RuPay Integration Guide

SCMP API

Payer Authentication

cybersource
A Visa Solution

Version: 22.01

Contents

Recent Revisions to This Document

22.01

Added Seamless Flow section to manual.

19.01

Initial release.

About This Guide

Audience and Purpose

This guide is written for application developers who want to use the SCMP API to integrate Payer Authentication services into their order management system to process RuPay payments.

It describes the tasks you must perform in order to complete this integration. Implementing Payer Authentication services requires software development skills. You must write code that uses the API request and response fields to integrate payer authentication services into your existing order management system.

Scope

This guide describes how to use the SCMP API to integrate payer authentication services with your order management system. It does not describe how to get started using the SCMP API nor does it explain how to use services other than payer authentication. For that information, see the following *Related Documents* section.

Conventions

The following special statements are used in this document:

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

Warning: A *Warning* contains information or instructions, which, if not heeded, can result in a security risk, irreversible loss of data, or significant cost in time or revenue or both.

Related Documentation

Refer to the Support Center for complete technical documentation:

- *Getting Started with Cybersource Advanced for the SCMP API* describes how to get started using the SCMP API. (PDF)

- *Decision Manager Developer Guide Using the SCMP API* describes how to integrate Decision Manager, a fraud detection service, with your order management system. (PDF)
- *Credit Card Services Using the SCMP API* describes how to integrate payment processing services into your business. (PDF)
- *Reporting Developer Guide* describes how to view and configure Business Center reports. (PDF)
- The API Versions page provides information about the API versions.
- The *SCMP API Field Reference Guide* (HTML) provides information about the individual API fields.

Customer Support

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

http://www.cybersource.com/support

Overview of RuPay Payer Authentication

Cybersource payer authentication services provide support to your web store for card authentication services for RuPay cards. Payer authentication for RuPay uses the same API services provided by Cybersource for other card brands. If you are currently using Cybersource payer authentication services for other card brands, you can enhance your existing integration to send the additional fields in the request that are required for RuPay cards. Payer authentication provides these services:

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

Unlike Visa and Mastercard cards, authentication is mandatory for RuPay cards. Without authentication, authorization cannot be performed and the transaction is declined by the RuPay network.

Authentication Modes

RuPay authenticates the cardholder in two ways:

- Redirection—This mode of payer authentication with a one-time password has the issuer hosting the password entry page. When a cardholder is being authenticated during a transaction, the issuer sends a password to the cardholder's phone so that the cardholder can enter the password into a displayed entry form. If the entered password matches the password that was sent, the cardholder is authenticated and the transaction can proceed. In the Redirection mode, the password authentication is directed away from the merchant to a URL that the issuer sends. The issuer hosts the password entry form at this URL. This redirection from the merchant to the issuer can cause lag time in the transaction processing due to network traffic.

- Seamless Server to Server—This mode of payer authentication with a one-time password has the merchant hosting the password entry page. This is an improved method of authenticating with a one-time password. The process of password authenticating is much the same but this method keeps the hosting of the password entry page with the merchant. The cardholder does not leave the merchant's web site during authentication. Keeping hosting of the password entry page with the merchant, reduces timeouts and processes transactions faster.

The first section of this guide describes the Redirection Flow of payer authentication while the second section describes the Seamless Flow mode.

Check Enrollment Service

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. To verify that the card is enrolled in a payer authentication program, request the Enrollment Check service (VEReq).

- 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, decline the payment and ask the customer for another form of payment.

Check Enrollment Request

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 Payer Authentication SCMP API Developer Guide.

For RuPay, you can use the same request fields in the Check Enrollment service that you currently use for Visa and Mastercard but four additional fields are required:

- **customer_ipaddress**

The IP address must be the IP address of the customer who is making the purchase on your web site. It must not be hard-coded or contain the address of the merchant's servers. RuPay requires sending the correct IP address because it is used to manage disputes.

- **pa_http_accept**

This field must contain the value of the Accept header sent by the customer's web browser.

pa_http_user_agent

This field must contain the value of the User-Agent header sent by the customer's web browser.

customer_cc_cv_number

In addition, you can send these optional fields in the request. If they are not sent in the request, the values configured for Cybersource during onboarding are used. To minimize errors, these configured values are recommended .

- **merchant_descriptor** (name of the merchant as configured in Cybersource, 1-23 alphanumeric characters)
- **merchant_descriptor_contact** (telephone number of the merchant)
- **merchant_descriptor_streetinvoiceHeader_merchantDescriptorStreet** (street name of the merchant)
- **merchant_descriptor_stateinvoiceHeader_merchantDescriptorState** (state, must use Indian state codes)
- **merchant_descriptor_postal_code** (maximum of nine alphanumeric characters, must be valid postal code)
- **merchant_descriptor_country** (value must be 'IN')

You can send the required and optional fields listed above for other card brands to keep your integration consistent.

Check Enrollment Response

The responses are similar for all card types.

- Enrolled Cards—You receive reply flag DAUTHENTICATE if the customer's card is enrolled in a payer authentication program. When you receive this response, you can proceed to "Step 2: Authenticating Enrolled Cards."
- Cards Not Enrolled—You receive response flag SOK if the account number is not enrolled in RuPay's payer authentication program. The other services in your request are declined. When you receive this reply, you cannot proceed to validate authentication or to card authorization.

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). Use an HTTP POST request web form that contains the PAReq data, the Termination URL (TermURL), and merchant data (MD).

The MD value must be posted for RuPay. If needed, you can include it for other card brands as well.

HTML Frame for Authentication

When your customers are redirected to the ACS URL, their browsers display the frame containing the card-issuing bank's password authentication page or the option to sign up for the program (activation form).

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

- Ensure that the HTML frame is large enough to accommodate the card-issuer's authentication or activation form, and text that describes the process to the customer.
- Provide a brief message outside the HTML frame to guide customers through the process. For example, "We are processing your request. Do not click the Back button or refresh the page or this transaction may be interrupted."

HTTP Post Form

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

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

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
```

PARes Message from the RuPay Card-Issuing Bank

The card-issuing bank sends a PARes message to your TermURL in response to the PAReq data that was sent with the web form. The PARes message is sent by using an HTTP POST request and contains the result of the requested authentication.

The signed PaRes field contains a base64-encoded string with this information:

- PARes—Digitally signed payer authentication response message that contains the authentication result. (Note that while the field name has a lowercase "a" (PaRes), the message name has an uppercase "A" (PARes)).
- MD—Merchant data, which must be submitted for RuPay.

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.

Validation Service Request

When you make the validation request, you must:

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

Important: With the Simple Order API 1.128 or later, Cybersource removes all space characters during the validation service. When you use an earlier Simple Order API version, manually remove the space characters, or the validation service request fails. For the SCMP API,manually remove the space characters or the validation service request fails.

- Send the **PaRes** value to Cybersource in the signed **PaRes** field of the validation service. The response 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. Do not pass any fields that Cybersource derives from the **PaRes** value into the request because that data could be overwritten.
- Separate requests—You must manually include the validation result values (Payer Authentication response fields) in the authorization service request (Card Authorization request fields), which are listed in this table:

Identifier	Payer Authentication Response Field	Card Authorization Request Field
XID	**pa_validate_xid**	**xid**
E-commerce indicator	**pa_validate_e_commerce_indicator**	**e_commerce_indicator**

Identifier	Payer Authentication Response Field	Card Authorization Request Field
CAVV	**pa_validate_cavv**	**cavv**

If you are currently passing additional card-specific values in the Payer Authentication Validate response for Visa and Mastercard, you can continue to pass them for RuPay.

Validation Service Response

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

- Success—You receive the or response flag `SOK`, and other service requests, including authorization, are processed normally.
- Failure—You receive reply flag `DAUTHENTICATIONFAILED` indicating that the authentication failed, so the other services in your request were not processed.
- 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.

Pass or Fail Message Page

After authentication is complete, redirect the customer to a page containing a success or failure message. Ensure that all messages that display to customers are accurate, complete, and that they address all possible scenarios for enrolled and non-enrolled cards. When authentication fails, a message such as this example, 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.
```

Example: Enrollment Service

In the enroll response, the URL returned by Cybersource provides the type of card. For instance, if a URL, includes "binType=S," the card/BIN type of the RuPay card is S, which is a single message BIN. When Cybersource returns this type of BIN, send the authorization service and capture service API requests to Cybersource at the same time.

Request

```
bill_address1=201 S. Division St.
bill_address1=201 S. Division St.
bill_city=Ann Arbor
bill_country=US
bill_state=MI
bill_zip=48104-2201
card_type=061
currency=INR
customer_cc_cv_number=123
customer_cc_expmo=12
customer_cc_expyr=2031
customer_cc_number=5082302886091
customer_email=null@cybersource.com
customer_firstname=John
customer_ipaddress=10.0.0.1
customer_lastname=Smith
customer_phone=999-999-9999
grand_total_amount=100
ics_applications=ics_pa_enroll
merchant_category_code=1234
merchant_descriptor=seller
merchant_descriptor_city=bangalore
merchant_descriptor_contact=945789541212
merchant_descriptor_country=IN
merchant_descriptor_postal_code=560078
merchant_descriptor_state=KA
merchant_id=npr_rupay
merchant_ref_number=S208441-1
pa_http_accept=accept
pa_http_user_agent=user
sender_id=ms_user
```

Response

```
URL: https://sl73cgkapq067.visa.com:10024/
```

```
ics_rcode=0
ics_rflag=DAUTHENTICATE
ics_rmsg=The cardholder is enrolled in Payer Authentication.  Please authenticate
 before proceeding with authorization.
merchant_ref_number=S208441-1
pa_enroll_acs_url=https://pnrstage.ic3.com:9448/cybersource/payerAuthentication/pa
ySecure/initiate?binType=D
pa_enroll_authentication_path=ENROLLED
pa_enroll_authentication_transaction_id=MjA3MTAwMjM1MDMyMDMxMjIxNDY=
pa_enroll_pareq=e0NCQ2l2fVQ2YVZsbjNlZlh5UzJLRzZiZ1N0c0JBQUVMdlNHTHp6MG42OTE0NC9HV2
lqMjVDUTRQcjlxbUN5TjYvVE1xV01Jejg2RkRReXN6ZTZJQUlSdVBEVnBRcWR3Mzg2Zjc5U1E5OHRVVndp
cnlibG1UOXVSUFVBbFd1elVRNFNwN1BvcS9rZS9RVGV2MS8zTkoyQXY5WS9Ob2hTcnk3VHBQQlRZTmRXN1
ZEb3JxRFp0L3poeVF3RDg4SDVWL2tLMThENzJsUEZtNTVaUlI5UGZUbk5JaFptQjYxS3BPelYwbFFTRVRK
QWxSc3doYzVWZ09UOENrYm9mNDEwYzVBVmR5dGJ0dDl1RkZkWG8vRDJiRUtoeG1UYXlXelVrQXFBRDBGTk
F1VUN5cWxBblBoQ2pJQnBTQUxiQzY1SWsxaFNwZTAyc1NkMGM4Q1ZJVHVlay81V3RPd1FjZVNUbkp5TnRE
cDZwUlVvSU94cDBZc21CeFBMa0tQYnl0d2UrRTh5T1hUa0RVZHE2b2tQWE1GamxqTmFSbFV5WGtDU2R2NE
Z4YXJTTjRaT2hmY2h0N3FzbzE0WXYwRlp3ZUxOTjFNeUgwRGNldWRFRlFLMXJNeVNINUJIQjBRVUtXdEdk
M014bTBuL2ozb2VFUEpqV1FiaTZyOWxYL1hGaE8xcTB1Z1V2TjRPNHN4dHNmeXZJZnhHemZXRXVsZzI4Y2
80TXlQZnhmazcvckNQU2FVajNoYWx3MzhUaVV5RXM4ZHJ0M2luVVlXTTA3dGJUUGJYcUx0YW50ZElGeVph
WFljbHh3ay96eDdYck5RTi9Ldy96Vml0ZzJZPQ==
pa_enroll_rcode=0
pa_enroll_rflag=DAUTHENTICATE
pa_enroll_rmsg=The cardholder is enrolled in Payer Authentication.  Please
 authenticate before proceeding with authorization.
pa_enroll_specification_version=rupay
pa_enroll_veres_enrolled=Y
pa_enroll_xid=MjA3MTAwMjM1MDMyMDMxMjIxNDY=
request_id=647024706263316997915
request_token=AxjzbwSTXsC3PqBwtooL/949TSosgFoiyDpxAgWXb6sw+6spuK+UDQAAASuY
```

Example: Validate Authentication Service

Request

```
ics_rcode=1
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
merchant_ref_number=S208441-1
pa_validate_authentication_result=0
pa_validate_authentication_status_msg=Success
pa_validate_cavv=MTAwMDAwMDAwMDAwMDAwMDAwMDAwMDI1MjM2
pa_validate_e_commerce_indicator=rpy
pa_validate_eci=05
pa_validate_eci_raw=05
```

```
pa_validate_pares_status=Y
pa_validate_rcode=1
pa_validate_rflag=SOK
pa_validate_rmsg=ics_pa_validate service was successful
pa_validate_specification_version=rupay
pa_validate_xid=ODMwOTE0MDkyNTM4
request_id=647034862963031073981 3
request_token=AxizLwSTXsIgFUXCMO9l/949TSosgRJQAgWhk6sw+6spuK+UAAAAQwwe
```

Response

```
ics_rcode=1
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
merchant_ref_number=S208441-1
pa_validate_authentication_result=0
pa_validate_authentication_status_msg=Success
pa_validate_cavv=MTAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDI1MjM2
pa_validate_e_commerce_indicator=rpy
pa_validate_eci=05
pa_validate_eci_raw=05
pa_validate_pares_status=Y
pa_validate_rcode=1
pa_validate_rflag=SOK
pa_validate_rmsg=ics_pa_validate service was successful
pa_validate_specification_version=rupay
pa_validate_xid=ODMwOTE0MDkyNTM4
request_id=647034862963031073981 3
request_token=AxizLwSTXsIgFUXCMO9l/949TSosgRJQAgWhk6sw+6spuK+UAAAAQwwe
```

Authorization Service

The authorization service format that you must send for RuPay is the same used for other card types. Send the CAVV and XID in the authorization service request with the card details for Cybersource to process this request with the RuPay card network.

For RuPay, the e-commerce indicator returned in the validation service response must be set to `rpy` or the authorization results in an error.

For an SMS type of card, send the authorization service and capture service requests at the same time. Sending just the authorization service request for an SMS type of card causes an error.

Example: Authorization

Request

```
bill_address1=123 Main St.
bill_city=Ann Arbor
bill_country=IN
bill_state=MI
bill_zip=48104-2201
card_type=061
cavv=MTAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDI1MjM2
client_lib_version=Oracle Corporation/1.8.0_172/Windows Server 2008 R2/
6.1/-/Java/5.2.1
currency=INR
customer_cc_cv_number=123
customer_cc_expmo=12
customer_cc_expyr=2031
customer_cc_number=5082302886091
customer_email=null@cybersource.com
customer_firstname=John
customer_lastname=Smith
customer_phone=999-999-10048
e_commerce_indicator=rpy
grand_total_amount=100
ics_applications=ics_auth
merchant_id=npr_rupay_test
merchant_ref_number=S208441-50
request_id=5378689648713406795329
sender_id=npr_rupay
xid=ODI4MTEyMjU5ODAy
```

Response

```
auth_auth_amount=100.00
auth_auth_avs=2
auth_auth_code=183217
auth_auth_time=2022-03-11T221339Z
auth_payment_service_data=320LTM06123908LTD040529TID30100000000000000000000000252
36RRN12914912328956
auth_rcode=1
auth_responsecode=100
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_status=SUCCESS
card_type=061
```

```
card_type_name=RUPAY
currency=INR
ics_rcode=1
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
merchant_ref_number=S208441-50
request_id=6470368185060310739813
request_token=Axj77wSTXsJljtUcxWtl/95NKiyBVYnqaVFkCqxWQdOIEC0MnVmH3VlNxXywaSa9hMsd
qjmK1soAsQpy
```

Handling Authorization Timeouts with Check Status

Typically, when a timeout occurs during an authorization, Cybersource automatically performs an authorization reversal. However, RuPay does not support online authorization reversals. When a timeout occurs during an authorization for a RuPay transaction, Cybersource includes an **auth_rflag** field set to `ETIMEOUT` in the authorization reply message. When you receive this value, check the status of the authorization by requesting the Check Status service.

The Check Status service includes a payment status field in the reply message. When the value of the payment status field is `AUTHORIZED`, proceed by requesting the capture service. When the value of the payment status field is `DECLINED`, the authorization is declined. You can request a different form of payment from the customer.

Example: Check Status

Request

```
merchant_id=npr_rupay_test
merchant_ref_number=S208441-50
ics_applications=ics_check_status
auth_request_id=5396859731856233201541
sender_id=npr_rupay_test
```

Response

```
ics_rcode=1
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
merchant_ref_number=S208441-1
request_id=5402857441596000201777
```

```
check_status_rcode=1
check_status_rflag=SOK
check_status_payment_status=AUTHORIZED
check_status_return_code=9999999
check_status.reason_code=100
request_token=AhjjbwSTJOO1iZDlZGwx3lFqAaRm3rIOnEIGiGTqzD7qym4r5QNAAQCo
ics_decision_reason_code=100
```

Possible Authentication Results

The following table lists the expected results based on the parameters included in your authorization request.

XID	CAVV	Authentication Value	Installment Identifier	ECI	Expected Result	Auth Mode	SCMP ERROR
Y	Y	N	N	ANY	redirection flow	2	
N	N	Y	N	ANY	s2s flow	3	
N	N	IGNORE	Y	R	s2s flow	3	
IGNORE	IGNORE	IGNORE	N	R	identifier error		Merchant Initiated auth must have Standing Instruction ID sent as mandatory field. Contact customer support for further details. installment_identifier
Y	N	Y	IGNORE	IGNORE	conflict error		Server to Server and Redirectional FlowType data are present together. Merchants must not send them together. Contact customer support for further details. transaction_token
N	Y	Y	IGNORE	IGNORE	conflict error		Server to Server and Redirectional FlowType data are present together. Merchants must not send them together. Contact customer support for further details. cavv
					s2s flow(default)	3	

XID	CAVV	Authentication Value	Installment Identifier	ECI	Expected Result	Auth Mode	SCMP ERROR
Y	Y	N	Y	R			SI is not supported on redirection flow. Contact customer support for further details. e_commerce_indicator
Y	Y	N	Y	rpy			SI is not supported on redirection flow. Contact customer support for further details. installment_identifier
Y	N	N	N	rpy			The following request field is either invalid or missing: authentication_transaction_context_id
N	Y	N	N	rpy			The following request field is either invalid or missing: authentication_transaction_context_id