successful.
	ACS URL URL	Authentication result 0
	PAReq PAReq value	CAVV CAVV value
	proofXML proofXML value	E-commerce indicator pb
	VERes enrolled Y	ECI 05
	XID XID value	PARes status Y
		XID XID value
Action	1 Add the signed PARes to the Validate Authentication request. 2 Ensure that the XID from the enrollment check matches that from the authentication validation. 3 Add the CAVV and ECI values to your authorization request.	

Test Case 61: Diners Club ProtectBuy Card Enrolled: Successful Authentication but Invalid PARes

Card Number	3005000000004373	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	We encountered a Payer Authentication problem: PARes signature digest value mismatch. PARes message has been modified.
	ACS URL URL value	Authentication result -1
	PAReq PAReq value	XID XID value
	proofXML proofXML value	
	VERes enrolled Y	
	XID XID value	
Action	Do not proceed with authorization. Instead, ask the customer for another form of payment.	

Test Case 62: Diners Club ProtectBuy Card Enrolled: Attempts Processing

Card Number	3005000000005271 Card enrollment option during purchase process	
Auth. Type	Activation during shopping	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 100
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	ics_pa_validate service was successful.
	ACS URL URL value	Authentication result 1
	PAReq PAReq value	CAVV CAVV value
	proofXML proofXML value	E-commerce indicator pb_attempted
	VERes enrolled Y	ECI 06
	XID XID value	PARes status A
		XID XID value
Action	<p>If you request Validate Authentication and authorization services separately, follow these steps:</p> <ol style="list-style-type: none"> 1 Add the signed PARes to the validation request. 2 Ensure that the XID from the enrollment check matches that from the authentication validation. 3 Add the CAVV and ECI values to your authorization request. <p>If you request the Validate Authentication and authorization services together, the process described above occurs automatically.</p>	

Test Case 63: Diners Club ProtectBuy Card Enrolled: Incomplete Authentication

Card Number	3005000000007376	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 100
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	<ul style="list-style-type: none"> ■ Issuer unable to perform authentication. ■ ics_pa_validate service was successful.
	ACS URL URL value	Authentication result 6
	PAReq PAReq value	E-commerce indicator internet
	proofXML proofXML value	ECI 07
	VERes enrolled Y	PARes status U
	XID XID value	XID XID value
Action	Ask the customer for another form of payment, or submit the transaction. No liability shift.	

Test Case 64: Diners Club ProtectBuy Card Enrolled: Unsuccessful Authentication

Card Number	3005000000005925	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
Details	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	<ul style="list-style-type: none"> ■ User failed authentication. ■ Payer cannot be authenticated.
	ACS URL URL value	Authentication result 9
	PARReq PARReq value	PARes status N
	proofXML proofXML value	XID XID value
	VERes enrolled Y	
	XID XID value	
Action	You are not permitted to submit this transaction for authorization. Instead ask the customer for another form of payment.	

Test Case 65: Diners Club ProtectBuy Card Enrolled: Unavailable Authentication

Card Number	3005000000006030	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
Details	ics_pa_enroll service was successful.	
	E-commerce indicator internet	
	proofXML proofXML value	
	VERes enrolled U	
Action	Submit your authorization request. No liability shift.	

Test Case 66: Diners Club ProtectBuy Card Enrolled: Authentication Error

Card Number	3005000000005602	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 475	Reason code 476
	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.	We encountered a Payer Authentication problem: Error Processing PAREs.
Details	ACS URL URL value	E-commerce indicator internet
	PARReq PARReq value	ECI 07
	proofXML proofXML value	
	VERes enrolled Y	
	XID XID value	
Action	Ask the customer for another form of payment. No liability shift.	

Test Case 67: Diners Club ProtectBuy Card Not Enrolled

Card Number	3005000000007269	
Auth. Type	Non-participating bank	
Results	Check Enrollment	Validate Authentication
Summary	Reason code 100	
	ics_pa_enroll service was successful.	
Details	E-commerce indicator internet	
	ECI 07	
	proofXML proofXML value	
	VERes enrolled N	
Action	Submit the transaction.	

Test Case 68: Diners Club ProtectBuy Enrollment Check: Time-Out

Card Number	3005000000001890	
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code	100
	ics_pa_enroll service was successful.	
Details	E-commerce indicator	internet
	proofXML	proofXML value
Action	After 10–12 seconds, proceed with the authorization request. No liability shift.	

Test Case 69: Diners Club ProtectBuy Enrollment Check Error

Card Number	3005000000009877	Error response
	3005000000004837	Incorrect Configuration: Unable to Authenticate
Auth. Type	Active authentication	
Results	Check Enrollment	Validate Authentication
Summary	Reason code	100
	ics_pa_enroll service was successful.	
Details	E-commerce indicator	internet
	proofXML	proofXML value
	VERes enrolled	U
Action	Proceed with the authorization request, and contact your support representative to resolve the issue. No liability shift. If you requested payer authentication and authorization together, the authorization is processed automatically.	

API Fields

This appendix describes the Simple Order API fields that you can use to access Payer Authentication services. The API and client toolkits can be downloaded from the CyberSource web site at the following URL:

http://www.cybersource.com/developers/develop/integration_methods/simple_order_and_soap_toolkit_api/

Formatting Restrictions

Unless otherwise noted, all field names are case sensitive and all fields accept special characters such as @, #, and %.



Note

The values of the **item_#_** fields must not contain carets (^) or colons (:) because these characters are reserved for use by the CyberSource services.

For Atos, the **billTo_** fields must not contain colons (:).

The values of all request fields must not contain new lines or carriage returns. However, they can contain embedded spaces and any other printable characters. All leading and trailing spaces will be removed.

Data Type Definitions

For more information about these data types, see the World Wide Web Consortium (W3C) *XML Schema Part 2: Datatypes* specification:

<http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/>

Data Type	Description
Integer	Whole number {..., -3, -2, -1, 0, 1, 2, 3, ...}.
String	Sequence of letters, numbers, spaces, and special characters, such as @ and #.

Request Fields

See *Credit Card Services Using the Simple Order API* ([PDF](#) | [HTML](#)) and *Getting Started with CyberSource Advanced* ([PDF](#) | [HTML](#)) for more information about using the Simple Order API to access CyberSource services using either name-value pairs or XML.



Note

The fields in the following table refer to the enroll and validate services only. Please review *Credit Card Services Using the Simple Order API* ([PDF](#) | [HTML](#)) for more information about the fields specific to the authorization.

Table 13 Request Fields

Field Name	Description	Required/ Optional	Type & Length
billTo_city	City of the billing address.	Enroll (O)	String (50)
billTo_country	Billing country for the account. Use the two-character country codes .	Enroll (O)	String (2)
billTo_email	Customer's email address, including the full domain name. Use the following format: name@host.domain (for example, jdoe@example.com). Required for American Express SafeKey (U.S.).	Enroll (O)	String (255)
billTo_firstName	Customer's first name. The value should be the same as the value that appears on the card. Required for American Express SafeKey (U.S.).	Enroll (O)	String (60)
billTo_lastName	Customer's last name. The value should be the same as the value that appears on the card. Required for American Express SafeKey (U.S.).	Enroll (O)	String (60)
billTo_phoneNumber	Telephone number of the customer. For countries other than US or CA, add the country code at the beginning of the phone number, if possible. Otherwise, the billing country is used to determine the country code.	Enroll (O)	String (15)

Table 13 Request Fields (Continued)

Field Name	Description	Required/ Optional	Type & Length
billTo_postalCode	<p>Postal code for the billing address. The postal code must consist of 5 to 9 digits.</p> <p>When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits]</p> <p>Example 12345-6789</p> <p>When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric]</p> <p>Example A1B 2C3</p> <p>Required only if the billTo_country field is US or CA.</p>	Enroll (O)	String (10)
billTo_state	State or province of the customer. Required for U.S. and Canada. Use the two-character state, province, or territory codes .	Enroll (O)	String (2)
billTo_street1	First line of the billing street address as it appears on the credit card issuer's records.	Enroll (O)	String (60)
billTo_street2	Additional address information, for example: <i>Attention: Accounts Payable</i>	Enroll (O)	String (60)
businessRules_ignoreValidateResult	<p>Enables you to continue processing the request even if payer authentication cannot be validated. For example, if the PARes is invalid, you receive the reply flag, which enables you to process the authorization. This field can contain one of these values:</p> <ul style="list-style-type: none"> ■ true: Ignore the results of validation and continue to process the request. ■ false: (default) If payer authentication cannot be validated, stop processing the request. 	Validate (O)	String (5)
card_accountNumber	Customer's card number.	Enroll (R) Validate (O)	Integer (20)

Table 13 Request Fields (Continued)

Field Name	Description	Required/ Optional	Type & Length
card_cardType	Type of card. For more information, see <i>Credit Card Services Using the Simple Order API</i> (PDF HTML). This field contain one of these values <ul style="list-style-type: none"> ■ 001: Visa ■ 002: Mastercard ■ 003: American Express ■ 005: Diners Club ■ 007: JCB ■ 024: Maestro (UK Domestic) ■ 042: Maestro (International) 	Enroll (R) Validate (R)	String (3)
card_expirationMonth	Expiration month (MM) of the card. Required for the Validate service if card_accountNumber is included.	Enroll (R) Validate (O)	String (2)
card_expirationYear	Expiration year (YYYY) of the card. Required for the Validate service if card_accountNumber is included.	Enroll (R) Validate (O)	String (4)
item_#_productName	Name of the product.	Enroll (O)	String (255)
item_#_productSKU	Merchant's product identifier code.	Enroll (O)	String (255)
item_#_quantity	Quantity of the product being purchased. The default value is 1.	Enroll (O)	Non-negative integer (10)
item_#_unitPrice	Per-item price of the product. This value cannot be negative. The amount will be truncated to the correct number of decimal places. You can include a decimal point (.) in this field, but you cannot include any other special characters. Note The item_#_unitPrice field is not required if the purchaseTotals_grandTotalAmount field is used.	Enroll (R) Validate (R)	String (15)
merchantID	Your CyberSource merchant ID.	Enroll (R) Validate (R)	String (30)
merchantReferenceCode	Merchant-generated order reference or tracking number.	Enroll (R) Validate (R)	String (50)
payerAuthEnrollService_httpAccept	Value of the <code>Accept</code> header sent by the customer's web browser. Note If the customer's browser provides a value, you must include it in your request.	Enroll (O)	String (255)

Table 13 Request Fields (Continued)

Field Name	Description	Required/ Optional	Type & Length
payerAuthEnrollService_ httpUserAgent	Value of the <code>User-Agent</code> header sent by the customer's web browser. Note If the customer's browser provides a value, you must include it in your request.	Enroll (O)	String (255)
payerAuthEnrollService_ MCC	Merchant category code. Important Required only for Verified by Visa transactions in Brazil. Do not use this request field for any other types of transactions.	Enroll (R)	Integer (4)
payerAuthEnrollService_ mobilePhone	Cardholder's mobile phone number. Important Required only for Verified by Visa transactions in Brazil. Do not use this request field for any other types of transactions.	Enroll (R)	Integer (25)
payerAuthEnrollService_ overridePaymentMethod	Specifies the Brazilian payment account type used for the transaction. This field overrides other payment types that might be specified in the request. Use one of the following values for this field: <ul style="list-style-type: none"> ■ NA: Not applicable. Do not override other payment types that are specified in the request. ■ CR: Credit card. ■ DB: Debit card. ■ VSAVR: Visa Vale Refeicao ■ VSAVA: Visa Vale Alimentacao Important Required only for Verified by Visa transactions in Brazil. Do not use this request field for any other types of transactions.	Enroll (R)	String (10)
payerAuthEnrollService_ productCode	Specifies the product code, which designates the type of transaction. Specify one of the following values for this field: <ul style="list-style-type: none"> ■ PHY: Goods or services purchase ■ CHA: Check acceptance ■ ACF: Account funding ■ QCT: Quasi-cash transaction ■ PAL: Prepaid activation and load Important Required only for Verified by Visa transactions in Brazil. Do not use this request field for any other types of transactions.	Enroll (R)	String (3)

Table 13 Request Fields (Continued)

Field Name	Description	Required/ Optional	Type & Length
payerAuthEnrollService_run	Whether to include payerAuthEnrollService in your request. The field has one of these values: <ul style="list-style-type: none"> ■ <code>true</code>: Include the service in your request. ■ <code>false</code> (default): Do not include the service in your request. 	Enroll (R)	String (5)
payerAuthValidateService_signedPAREs	Payer authentication result (PAREs) message returned by the card-issuing bank. If you need to show proof of enrollment checking, you may need to decrypt and parse the string for the information required by the payment card company. For more information, see "Storing Payer Authentication Data," page 117 . Note The field is in base64. You must remove all carriage returns and line feeds before adding the PAREs to the request.	Validate (R)	String (no limit, may be very large)
payerAuthValidateService_run	Whether to include payerAuthValidateService in your request. The field can contain one of these values: <ul style="list-style-type: none"> ■ <code>true</code>: Include the service in your request. ■ <code>false</code> (default): Do not include the service in your request. 	Validate (R)	String (5)
purchaseTotals_currency	Currency used for the order. Use the standard ISO codes located in the Support Center .	Enroll (R) Validate (R)	String (5)
purchaseTotals_grandTotalAmount	Grand total for the order. In your request, you must include either this field or item_#_unitPrice . For more information, see Credit Card Services Using the Simple Order API (PDF HTML) . Note The purchaseTotals_grandTotalAmount field is not optional if the item_#_unitPrice field is not used.	Enroll (O) Validate (O)	String (15)
shipTo_city	City of the shipping address. Required if any shipping address information is included. Required for American Express SafeKey (U.S.).	Enroll (O)	String (50)
shipTo_country	Country of the shipping address. Use the two-character ISO Standard Country Codes . Required for American Express SafeKey (U.S.).	Enroll (O)	String (2)
shipTo_firstName	First name of the recipient.	Enroll (O)	String (60)

Table 13 Request Fields (Continued)

Field Name	Description	Required/ Optional	Type & Length
shipTo_lastName	Last name of the recipient.	Enroll (O)	String (60)
shipTo_phoneNumber	Phone number for the shipping address. For information on formatting, see billTo_phoneNumber .	Enroll (O)	String (15)
shipTo_postalCode	Postal code for the shipping address. The postal code must consist of 5 to 9 digits. When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits] Example 12345-6789 When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric] Example A1B 2C3 Required only if the shipTo_country field is US or CA. Required for American Express SafeKey (U.S.).	Enroll (O)	String (10)
shipTo_shippingMethod	Shipping method for the product. Possible values: <ul style="list-style-type: none">■ lowcost: Lowest-cost service■ sameday: Courier or same-day service■ oneday: Next-day or overnight service■ twoday: Two-day service■ threeday: Three-day service■ pickup: Store pick-up■ other: Other shipping method■ none: No shipping method because product is a service or subscription Required for American Express SafeKey (U.S.).	Enroll (O)	String (10)
shipTo_state	State or province of the shipping address. Use the State, Province, and Territory Codes for the United States and Canada . Required if shipTo_country is CA or US. Required for American Express SafeKey (U.S.).	Enroll (O)	String (2)

Table 13 Request Fields (Continued)

Field Name	Description	Required/ Optional	Type & Length
shipTo_street1	First line of the shipping address. Required if any shipping address information is included. Required for American Express SafeKey (U.S.).	Enroll (O)	String (60)
shipTo_street2	Second line of the shipping address. Required for American Express SafeKey (U.S.).	Enroll (O)	String (60)

Reply Fields

Table 14 Reply Fields

Field Name	Description	Returned By	Type & Length
decision	Summarizes the result of the overall request. The field can contain one of these values: ■ ACCEPT ■ ERROR ■ REJECT	Enroll Validate	String (255)
invalidField_0...N	Fields in the request that contained invalid data.	Enroll Validate	String (255)
merchantReferenceCode	Your order reference or tracking number.	Enroll Validate	String (255)
missingField_0...N	Required fields that were missing from the request.	Enroll Validate	String (255)
payerAuthEnrollReply_acsURL	URL for the card-issuing bank's authentication form that you receive when the card is enrolled. The field length can be very large.	Enroll	String (no length limit)

Table 14 Reply Fields (Continued)

Field Name	Description	Returned By	Type & Length
payerAuthEnrollReply_authenticationPath	<p>Indicates what the customer sees during the authentication process. This field can contain one of these values:</p> <ul style="list-style-type: none"> ■ ADS: (card not enrolled) customer prompted to activate the card during the checkout process. ■ ATTEMPTS: (attempts processing) customer briefly sees <i>Processing...</i> before the checkout process is completed. ■ ENROLLED: (card enrolled) customer sees the card issuer's authentication window. ■ UNKNOWN: card enrollment status cannot be determined. ■ NOREDIRECT: (card not enrolled, authentication unavailable, or error occurred) customer sees nothing. <p>The following values can be returned if you are using rules-based Payer Authentication. See "Rules-Based Payer Authentication," page 135:</p> <ul style="list-style-type: none"> ■ RIBA: The card-issuing bank supports risk-based authentication, but whether the cardholder is likely to be challenged cannot be determined. ■ RIBA_PASS: The card-issuing bank supports risk-based authentication and it is likely that the cardholder will not be challenged to provide credentials, also known as "silent authentication." 	Enroll	String (255)

Table 14 Reply Fields (Continued)

Field Name	Description	Returned By	Type & Length
payerAuthEnrollReply_commerceIndicator	<p>Commerce indicator for cards not enrolled. This field contains one of these values:</p> <ul style="list-style-type: none"> ■ <code>internet</code>: Card not enrolled, or card type not supported by payer authentication. No liability shift. ■ <code>js_attempted</code>: JCB card not enrolled, but attempt to authenticate is recorded. Liability shift. ■ <code>js_failure</code>: You receive this result if JCB's directory service is not available. No liability shift. ■ <code>spa</code>: Mastercard card not enrolled. No liability shift. ■ <code>vbv_attempted</code>: Visa card not enrolled, but attempt to authenticate is recorded. Liability shift. ■ <code>vbv_failure</code>: For the payment processors Barclays, Streamline, AIBMS, or FDC Germany, you receive this result if Visa's directory service is not available. No liability shift. 	Enroll	String (255)
payerAuthEnrollReply_eci	<p>Note This field applies only to non U.S.-issued cards.</p> <p>Numeric electronic commerce indicator (ECI) returned only for Visa, American Express, JCB, and Diners Club transactions when the card is not enrolled. For more information, see "B. Interpreting the Reply," page 25.</p> <p>If you are not using the CyberSource payment services, you must send this value to your payment processor in the subsequent request for card authorization. This field contains one of these values:</p> <ul style="list-style-type: none"> ■ <code>06</code>: The card can be enrolled. Liability shift. ■ <code>07</code>: The card cannot be enrolled. No liability shift. 	Enroll	String (255)
payerAuthEnrollReply_paReq	<p>Payer authentication request (PAREq) message that you need to forward to the ACS. The field length can be very large. The value is in base64.</p>	Enroll	String (No length limit)

Table 14 Reply Fields (Continued)

Field Name	Description	Returned By	Type & Length
payerAuthEnrollReply_ proofXML	<p>Date and time of the enrollment check combined with the VEReq and VERes elements. If you ever need to show proof of enrollment checking, you will need to parse the string for the information required by the payment card company. For more information, see "Storing Payer Authentication Data," page 117. The value can be very large.</p> <ul style="list-style-type: none"> ■ For cards issued in the U.S. or Canada, Visa may require this data for specific merchant category codes. ■ For cards not issued in the U.S. or Canada, your bank may require this data as proof of enrollment checking for any payer authentication transaction that you re-present because of a chargeback. 	Enroll	String (no length limit)
payerAuthEnrollReply_ proxyPAN	Encrypted version of the card number used in the payer authentication request message.	Enroll	String (255)
payerAuthEnrollReply_ reasonCode	Numeric value corresponding to the result of the Enrollment Check service request. For a list of possible values, see Appendix B, "Reason Codes," on page 95.	Enroll	Integer (5)
payerAuthEnrollReply_ ucafCollectionIndicator	<p>Indicates that authentication is not required because the customer is not enrolled. Add the value of this field to the authorization field ucaf_collectionIndicator. This field can contain these values: 0, 1.</p> <p>Note This field is returned for only Mastercard SecureCode transactions.</p>	Enroll	String (255)

Table 14 Reply Fields (Continued)

Field Name	Description	Returned By	Type & Length
payerAuthEnrollReply_ veresEnrolled	<p>Result of the enrollment check. This field can contain one of these values:</p> <ul style="list-style-type: none"> ■ Y: Card enrolled; you must authenticate. Liability shift. ■ N: Card not enrolled; proceed with authorization. Liability shift. ■ U: Unable to authenticate regardless of the reason. No liability shift. <p>Note This field only applies to the Asia, Middle East, and Africa Gateway. If you are configured for this processor, you must send the value of this field in your authorization request.</p> <p>The following value can be returned if you are using rules-based Payer Authentication. See "Rules-Based Payer Authentication," page 135:</p> <ul style="list-style-type: none"> ■ B: Indicates that authentication was bypassed. 	Enroll	String (255)
payerAuthEnrollReply_xid	Transaction identifier generated by CyberSource for successful enrollment checks. Use this value to match an outgoing PAREq with an incoming PAREs. If your payment processor is Barclays, CyberSource forwards the XID with your card authorization service request. The value is in base64.	Enroll	String (255)
payerAuthValidateReply_ authenticationResult	<p>Raw authentication data that comes from the card-issuing bank. Primary authentication field that indicates if authentication was successful and if liability shift occurred. You should examine first the result of this field. This field contains one of these values:</p> <ul style="list-style-type: none"> ■ -1: Invalid PAREs. ■ 0: Successful validation. ■ 1: Cardholder is not participating, but the attempt to authenticate was recorded. ■ 6: Issuer unable to perform authentication. ■ 9: Cardholder did not complete authentication. 	Validate	String w/ numbers only (255)
payerAuthValidateReply_ authenticationStatus Message	<p>Message that explains the content of payerAuthValidateReply_authenticationResult.</p>	Validate	String (255)

Table 14 Reply Fields (Continued)

Field Name	Description	Returned By	Type & Length
payerAuthValidateReply_cavv	<p>Unique identifier generated by the card-issuing bank after the customer is authenticated. The value is in base64. When you request the card authorization service, CyberSource automatically converts the value, not the field name, to the format required by your payment processor.</p> <p>Note This field is generated only for Verified by Visa, American Express SafeKey, JCB, and Diners Club transactions.</p>	Validate	String (255)
payerAuthValidateReply_cavvAlgorithm	<p>Field returned when payerAuthValidateReply_paresStatus contains the values Y (successful authentication) or A (attempted authentication). This field contains one of these values:</p> <ul style="list-style-type: none"> ■ 2: Visa, American Express, JCB, and Diners Club ■ 3: Mastercard and Maestro <p>Note This field only applies if you use the Atos processor. If you use Atos, send the value of this field in the ccAuthService_cavvAlgorithm request field of the authorization service.</p>	Validate	Integer (1)

Table 14 Reply Fields (Continued)

Field Name	Description	Returned By	Type & Length
payerAuthValidateReply_commerceIndicator	<p>Indicator used to differentiate different types of transactions. The authentication failed if this field is not returned. The value of this field is passed automatically to the authorization service if you request the services together. This field contains one of these values:</p> <ul style="list-style-type: none"> ■ aesk: American Express SafeKey authentication verified successfully. ■ aesk_attempted: Card not enrolled in American Express SafeKey, but the attempt to authenticate was recorded. ■ internet: Authentication failed. ■ js: J/Secure authentication verified successfully. ■ js_attempted: Card not enrolled in J/Secure, but the attempt to authenticate was recorded. ■ moto: Mail or telephone order. ■ pb_attempted: Card not enrolled in Diners Club ProtectBuy, but the attempt to authenticate was recorded. ■ recurring: Recurring transaction. ■ spa: Mastercard SecureCode authentication verified successfully. ■ spa_failure: Mastercard SecureCode failed authentication. ■ vbv: Verified by Visa authentication verified successfully. ■ vbv_attempted: Card not enrolled in Verified by Visa, but the attempt to authenticate was recorded. ■ vbv_failure: Verified by Visa authentication unavailable. <p>Note For Visa, if the payment processor is Streamline, Barclays, AIBMS, or FDC Germany, you receive vbv_failure instead of internet when payerAuthValidateReply_eci is 07.</p>	Validate	String (255)

Table 14 Reply Fields (Continued)

Field Name	Description	Returned By	Type & Length
payerAuthValidateReply_eci	<p>Numeric electronic commerce indicator (ECI) returned only for Visa, American Express, JCB, and Diners Club transactions. You must send this value to your payment processor in the subsequent request for card authorization. This field contains one of these values:</p> <ul style="list-style-type: none"> ■ 05: Successful authentication ■ 06: Authentication attempted ■ 07: Failed authentication (No response from the merchant because of a problem.) 	Validate	String (255)
payerAuthValidateReply_eciRaw	<p>ECI value that can be returned for Visa, Mastercard, American Express, JCB, and Diners Club. The field is absent when authentication fails. If your payment processor is Streamline, you must pass the value of this field instead the value of payerAuthValidateReply_eci or payerAuthValidateReply_ucafCollectionIndicator.</p> <p>This field can contain one of these values:</p> <ul style="list-style-type: none"> ■ 01: Incomplete authentication (Mastercard) ■ 02: Successful authentication (Mastercard) ■ 05: Successful authentication (Visa, American Express, JCB, and Diners Club) ■ 06: Authentication attempted (Visa, American Express, JCB, and Diners Club) 	Validate	String (255)
payerAuthValidateReply_paresStatus	<p>Raw result of the authentication check. This field can contain one of these values:</p> <ul style="list-style-type: none"> ■ A: Proof of authentication attempt was generated. ■ N: Customer failed or cancelled authentication. Transaction denied. ■ U: Authentication not completed regardless of the reason. ■ Y: Customer was successfully authenticated. <p>Note This field only applies to the Asia, Middle East, and Africa Gateway. If you are configured for this processor, you must send the value of this field in your authorization request.</p>	Validate	String (255)

Table 14 Reply Fields (Continued)

Field Name	Description	Returned By	Type & Length
payerAuthValidateReply_reasonCode	Numeric value corresponding to the result of the validation request. For a list of possible values, see Appendix B, "Reason Codes," on page 95 .	Validate	Integer (5)
payerAuthValidateReply_ucafAuthenticationData	AAV is a unique identifier generated by the card-issuing bank after the customer is authenticated. The value is in base64. Include the data in the card authorization request. Note This field is returned for only Mastercard SecureCode transactions.	Validate	String (255)
payerAuthValidateReply_ucafCollectionIndicator	Numeric electronic commerce indicator (ECI). The field is absent when authentication fails. You must send this value to your payment processor in the request for card authorization. This field contain one of these values: <ul style="list-style-type: none"> 0: UCAF collection is not supported at your web site. Customer authentication was not completed. 1: UCAF collection is supported at your web site, but UCAF was not populated. Customer authentication was not completed. 2: UCAF collection is supported at your web site, and UCAF was populated. Customer completed authentication. Note This field is returned for only Mastercard SecureCode transactions.	Validate	String (255)
payerAuthValidateReply_xid	Transaction identifier generated by CyberSource for validation checks. Use this value, which is in base64, to match the PAREq with the PAREs. CyberSource forwards the XID with the card authorization service to these payment processors: <ul style="list-style-type: none"> Barclays Streamline when the commerce indicator is <code>spa</code> 	Validate	String (255)
purchaseTotals_currency	Currency used for the order. Use the standard ISO codes located in the Support Center .	Enroll Validate	String (255)
reasonCode	Numeric value corresponding to the result of the overall request. See Appendix B, "Reason Codes," on page 95 for a list of possible values.	Enroll Validate	Integer (5)
requestID	Identifier for the request.	Enroll Validate	String (255)

Table 14 Reply Fields (Continued)

Field Name	Description	Returned By	Type & Length
requestToken	<p>Identifier for the request generated by CyberSource.</p> <p>Request token data created by CyberSource for each reply. The field is an encoded string that contains no confidential information such as an account or card verification number. The string can contain a maximum of 256 characters.</p>	<p>Enroll</p> <p>Validate</p>	String (256)

Reason Codes

The following table lists the reason codes that are returned with the reply. CyberSource reserves the right to add new reason codes at any time. If your error handler receives a reason code that it does not recognize, it should use the decision field to determine the result.

Table 15 Reason Codes

Reason Code	Description
100	Successful transaction.
101	The request is missing one or more required fields. Possible action: See the reply fields missingField_0...N for the missing fields. Resend the request with the complete information.
102	One or more fields in the request contains invalid data. Possible action: See the reply fields invalidField_0...N for the invalid fields. Resend the request with the correct information.
150	Error: General system failure. Possible action: Wait a few minutes and resend the request.
151	Error: The request was received, but a server time-out occurred. This error does not include time-outs between the client and the server. Possible action: Wait a few minutes and resend the request.
152	Error: The request was received, but a service time-out occurred. Possible action: Wait a few minutes and resend the request.
234	A problem exists with your CyberSource merchant configuration. Possible action: Do not resend the request. Contact Customer Support to correct the configuration problem.
475	The customer is enrolled in Payer Authentication. Authenticate the cardholder before continuing with the transaction.
476	The customer cannot be authenticated. Possible action: Review the customer's order.

Request and Reply Examples

This appendix contains examples for the check enrollment service and the validate authentication service for all card types. All examples are in name-value pair format.



These examples contain only the fields essential to the demonstration. Do not prepare your implementation according to the fields that you see in these examples. They are provided for your information only.

Check Enrollment Example



Although the **payerAuthEnrollReply_proofXML** field is shown only in the Visa card replies, this field is returned for all card types.

The following is an example of a request for the check enrollment service:

Example Check Enrollment

```
payerAuthEnrollService_run=true
merchantID=infodev
merchantReferenceCode=23AEE8CB6B62EE2AF07
item_0_unitPrice=19.99
purchaseTotals_currency=USD
card_expirationMonth=12
card_expirationYear=2015
card_accountNumber=xxxxxxxxxxxxxxxxxx
card_cardType=001
```


Transaction Reply for Visa with Verified by Visa

The **payerAuthEnrollReply_proofXML** field is returned in replies for both enrolled and unenrolled cards. For more information on this field, see ["Storing Payer Authentication Data," page 117](#). For an example, see ["ProofXML," page 102](#).

Enrolled card: The decision and the reason codes mean that the card is enrolled and that you must proceed with validation.

Example Transaction Reply for Visa Card Enrolled in Verified by Visa

```
requestID=0340290070000167905080
merchantReferenceCode=23AEE8CB6B62EE2AF07
purchaseTotals_currency=USD
decision=REJECT
reasonCode=475
payerAuthEnrollReply_reasonCode=475
payerAuthEnrollReply_acsURL=https://www.example.com
payerAuthEnrollReply_paReq=value in base64:
eJxVUuFygjAMfhXPw9Tkv9g6...
payerAuthEnrollReply_proofXML=see example "ProofXML," page 102.
payerAuthEnrollReply_proxyPAN=Cpj25JL53E9sqNKj
payerAuthEnrollReply_xid=dOaE6u0nNpCBQHZAebKyADw4aQE=
```

Unenrolled card: The decision and the reason codes mean that the card is unenrolled and that you can proceed with the transaction.

Example Transaction Reply for Unenrolled Visa Card

```
requestID=0340290070000167905080
merchantReferenceCode=23AEE8CB6B62EE2AF07
purchaseTotals_currency=USD
decision=ACCEPT
reasonCode=100
payerAuthEnrollReply_reasonCode=100
payerAuthEnrollReply_commerceIndicator=vbv_attempted
payerAuthEnrollReply_eci=06
payerAuthEnrollReply_proofXML=see example "ProofXML," page 102.
```

Transaction Reply for Mastercard with SecureCode

The **payerAuthEnrollReply_proofXML** field is returned in replies for both enrolled and unenrolled cards. For more information on this field, see ["Storing Payer Authentication Data," page 117](#). For an example, see ["ProofXML," page 102](#).

Enrolled: The decision and the reason codes mean that the card is enrolled and that you must proceed with validation.

Example Transaction Reply for Mastercard Enrolled in SecureCode

```
requestID=0340290070000167905080
merchantReferenceCode=cybs_test
purchaseTotals_currency=USD
decision=REJECT
reasonCode=475
payerAuthEnrollReply_reasonCode=475
payerAuthEnrollReply_acsURL=https://www.example.com
payerAuthEnrollReply_paReq=value in base64:
5oBF+dJuGBB4Lq9HpAGgkQV...
payerAuthEnrollReply_proxyPAN=Cpj25JL53E9sqNKj
payerAuthEnrollReply_xid=dOaE6u0nNpCBQHZAebKyADw4aQE=
payerAuthEnrollReply_proofXML=see example "ProofXML," page 102.
payerAuthEnrollReply_proxyPAN=Cpj25JL53E9sqNKj
payerAuthEnrollReply_xid=dOaE6u0nNpCBQHZAebKyADw4aQE=
```

Unenrolled card: The decision and the reason codes mean that the card is unenrolled and that you can proceed with the transaction.

Example Transaction Reply for Unenrolled Mastercard

```
requestID=0687782849850167904150
merchantReferenceCode=14344
decision=Accept
reasonCode=100
payerAuthEnrollReply_reasonCode=100
payerAuthEnrollReply_commerceIndicator=spa
payerAuthEnrollReply_ucafCollectionIndicator=1
payerAuthEnrollReply_proofXML=see example "ProofXML," page 102.
```

Transaction Reply for JCB with J/Secure

```
requestID=0340290070000167905080
merchantReferenceCode=23AEE8CB6B62EE2AF07
decision=ACCEPT
reasonCode=100
purchaseTotals_currency=USD
payerAuthEnrollReply_reasonCode=100
payerAuthEnrollReply_acsURL=https://www.example.com
payerAuthEnrollReply_paReq=value in base64:
eJxVUuFygjAMfhXPw9Tkv9g6...
payerAuthEnrollReply_proxyPAN=Cpj25JL53E9sqNKj
payerAuthEnrollReply_xid=dOaE6u0nNpCBQHZAebKyADw4aQE=
```

Validate Authentication

This example shows a request for the Validate Authentication service.

```

payerAuthValidateService_run=true
merchantID=infodev
merchantReferenceCode=23AEE8CB6B62EE2AF07
card_expirationMonth=12
card_expirationYear=2015
card_accountNumber=xxxxxxxxxxxxxxxx
card_cardType=001
purchaseTotals_currency=USD
payerAuthValidateService_signedPARES=value in base64:
HTNH2esM9VG08e...

```

Transaction Reply for Visa with Verified by Visa

```

requestID=0348277000000167904548
merchantReferenceCode=23AEE8CB6B62EE2AF07
decision=ACCEPT
reasonCode=100
purchaseTotals_currency=USD
payerAuthValidateReply_reasonCode=100
payerAuthValidateReply_authenticationResult=0
payerAuthValidateReply_authenticationStatusMessage=Success
payerAuthValidateReply_cavv=KuptWQm6guKE7DJNzDaBrlCD1B0=
payerAuthValidateReply_commerceIndicator=vbv
payerAuthValidateReply_eci=05
payerAuthValidateReply_xid=dOaE6u0nNpCBQHzAebKyADw4aQE=
merchantID=infodev
merchantReferenceCode=23AEE8CB6B62EE2AF07
purchaseTotals_currency=USD
card_expirationMonth=12
card_expirationYear=2015
card_accountNumber=xxxxxxxxxxxxxxxx
card_cardType=002

```

Transaction Reply for Mastercard with SecureCode

```
requestID=0682438330010167904548
merchantReferenceCode=23AEE8CB6B62EE2AF07
purchaseTotals_currency=USD
decision=ACCEPT
reasonCode=100
payerAuthValidateReply_reasonCode=100
payerAuthValidateReply_authenticationResult=0
payerAuthValidateReply_commerceIndicator=spa
payerAuthValidateReply_ucafAuthenticationData=jGCgOLutbHbJABEAAAHFF6I=
payerAuthValidateReply_ucafCollectionIndicator=2
payerAuthValidateReply_xid=EsHyaAcPr0eTma3
```

Transaction Reply for JCB with J/Secure

```
requestID=0348277000000167904548
merchantReferenceCode=23AEE8CB6B62EE2AF07
decision=ACCEPT
reasonCode=100
purchaseTotals_currency=USD
payerAuthValidateReply_reasonCode=100
payerAuthValidateReply_authenticationResult=0
payerAuthValidateReply_authenticationStatusMessage=Success
payerAuthValidateReply_cavv=KuptWQm6guKE7DJNzDaBrLCD1B0=
payerAuthValidateReply_commerceIndicator=js
payerAuthValidateReply_eci=05
payerAuthValidateReply_xid=dOaE6u0nNpCBQHZAebKyADw4aQE=
```

ProofXML

ProofXML usually appears in code as a string. It is provided in the following form to enhance readability.

```
<AuthProof>
  <Time>2009 Jan 19 11:01:52</Time>
  <DSUrl>https:216.150.137.86:443/merchantacsfrontend/VeReq.jsp</
DSUrl>
  <VEReqProof>
    <Message id="xfm5_3_0.6784">
      <VEReq>
        <version>1.0.2</version>
        <pan>XXXXXXXXXXXX0051</pan>
        <Merchant>
          <acqBIN>123456</acqBIN>
          <merID>1234567800000000</merID>
        </Merchant>
        <Browser>
          <accept>null</accept>
          <userAgent>null</userAgent>
        </Browser>
      </VEReq>
    </Message>
  </VEReqProof>
  <VEResProof>
    <Message id="xfm5_3_0.6784">
      <VERes>
        <version>1.0.2</version>
        <CH>
          <enrolled>N</enrolled>
        </CH>
      </VERes>
    </Message>
  </VEResProof>
</AuthProof>
```

Web Site Modification Reference

This appendix contains information about modifying your web site to integrate Payer Authentication services into your checkout process. It also provides links to payment card company web sites where you can download the appropriate logos.

Web Site Modification Checklist

1 Modify web page buttons:

- Order submission button: disable the final “buy” button until the customer completes all payment and authentication requirements.
- Browser back button: account for unexpected customer behavior. Use session checks throughout the authentication process to prevent authenticating transactions twice. Avoid confusing messages, such as warnings about expired pages.

2 Add appropriate logos:

- Make sure you have downloaded the appropriate logos of the cards that you support and place these logos next to the card information entry fields on your checkout pages. For more information about obtaining logos and using them, see ["3D Secure Services Logos," page 104](#).

3 Add informational message:

- Add a message next to the final “buy” button and the card logo to inform your customers that they may be prompted to provide their authentication password or to sign up for the authentication program specific to their card. For examples of messages you can use, see ["Informational Message Examples," page 105](#).

3D Secure Services Logos

The following table contains links to payment card company web sites from which you can download logos and information about how to incorporate them into your online checkout process.

3D Secure service	Where to download logos and information
Verified by Visa	http://usa.visa.com/merchants/grow-your-business/payment-technologies/verified-by-visa.jsp This web site contains information about Verified by Visa and links where you can download logos. The page also contains links to a best practice guide for implementing Verified by Visa and a link to a Merchant Toolkit. See the list of links at the right margin of the web page to download these files.
Mastercard and Maestro SecureCode	http://www.mastercard.us/merchants/securecode.html This web site contains information about SecureCode, links where you can download logos, and information about integrating the SecureCode information into your web site checkout page. For information about Maestro logos, go to: http://www.mastercardbrandcenter.com/us/howtouse/bms_mae.shtml
American Express SafeKey	https://network.americanexpress.com/uk/en/safekey/ This web site contains information about SafeKey and links where you can download logos.
JCB J/Secure	http://partner.jcbcard.com/security/jsecure/logo.html This web site contains information about J/Secure and links where you can download logos.
Diners Club ProtectBuy	http://www.dinersclubprotect-buy.net/Public/MerchantTools.aspx This web site contains information about Diners Club ProtectBuy and links where you can download logos.

Informational Message Examples

Add a brief message adjacent to your final buy button on your checkout page to inform customers that they may be prompted to provide their authentication password or to enroll in the authentication program specific for their card.

The following examples may be used, but consult your specific card authentication program to make sure you conform to their messaging requirements.

Example 1

To help prevent unauthorized use of *<card_type>* cards online, *<your_business_name>* participates in *<card_authentication_program>*.

When you submit your order, you may receive a *<card_authentication_program>* message from your *<card_type>* card issuer. If your card or issuer does not participate in the program, you will be returned to our secure checkout to complete your order. Please wait while the transaction is processed. Do not click the Back button or close the browser window.

Example 2

Your card may be eligible for enrollment or is enrolled in the Verified by Visa, Mastercard or Maestro SecureCode, American Express SafeKey, JCB J/Secure, or Diners Club ProtectBuy programs. After you submit your order, your card issuer may prompt you for your password before you complete your purchase.

Payer Authentication Transaction Details in the Business Center

This appendix describes how to search the Business Center for details of transactions that are screened by Payer Authentication. Transaction data is stored for 12 months so that you can send it to payment card companies if necessary.

Searching for Payer Authentication Details

Payer Authentication data that is returned in API reply fields can be searched by using Transaction Search in the Business Center.

With other services, green means that the service request was successful, red means that it failed, and black means that the service request was not run. However, you need to interpret the result of the enrollment check differently:

- If the card is enrolled, the application result is shown in red, which indicates that you need to authenticate the user before you can request card authorization.
- If the card is not enrolled, the application result is shown in green because you do not need to authenticate the user. You can authorize the card immediately.

Enrolled Card

When a card is enrolled, the process consists of two steps: after you check for enrollment, you need to authenticate the customer.

Enrollment Check

The following figure shows the details page of an enrollment check for an enrolled card. You receive Payer Authentication information in several locations:

- Request Information section: The enrollment check service is shown in red because the card is enrolled. You receive the corresponding reply information (blue boxes). If the card authorization service had been requested at the same time, it would not have been run and would appear in black.

You can obtain additional information about related orders by clicking the links on the right (Event Search and Details).

- Payment Information section: When authentication is required, save the XID for use later. You do not receive an ECI because the authentication is not complete, and you do not receive an AAV_CAVV for an enrollment check.

When you receive a result similar to the following figure, you need to authenticate the user by requesting the validation service.

Figure 8 Enrollment Check Details

Transaction Search Details

[I need help with this page.](#)

Request Information	
Merchant ID	ics2test
Request ID	1889453160000167904548
Merchant Reference Number	cybs_test
Date	Sep 04 2007 03:35:16 PM
Applications	Payer Authentication Enrollment
Reply	Payer needs to be authenticated
Reply Code	0
Reply Message	The cardholder is enrolled in Payer Authentication. Please authenticate before proceeding with authorization.
Client Version	Perl5.0/solaris2.6/sol25/C/3.4.8
Client User	

Related Events

Similar Searches [By Name](#)
[By Email Address](#)
[By Payer Authentication History](#)

Extended Views [View Payer Authentication Details](#)

Details

Customer Information	
Billing Information	
Name	VIMAL PATEL
Company	Cybersource Corporation
Address	1295 Charleston Road Mountain View CA , 94043 US
Phone Number	
Email Address	vimal.67@gmail.com
IP Address	10.2.7.18

Payment Information			
Payer Authentication	ECI	AAV/CAVV	XID a/Q7zFs2EdyKlZjve2/X4gEAAAc=

Events Related to Payer Authentication

When the XID value is available, you also have the option to search for other parts of the transaction with the By Payer Authentication History under Similar Searches link.

For example, in the previous figure, you can use the link to find the details page that shows the associated card validation and authorization results. The following figure shows the results page:

Figure 9 Transaction Search Details - Example 1

Transaction Search Results [I need help with this page.](#)

Search Parameters [Export Results](#)

Start: Mar 11 2007 12:00 AM
End: Sep 11 2007 11:59 PM
Payer Authentication ID (XID): a/Q7zFs2EdyKlZjve2/X4gEAAAc=
Matching Transactions: 2

Merchant ID Date and Time	Request ID Merchant Reference Number	Name Email Address	Amount Account Suffix	Applications
ics2test Sep 04 2007 03:36:04 PM	1889453640000167904548 cybs_test	VIMAL PATEL vimal.67@gmail.com	1.00 USD 1007	Payer Authentication Validation
ics2test Sep 04 2007 03:35:16 PM	1889453160000167904548 cybs_test	VIMAL PATEL vimal.67@gmail.com	1.00 USD 1007	Payer Authentication Enrollment

- The most recent event is the successful authentication. If you click the request ID, you see the authentication details page. Because this event also returned an XID value, the By Payer Authentication History link is present. If you click it, you are returned to the results page.
- The older event is the enrollment check.

If the card authorization service had been requested at the same time as Payer Authentication, authorization would not have run with the enrollment check but with the validate authentication request. The following figure shows these events:

Figure 10 Transaction Search Details - Example 2

Transaction Search Results [I need help with this page.](#)

Search Parameters [Export Results](#)

Date Range: Custom range
Start: Jun 15 2006 12:00 AM
End: Dec 15 2006 11:59 PM
Payer Auth ID (XID): HhxPrE5EEduE8FSIXW0bLAQEbgg=
Matching Transactions: 2

Merchant ID Date and Time	Request ID Merchant Reference Number	Name Email Address	Amount Account Suffix	Applications
revent Sep 27 2006 11:18:34 AM	1593741442830167904065 1159373664380		3.00 USD 4468	Credit Card Authorization Payer Authentication Validation
revent Sep 27 2006 11:18:23 AM	1593741342490167904065 1159373664380		3.00 USD 4468	Credit Card Authorization Payer Authentication Enrollment

- The most recent event is the combined successful customer authentication and card authorization. If you click the request ID, you see the details page.
- The older event is the enrollment check in red because the card is enrolled.

Payer Authentication Details

You also can search for the Payer Authentication data with the View Payer Authentication Details link located under Extended Views. The following figure and the XML code that follows shows details for the above transaction. The XML code is returned if you click Export to XML File. CyberSource stores Payer Authentication information for 12 months after the transaction. For more information about this XML report, see "[Payer Authentication Detail Report](#)," page 123.

Figure 11 Payer Authentication Data in Transaction Search Details Window

Payer Authentication Search Details [I need help with this page.](#)

Request Information

CyberSource Merchant ID
 Request ID [1889453160000167904548](#)
 Unique Transaction Identifier (XID) a/Q7zFs2EdyKlZjve2/X4gEAAAc=
 Transaction Date Sep 04 2007 03:35:16 PM
 Transaction Type Payer Authentication Enrollment

[Export to XML File](#)

Proof XML

Date 20070904 15:30:21
 Directory Server URL https:
 Primary Account Number (PAN) XXXXXXXXXXXX1007
 Acquirer BIN 1234567
 Merchant ID special_id
 Data Server Password XXXXXXXX
 Card Enrollment Result Y

Verify Enrollment Request

Primary Account Number (PAN) XXXXXXXXXXXX1007
 Acquirer BIN 1234567
 Merchant ID special_id

Verify Enrollment Response

Card Enrollment Result Y
 Account Identifier G7XnvRUvB6jKH5/KxVBwYnx6cyw=
 ACS URL

Payer Authentication Request

Acquirer BIN 1234567
 Merchant ID special_id
 Merchant Name CyberSource
 Merchant Country US
 Merchant URL http://www.
 Unique Transaction Identifier (XID) a/Q7zFs2EdyKlZjve2/X4gEAAAc=
 Purchase Date Sep 04 2007 03:30:21 PM
 Purchase Amount 1.00 USD
 Account Identifier G7XnvRUvB6jKH5/KxVBwYnx6cyw=
 Card Expiration Date 0905

```

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE Result SYSTEM "https://ebc.cybersource.com/ebc/reports/dtd/
payerauthdetails.dtd">
<Result>
  <PayerAuthDetail>
    <RequestID>1889453160000167904548</RequestID>
    <MerchantID>example</MerchantID>
    <TransactionDate>Sep 04 2007 03:35:16 PM</TransactionDate>
    <TransactionType>ics_pa_enroll</TransactionType>
    <ProofXML>
      <Date>20070904 15:30:21</Date>
      <DSURL>https:123.456.789.01:234</DSURL>
      <PAN>XXXXXXXXXXXX1007</PAN>
      <AcqBIN>1234567</AcqBIN>
      <MerID>00032805455400000</MerID>
      <Password>XXXXXXXX</Password>
      <Enrolled>Y</Enrolled>
    </ProofXML>
    <VEReq>
      <PAN>XXXXXXXXXXXX1007</PAN>
      <AcqBIN>1234567</AcqBIN>
      <MerID>special_id</MerID>
    </VEReq>
    <VERes>
      <Enrolled>Y</Enrolled>
      <AcctID>G7XnvRUvB6jKH5/KxVBwYnx6cyw=</AcctID>
      <URL>https://www.example_url.com</URL>
    </VERes>
    <PAREq>
      <AcqBIN>1234567</AcqBIN>
      <MerID>00032805455400000</MerID>
      <Name>Example_Merchant</Name>
      <Country>US</Country>
      <URL>http://www.example_merchant.com</URL>
      <XID>a/Q7zFs2EdyKlZjve2/X4gEAAAc=</XID>
      <Date>Sep 04 2007 03:30:21 PM</Date>
      <PurchaseAmount>1.00 USD</PurchaseAmount>
      <AcctID>G7XnvRUvB6jKH5/KxVBwYnx6cyw=</AcctID>
      <Expiry>0905</Expiry>
    </PAREq>
  </PayerAuthDetail>
</Result>

```

Authentication Validation

The following figure shows a details page in which the validation and the card authorization services were processed successfully. The red boxes show where Payer Authentication data is located in the Transaction Search Details window:

- Request Information section: The validation service succeeded. You receive the reason code 100, and the corresponding reply message. The necessary Payer Authentication information was passed to the card authorization service, which was processed successfully. Both services are shown in green.
- Payment Information section: You received a value for all three parameters because the validation was successful. You may not receive an ECI value when a system error prevents the card issuer from performing the validation or when the cardholder does not complete the process.

Figure 12 Transaction Search Details - Authentication Validation

Transaction Search Details [I need help with this page.](#)

Request Information		Status	Amount	Action	Date
Merchant ID	ocvp1	Credit Card Authorization	66.00 USD		Mar 31 2006 12:37:06 PM
Request ID	1438292990130167904064				
Merchant Reference Number	1143829299008				
Date	Mar 31 2006 12:37:06 PM				
Applications	Credit Card Authorization Payer Authentication Validation			Available Actions Settlement Create Subscription	
Reason Code	100			Similar Searches: By Name By Email Address By Payer Authentication History	
Reply Message	Request was processed successfully.				
Client Library	3.7.11				
Client Application	HOP				
Client Application Version	2				
Client User	HOP				

Customer Information	
Billing Information	
Name	
Company	
Address	8310 Capital of Texas Austin TX , 78731 US
Phone Number	
Email Address	null@cybersource.com
IP Address	

Payment Information				
Processor	Payment Method	Account Suffix	Expiration Date	
smartfdc	MasterCard	4617	02/2009	
Credit Card Authorization	Authorization Code	Amount	Action	Trans Ref No Reason Code
	123456	66.00 USD		9038226693 100
	CVN	AVS		
	Y - Match: address and 5-digit postal code match			
	Reply Message			
	Request was processed successfully.			
Payer Authentication	ECI	AAV/CAVV	XID	
	2	jLw8xEMqcxPMABEAAADH1UGO/7k = ZWWFOMDkEdqNhdAcOxvIjwQGAQc=		

Card Not Enrolled

When the card is not enrolled, the enrollment check service result is shown in green, and the card authorization request (if requested at the same time) proceeds normally.

Payer Authentication Details

You can also search for the Payer Authentication data by using the View Payer Authentication Details link located under Extended Views. The following figure and the XML code that follows shows those details for the above transaction. The XML code is returned if you click Export to XML File. Payer Authentication information is stored for 12 months after the transaction. For more information on this XML report, see "[Payer Authentication Detail Report](#)," [page 123](#).

Figure 13 Payer Authentication Details - Card Not Enrolled

Payer Authentication Search Details

[I need help with this page.](#)

Request Information

CyberSource Merchant ID **example**
 Request ID **[1897243130000167904548](#)**
 Unique Transaction Identifier (XID)
 Transaction Date **Sep 13 2007 03:58:36 PM**
 Transaction Type **Payer Authentication Enrollment**

[Export to XML File](#)

Proof XML

Date **20070913 15:53:37**
 Directory Server URL **https:**
 Primary Account Number (PAN) **XXXXXXXXXXXX0008**
 Acquirer BIN **123456**
 Merchant ID **special_id**
 Data Server Password
 Card Enrollment Result **N**

Verify Enrollment Request

Primary Account Number (PAN) **XXXXXXXXXXXX0008**
 Acquirer BIN **123456**
 Merchant ID **special_id**

Verify Enrollment Response

Card Enrollment Result **N**
 Account Identifier
 ACS URL

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE Result SYSTEM "https://ebc.cybersource.com/ebc/reports/dtd/
payerauthdetails.dtd">
<Result>
  <PayerAuthDetail>
    <RequestID>1897243130000167904548</RequestID>
    <MerchantID>example</MerchantID>
    <TransactionDate>Sep 13 2007 03:58:36 PM</TransactionDate>
    <TransactionType>ics_pa_enroll</TransactionType>
    <ProofXML>
      <Date>20070913 15:53:37</Date>
      <DSURL>https:123.456.789.01:234</DSURL>
      <PAN>XXXXXXXXXXXX0008</PAN>
      <AcqBIN>123456</AcqBIN>
      <MerID>special_id</MerID>
      <Password />
      <Enrolled>N</Enrolled>
    </ProofXML>
    <VEReq>
      <PAN>XXXXXXXXXXXX0008</PAN>
      <AcqBIN>123456</AcqBIN>
      <MerID>special_id</MerID>
    </VEReq>
    <VERes>
      <Enrolled>N</Enrolled>
      <AcctID />
      <URL />
    </VERes>
  </PayerAuthDetail>
</Result>
```

Transaction Details

The red boxes show where Payer Authentication data is located in the Transaction Search Details window:

- Request Information section: The service is shown in green. You can obtain additional information about related orders by clicking the link on the right.
- Payment Information section: You see the detailed information for the authorization service:
 - The ECI value is 1: Authentication is not required because the customer's Mastercard card is not enrolled.
 - The AAV/CAVV area is empty because you receive a value only if the customer is authenticated.
 - The XID area is empty because the card is not enrolled.

Figure 14 Transaction Search Details - Card Not Enrolled

Transaction Search Details [I need help with this page.](#)

Request Information	
Merchant ID	ics2test
Request ID	1897243130000167904548
Merchant Reference Number	cybs_test
Date	Sep 13 2007 03:58:36 PM
Applications	Payer Authentication Enrollment
Reply	Success
Reply Code	1
Reply Message	Request was processed successfully.
Client Version	Perl5.0/solaris2.6/sol25/C/3.4.8
Client User	

Similar Searches: [By Name](#) [By Email Address](#)

Extended Views: [View Payer Authentication Details](#)

Customer Information	
Billing Information	
Name	JOHN DOE
Company	Cybersource
Address	1295 Charleston Road Mountain View CA , 94043 US
Phone Number	
Email Address	null@cybersource.com
IP Address	10.2.7.48

Payment Information			
Payer Authentication	ECI	AAV/CAVV	XID
	1		

Offer-Line Details							
Item	Quantity	SKU	Name	Type	Price	Tax	Currency
0	1	27100911	Test Product	default	1.00	0.00	

Payer Authentication Search

Search for transactions that used the Payer Authentication and card authorization services. When searching for transactions, consider the following:

- Search options:
 - Use the XID as search parameter to find both parts of a transaction processed with an enrolled card. When using the XID as search option, make sure to keep the = sign at the end of the string.
 - The list of applications is simplified to facilitate searching for the relevant service requests.
 - Payer Authentication information is available for 12 months after the transaction date.
- Search Results: The results options include the XID and the customer's account number (PAN). Use the XID to find all parts of the transaction.
- Payer Authentication Details: All transaction details are discussed under ["Searching for Payer Authentication Details," page 106](#).

Storing Payer Authentication Data

Payment card companies allow a certain number of days between the Payer Authentication and the authorization requests. If you settle transactions older than the pre-determined number of days, payment card companies may require that you send them the AAV, CAVV, or the XID if a chargeback occurs. The requirements depend on the card type and the region. For more information, see your agreement with your payment card company. After your transactions are settled, you can also use this data to update the statistics of your business.

You may be required to show the values that you receive in the PAREs, the proof XML, and the PAREq fields as proof of enrollment checking for any payer authentication transaction that you present again because of a chargeback. Your account provider may require that you provide all data in human-readable format, so make sure that you can decode the PAREq and PAREs. For example enrollment replies, see ["Transaction Reply for Visa with Verified by Visa," page 97](#). The replies are similar for all card types. Although the proof XML field is shown only in the Visa card replies, this field is returned for all card types.

Payment card companies have implemented the [3D Secure](#) protocol differently throughout the world. CyberSource recommends that you contact your merchant account provider to find out what is required. For more information on decrypting and providing the PAREs, contact your account manager.

Payer Authentication Reports

This chapter describes the reports that you can download from the Business Center. All reports on the production servers are retained for 16 months although the transaction history is kept in the database for six months only. All reports on the test servers are deleted after two weeks. Only transactions that were processed are reported. Those that resulted in system error or time-out are not. For more information about API replies and their meanings, see [Appendix A, "API Fields," on page 78](#).



Important

To obtain the reports, you must file a support ticket in the Support Center.

Payer Authentication Summary Report

This daily, weekly, and monthly summary report shows for each currency and type of card that you support the performance of the enrollment and validation services as number of transactions and total amount for groups of transactions. You can use this information to estimate how your transactions are screened by Payer Authentication: successful, attempted, and incomplete authentication. The cards reported are Visa, Mastercard, Maestro, American Express, JCB, and Diners Club. This daily report is generally available by 7:00 AM Eastern Time. The data in this report remains available for six months.

Downloading the Report

To view a report, follow these steps:

Step 1 In the navigation pane, select **Reports > Report Search**.

Figure 15 Report Search Window

Report Search [I need help with this page.](#)

To view or download reports, select the report and the time period. To access reports to which you are no longer subscribed, select "All".

Report Search Criteria

Report: Payer Authentication Report

Frequency: Daily

Daily Report Search

Date: April 9 2006

Reports for Apr 09, 2006

No Reports Available

Downloadable Reports for Apr 09, 2006

No Reports Available

Step 2 Select the report and the type that you want to see.

The type of report that you choose (daily, weekly, or monthly) determines the date or time range that appears below.

Step 3 Select the appropriate date or time range and submit your search request.

- If reports are available, a list appears.

Figure 16 Report Search Results

Report Search Results

Search Parameters: Report = All , Frequency = Daily , Date = Mar 30, 2006

Reports

Report Name
Payer Authentication Report

Downloadable Reports

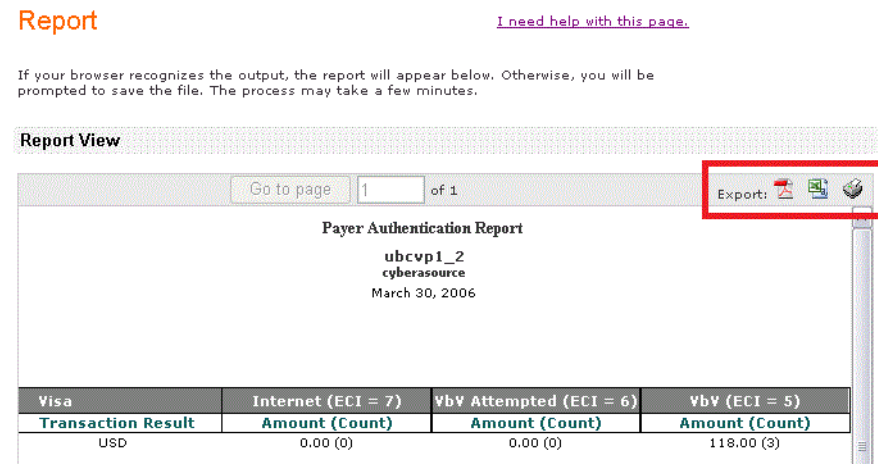
No Reports Available

- If no reports are available, the Business Center displays the message *No Reports Available*.

Step 4 Click **Payer Authentication Report**.

The report opens.

Figure 17 Payer Authentication Report



This report shows three successfully authenticated Visa transactions.

You can look at the report online by navigating between pages, but to store the content, export the report either in PDF format or as a spreadsheet as shown on the figure.

Matching the Report to the Transaction Search Results

You can find the transactions that are reported in the Transaction Search section of the Business Center. The figure below shows the search results that contain the transactions that appear in the above report. For more information on the search results and their details, see "Searching for Payer Authentication Details," page 106.

Figure 18 Payer Authentication Report Details

Mar 30 2006				
ubcvp1_2	1437540121000167904064	PATRICK MCMAHON	1.00 USD	Credit Card Authorization
Mar 30 2006 03:42:16 PM	1143754012100	null@cybersource.com	0771	Payer Authentication Validation
ubcvp1_2	1437543646410167904065	P MAN	101.00 USD	Credit Card Authorization
Mar 30 2006 03:41:17 PM	1143754364636	null@cybersource.com	0771	Payer Authentication Validation
ubcvp1_2	1437538846880167904064	PATRICK MCMAHON	16.00 USD	Credit Card Authorization
Mar 30 2006 03:40:09 PM	1143753884687	null@cybersource.com	0771	Payer Authentication Validation

Interpreting the Report

The header of all reports shows the title, the ID of the user who downloaded the report, the merchant ID, and the date or date range of the report. The report is divided by card type. In each section, all currencies are reported alphabetically. For each currency, you receive a summary of your Payer Authentication validation results displayed as total amount and number of transactions. The table below summarizes in the last two columns.

Table 16 Payer Authentication Report Interpretation

Card Type	Interpretation	Protected?	Reported	
			Commerce Indicator	ECI
Visa, American Express, and JCB	No authentication	No	Internet	7
	Recorded attempt to authenticate	Yes	VbV, Aesk, or JS Attempted	6
	Successful authentication	Yes	VbV, JS, or Aesk	5
Mastercard and Maestro	No authentication	No	Internet ²	7 ¹
	Incomplete authentication	No	SPA Failure ³	1
	Successful authentication	Yes	SPA	2
Diners Club	No authentication	No	Internet	7
	Recorded attempt to authenticate	Yes	PB Attempted	6
	Successful authentication	Yes	PB	5

¹ Although the report heading is 7, you receive a collection indicator value of 1, or the reply field is empty.
² Although the report heading is Internet, you receive `spa_failure` in the commerce indicator reply field.
³ Although the report heading is SPA Failure, you receive `spa` in the commerce indicator reply field.

Transactions are divided into two groups: those for which you are protected and those for which you are not:

- For Visa, American Express, JCB, and Diners Club: liability shift for VbV and VbV attempted
- For Mastercard and Maestro: liability shift only for SPA
- For all other results: no liability shift

Comparing Payer Authentication and Payment Reports

You may see differences between the Payer Authentication report and the payment reports because an authenticated transaction may not be authorized.

The values (amounts and counts) that you see in the Payer Authentication report may not match exactly your other sources of reconciliation because this report shows the transactions that were validated by Payer Authentication, not necessarily the transactions that were authorized. You are even more likely to see reconciliation discrepancies if you process your authorizations outside of CyberSource.

Example Payer Authentication Reports Compared to Payment Reports

For 10,000 orders, you may receive the following results:

- 9900 successful enrollment checks (Payer Authentication report)
- 9800 successful authentication checks (Payer Authentication report)
- 9500 successful authorization checks (Payment report)

The amounts and numbers can be higher in the Payer Authentication report than in the payment reports. In this example, you would see the results of the first two numbers in the Payer Authentication report and the last one in the payment reports.

To reconcile your reports more easily when using Payer Authentication, we recommend that you attempt to authenticate the same amount that you want to authorize.

Payer Authentication Detail Report

This section describes the XML report that you download when you click the Export to XML feature in the Payer Authentication details page of the Business Center. The data in this report remains available for 12 months. You can obtain the DTD in the **Reports > DTDs** section of the Business Center.

File Name

The file that you download is named according to this format:

<MerchantID>-<RequestID>-<TransactionType>.xml

Example example_merchant-18843407700000167904548-ics_pa_enroll.xml

Date and Time

In the report, the date and time are shown in this format:

YYYY-MM-DDTHH:MM:SS[+ | -]HH:MM:

- YYYY-MM-DD is the year, month, and day.
- THH:MM:SS is the time (hours, minutes, and seconds). The T separates the date and the time.
- [+ | -]HH:MM is the time zone's offset from Greenwich Mean Time (GMT), with HH representing hours and MM representing minutes. The number is prefixed by either a plus (+) or minus (-) to indicate whether the offset adds to or subtracts from GMT. For example, the offset for Pacific Daylight Time (PDT) is -07:00.

Example 2016-07-31T16:31:18-07:00 equals **July 31, 2016, at 16:31:18 (4:31:18 p.m. PDT)**

Report

<Result>

The <Result> element is the root element of the report.

```
<Result>
  (PayerAuthDetail+)
</Result>
```

Table 17 Child Elements of <Report>

Element Name	Description
<PayerAuthDetail>	Contains the transaction in the report. For a list of child elements, see <PayerAuthDetail> .

Example <Report> Element

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE Report SYSTEM "https://ebctest.cybersource.com/ebctest/reports/dtd/
payerauthdetails.dtd">
<Result>
  <PayerAuthDetail>
    ...
  </PayerAuthDetail>
</Result>
```

<PayerAuthDetail>

The <PayerAuthDetail> element contains information about a single transaction.

```
<PayerAuthDetail>
  (RequestID)
  (MerchantID)
  (TransactionDate)
  (TransactionType)
  (ProofXML)?
  (VEReq)?
  (VERes)?
  (PAREq)?
  (PAREs)?
  (AuthInfo)?
</PayerAuthDetail>
```

Table 18 Child Elements of <PayerAuthDetail>

Element Name	Description	Type & Length
<RequestID>	Unique identifier generated by CyberSource for the transaction. This field corresponds to the requestID API field.	Numeric (26)
<MerchantID>	CyberSource merchant ID used for the transaction.	String (30)
<TransactionDate>	Date on which the transaction was processed.	DateTime (25)
<TransactionType>	CyberSource service requested in SCMP format. This field can contain one of the following values: <ul style="list-style-type: none"> ■ ics_auth: Card authorization service ■ ics_pa_enroll: Payer Authentication Enrollment Check ■ ics_pa_validate: Payer Authentication Validation 	String (20)
<ProofXML>	Data that includes the date and time of the enrollment check and the VEReq and VERes elements. This field corresponds to the payerAuthEnrollReply_proofXML API field. For a list of child elements, see "ProofXML," page 102 .	String (1024)
<VEReq>	Verify Enrollment Request (VEReq) sent by the merchant's server to the directory server and by the directory server to the ACS to determine whether authentication is available for the customer's card number. For a list of child elements, see "<VEReq>," page 127 .	
<VERes>	Verify Enrollment Response (VERes) sent by the directory server. For a list of child elements, see "<VERes>," page 128 .	
<PAREq>	Payer Authentication Request message that you send to the ACS through the payment card company. Corresponds to the payerAuthEnrollReply_paReq API field. For a list of child elements, see "<PAREq>," page 129 .	
<PAREs>	Payer Authentication Response message sent by the ACS. For a list of child elements, see "<PAREs>," page 130 .	
<AuthInfo>	Address and card verification data. For a list of child elements, see "<AuthInfo>," page 132 .	

Example <PayerAuthDetail> Element

```

<PayerAuthDetail>
  <RequestID>0004223530000167905139</RequestID>
  <MerchantID>example_merchant</MerchantID>
  <TransactionDate>2007-07-25T18:23:22-07:00</TransactionDate>
  <TransactionType>ics_pa_enroll</TransactionType>
  <ProofXML>
    ...
  </ProofXML>
  <VEReq>
    ...
  </VEReq>
  <VERes>
    ...
  </VERes>
  <PAREq>
    ...
  </PAREq>
  <PAREs>
    ...
  </PAREs>
</PayerAuthDetail>

```

<ProofXML>

The `<ProofXML>` element contains data that includes the date and time of the enrollment check and the `VEReq` and `VERes` elements. This element corresponds to the **payerAuthEnrollReply_proofXML** API field.

```

<ProofXML>
  (Date)
  (DSURL)
  (PAN)
  (AcqBIN)
  (MerID)
  (Password)
  (Enrolled)
</ProofXML>

```

Table 19 Child Elements of <ProofXML>

Element Name	Description	Type & Length
<Date>	Date when the proof XML is generated. Note Although the date and time should appear sequentially during all stages of the processing of an order, they may not because of differing time zones and synchronization between servers.	DateTime (25)
<DSURL>	URL for the directory server where the proof XML originated.	String (50)

Table 19 Child Elements of <ProofXML> (Continued)

Element Name	Description	Type & Length
<PAN>	Customer's masked account number. This element corresponds to the payerAuthEnrollReply_proxyPAN API field.	String (19)
<AcqBIN>	First six digits of the acquiring bank's identification number.	Numeric (6)
<MerID>	Identifier provided by your acquirer; used to log in to the ACS URL.	String (24)
<Password>	Merchant's masked authentication password to the ACS; provided by your acquirer. Applies only to cards issued outside the U.S.	String (8)
<Enrolled>	Result of the enrollment check. This field can contain one of these values: <ul style="list-style-type: none"> ■ Y: Authentication available. ■ N: Cardholder not participating. ■ U: Unable to authenticate regardless of the reason. 	String (1)

Example <ProofXML> Element

```

<ProofXML>
  <Date>20070725 11:18:51</Date>
  <DSURL>https:123.456.789.01:234/DSMsgServlet</DSURL>
  <PAN>XXXXXXXXXXXX0771</PAN>
  <AcqBIN>123456</AcqBIN>
  <MerID>4444444</MerID>
  <Password />
  <Enrolled>Y</Enrolled>
</ProofXML>

```

<VEReq>

The <VEReq> element contains the enrollment check request data.

```

<VEReq>
  (PAN)
  (AcqBIN)
  (MerID)
</VEReq>

```

Table 20 Child Elements of <VEReq>

Element Name	Description	Type & Length
<PAN>	Customer's masked account number. This element corresponds to the payerAuthEnrollReply_proxyPAN API field.	String (19)
<AcqBIN>	First six digits of the acquiring bank's identification number.	Numeric (6)
<MerID>	Identifier provided by your acquirer; used to log in to the ACS URL.	String (24)

Example <VEReq> Element

```

<VEReq>
  <PAN>XXXXXXXXXXXX0771</PAN>
  <AcqBIN>123456</AcqBIN>
  <MerID>example</MerID>
</VEReq>

```

<VERes>

The <VERes> element contains the enrollment check reply data.

```

<VERes>
  (Enrolled)
  (AcctID)
  (URL)
</VERes>

```

Table 21 Child Elements of <VERes>

Element Name	Description	Type & Length
<Enrolled>	Result of the enrollment check. This field can contain one of these values: <ul style="list-style-type: none"> ■ Y: Authentication available. ■ N: Cardholder not participating. ■ U: Unable to authenticate regardless of the reason. 	String (1)
<AcctID>	Masked string used by the ACS.	String (28)
<URL>	URL of Access Control Server where to send the PAREq. This element corresponds to the payerAuthEnrollReply_acsURL API field.	String (1000)

Example <VERes> Element

```

<VERes>
  <Enrolled>Y</Enrolled>
  <AcctID>NDAXMjAwMTAxMTAwMDc3MQ==</AcctID>
  <URL>https://www.example_url.com</URL>
</VERes>

```

<PAREq>

The <PAREq> element contains the payer authentication request message. This element corresponds to the **payerAuthEnrollReply_paReq** API field.

```
<PAREq>
  (AcqBIN)
  (MerID)
  (Name)
  (Country)
  (URL)
  (XID)
  (Date)
  (PurchaseAmount)
  (AcctID)
  (Expiry)
</PAREq>
```

Table 22 Child Elements of <PAREq>

Element Name	Description	Type & Length
<AcqBIN>	First six digits of the acquiring bank's identification number.	Numeric (6)
<MerID>	Identifier provided by your acquirer; used to log in to the ACS URL.	String (24)
<Name>	Merchant's company name.	String (25)
<Country>	Two-character code for the merchant's country of operation.	String (2)
<URL>	Merchant's business web site.	String
<XID>	Unique transaction identifier generated by CyberSource for each Payment Authentication Request (PAREq) message. The PAREs sent back by the issuing bank contains the XID of the PAREq. To ensure that both XIDs are the same, compare it to the XID in the reply. To find all requests related to a transaction, you can also search transactions for a specific XID.	String (28)
<Date>	Date and time of request. Note Although the date and time should appear sequentially during all stages of the processing of an order, they may not because of differing time zones and synchronization between servers.	DateTime (25)
<Purchase Amount>	Authorization amount and currency for the transaction. This element corresponds to the totals of the offer lines or from the following fields: ■ ccAuthReply_amount (see <i>Credit Card Services Using the Simple Order API</i> [PDF HTML]) or purchaseTotals_grandTotalAmount from external data.	Amount (15)
<AcctID>	Masked string used by the ACS.	String (28)
<Expiry>	Expiration month and year of the customer's card.	Number (4)

Example <PAREq> Element

```

<PAREq>
  <AcqBIN>123456</AcqBIN>
  <MerID>444444</MerID>
  <Name>example</Name>
  <Country>US</Country>
  <URL>http://www.example.com</URL>
  <XID>fr2VCDrbEdyC37MOPfIzMwAHBwE=</XID>
  <Date>2007-07-25T18:18:51-07:00</Date>
  <PurchaseAmount>1.00 USD</PurchaseAmount>
  <AcctID>NDAXMjAwMTAxMTAwMDc3MQ==</AcctID>
  <Expiry>0811</Expiry>
</PAREq>

```

<PAREs>

The <PAREs> element contains the payer authentication reply message.

```

<PAREs>
  (AcqBIN)
  (MerID)
  (XID)
  (Date)
  (PurchaseAmount)
  (PAN)
  (AuthDate)
  (Status)
  (CAVV)
  (ECI)
</PAREs>

```

Table 23 Child Elements of <PAREs>

Element Name	Description	Type & Length
<AcqBIN>	First six digits of the acquiring bank's identification number.	Numeric (6)
<MerID>	Identifier provided by your acquirer; used to log in to the ACS URL.	String (24)
<XID>	XID value returned in the customer authentication reply. This element corresponds to the payerAuthEnrollReply_xid and payerAuthValidateReply_xid API fields.	String (28)
<Date>	Date and time of request. Note Although the date and time should appear sequentially during all stages of the processing of an order, they may not because of differing time zones and synchronization between servers.	DateTime (25)

Table 23 Child Elements of <PAREs> (Continued)

Element Name	Description	Type & Length
<PurchaseAmount>	Authorization amount and currency for the transaction. This element corresponds to the totals of the offer lines or from the following fields: <ul style="list-style-type: none"> ■ ccAuthReply_amount (see <i>Credit Card Services Using the Simple Order API</i> [PDF HTML]) or purchaseTotals_grandTotalAmount from external data 	Amount (15)
<PAN>	Customer's masked account number. This element corresponds to the payerAuthEnrollReply_proxyPAN API field.	String (19)
<AuthDate>	Date and time of request. Note Although the date and time should appear sequentially during all stages of the processing of an order, they may not because of differing time zones and synchronization between servers.	DateTime (25)
<Status>	Result of the authentication check. This field can contain one of these values: <ul style="list-style-type: none"> ■ Y: Customer was successfully authenticated. ■ N: Customer failed or cancelled authentication. Transaction denied. ■ U: Authenticate not completed regardless of the reason. ■ A: Proof of authentication attempt was generated. 	String (1)
<CAVV>	CAVV (Visa, American Express, JCB, and Diners Club cards = * below) or AAV (Mastercard, and Maestro cards = ** below) returned in the customer authentication reply. This element corresponds to the payerAuthValidateReply_cavv (*) and payerAuthValidateReply_ucafAuthenticationData (**) API fields.	String (50)
<ECI>	Electronic commerce indicator returned in the customer authentication reply. This element corresponds to the payerAuthValidateReply_eci (*) and payerAuthValidateReply_ucafCollectionIndicator (**) API fields.	Numeric (1)

Example <Card> Element

```

<PAREs>
  <AcqBIN>123456</AcqBIN>
  <MerID>4444444</MerID>
  <XID>Xe5DcjrqEdyC37MOPfIzMwAHBwE=</XID>
  <Date>2007-07-25T20:05:18-07:00</Date>
  <PurchaseAmount>1002.00 USD</PurchaseAmount>
  <PAN>0000000000000771</PAN>
  <AuthDate>2007-07-25T20:05:18-07:00</AuthDate>
  <Status>Y</Status>
  <CAVV>AAAAAAAAAAAAAAAAAAAAAAAAAAAA=</CAVV>
  <ECI>5</ECI>
</PAREs>

```

<AuthInfo>

The <AuthInfo> element contains address and card verification information.

```

<AuthInfo>
  (AVSResult)
  (CVVResult)
</AuthInfo>

```

Table 24 Child Elements of <AuthInfo>

Element Name	Description	Type & Length
<AVSResult>	Optional results of the address verification test. See ccAuthReply_avsCode or afsService_avsCode (if from external data) in <i>Credit Card Services Using the Simple Order API</i> (PDF HTML).	String (1)
<CVVResult>	Optional results of the card verification number test. See ccAuthReply_cvvCode or afsService_cvCode (if from external data) in <i>Credit Card Services Using the Simple Order API</i> (PDF HTML).	String (1)

Example <AuthInfo> Element

```

<AuthInfo>
  <AVSResult>Y</AVSResult>
  <CVVResult/>
</AuthInfo>

```

Examples

These examples show a complete transaction: the failed enrollment check (enrolled card) and the subsequent successful authentication.

Failed Enrollment Check

```
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE Result SYSTEM "https://ebc.cybersource.com/ebc/reports/dtd/
payerauthdetails.dtd">
<Result>
  <PayerAuthDetail>
    <RequestID>1895549430000167904548</RequestID>
    <MerchantID>sample_merchant_id</MerchantID>
    <TransactionDate>Sep 11 2007 04:55:44 PM</TransactionDate>
    <TransactionType>ics_pa_enroll</TransactionType>
    <ProofXML>
      <Date>20070911 16:51:00</Date>
      <DSURL>https:123.456.789.01:234/DSMsgServlet</DSURL>
      <PAN>XXXXXXXXXXXX0771</PAN>
      <AcqBIN>123456</AcqBIN>
      <MerID>4444444</MerID>
      <Password />
      <Enrolled>Y</Enrolled>
    </ProofXML>
    <VEReq>
      <PAN>XXXXXXXXXXXX0771</PAN>
      <AcqBIN>123456</AcqBIN>
      <MerID>example</MerID>
    </VEReq>
    <VERes>
      <Enrolled>Y</Enrolled>
      <AcctID>NDAXMjAwMTAxMTAwMDc3MQ==</AcctID>
      <URL>https://www.sample_url.com</URL>
    </VERes>
    <PAREq>
      <AcqBIN>123456</AcqBIN>
      <MerID>example</MerID>
      <Name>Merchant Name</Name>
      <Country>US</Country>
      <URL>http://www.merchant_url.com</URL>
      <XID>2YNANGDBEdydJ6WI6aFJWAAHBwE=</XID>
      <Date>Sep 11 2007 04:51:00 PM</Date>
      <PurchaseAmount>1.00 USD</PurchaseAmount>
      <AcctID>NDAXMjAwMTAxMTAwMDc3MQ==</AcctID>
      <Expiry>0811</Expiry>
    </PAREq>
  </PayerAuthDetail>
</Result>
```

Successful Authentication

```

<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE Result SYSTEM "https://ebc.cybersource.com/ebc/reports/dtd/
payerauthdetails.dtd">
<Result>
  <PayerAuthDetail>
    <RequestID>1895549900000167904548</RequestID>
    <MerchantID>ics2test</MerchantID>
    <TransactionDate>Sep 11 2007 04:56:31 PM</TransactionDate>
    <TransactionType>ics_pa_validate</TransactionType>
    <PRes>
      <AcqBIN>469216</AcqBIN>
      <MerID>6678516</MerID>
      <XID>2YNANGDBEdydJ6WI6aFJWAAHBwE=</XID>
      <Date>Sep 11 2007 04:51:00 PM</Date>
      <PurchaseAmount>1.00 USD</PurchaseAmount>
      <PAN>0000000000000771</PAN>
      <AuthDate>Sep 11 2007 04:51:00 PM</AuthDate>
      <Status>Y</Status>
      <CAVV>AAAAAAAAAAAAAAAAAAAAAAAAAAAA=</CAVV>
      <ECI>5</ECI>
    </PRes>
  </PayerAuthDetail>
</Result>

```

Rules-Based Payer Authentication

Rules-based Payer Authentication enables you to specify rules that define how transactions are authenticated by a [3D Secure](#) card authentication program. For example, you can decide to turn off active authentication for transactions that would otherwise require customer interaction to avoid degrading the customer experience. However, you may decide to authenticate customers from card-issuing banks that use risk-based authentication because the authentication is performed without customer interaction.

To enable your account for rules-based Payer Authentication, contact your CyberSource sales representative.

**Note**

Depending on the card type and country, active mandates will supersede rules-based Payer Authentication and will revert to traditional 3D Secure.

Available Rules

By default, when Payer Authentication is enabled on your account, authentication is attempted on all transactions.

For transaction types that are not bypassed, you may be required to complete authentication.

You can enable one or more of the following authentication transaction types. Any transaction types that are set to bypass authentication will return the reason code 100. If you receive reason code 475 from the enrollment check, you will be required to complete validation even if no customer participation is needed.

Table 25 Rules-Based Payer Authentication Types

Authentication Type	Description	Test Case Example
Active Authentication	Customer is prompted to authenticate.	Test Case 1: Verified by Visa Card Enrolled: Successful Authentication
Activation During Shopping	Customer is prompted to enroll in a 3D Secure card authentication program. This transaction type provides full 3D Secure benefits.	Test Case 3: Verified by Visa Card Enrolled: Attempts Processing
Non-Participating Bank	Card-issuing bank does not participate in a 3D Secure program. When enrollment is checked, this transaction type provides full 3D Secure benefits, including fraud chargeback liability shift for customer “I didn’t do it” transactions and interchange reduction of 5-59 basis points.	Test Case 9: Verified by Visa Card Not Enrolled
Passive Authentication	Customer is not prompted to authenticate. This transaction type provides full 3D Secure benefits when passive authentication is completed.	Test Case 12: Verified by Visa Enrollment RIBA_PASS
Risk-Based Bank	Card-issuing bank uses risk-based authentication. The likely outcome is the customer is not challenged to enter credentials. Most authentications proceed without customer interaction. This transaction type provides full 3D Secure benefits.	Test Case 14: Verified by Visa Enrollment RIBA

API Replies



Note

By default, API replies that are specifically associated with rules-based Payer Authentication are turned off. Contact CyberSource Customer Support to enable these API replies when rules are triggered.

Bypassed Authentication Transactions

When card authentication is bypassed as a result of your rules-based Payer Authentication configuration, you can receive the following value for enrollment checks:

- **payerAuthEnrollReply_veresEnrolled** = B (indicates that authentication was bypassed)

Risk-Based Bank Transactions

When a transaction involves a card-issuing bank that supports risk-based authentication, you may receive the following authentication path replies, depending on whether the card-issuing bank deems the transaction risky:

■ `payerAuthEnrollReply_authenticationPath`

- `= RIBA`

The card-issuing bank supports risk-based authentication, but whether the cardholder is likely to be challenged cannot be determined.

- `= RIBA_PASS`

The card-issuing bank supports risk-based authentication, and it is likely that the cardholder will not be challenged to provide credentials, also known as *silent authentication*.

Glossary

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Numerics

3D Secure Security protocol for online credit card and debit card transactions used by Verified by Visa, Mastercard SecureCode, American Express SafeKey, JCB JSecure, and Diners Club ProtectBuy.

A

AAV Account Authentication Value. Unique 32-character transaction token for a 3D Secure transaction. For Mastercard SecureCode, the AAV is named the [UCAF](#). For Verified by Visa, the AAV is named the [CAVV](#).

acquirer The financial institution that accepts payments for products or services on behalf of a merchant. Also referred to as “acquiring bank.” This bank accepts or acquires transactions that involve a credit card issued by a bank other than itself.

acquirer BIN A 6-digit number that uniquely identifies the acquiring bank. There is a different acquirer BIN for Mastercard (starts with 5) and Visa (starts with 4) for every participating acquirer.

acquiring processor Processor that provides credit card processing, settlement, and services to merchant banks.

ACS Access Control Server. The card-issuing bank’s host for the payer authentication data.

ACS URL The URL of the Access Control Server of the card-issuing bank that is returned in the reply to the request to check enrollment. This is where you must send the [PAREq](#) so that the customer can be authenticated.

ADS Activation During Shopping. The card issuer’s ability to ask the cardholder to enroll in the card authentication service when the merchant posts to the [ACS URL](#)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A (Continued)

American Express	A globally issued card type that starts with 3 and which is identified as card type 003 by CyberSource. These cards participate in a card authentication service (SafeKey) provided by 3D Secure .
API	Application Programming Interface. A specification that can be used by software components to communicate with each other.
authentication result	Raw data sent by the card issuer that indicates the status of authentication. It is not required to pass this data into the authorization.
authorization	A request sent to the card issuing bank that ensures a cardholder has the funds available on their credit card for a specific purchase. A positive authorization causes an authorization code to be generated and the funds to be held. Following a payer authentication request, the authorization must contain payer authentication-specific fields containing card enrollment details. If these fields are not passed correctly to the bank, it can invalidate the liability shift provided by card authentication. Systemic failure can result in payment card company fines.

B

base64	Standard encoding method for data transfer over the Internet.
BIN	Bank Identification Number. The 6-digit number at the beginning of the card that identifies the card issuer.

C

CAVV	Cardholder Authentication Verification Value. A base64-encoded string sent back with Verified by Visa -enrolled cards that specifically identifies the transaction with the issuing bank and Visa. Standard for collecting and sending AAV data for Verified by Visa transactions. See AAV .
CAVV algorithm	A one-digit reply passed back when the PAREs status is a Y or an A. If your processor is ATOS, this must be passed in the authorization, if available.
CVV	Card Verification Value. Security feature for credit cards and debit cards. This feature consists of two values or codes: one that is encoded in the magnetic strip and one that is printed on the card. Usually the CVV is a three-digit number on the back of the card. The CVV for American Express cards is a 4-digit number on the front of the card. CVVs are used as an extra level of validation by issuing banks.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

D

Diners Club	A globally issued card type that starts with a 3 or a 5. CyberSource identifies Diners Club cards with a card type of 005. These cards participate in a card authentication service (ProtectBuy) provided by 3D Secure
Directory Servers	The Visa and Mastercard servers that are used to verify enrollment in a card authentication service.
Discover	Primarily, a U.S. card type that starts with a 6. CyberSource identifies Discover cards with a card type of 004. These cards do not participate in a card authentication service provided by 3D Secure.

E

ECI (ECI Raw)	The numeric commerce indicator that indicates to the bank the degree of liability shift achieved during payer authentication processing.
E-Commerce Indicator	Alpha character value that indicates the transaction type, such as MOTO or INTERNET.
Enroll	CyberSource transaction type used for verifying whether a card is enrolled in the SecureCode or Verified by Visa service.

H

HTTP	Hypertext Transfer Protocol. An application protocol used for data transfer on the Internet.
HTTP POST request	POST is one of the request methods supported by the HTTP protocol. The POST request method is used when the client needs to send data to the server as part of the request, such as when uploading a file or submitting a completed form.
HTTPS	Hypertext Transfer Protocol combined with SSL/TLS (Secure Sockets Layer/Transport Layer Security) to provide secure encryption of data transferred over the Internet.

I

issuer	The bank that issued a credit card.
---------------	-------------------------------------

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

J

J/Secure	The 3D Secure program of JCB .
JCB	Japan Credit Bureau. A globally issued card type that starts with a 3. CyberSource identifies JCB cards with a card type of 007. These cards participate in a card authentication service (J/Secure) provided by 3D Secure .
Joint e-Commerce Framework Testing	Formerly known as PIT testing. This is a set of payment integration tests that simulate realistic scenarios that would have an impact on your business in a production environment. Each test is designed to ensure that your implementation of Payer Authentication services processes the data correctly. CyberSource provides you with a test plan that includes descriptions of expected results. You must schedule time with your CyberSource contact to review your test results. These tests may also be called “JEF” tests.

M

Maestro	<p>A card brand owned by Mastercard that includes several debit card BINs within the U.K., where it was formerly known as Switch, and in Europe. Merchants who accept Maestro cards online are required to use SecureCode, Mastercard’s card authentication service. CyberSource identifies Maestro cards with the 024 and 042 card types.</p> <p>Note that many international Maestro cards are not set up for online acceptance and cannot be used even if they participate in a SecureCode card authentication program.</p>
Mastercard	A globally issued card that includes credit and debit cards. These cards start with a 5. CyberSource identifies these cards as card type 002 for both credit and debit cards. These cards participate in a card authentication service (SecureCode) provided by 3D Secure .
MD	Merchant-defined Data that is posted as a hidden field to the ACS URL . You can use this data to identify the transaction on its return. This data is used to match the response from the card-issuing bank to a customer’s specific order. Although payment card companies recommend that you use the XID , you can also use data such as an order number. This field is required, but including a value is optional. The value has no meaning for the bank, and is returned to the merchant as is.
Merchant ID	Data that must be uploaded for the Mastercard and Visa card authentication process for each participating merchant. The Merchant ID is usually the bank account number or it contains the bank account number. The data is stored on the Directory Servers to identify the merchant during the enrollment check.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

M (Continued)

MPI Merchant Plug-In. The software used to connect to [Directory Servers](#) and to decrypt the [PAREs](#).

P

PAN Primary Account Number. Another term for a credit card number.

PAReq Payer Authentication Request. Digitally signed base64-encoded payer authentication request message, containing a unique transaction ID, that a merchant sends to the card-issuing bank. Send this data without alteration or decoding. Note that the field name has a lowercase “a” (PaReq), whereas the message name has an uppercase “A” (PAReq).

PARes Payer Authentication Response. Compressed, base64-encoded response from the card-issuing bank. Pass this data into CyberSource for validation.

PARes Status Payer Authentication Response status. One-character length status passed back by Visa and Mastercard that is required data for Asia, Middle East, and Africa Gateway authorizations.

processor Financial entity that processes payments. Also see [acquiring processor](#).

ProofXML CyberSource field that contains the [VEReq](#) and [VERes](#) for merchant storage. Merchants can use this data for future chargeback repudiation.

ProtectBuy Trademarked name for the Diners Club card authentication service.

R

request ID A 22- or 23-digit number that uniquely identifies each transaction sent to CyberSource. Merchants should store this number for future reference.

risk-based authentication Risk-based authentication is provided by the card-issuing bank. The card-issuing bank gathers a cardholder’s transaction data or leverages what data they have to silently authenticate the cardholder based on the degree of risk that they perceive the transaction to have. They base their risk assessment on factors such as cardholder spending habits, order or product velocity, the device IP address, order amount, and so on.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

S

SafeKey	Trademarked name for the American Express card authentication service.
SCMP API	CyberSource's legacy name-value pair API that has been superseded by the Simple Order API .
SecureCode	Trademarked name for Mastercard's card authentication service.
Simple Order API	CyberSource's current API, which provides three ways to access CyberSource services: name-value pair (NVP), XML, and SOAP.
Solo	A debit card type that was owned by Maestro. It was permanently discontinued March 31, 2011.
Switch	See Maestro .

T

TermURL	Termination URL on a merchant's web site where the card-issuing bank posts the payer authentication response (PAREs) message.
----------------	---

U

UCAF	Universal Cardholder Authentication Field. A base64-encoded string sent back with Mastercard SecureCode -enrolled cards that specifically identifies the transaction with the issuing bank and Mastercard. Standard for collecting and sending AAV data for Mastercard SecureCode transactions. See AAV .
UCAF collection indicator	Value of 1 or 2 that indicates whether a Mastercard cardholder has authenticated themselves or not.

V

validate	CyberSource service for decoding and decrypting the PAREs to determine success. The <i>validate</i> service returns the needed values for authorization.
VEReq	Verify Enrollment Request. Request sent to the Directory Servers to verify that a card is enrolled in a card authentication service.
VERes	Verify Enrollment Response. Response from the Directory Servers to the VEReq .

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**V (Continued)**

VERes enrolled Verify Enrollment Response enrolled. One-character length status passed back by Visa and Mastercard that is required data for Asia, Middle East, and Africa Gateway authorizations.

Verified by Visa (VbV) Trademarked name for Visa's card authentication service.

Visa A globally issued card that includes credit and debit cards. These cards start with a 4. CyberSource identifies these cards as card type 001 for both credit and debit cards. These cards participate in a card authentication service ([Verified by Visa](#)) provided by [3D Secure](#).

X

XID String used by both Visa and Mastercard which identifies a specific transaction on the [Directory Servers](#). This string value should remain consistent throughout a transaction's history.

Index

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Numerics

16- and 19-digit Visa cards [37](#)

A

AAV

payerAuthValidateReply_
ucafAuthenticationData field [93](#)

Access Control Server (ACS) [16](#)

aesk_attempted [60](#)

AIBMS

commerce indicator, enrollment [87](#)
commerce indicator, validation [91](#)

American Express

card tests [60](#)
formal payer authentication implementation
testing [14](#)
SafeKey [11](#)
validation results [60](#)

application results in Business Center [106](#)

Asia, Middle East, and Africa Gateway

payerAuthEnrollReply_veresEnrolled
field [89](#)
payerAuthValidateReply_paresStatus
field [92](#)

authentication form

from issuing bank [16](#)
URL [85](#)

authorizations, expired or multiple [23](#)

B

Barclays

commerce indicator, enrollment [87](#)
commerce indicator, validation [91](#)

Barclays, enrollment XID [89](#)

Barclays, validation XID [93](#)

base64 format, converting [23](#)

Brazil transactions (Verified by Visa)

payerAuthEnrollService_MCC field [82](#)
payerAuthEnrollService_mobilePhone
field [82](#)
payerAuthEnrollService_
overridePaymentMethod field [82](#)
payerAuthEnrollService_productCode
field [82](#)

C

card authorization with payer authentication [23](#)

CAVV [90](#)

chargeback protection

subscription payments [23](#)

check enrollment service

description [11](#)
requesting [15](#)

credit card types accepted [81](#)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

D

- data storage [117](#)
- detail report [123](#)
- Diners Club
 - ProtectBuy [11](#)
- Diners Club card tests [72](#)
- Diners Club ProtectBuy
 - validation results [72](#)

E

- e-commerce indicator (ECI) [92](#)
- enrolled card
 - password [12](#)
- enrollment data storage [117](#)
- example code
 - payerAuthEnrollService [96](#)
 - payerAuthValidateService [100](#)

F

- FDC Germany
 - commerce indicator, enrollment [87](#)
 - commerce indicator, validation [91](#)

I

- issuing bank
 - authentication form [16](#)
 - authentication form, URL [85](#)
 - CAVV [90](#)
 - enrollment check [15](#)

J

- J/Secure [11](#)
- J/Secure, validation results [66](#)
- JCB
 - formal payer authentication implementation
 - testing [14](#)
 - J/Secure [11](#)
 - tests [66](#)

M

- Maestro
 - (U.K. domestic) tests [46](#)
 - formal payer authentication implementation
 - testing [14](#)
 - tests [55](#)
- Maestro cards
 - SecureCode [11](#)
- Mastercard
 - formal payer authentication implementation
 - testing [14](#)
 - SecureCode [11](#)
- Mastercard Directory Server [15](#)
- Mastercard SecureCode
 - validation results [46](#)
- Mastercard tests [46](#)

P

- PAReq [16](#)
- PAReq and PARES storage [117](#)
- PARES [143](#)
- password
 - for enrolled card [12](#)
- password, enrolled card [16](#)
- payer authentication details
 - enrolled card [109](#)
 - storage duration [109](#)
 - unenrolled card [113](#)
- payer authentication report
 - comparing to payment reports [122](#)
 - frequency [118](#)
 - interpreting [120](#)
 - transactions reported [118](#)
- payer authentication search options [116](#)
- payerAuthEnrollService
 - example code [96](#)
- payerAuthValidateService
 - example code [100](#)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

pb_attempted [72](#)
proofXML storage [117](#)

R

reason codes
 validation [93](#)
reports
 detail [123](#)
 detail, XML format [124](#)
 downloading summary report [119](#)
 retention time limit [118](#)
 summary [118](#)
risk-based authentication [136](#)

S

SafeKey [11](#)
SecureCode [11](#)
settling transactions, time limit [117](#)
storing payer authentication data [109](#)
Streamline
 commerce indicator, enrollment [87](#)
 commerce indicator, validation [91](#)
 ECI raw [92](#)
subscription payments, chargeback
 protection [23](#)
summary report [118](#)

T

testing [31](#)
tests
 American Express [60](#)
 Diners Club cards [72](#)
 JCB J/Secure [66](#)
 Maestro cards [55](#)
 Mastercard cards [46](#)
 Visa cards [37](#)
transaction details
 enrollment check information [106](#)
transaction history, retention time limit [118](#)

transaction search
 authenticated card [112](#)
 enrolled card [106](#)
 unenrolled card [113](#)
 using [106](#)

U

unenrolled card, payer authentication details [113](#)

V

validate authentication service
 description [11](#)
 requesting [17](#)
vbv_attempted [37](#)
Verified by Visa
 Brazilian transaction requirements, account
 type [82](#)
 Brazilian transaction requirements, merchant
 category code [82](#)
 Brazilian transaction requirements, mobile
 phone [82](#)
 Brazilian transaction requirements, product
 code [82](#)
 validation results [37, 60](#)
Visa
 formal payer authentication implementation
 testing [14](#)
 Verified by Visa [11](#)
Visa card tests [37](#)
Visa Directory Server [15](#)
Visa Vale Alimentacao (VSAVA) [82](#)
Visa Vale Refeicao (VSAVR) [82](#)
Visa, 16- and 19-digit cards [37](#)

X

XID
 API field [89](#)
 validate in reply [93](#)
XML report sample [133](#)