Google Pay

Using the SCMP API

May 2019

CyberSource®
the power of payment

CyberSource Corporation HQ | P.O. Box 8999 | San Francisco, CA 94128-8999 | Phone: 800-530-9095

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

Copyright

Restricted Rights Legends

Trademarks

Contents

Recent Revisions to This Document

Release	Changes
May 2019	This revision contains only editorial changes and no technical updates.
April 2019	Added the following request fields that support tokenized transactions using a network token with 3D Secure or SecureCode (see "API Request Fields," page 19): ■ directory_server_transaction_id ■ network_token_cryptogram ■ pa_specification_version Added the following reply field that supports tokenized transactions using a network token with 3D Secure or SecureCode (see "API Reply Fields," page 26): directory_server_transaction_id Added support for the processor *Elavon Americas*. See "Supported Processors, Card Types, and Optional Features," page 9. Added support for the following optional features by Elavon Americas (see "Supported Processors, Card Types, and Optional Features," page 9): ■ Merchant-Initiated transactions ■ Multiple partial captures ■ Recurring payments
March 2019	Added support for the processor *Credit Mutuel-CIC*. See "Supported Processors, Card Types, and Optional Features," page 9. Added support for Recurring Payments as an optional feature for the processors *Credit Mutuel-CIC* and *SIX*. See "Supported Processors, Card Types, and Optional Features," page 9.
July 2018	All processors: updated optional features. See "Supported Processors, Card Types, and Optional Features," page 9. Added support for the processor *Worldpay VAP*. See "Supported Processors, Card Types, and Optional Features," page 9.
June 2018	Added a new chapter on formatting encrypted data. See Chapter 2, "Formatting Encrypted Payment Data," on page 14.
April 2018	Initial release.

About This Guide

Audience and Purpose

This document is written for merchants who want to enable customers to use Google Pay to pay for in-app purchases. This document provides an overview of integrating the Google API and describes how to request the CyberSource API to process an authorization.

This document describes the Google Pay service and the CyberSource API. You must request the Google API to receive the customer's encrypted payment data before requesting the CyberSource API to process the transaction.

Conventions

Notes and Important Statements

Note

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

Important

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

Text and Command Conventions

Convention	Usage
Bold	■ 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**.
`Screen text`	■ XML elements. ■ Code examples and samples. ■ Text that you enter in an API environment; for example: Set the **davService_run** field to `true`.

Related Documents

CyberSource Documents:

- *Getting Started with CyberSource Advanced for the SCMP API* (PDF | HTML)
- SCMP API Documentation and Downloads page
- *Credit Card Services Using the SCMP API* (PDF | HTML)
- *Payment Network Tokenization Using the SCMP API* (PDF | HTML)

Google Pay documents:

- Google Pay API: https://developers.google.com/pay/api/

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

CHAPTER 1

Introduction

Google Pay Overview

Google Pay is a simple, secure in-app mobile and Web payment solution. You can choose CyberSource to process Google Pay transactions through all e-commerce channels.

You can simplify your payment processing by allowing CyberSource to decrypt the payment data for you during processing.

This method integrates simply and allows you to process transactions without seeing the payment network token and transaction data.

---

1. Using the Google API, request the customer's encrypted payment data.
2. Using the CyberSource API, construct and submit the authorization request and include the encrypted payment data from the Google Pay call back.
3. CyberSource decrypts the encrypted payment data to create the payment network token and processes the authorization request.

For complete details, see "How Google Pay Works," page 11.

Payment Network Tokenization

Payment network tokenization enables you to securely request a payment transaction with a payment network token instead of a customer's primary account number (PAN).

The payment network token is included in the customer's encrypted payment data, which is returned by the payment processor.

For in-app and browser transactions, payment network tokenization uses some of the CyberSource payer authentication request fields. This approach simplifies your implementation if your order management system already uses payer authentication.

Requirements

- Create a CyberSource merchant evaluation account if you do not have one already: https://www.cybersource.com/register/
- Have a merchant account with a supported processor (see "Supported Processors, Card Types, and Optional Features," page 9).
- Install the CyberSource SCMP API client.
- Create a Google developer account and embed Google Pay into your application or web sites.
- For details about integrating Google Pay, see Google Pay's API documentation.

Note

All optional features are described in *Payment Network Tokenization Using the SCMP API*.

Supported Processors, Card Types, and Optional Features

Table 1 Supported Processors, Card Types, and Optional Features

Processors	Card Types	Optional Feature
American Express Direct	American Express	Recurring Payments
Barclays	■ Visa ■ Mastercard	■ Recurring Payments ■ Multiple partial captures
Chase Paymentech Solutions	■ Visa ■ Mastercard ■ American Express ■ Discover	Recurring Payments
Credit Mutuel-CIC	■ Visa ■ Mastercard ■ Cartes Bancaires	Recurring Payments

Table 1 Supported Processors, Card Types, and Optional Features (Continued)

Processors	Card Types	Optional Feature
CyberSource through VisaNet. The supported acquirers are: ■ Australia and New Zealand Banking Group Limited (ANZ) ■ Vantiv ■ Westpac	Visa, Mastercard	Recurring payments
Elavon Americas	Visa, Mastercard, American Express, JCB, Discover	■ Merchant-Initiated transactions ■ Multiple partial captures ■ Recurring payments
FDC Compass	Visa, Mastercard, American Express	Recurring payments
FDC Nashville Global	Visa, Mastercard, American Express, Discover	■ Recurring payments ■ Multiple partial captures
JCN Gateway	JCB	Multiple partial captures
GPN	Visa, Mastercard, American Express	■ Recurring payments ■ Split shipments
OmniPay Direct. The supported acquirers are: ■ Bank of America Merchant Services ■ First Data Europe through OmniPay Direct ■ Global Payments International Acquiring through OmniPay Direct	Visa, Mastercard	Recurring payments
SIX	Visa, Mastercard	Recurring payments
Streamline	Visa, Mastercard	Recurring payments
TSYS Acquiring Solutions	Visa, Mastercard, American Express	Recurring payments
Worldpay VAP Worldpay VAP was previously called *Litle*.	Visa, Mastercard	Recurring payments

How Google Pay Works

1 The customer chooses the *Google Pay* button. Using the Google API, your system initiates the Google Pay request identifying **cybersource** as your payment gateway, passing your CyberSource merchant ID as the gateway merchant ID.

2 The customer confirms the payment. The Google API contacts Google Pay services to retrieve the consumer's payment parameters.

3 If the customer's selected payment credentials are tokenized or you are tokenizing new payment credentials, the Google Pay service contacts the appropriate payment network to retrieve the appropriate cryptogram.

4 The payment network returns the appropriate token and cryptogram to the Google Pay service.

5 Google creates encrypted payment data using the gateway-specific key that is supplied in the Wallet request and includes it in the Google API response.

6 The Google Pay call back returns the encrypted payment data.

7 Your system prepares the Google Pay response information for submission to the CyberSource service.

   a CyberSource sends the authorization request to the acquirer.

   b The acquirer processes the request from CyberSource and creates the payment network authorization request.

c The payment network processes the request from the acquirer and creates the issuer authorization request.

d The issuer processes the request from the payment network. The issuer looks up the payment information and returns an approved or declined authorization message to the payment network.

e The payment network returns the authorization response to the acquirer.

f The acquirer returns the authorization response to CyberSource.

8 CyberSource returns the authorization response to your system.

9 Your system returns the authorization response to the payment application.

10 The payment application displays the confirmation or decline message to the customer.

a The acquirer submits the settlement request to the issuer for funds.

b The issuer supplies the funds to the acquirer for the authorized transactions.

Additional CyberSource Services

Refer to *Credit Card Services Using the SCMP API* for information on how to request these follow-on services.

Table 2 CyberSource Services

CyberSource Service	Description
Capture	A follow-on service that uses the request ID returned from the previous authorization. The request ID links the capture to the authorization. This service transfers funds from the customer's account to your bank and usually takes two to four days to complete.
Sale	A sale is a bundled authorization and capture. Request the authorization and capture services at the same time. CyberSource processes the capture immediately.
Authorization Reversal	A follow-on service that uses the request ID returned from the previous authorization. An authorization reversal releases the hold that the authorization placed on the customer's credit card funds. Use this service to reverse an unnecessary or undesired authorization.

Transaction Endpoints

CAS (test transactions):

http://ics2testa.ic3.com

Production (live transactions):

http://ics2a.ic3.com

CHAPTER 2

Formatting Encrypted Payment Data

Formatting the Payment Blob

To transmit Google Pay responses to CyberSource securely, you must first encode them using Base64. Example 1 shows a Google Pay response.

Example 1 Google Pay Response

```
{"signature":"MEUCIQDhTxhHqwY8pXB9hpYxaSK5jFgsqpG2E1rX77QXssK8tAIgUBvYYAI/bnBS8T/
Tfxnm2AF981Mv5y0pHyGexM5dMJk\u003d","protocolVersion":"ECv1","signedMessage":"{\"encr
yptedMessage\":\"odyUGGA7B+blletYcJbS43AQUFQJpWEFCN4UuUExQ5LX0\/
XcLwKElXcB95nMnmPO9lM2KGp13FYsL768ccCzAjBGLYF+fugcJTcvkrUhcNSyXr7hwf12BEsrweqJM6I7Vs5
lfrPAukRJeLDQG4FxmTLW49QyP8vIZC+tz2c+Z3zozzI5oB9jE8fA2dolFa13Cu6gXqdKH\/
IHRh7UniLUuTy+0G5FQV2pwST2uBSNNkZhb8WYJDHbxBjz0UebVP+ObmT5cc8AKU5dgHRdfr4GKpEZ4EBzB90
BPxLqYHpopriJ6lbFgFVsQQ6\/
8HBqQ7ImIMH5y7G8p8qAFkWnB78ZcL0Fh5BjXojkxGoFp2gjAsrhhttHAFbe3WQBuPkwJu09\/6\/
MyJpCSrpMHFouF\/
dj0SYjQ+xI097lCHZec7jQrAhISLWZ9DZkuMvGKPWpu0CKn2XqTXQ=\",\"ephemeralPublicKey\":\"MFk
wEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEnn4yjy0N6xlXO8\/8j7\/
4jvmLJCYAqgXLwP1FhjuTgIM9oCtPijZfI9so2QEOs2ZnVp3D0dl3JYIDVe+396KkAQ==\",\"tag\":\"DRp
cc+YQ33RNgsTcxztnJbMJnirbU5DW3dStjfhFiwc=\"}"}
```

Example 2 shows how to transform the Google Pay payment information into the Base64-encoded blob.

Example 2 Android Code

```
new String(Base64.encode(paymentData.getPaymentMethodToken().getToken().getBytes()))
```

To construct the following blob, encode Example 1 using Base64 and include it in the CyberSource payment request. Example 3 shows a formatted Google Pay blob.

Example 3 Google Pay Blob

```
eyJzaWduYXR1cmUiOiJNRVVDSVFEaFR4aEhxd1k4cFhCOWhwWXhhU0s1akZnc3FwRzJFMXJYNzdRWHNzSzh0Q
UlnVUJ2WVlBSS9ibkJTOFQvVGZ4bm0yQUY5ODFNdjV5MHBIeUdleE01ZE1Ka1x1MDAzZCIsInByb3RvY29sVm
Vyc2lvbiI6IkVDdjEiLCJzaWduZWRNZXNzYWdlIjoie1wiZW5jcnlwdGVkTWVzc2FnZVwiOlwib2R5VUdHQTd
CK2JsbGV0WWNKYlM0M0FRVUZRSnBXRUZDTjRVdVVFeFE1TFgwXC9YY0x3S0VsWGNCOTVuTW5tUE85bE0yS0dw
MTNGWXNMNzY4Y2NDekFqQkdMWUYrZnVnY0pUY3ZrclVoY05TeVhyN2h3ZjEyQkVzcndlcUpNNkk3VnM1bGZyU
EF1a1JKZUxEUUc0RnhtVExXNDlReVA4dklaQyt0ejJjK1ozem96ekk1b0I5akU4ZkEyZG9sRmExM0N1NmdYcW
RLSFwvSUhSaDdVbmlMVXVUeSswRzVGUVYycHdTVDJ1QlNOTmtaaGI4V1lKREhieEJqejBVZWJWUCtPYm1UNWN
jOEFLVTVkZ0hSZGZyNEdLcEVaNEVCekI5MEJQeExxWUhwb3ByaUo2bGJGZ0ZWc1FRNlwvOEhCcVE3SW1JTUg1
eTdHOHA4cUFGa1duQjc4WmNMMEZoNUJqWG9qa3hHb0ZwMmdqQXNyaGh0dEhBRmJlM1dRQnVQa3dKdTA5XC82X
C9NeUpwQ1NycE1IRm91RlwvZGowU1lqUSt4STA5N2xDSFplYzdqUXJBaElTTFdaOURaa3VNdkdLUFdwdTBDS2
4yWHFUWFE9XCIsXCJlcGhlbWVyYWxQdWJsaWNLZXlcIjpcIk1Ga3dFd1lIS29aSXpqMENBUVlJS29aSXpqMER
BUWNEUWdBRW5uNHlqeTBONnhsWE84XC84ajdcLzRqdm1MSkNZQXFnWEx3UDFGaGp1VGdJTTlvQ3RQaWpaZkk5
c28yUUVPczJablZwM0QwZGwzSllJRFZlKzM5NktrQVE9PVwiLFwidGFnXCI6XCJEUnBjYytZUTMzUk5nc1Rje
Hp0bkpiTUpuaXJiVTVEVzNkU3RqZmhGaXdjPVwifSJ9
```

CHAPTER 3

Authorizing a Payment

CyberSource Decryption

Transaction Authorization

To request an authorization for a Google Pay transaction:

Note See "API Request Fields," page 19, and "API Reply Fields," page 26, for detailed field descriptions.

Step 1 Set the **encrypted_payment_data** field to the string value generated from the Full Wallet response.

Step 2 Set the **payment_solution** field to `012`.

Example 4 Authorization Request

```
bill_address1=111 S. Division St.
bill_address2=Suite 123
bill_city=Ann Arbor
bill_country=US
bill_state=MI
bill_zip=48104-2201
encrypted_payment_data=ABCDEFabcdefABCDEFabcdef0987654321234567
card_type=001
currency=usd
customer_email=demo@example.com
customer_firstname=James
customer_ipaddress=66.123.123.2
customer_lastname=Smith
customer_phone=999-999-9999
grand_total_amount=100.00
ics_applications=ics_auth
merchant_id=demomerchant
merchant_ref_number=demorefnum
solution_type=012
```

Example 5 Authorization Reply

```
request_token=Ahj/7wSR5C/kX63O2hAKIkGLNkwcsmrSHHlU5tGHRT/hHgzc8BT/hHgk
currency=usd
request_id=4465837560045000001541
auth_rflag=SOK
ics_rmsg=Request was processed successfully.
auth_auth_amount=100.00
auth_rcode=1
auth_trans_ref_no=13209254CGJSMQCQ
auth_auth_code=888888
auth_rmsg=Request was processed successfully.
ics_rflag=SOK
auth_auth_response=100
auth_avs_raw=I1
auth_auth_time=2015-11-03T204917Z
merchant_ref_number=demorefnum
ics_rcode=1
token_prefix=294672
token_suffix=4397
token_expirationMonth=08
token_expirationYear=2021
```

APPENDIX A

API Fields

Data Type Definitions

Data Type	Description
Date and time	Format is YYYY-MM-DDThhmmssZ, where: ■ T separates the date and the time. ■ Z indicates Coordinated Universal Time (UTC), which equals Greenwich Mean Time (GMT). Example: 2016-08-11T22:47:57Z equals August 11, 2016, at 22:47:57 (10:47:57 p.m.)
Decimal	Number that includes a decimal point Examples: 23.45, -0.1, 4.0, 90809.0468
Integer	Whole number {..., -3, -2, -1, 0, 1, 2, 3, ...}
Nonnegative integer	Whole number greater than or equal to zero {0, 1, 2, 3, ...}
Positive integer	Whole number greater than zero {1, 2, 3, ...}
String	Sequence of letters, numbers, spaces, and special characters

Relaxed Requirements for Address Data and Expiration Date

To enable relaxed requirements for address data and expiration date, contact CyberSource Customer Support to have your account configured for this feature. For details about relaxed requirements, see the Relaxed Requirements for Address Data and Expiration Date page.

API Request Fields


Note

Unless otherwise noted, all fields are order and case insensitive, and the fields accept special characters such as @, #, and %.

Table 3 Request Fields

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
bill_address1	First line of the billing street address.	ics_auth (R)[2]	String (60)
bill_address2	Additional address information. **Example** Attention: Accounts Payable	ics_auth (O)	String (60)
bill_city	City of the billing address.	ics_auth (R)[2]	String (50)
bill_country	Country of the billing address. Use the two-character *ISO Standard Country Codes*.	ics_auth (R)[2]	String (2)
bill_state	State or province of the billing address. For an address in the U.S. or Canada, use the *State, Province, and Territory Codes for the United States and Canada*.	ics_auth (R)[2]	String (2)
bill_zip	Postal code for the billing 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	ics_auth (R)[2]	String (9)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

2 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 18. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 3 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
card_type	Type of card to authorize. Possible values: ■ `001`: Visa ■ `002`: Mastercard ■ `003`: American Express ■ `004`: Discover	ics_auth (O)	String (3)
cavv	***Visa*** Cryptogram for payment network tokenization transactions. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats. ***American Express*** For a 20-byte cryptogram, set this field to the cryptogram for payment network tokenization transactions. For a 40-byte cryptogram, set this field to block A of the cryptogram for payment network tokenization transactions. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats. ***Discover*** Cryptogram for payment network tokenization transactions. The value for this field can be a 20 or 40-character hex binary. All cryptograms use one of these formats. ***CyberSource through VisaNet*** The value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCR8 ■ Position: 77-78 ■ Field: CAVV version and authentication action.	ics_auth (R)	String (40)
currency	Currency used for the order: USD	ics_auth (R)	String (5)
customer_cc_cv_number	CVN.	ics_auth (O)	Nonnegative integer (4)
customer_cc_expmo	Two-digit month in which the payment network token expires. Format: MM. Possible values: `01` through `12`.	ics_auth (R)	String (2)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

2 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 18. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 3 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
customer_cc_expyr	Four-digit year in which the payment network token expires. Format: YYYY.	ics_auth (R)	Nonnegative integer (4)
customer_cc_number	The payment network token value. This value is obtained by decrypting the customer's encrypted payment data. Populate this field with the decrypted `dpan` value.	ics_auth (R)	Nonnegative integer (20)
customer_email	Customer's email address.	ics_auth (R)[2]	String (255)
customer_firstname	Customer's first name. For a credit card transaction, this name must match the name on the card.	ics_auth (R)[2]	String (60)
customer_ipaddress	Customer's IP address.	ics_auth (O)	String (15)
customer_lastname	Customer's last name. For a credit card transaction, this name must match the name on the card.	ics_auth (R)[2]	String (60)
customer_phone	Customer's phone number. CyberSource recommends that you include the country code when the order is from outside the U.S.	ics_auth (O)	String (15)
directory_server_transaction_id	Identifier generated during the authentication transaction by the Mastercard Directory Server and passed back with the authentication results.	ics_auth (O)	String (36)
e_commerce_indicator	For a payment network tokenization transaction. Possible values: ▪ `aesk:` American Express card type ▪ `spa:` Mastercard card type ▪ `internet:` Visa card type ▪ `dipb:` Discover card type **Important** For Visa in-app transactions, the `internet` value is mapped to the Visa ECI value 7.	ics_auth (R for merchant decryption, O for CyberSource decryption)	String (20)
eci_raw	Raw electronic commerce indicator (ECI).	ics_auth	String (2)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

2 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 18. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 3 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
encrypted_payment_data	The encrypted payment data value. If you are using the CyberSource decryption option, populate this field with the encrypted payment data value returned by the Full Wallet request. See "Google Pay Overview," page 8.	ics_auth (R)	
grand_total_amount	Grand total for the order. This value cannot be negative. You can include a decimal point (.), but you cannot include any other special characters. CyberSource truncates the amount to the correct number of decimal places.	ics_auth (R)	Decimal (60)
ics_applications	CyberSource services to process for the request: `ics_auth`	ics_auth (R)	String (255)
merchant_id	Your CyberSource merchant ID. Use the same merchant ID for evaluation, testing, and production.	ics_auth (R)	String (30)
merchant_ref_number	Merchant-generated order reference or tracking number. CyberSource recommends that you send a unique value for each transaction so that you can perform meaningful searches for the transaction. For information about tracking orders, see *Getting Started with CyberSource Advanced for the SCMP API*.	ics_auth (R)	String (50)
network_token_cryptogram	Token authentication verification value cryptogram. For token-based transactions with 3D Secure or SecureCode, you must submit both types of cryptograms: network token and 3D Secure/ SecureCode. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats.	ics_auth (O)	String (40)
pa_specification_version	The 3D Secure version that you used for Secured Consumer Authentication (SCA); for example, 3D Secure version 1.0.2 or 2.0.0.	ics_auth (O)	String (20)
payment_network_token_assurance_level	Confidence level of the tokenization. This value is assigned by the token service provider. **Note** This field is supported only for CyberSource through VisaNet and FDC Nashville Global.	ics_auth (O)	String (2)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

2 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 18. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 3 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
payment_network_token_device_tech_type	Type of technology used in the device to store token data. Possible value: `002`: Host card emulation (HCE) Emulation of a smart card by using software to create a virtual and exact representation of the card. Sensitive data is stored in a database that is hosted in the cloud. For storing payment credentials, a database must meet very stringent security requirements that exceed PCI DSS. **Note** This field is supported only for FDC Compass.	ics_auth (O)	Integer (3)
payment_network_token_requestor_id	Value that identifies your business and indicates that the cardholder's account number is tokenized. This value is assigned by the token service provider and is unique within the token service provider's database. **Note** This field is supported only for CyberSource through VisaNet, FDC Nashville Global, and Chase Paymentech Solutions.	ics_auth (O)	Integer (11)
payment_network_token_transaction_type	Type of transaction that provided the token data. This value does not specify the token service provider; it specifies the entity that provided you with information about the token. Possible value: `1`: In-app transaction. An application on the customer's mobile device provided the token data for an e-commerce transaction.	ics_auth (R)	String (1)
payment_solution	Identifies Google Pay as the payment solution that is being used for the transaction: Set the value for this field to `012`. **Note** This unique ID differentiates digital solution transactions within the CyberSource platform for reporting purposes.	ics_auth (R)	String (3)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

2 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 18. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 3 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
pos_environment	Operating environment. Possible values: ■ 0: No terminal used or unknown environment. ■ 1: On merchant premises, attended. ■ 2: On merchant premises, unattended, or cardholder terminal. Examples: oil, kiosks, self-checkout, home computer, mobile telephone, personal digital assistant (PDA). Cardholder terminal is supported only for Mastercard transactions on CyberSource through VisaNet. ■ 3: Off merchant premises, attended. Examples: portable POS devices at trade shows, at service calls, or in taxis. ■ 4: Off merchant premises, unattended, or cardholder terminal. Examples: vending machines, home computer, mobile telephone, PDA. Cardholder terminal is supported only for Mastercard transactions on CyberSource through VisaNet. ■ 5: On premises of cardholder, unattended. ■ 9: Unknown delivery mode. ■ S: Electronic delivery of product. Examples: music, software, or eTickets that are downloaded over the internet. ■ T: Physical delivery of product. Examples: music or software that is delivered by mail or by a courier. This field is supported only for American Express Direct and CyberSource through VisaNet. ***CyberSource through VisaNet*** For Mastercard transactions, the only valid values are 2 and 4.	ics_auth (O)	String (1)
ucaf_authentication_data	Cryptogram for payment network tokenization transactions with Mastercard.	ics_auth (R)	String (32)
ucaf_collection_indicator	Required field for payment network tokenization transactions with Mastercard. Set the value for this field to 2.	ics_auth (R)	String with numbers only (1)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

2 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 18. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 3 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
xid	***Visa*** Cryptogram for payment network tokenization transactions. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats. ***American Express*** For a 20-byte cryptogram, set this field to the cryptogram for payment network tokenization transactions. For a 40-byte cryptogram, set this field to block A of the cryptogram for payment network tokenization transactions. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats.	ics_auth (R)	String (40)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

2 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 18. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

API Reply Fields

Important

Because CyberSource can add reply fields, reply codes, and reply flags at any time:

- You must parse the reply data according to the names of the fields instead of the field order in the reply. For more information about parsing reply fields, see the documentation for your client.
- Your error handler should be able to process new reply codes and reply flags without problems.
- Your error handler should use the **ics_rcode** field to determine the result if it receives a reply flag that it does not recognize.

Note

Your payment processor can include additional API reply fields that are not documented in this guide. See *Credit Card Services Using the SCMP API* for detailed descriptions of additional API reply fields.

Table 4 Reply Fields

Field	Description	Returned By	Data Type & Length
auth_auth_amount	Amount that was authorized.	ics_auth	Decimal (15)
auth_auth_avs	AVS result code. See *Credit Card Services Using the SCMP API* for a detailed list of AVS values.	ics_auth	String (1)
auth_auth_code	Authorization code. Returned only when the processor returns this value.	ics_auth	String (7)
auth_auth_response	For most processors, this value is the error message sent directly from the bank. Returned only when the processor returns this value.	ics_auth	String (10)
auth_auth_time	Time of authorization. Format: YYYY-MM-DDThh:mm:ssZ Example: 2019-08-11T22:47:57Z equals August 11, 2019, at 22:47:57 (10:47:57 p.m.). The T separates the date and the time. The Z indicates UTC.	ics_auth	Date and time (20)
auth_avs_raw	AVS result code sent directly from the processor. Returned only when the processor returns this value.	ics_auth	String (10)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 4 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
auth_payment_card_service	Mastercard service that was used for the transaction. Mastercard provides this value to CyberSource. Possible value: 53: Mastercard card-on-file token service ***CyberSource through VisaNet*** The value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCR6 ■ Position: 133-134 Field: Mastercard Merchant on-behalf service. **Note** This field is returned only for CyberSource through VisaNet.	ics_auth	String (2)
auth_payment_card_service_result	Result of the Mastercard card-on-file token service. Mastercard provides this value to CyberSource. Possible values: ■ C: Service completed successfully. ■ F: One of the following: • Incorrect Mastercard POS entry mode. The Mastercard POS entry mode should be 81 for an authorization or authorization reversal. • Incorrect Mastercard POS entry mode. The Mastercard POS entry mode should be 01 for a tokenized request. • Token requestor ID is missing or formatted incorrectly. ■ I: One of the following: • Invalid token requestor ID. • Suspended or deactivated token. • Invalid token (not in mapping table). ■ T: Invalid combination of token requestor ID and token. ■ U: Expired token. ■ W: Primary account number (PAN) listed in electronic warning bulletin.This field is returned only for CyberSource through VisaNet. **Note** This field is returned only for CyberSource through VisaNet.	ics_auth	String (1)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 4 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
auth_rcode	Indicates whether the service request was successful. Possible values: ■ `-1`: An error occurred. ■ `0`: The request was declined. ■ `1`: The request was successful.	ics_auth	Integer (1)
auth_reversal_ payment_card_service	Mastercard service that was used for the transaction. Mastercard provides this value to CyberSource. Possible value: 53: Mastercard card-on-file token service ***CyberSource through VisaNet*** The value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCR6 ■ Position: 133-134 Field: Mastercard Merchant on-behalf service. **Note** This field is returned only for CyberSource through VisaNet.	ics_auth_ reversal	String (2)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 4 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
auth_reversal_ payment_card_service_ result	Result of the Mastercard card-on-file token service. Mastercard provides this value to CyberSource. Possible values: ■ C: Service completed successfully. ■ F: One of the following: • Incorrect Mastercard POS entry mode. The Mastercard POS entry mode should be 81 for an authorization or authorization reversal. • Incorrect Mastercard POS entry mode. The Mastercard POS entry mode should be 01 for a tokenized request. • Token requestor ID is missing or formatted incorrectly. ■ I: One of the following: • Invalid token requestor ID. • Suspended or deactivated token. • Invalid token (not in mapping table). ■ T: Invalid combination of token requestor ID and token. ■ U: Expired token. ■ W: Primary account number (PAN) listed in electronic warning bulletin.This field is returned only for CyberSource through VisaNet. **Note** This field is returned only for CyberSource through VisaNet.	ics_auth_ reversal	String (1)
auth_rflag	One-word description of the result of the entire request. See *Credit Card Services Using the SCMP API* for a detailed list of **rflag** values.	ics_auth	String (50)
auth_rmsg	Message that explains the reply flag **auth_rflag**. Do not display this message to the customer, and do not use this field to write an error handler.	ics_auth	String (255)
auth_trans_ref_no	Reference number for the transaction. This value is not returned for all processors.	ics_auth	String (60)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 4 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
auth_transaction_ qualification	Type of authentication for which the transaction qualifies as determined by the Mastercard authentication service, which confirms the identity of the cardholder. Mastercard provides this value to CyberSource. Possible values: ■ 1: Transaction qualifies for Mastercard authentication type 1. ■ 2: Transaction qualifies for Mastercard authentication type 2. ***CyberSource through VisaNet*** The value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCR6 ■ Position: 132 Field: Mastercard Member Defined Data. **Note** This field is returned only for CyberSource through VisaNet.	ics_auth	String (1)
card_suffix	Last four digits of the cardholder's account number. This field is returned only for tokenized transactions. You can use this value on the receipt that you give to the cardholder. ***CyberSource through VisaNet*** The value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCRB ■ Position: 85 Field: American Express last 4 PAN return indicator. **Note** This field is returned only for CyberSource through VisaNet and FDC Nashville Global.	ics_auth	String (4)
currency	Currency used for the order. For the possible values, see the *ISO Standard Currency Codes*.	ics_auth	String (5)
ics_rcode	Indicates whether the service request was successful. Possible values: ■ `-1`: An error occurred. ■ `0`: The request was declined. ■ `1`: The request was successful.	ics_auth	Integer (1)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 4 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
ics_rflag	One-word description of the result of the entire request. See *Credit Card Services Using the SCMP API* for a detailed list of **rflag** values.	ics_auth	String (50)
ics_rmsg	Message that explains the reply flag **ics_rflag**. Do not display this message to the customer, and do not use this field to write an error handler.	ics_auth	String (255)
merchant_ref_number	Order reference or tracking number that you provided in the request. If you included multi-byte characters in this field in the request, the returned value might include corrupted characters.	ics_auth	String (50)
payment_network_token_account_status	Possible values: ■ N: Nonregulated ■ R: Regulated **Note** This field is returned only for CyberSource through VisaNet.	ics_auth	String (1)
payment_network_token_assurance_level	Confidence level of the tokenization. This value is assigned by the token service provider. **Note** This field is returned only for CyberSource through VisaNet and FDC Nashville Global.	ics_auth	String (2)
payment_network_token_original_card_category	Mastercard product ID associated with the primary account number (PAN). For the possible values, see "Mastercard Product IDs" in *Credit Card Services Using the SCMP API.* ***CyberSource through VisaNet*** For the possible values, see "Mastercard Product IDs" in *Credit Card Services for CyberSource through VisaNet Using the SCMP API*. **Note** This field is returned only for Mastercard transactions for CyberSource through VisaNet.	ics_auth	String (3)
payment_network_token_requestor_id	Value that identifies your business and indicates that the cardholder's account number is tokenized. This value is assigned by the token service provider and is unique within the token service provider's database. This value is returned only if the processor provides it. **Note** This field is returned only for CyberSource through VisaNet and FDC Nashville Global.	ics_auth	Integer (11)
request_id	Identifier for the request generated by the client.	ics_auth	String (26)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.

Table 4 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
request_token	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.	ics_auth	String (256)
token_expiration_month	Month in which the token expires. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction. Format: MM. Possible values: `01` through `12`.	ics_auth	String (2)
token_expiration_year	Year in which the token expires. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction. Format: YYYY.	ics_auth	String (4)
token_prefix	First six digits of token. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction.	ics_auth	String (6)
token_suffix	Last four digits of token. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction.	ics_auth	String (4)

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.