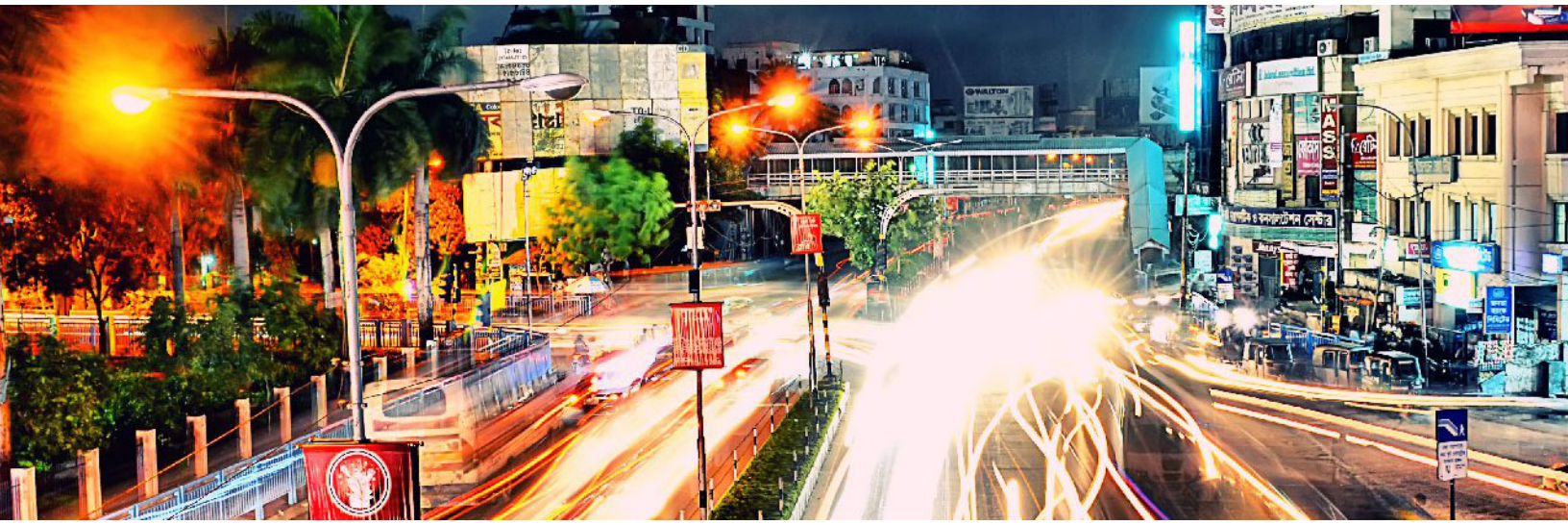
Google Pay

Using the Simple Order API



CyberSource®
A Visa Solution

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

Revision: May 2020

Contents

Recent Revisions to This Document

Release	Changes
May 2020	Updated information about recurring payments. See "Supported Processors, Card Types, and Optional Features," page 9.
April 2020	Added information about optional features. See "Supported Processors, Card Types, and Optional Features," page 9.
February 2020	Added support for the processor *Moneris*. See Moneris, page 10.
January 2020	Updated the **purchaseTotals_grandTotalAmount r**equest field. See purchaseTotals_grandTotalAmount, page 27.
November 2019	Changed *payment network tokenization* to *authorizations with payment network tokens* throughout this document. Updated information about payment network tokens. See "Payment Network Tokens," page 8. SIX: added an Important statement. See SIX, page 10.
September 2019	Added information about configuring Google Pay. See "Configuring Google Pay," page 14. Updated the authorization reply example. See Example 7, "Authorization Response," on page 18. Updated the **paymentNetworkToken_transactionType** request field. See paymentNetworkToken_transactionType, page 26. Updated the following reply fields. See "API Reply Fields," page 29. ■ token_expirationMonth ■ token_expirationYear ■ token_prefix ■ token_suffix

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

Important Statements

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**.

Convention	Usage
`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 Simple Order API* (PDF | HTML)
- Simple Order API and SOAP Toolkit API Documentation and Downloads page
- *Credit Card Services Using the Simple Order API* (PDF | HTML)
- *Authorizations with Payment Network Tokens Using the Simple Order 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 Tokens

Authorizations with payment network tokens enable 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 information about authorizations with payment network tokens, see *Authorizations with Payment Network Tokens Using the Simple Order API* (PDF | HTML).

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 Simple Order API client.
- Create a Google developer account and embed Google Pay into your application or web sites.
- For details about integrating Google Pay, see the Google Pay API documentation.

Supported Processors, Card Types, and Optional Features

Merchant-initiated transactions and multiple partial captures are described in *Authorizations with Payment Network Tokens Using the Simple Order API* (PDF | HTML). Recurring payments and split shipments are described in *Credit Card Services Using the Simple Order API* (PDF | HTML).

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
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

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

Processors	Card Types	Optional Feature
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	Split shipments
Moneris	Visa, Mastercard, American Express	■ Merchant-Initiated transactions ■ Recurring payments
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 **Important** SIX is supported only for card-present processing.	Visa, Mastercard	Recurring payments
Streamline	Visa, Mastercard	Recurring payments
TSYS Acquiring Solutions	Visa, Mastercard, American Express	Multiple partial captures
Worldpay VAP Worldpay VAP was previously called Litle. Litle was purchased by Vantiv, which was then purchased by Worldpay VAP. If you have any questions about this situation, contact your account manager at Worldpay VAP.	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 Simple Order 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): https://ics2wstest.ic3.com/commerce/1.x/transactionProcessor/CyberSourceTransaction_1.104.xsd

Production (live transactions): https://ics2ws.ic3.com/commerce/1.x/transactionProcessor/CyberSourceTransaction_1.104.xsd

CHAPTER 2

Formatting Encrypted Payment Data

Configuring Google Pay

You must provide your CyberSource merchant ID to Google in order to ensure proper encryption of the Google Pay payload and authenticity of the request.

For a Google Pay tutorial, see:

https://developers.google.com/pay/api/android/guides/tutorial

Set the gateway and gateway merchant ID to the appropriate indicators. The following code examples show how to configure the PaymentMethodTokenizationParameters object using CyberSource as the gateway.

Example 1 Java Code

```
.setPaymentMethodTokenizationType(WalletConstants.PAYMENT_METHOD_
TOKENIZATION_TYPE_PAYMENT_GATEWAY)
.addParameter("gateway", "cybersource")
.addParameter("gatewayMerchantId", "[yourCyberSourceMID]")
```

Example 2 Java Script

```
tokenizationType: 'PAYMENT_GATEWAY',
  parameters: {
    gateway: 'cybersource',
    gatewayMerchantId: '[yourCyberSourceMID]'
  }
```

Formatting the Payment Blob

To transmit Google Pay responses to CyberSource securely, you must first encode them using Base64. Example 3 shows a Google Pay response.

Example 3 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 4 shows how to transform the Google Pay payment information into the Base64-encoded blob.

Example 4 Android Code

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

To construct the following blob, encode Example 3 using Base64 and include it in the CyberSource payment request. Example 5 shows a formatted Google Pay blob.

Example 5 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

See "API Request Fields," page 21, and "API Reply Fields," page 29, for detailed field descriptions.

To request an authorization for a Google Pay transaction:

Step 1 Set the **encryptedPayment_data** field to the value of the **encryptedMessage** field that was returned in the Full Wallet response.

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

Example 6 Authorization Request

```
<requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.121">
    <merchantID>demomerchant</merchantID>
    <merchantReferenceCode>demorefnum</merchantReferenceCode>
    <billTo>
        <firstName>James</firstName>
        <lastName>Smith</lastName>
        <street1>1295 Charleston Road</street1>
        <city>Test City</city>
        <state>CA</state>
        <postalCode>99999</postalCode>
        <country>US</country>
        <email>demo@example.com</email>
    </billTo>
    <purchaseTotals>
        <currency>USD</currency>
        <grandTotalAmount>5.00</grandTotalAmount>
    </purchaseTotals>
    <encryptedPayment>
        <data>ABCDEFabcdefABCDEFabcdef0987654321234567</data>
    </encryptedPayment>
    <card>
        <cardType>001</cardType>
    </card>
    <ccAuthService run="true"/>
    <paymentSolution>012</paymentSolution>
</requestMessage>
```

Example 7 Authorization Response

```
<c:replyMessage>
    <c:merchantReferenceCode>demorefnum</c:merchantReferenceCode>
    <c:requestID>4465840340765000001541</c:requestID>
    <c:decision>ACCEPT</c:decision>
    <c:reasonCode>100</c:reasonCode>
    <c:requestToken>Ahj/7wSR5C/4Icd2fdAKakGLadfg5535r/ghx3Z90AoBj3u</c:requestToken>
    <c:purchaseTotals>
        <c:currency>USD</c:currency>
    </c:purchaseTotals>
    <c:ccAuthReply>
        <c:reasonCode>100</c:reasonCode>
        <c:amount>5.00</c:amount>
        <c:authorizationCode>888888</c:authorizationCode>
        <c:avsCode>X</c:avsCode>
        <c:avsCodeRaw>I1</c:avsCodeRaw>
        <c:authorizedDateTime>2015-11-03T20:53:54Z</c:authorizedDateTime>
        <c:processorResponse>100</c:processorResponse>
        <c:reconciliationID>11267051CGJSMQDC</c:reconciliationID>
    </c:ccAuthReply>
    <c:token>
        <c:prefix>294672</c:prefix>
        <c:suffix>4397</c:suffix>
        <c:expirationMonth>08</c:expirationMonth>
        <c:expirationYear>2021</c:expirationYear>
    </c:token>
</c:replyMessage>
```

APPENDIX A

API Fields

Data Type Definitions

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

Table 3 Data Type Definitions

Data Type	Description
Date and time	Format is YYYY-MM-DDThh:mm:ssZ, where: ■ T separates the date and the time ■ Z indicates Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT) **Example** 2019-08-11T22:47:57Z equals August 11, 2019, at 22:47:57 (10:47:57 p.m.).
Integer	Whole number {..., -3, -2, -1, 0, 1, 2, 3, ...}
String	Sequence of letters, numbers, spaces, and special characters

Numbered Elements

The CyberSource XML schema includes several numbered elements. You can include these complex elements more than once in a request. For example, when a customer order includes more than one item, you must include multiple `<item>` elements in your request. Each item is numbered, starting with `0`. The XML schema uses an `id` attribute in the item's opening tag to indicate the number. For example:

```
<item id="0">
```

As a name-value pair field name, this tag is called `item_0`. In this portion of the field name, the underscore before the number does not indicate hierarchy in the XML schema. The item fields are generically referred to as `item_#_<element name>` in the documentation.

Below is an example of the numbered `<item>` element and the corresponding name-value pair field names. If you are using the Simple Object Access Protocol (SOAP), the client contains a corresponding `Item` class.

Example 8 Numbered XML Schema Element Names and Name-Value Pair Field Names

XML Schema Element Names	Corresponding Name-Value Pair Field Names

`<item id="0">`
`  <unitPrice>`
`  <quantity>`
`</item>`
	
	`item_0_unitPrice`
	`item_0_quantity`

`<item id="1">`
`  <unitPrice>`
`  <quantity>`
`</item>`
	
	`item_1_unitPrice`
	`item_1_quantity`

When a request in XML format includes an `<item>` element, the element must include an `id` attribute. For example: `<item id="0">`.

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

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

Table 4 Request Fields

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
billTo_city	City of the billing address.	ccAuthService (R)[2]	String (50)
billTo_country	Country of the billing address. Use the two-character *ISO Standard Country Codes*.	ccAuthService (R)[2]	String (2)
billTo_email	Customer's email address.	ccAuthService (R)[2]	String (255)
billTo_firstName	Customer's first name. For a credit card transaction, this name must match the name on the card.	ccAuthService (R)[2]	String (60)
billTo_ipAddress	Customer's IP address.	ccAuthService (O)	String (15)
billTo_lastName	Customer's last name. For a credit card transaction, this name must match the name on the card.	ccAuthService (R)[2]	String (60)
billTo_phoneNumber	Customer's phone number. CyberSource recommends that you include the country code when the order is from outside the U.S.	ccAuthService (O)	String (15)
billTo_postalCode	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	ccAuthService (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 20. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 4 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
billTo_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*.	ccAuthService (R)[2]	String (2)
billTo_street1	First line of the billing street address.	ccAuthService (R)[2]	String (60)
billTo_street2	Additional address information. **Example** Attention: Accounts Payable	ccAuthService (O)	String (60)
card_accountNumber	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.	ccAuthService (R)	Nonnegative integer (20)
card_cardType	Type of card to authorize. Possible values: ■ `001`: Visa ■ `002`: Mastercard ■ `003`: American Express ■ `004`: Discover	ccAuthService (R)	String (3)
card_cvNumber	CVN.	ccAuthService (R)	Nonnegative integer (4)
card_expirationMonth	Two-digit month in which the payment network token expires. Format: MM. Possible values: `01` through `12`.	ccAuthService (R)	String (2)
card_expirationYear	Four-digit year in which the payment network token expires. Format: YYYY.	ccAuthService (R)	Nonnegative integer (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.

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 20. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 4 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
ccAuthService_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.	ccAuthService (R)	String (40)
ccAuthService_ directoryServerTrans actionID	Identifier generated during the authentication transaction by the Mastercard Directory Server and passed back with the authentication results.	ccAuthService (O)	String (36)
ccAuthService_eciRaw	Raw electronic commerce indicator (ECI).	ccAuthService (O)	String (2)
ccAuthService_ networkTokenCryptogram	Token authentication verification value cryptogram. For token-based transactions with 3D Secure, you must submit both types of cryptograms: network token and 3D Secure. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats.	ccAuthService (O)	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 20. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 4 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
ccAuthService_ paSpecificationVersion	The 3D Secure version that you used for strong customer authentication (SCA); for example, 3D Secure version 1.0.2 or 2.0.0.	ccAuthService (O)	String (20)
ccAuthService_run	Whether to include **ccAuthService** in your request. Possible values: ■ `true`: Include the service in your request. ■ `false` (default): Do not include the service in your request.	ccAuthService (R)	
ccAuthService_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.	ccAuthService (R)	String (40)
encryptedPayment_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)	
item_#_productCode	Type of product. This value is used to determine the product category: electronic, handling, physical, service, or shipping. The default is `default`. See "Numbered Elements," page 19.	ccAuthService (O)	String (255)
item_#_productName	Name of the product. This field is required when the **item_#_productCode** value is not `default` or one of the values related to shipping and/or handling. See "Numbered Elements," page 19.	ccAuthService (See description)	String (255)

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 20. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 4 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
item_#_productSKU	Identification code for the product. This field is required when the **item_#_productCode** value is not `default` or one of the values related to shipping and/or handling. See "Numbered Elements," page 19.	ccAuthService (See description)	String (255)
item_#_quantity	The default is 1. This field is required when the **item_#_productCode** value is not `default` or one of the values related to shipping and/or handling. See "Numbered Elements," page 19.	ccAuthService (See description)	Integer (10)
item_#_taxAmount	Total tax to apply to the product. This value cannot be negative. See "Numbered Elements," page 19.	ccAuthService (See description)	String (15)
item_#_unitPrice	Per-item price of the product. This value cannot be negative.You can include a decimal point (.), but you cannot include any other special characters. See "Numbered Elements," page 19.	ccAuthService (See description)	String (15)
merchantID	Your CyberSource merchant ID. Use the same merchant ID for evaluation, testing, and production.	ccAuthService (R)	String (30)
merchantReferenceCode	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 Simple Order API*.	ccAuthService (R)	String (50)
paymentNetworkToken_ assuranceLevel	Confidence level of the tokenization. This value is assigned by the token service provider.	ccAuthService (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 20. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 4 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
paymentNetworkToken_ deviceTechType	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.	ccAuthService (O)	Integer (3)
paymentNetworkToken_ requestorID	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.	ccAuthService (O)	String (11)
paymentNetworkToken_ transactionType	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.	ccAuthService (R)	String (1)
paymentSolution	Identifies Google Pay as the payment solution that is being used for the transaction: Set the value for this field to `012`. This unique ID differentiates digital solution transactions within the CyberSource platform for reporting purposes.	ccAuthService (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 20. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 4 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
pos_environment	Operating environment. This field is supported only for American Express Direct and CyberSource through VisaNet. 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 courier. ***CyberSource through VisaNet*** For Mastercard transactions, the only valid values are `2` and `4`.	ccAuthService (O)	String (1)
purchaseTotals_currency	Currency used for the order: USD	ccAuthService (R)	String (5)
purchaseTotals_ grandTotalAmount	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.	ccAuthService (R)	String (15)

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 20. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

Table 4 Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
ucaf_authenticationData	Cryptogram for payment network tokenization transactions with Mastercard.	ccAuthService (R)	String (32)
ucaf_collectionIndicator	Required field for payment network tokenization transactions with Mastercard. Set the value for this field to `2`.	ccAuthService (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 20. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.

API Reply Fields

Because CyberSource can add reply fields and reason codes 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 reason codes without problems.
- Your error handler should use the **decision** field to determine the result if it receives a reply flag that it does not recognize.

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

Table 5 Reply Fields

Field	Description	Returned By	Data Type & Length
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.	ccAuthReply	String (4)
ccAuthReply_amount	Amount that was authorized.	ccAuthReply	String (15)
ccAuthReply_ authorizationCode	Authorization code. Returned only when the processor returns this value.	ccAuthReply	String (7)
ccAuthReply_ authorizedDateTime	Time of authorization.	ccAuthReply	Date and time (20)
ccAuthReply_avsCode	AVS results. See *Credit Card Services Using the Simple Order API* for a detailed list of AVS codes.	ccAuthReply	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 5 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
ccAuthReply_ avsCodeRaw	AVS result code sent directly from the processor. Returned only when the processor returns this value.	ccAuthReply	String (10)
ccAuthReply_cvCode	CVN result code. See *Credit Card Services Using the Simple Order API* for a detailed list of CVN codes.	ccAuthReply	String (1)
ccAuthReply_cvCodeRaw	CVN result code sent directly from the processor. Returned only when the processor returns this value.	ccAuthReply	String (10)
ccAuthReply_ paymentCardService	Mastercard service that was used for the transaction. Mastercard provides this value to CyberSource. Possible value: `53`: Mastercard card-on-file token service **Note** This field is returned only for CyberSource through VisaNet.	ccAuthReply	String (2)
ccAuthReply_ paymentCardService 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. **Note** This field is returned only for CyberSource through VisaNet.	ccAuthReply	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 5 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
ccAuthReply_ processorResponse	For most processors, this is the error message sent directly from the bank. Returned only when the processor returns this value.	ccAuthReply	String (10)
ccAuthReply_reasonCode	Numeric value corresponding to the result of the credit card authorization request. See *Credit Card Services Using the Simple Order API* for a detailed list of reason codes.	ccAuthReply	Integer (5)
ccAuthReply_ reconciliationID	Reference number for the transaction. This value is not returned for all processors.	ccAuthReply	String (60)
ccAuthReply_ transactionQualification	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. **Note** This field is returned only for CyberSource through VisaNet.	ccAuthReply	String (1)
ccAuthReversalReply_ paymentCardService	Mastercard service that was used for the transaction. Mastercard provides this value to CyberSource. Possible value: `53`: Mastercard card-on-file token service **Note** This field is returned only for CyberSource through VisaNet.	ccAuthReversal Reply	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 5 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
ccAuthReversalReply_ paymentCardService 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. **Note** This field is returned only for CyberSource through VisaNet.	ccAuthReversal Reply	String (1)
decision	Summarizes the result of the overall request. Possible values: ■ `ACCEPT` ■ `ERROR` ■ `REJECT` ■ `REVIEW`: Returned only when you use CyberSource Decision Manager.	ccAuthReply	String (6)
invalidField_0 through invalidField_N	Fields in the request that contained invalid data. For information about missing or invalid fields, see *Getting Started with CyberSource Advanced for the Simple Order API*.	ccAuthReply	String (100)

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 5 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
merchantReferenceCode	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.	ccAuthReply	String (50)
missingField_0 through missingField_N	Required fields that were missing from the request. For information about missing or invalid fields, see *Getting Started with CyberSource Advanced for the Simple Order API*.	ccAuthReply	String (100)
paymentNetworkToken_accountStatus	Possible values: ■ `N`: Nonregulated ■ `R`: Regulated This field is returned only for CyberSource through VisaNet.	ccAuthReply	String (1)
paymentNetworkToken_assuranceLevel	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.	ccAuthReply	String (2)
paymentNetworkToken_originalCardCategory	Mastercard product ID associated with the primary account number (PAN). For the possible values, see "Mastercard Product IDs" in *Credit Card Services Using the Simple Order API*. ***CyberSource through VisaNet*** For the possible values, see "Mastercard Product IDs" in *Credit Card Services for CyberSource through VisaNet Using the Simple Order API*. **Note** This field is returned only for Mastercard transactions on CyberSource through VisaNet.	ccAuthReply	String (3)
paymentNetworkToken_requestorID	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 supported only for CyberSource through VisaNet and FDC Nashville Global.	ccAuthService	String (11)
purchaseTotals_currency	Currency used for the order. For the possible values, see the *ISO Standard Currency Codes*.	ccAuthReply	String (5)
reasonCode	Numeric value corresponding to the result of the overall request. See *Credit Card Services Using the Simple Order API* for a detailed list of reason codes.	ccAuthReply	Integer (5)

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 5 Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
requestID	Identifier for the request generated by the client.	ccAuthReply	String (26)
requestToken	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.	ccAuthReply	String (256)
token_expirationMonth	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`.	ccAuthReply	String (2)
token_expirationYear	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.	ccAuthReply	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.	ccAuthReply	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.	ccAuthReply	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.