Authorizations with Payment Network Tokens

Simple Order API

cybersource
A Visa Solution

Developer Guide

Version: 23.02

Contents

Recent Revisions to This Document

23.02

Added FDC Nashville Global and Worldpay VAP.

23.01

Removed FDC Compass, FDC Nashville Global, Moneris, and Worldpay VAP.

22.04

Barclays

Removed Barclays as a supported processor for recurring payments. See Recurring Payments (on page 14).

Credit Mutuel-CIC

Removed Credit Mutuel-CIC as a supported processor for recurring payments. See Recurring Payments (on page 14).

HBoS

Added HBoS as a supported processor for authorizations with payment network tokens, recurring payments, merchant-initiated transactions and subsequent authorizations. See Authorizations with Payment Network Tokens (on page 7), Recurring Payments (on page 14), Merchant-Initiated Transactions (on page 11), and Subsequent Authorizations (on page 17).

HSBC

Removed HSBC as a supported processor for recurring payments and merchant-initiated transactions. See Recurring Payments (on page 14) and Merchant-Initiated Transactions (on page 11).

OmniPay Direct

Removed OmniPay Direct as a supported processor for recurring payments. See Recurring Payments (on page 14).

Streamline

Removed Streamline as a supported processor for recurring payments. See Recurring Payments (on page 14).

22.03

Visa Platform Connect

The deprecated API request and response fields, both named **paymentNetworkToken_assuranceLevel**, were replaced with new fields, both named **paymentNetworkToken_assuranceMethod**.

See Request Fields (on page 21) and Response Fields (on page 36).

22.02

Visa Platform Connect

Updated the **paymentNetworkToken_transactionType** field to include values `2` and `3`.

22.01

Barclays

Added Diners Club and Discover as supported card types for Barclays. See Supported Processors and Card Types (on page 7).

21.03

FDC Compass

Updated the **paymentNetworkToken_assuranceLevel** request and response fields. See Request Fields (on page 21) and Response Fields (on page 36) .

Vero

Added support for the processor to Merchant-Initiated Transactions (on page 11), Recurring Payments (on page 14), and Subsequent Authorizations (on page 17).

21.02

Visa Platform Connect

Updated In–App Transactions (on page 8) and the request field **paymentNetworkToken_requestorID**.

About This Guide

This section describes the audience and purpose of this guide as well as conventions and related documentation. See below for information about how to use this guide and where to find further information.

Audience and Purpose

This document is written for application developers who want to use payment network tokens in an order management system that already uses Cybersource credit card services. This document assumes that you are already familiar with the Cybersource credit card services as described in the *Credit Card Services Guide*.

Updating the Cybersource credit card services requires software development skills. You must write code that uses the API request and response fields to integrate authorizations with payment network tokens into your existing order management system.

Conventions

The following special statements are used in this document:

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

Related Documentation

Refer to the Support Center for complete technical documentation:

https://docs.cybersource.com/en/index.html

Customer Support

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

http://www.cybersource.com/support

Authorizations with Payment Network Tokens

This guide explains how to request an authorization with a token instead of a primary account number (PAN).

This document describes how to integrate the pass-through processing of tokens into your order management system. It does not describe the process of substituting a PAN with a token, also known as *token provisioning*. For information about token provisioning, contact your token service provider.

For an incremental authorization, you do not need to include any payment network tokenization fields in the authorization request because Cybersource obtains the payment network tokenization information from the original authorization request.

Supported Processors and Card Types

Processors and Card Types

Processor	Card Types
American Express Direct	American Express
Barclays	Visa, Mastercard, JCB, Maestro (International), Maestro (UK Domestic), Diners Club, Discover If you support Maestro (UK Domestic), you must also support Maestro (International), and you must support Mastercard Identity Check for both card types.
Chase Paymentech Tandem	Visa, Mastercard, American Express, Discover, Diners Club, JCB, China UnionPay
Chase Paymentech Solutions	Visa, Mastercard, American Express, Discover, Diners Club, JCB, Carte Blanche, Maestro (International)
Cielo 3.0	Visa, Mastercard, Elo
Credit Mutuel-CIC	Visa, Mastercard, Cartes Bancaires
Elavon Americas	Visa, Mastercard, American Express, JCB, Diners Club, Discover, China UnionPay
FDC Nashville Global	Visa, Mastercard
GPN	Visa, Mastercard, American Express, Discover, Diners Club, JCB

Processors and Card Types (continued)

Processor	Card Types
HSBC HSBC is the Cybersource name for HSBC U.K.	Visa, Mastercard, Maestro (UK Domestic), Maestro (International), Visa Electron
HBoS	Visa, Mastercard
JCN Gateway	JCB
OmniPay Direct	Visa, Mastercard, Discover, Diners Club, Maestro (UK Domestic), Maestro (International)
SIX	Visa, Mastercard
Streamline	Visa, Mastercard
TSYS Acquiring Solutions	Visa, Mastercard, American Express
Vero	Visa, Mastercard, Elo
Visa Platform Connect	Visa, Mastercard, American Express, Discover, JCB, Diners Club
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

In-App Transactions

For in-app transactions, include the following required fields in the authorization request:

billTo_city

billTo_country

billTo_email

billTo_firstName

billTo_lastName

billTo_postalCode

Required only for transactions in the U.S. and Canada.

billTo_state

Required only for transactions in the U.S. and Canada.

billTo_street1

card_accountNumber

Set to the token value that you received from the token service provider.

card_cardType

Cybersource strongly recommends that you send the card type even if it is optional for your processor. Omitting the card type can cause the transaction to be processed with the wrong card type.

card_expirationMonth

Set to the token expiration month that you received from the token service provider.

card_expirationYear

Set to the token expiration year that you received from the token service provider.

ccAuthService_cavv

For 3D Secure in-app transactions, set to the 3D Secure cryptogram. Otherwise, set to the network token cryptogram.

ccAuthService_commerceIndicator

ccAuthService_networkTokenCryptogram

ccAuthService_run

Set to `true`.

merchantID

merchantReferenceCode

purchaseTotals_currency

purchaseTotals_grandTotalAmount or item_#_unitPrice

paymentNetworkToken_transactionType

paymentNetworkToken_requestorID

Required on .

Include 3D Secure data in the following fields:

- For Visa requests, include the **ccAuthService_cavv** field set to the Visa Secure cryptogram.
- For Mastercard requests, include:
    - **ucaf_authenticationData**—set to the Identity Check cryptogram.

      ucaf_collectionIndicator—set to `2`.
- For JCB requests, include the **ccAuthService_cavv** field set to the J/Secure cryptogram.

See Simple Order API Fields (on page 21) for:

- Detailed descriptions of these required request fields
- Optional request fields
- Response fields

After a successful authorization request, the rest of the credit card processing proceeds as described in the *Credit Card Services Guide*.

Optional Features

Merchant-Initiated Transactions

Service:

- Authorization

Card type:

- Visa

Supported digital payments:

- Apple Pay
- Google Pay
- Samsung Pay

Processors:

Processors That Support Merchant-Initiated Transactions

Processors Supported	Digital Payments
Chase Paymentech Solutions	Apple Pay, Google Pay, Samsung Pay The only scenarios supported on Chase Paymentech Solutions are reauthorizations and unscheduled card-on-file transactions.
Elavon Americas	Apple Pay, Google Pay, Samsung Pay
HBoS	Apple Pay, Google Pay, Samsung Pay
Vero	Apple Pay, Google Pay
Visa Platform Connect	Apple Pay, Google Pay, Samsung Pay

For details on merchant-initiated transactions, see *Credit Card Services Optional Features*.

Multiple Partial Captures

See the following table.

Processors That Support Multiple Partial Captures

Processors	Supported Digital Payments
American Express Direct	Apple Pay, Samsung Pay
Barclays	Apple Pay, Google Pay, Samsung Pay
Chase Paymentech Solutions	Apple Pay, Samsung Pay
Elavon Americas	Apple Pay, Google Pay, Samsung Pay
HSBC HSBC is the Cybersource name for HSBC U.K.	Apple Pay, Google Pay, Samsung Pay
JCN Gateway	Apple Pay, Google Pay, Samsung Pay
Omnipay Direct	Apple Pay, Google Pay, Samsung Pay
Streamline	Apple Pay, Samsung Pay See Multiple Partial Captures on Streamline (on page 13).
TSYS Acquiring Solutions	Apple Pay, Samsung Pay

Important: *Multiple partial captures* and *split shipments* are not the same feature.

- The multiple partial captures feature is provided by the processor. This feature enables you to request multiple partial captures for one authorization.
- The split shipments feature is provided by Cybersource. This feature supports three different scenarios: multiple authorizations, multiple captures, and multiple authorizations with multiple captures. For more information, see Split Shipments (on page 16).

This feature enables you to request multiple partial captures for one authorization. You must ensure that the total amount of all the captures does not exceed the authorized amount.

Special Request Fields for Multiple Partial Captures

Processors:

- Barclays. The special request fields are required.
- FDMS Nashville. The special request fields are required for Visa and Mastercard transactions. They are not supported for other card types.
- OmniPay Direct. Cybersource strongly recommends that you include the special request fields.
- TSYS Acquiring Solutions. The special request fields are required.

Include the following special request fields in each capture request when you are requesting multiple partial captures:

- **ccCaptureService_sequence**
- **ccCaptureService_totalCount**

When you do not know the total number of captures that you are going to request, set the capture total count to an estimated value or `99` for all capture requests except the final one. For the final capture request, set the capture total count and the capture sequence to the same value.

Multiple Partial Captures on Streamline

Streamline might consider a partial capture to be a duplicate and reject the transaction when one or more of the following fields are the same for a merchant ID. You must ensure that you do not submit duplicate transaction information when using multiple partial captures; otherwise Streamline might reject the transaction.

- transaction date
- **card_accountNumber**
- **merchantReferenceCode**
- **purchaseTotals_grandTotalAmount**

Recurring Payments

Service:

- Authorization

Card Types:

- Visa
- Mastercard
- American Express
- Discover
- Diners Club
- JCB

Supported digital payments:

- Apple Pay
- Google Pay
- Samsung Pay

Processors:

See the following table.

Processors That Support Recurring Payments

Processors	Card Types	Supported Digital Payments
American Express Direct	American Express	Apple Pay, Google Pay, Samsung Pay
Chase Paymentech Solutions	Visa, Mastercard, American Express, Discover	Apple Pay, Chase Pay, Google Pay, Samsung Pay
Elavon Americas	Visa, Mastercard, American Express, JCB, Diners Club, Discover, China UnionPay	Apple Pay, Google Pay, Samsung Pay

Processors That Support Recurring Payments (continued)

Processors	Card Types	Supported Digital Payments
	When you request a recurring payment transaction with Visa, Elavon Americas requires you to be in compliance with the Visa merchant-initiated transactions mandate by including additional data in the request. You must do one of the following: • Include additional data as described in Merchant-Initiated Transactions (on page 11). • Make the request using the Token Management Service, which meets the merchant-initiated transactions requirements.	
GPN	Visa, Mastercard, American Express, Discover, Diners Club, JCB	Apple Pay, Google Pay, Samsung Pay
HBoS	Visa, Mastercard	Apple Pay, Google Pay, Samsung Pay
SIX	Visa, Mastercard, Discover, Diners Club, JCB, Maestro (International), Maestro (UK Domestic), China UnionPay, Visa Electron	Apple Pay, Google Pay

Processors That Support Recurring Payments (continued)

Processors	Card Types	Supported Digital Payments
TSYS Acquiring Solutions	Visa, Mastercard, American Express, Discover	Apple Pay, Google Pay, Samsung Pay
Vero	Visa, Mastercard, Elo	Apple Pay, Google Pay
	Visa, Mastercard, American Express, Diners Club, JCB, Discover	Australia and New Zealand Banking Group Ltd.—Apple Pay, Google Pay CitiBank Singapore Ltd.—Apple Pay Global Payments Asia Pacific—Apple Pay Vantiv—Apple Pay, Google Pay, Samsung Pay Westpac—Apple Pay, Google Pay

The recurring payments feature is described in *Credit Card Services Optional Features*.

Relaxed Requirements for Address Data and Expiration Date

To enable relaxed requirements for address data and expiration date, contact customer support to configure your account for this feature. For details about relaxed requirements, see Relaxed Address Data and Expiration Date.

Split Shipments

For details about split shipments, see the *Credit Card Services Optional Features*.

Services:

- Authorization
- Capture

Processors:

See the following table.

Processors That Support Split Shipments

Processor	Supported Digital Payments
GPN	Apple Pay, Google Pay, Samsung Pay
	Apple Pay, Samsung Pay **Important:** Split shipments are not available for Mastercard transactions in the IDR currency on .

The split-shipment feature enables you to split an order into multiple shipments with multiple captures.

Important: Split shipments are not available for Mastercard transactions in the IDR currency.

Important: Multiple partial captures and split shipments are not the same feature.

- The multiple partial captures feature is provided by the processor. This feature enables you to request multiple partial captures for one authorization. For more information, see Multiple Partial Captures (on page 12).
- The split shipments feature is provided by Cybersource. This feature supports three different scenarios: multiple authorizations, multiple captures, and multiple authorizations with multiple captures.

Subsequent Authorizations

Service:

- Authorization

Processors and card types:

See the following table.

Processors That Support Subsequent Authorizations

Processor	Card Types	Supported Digital Payments
HBoS	Visa, Mastercard	Apple Pay, Google Pay, Samsung Pay
JCN Gateway	JCB	Apple Pay
Streamline	Visa, Mastercard	Apple Pay, Samsung Pay
Vero	Visa, Mastercard, Elo	Apple Pay

When a customer purchases multiple items in one order, authorize and capture the amount of each item when you are ready to ship it.

Request a Subsequent Authorization

1. Request the authorization for the first item.
2. In each subsequent authorization request:

- Do not include the **ccAuthService_cavv** field.
- Include **subsequentAuth**=`true`.

API Fields

Formatting Restrictions

Do not use the following characters: < > $ % ^ * _ = [ ] \ { } | ; ~ ` Using these characters may result in data validation errors.

Data Type Definitions

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

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:** 2021-01-11T22:47:57Z is January 11, 2021, 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. Each item field is 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.

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`

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

Simple Order API Fields

Request Fields

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_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. It is recommended 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]	ccAuthService (R)[2]	String (9)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	Example: A1B 2C3		
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 (R)	String (60)
card_accountNumber	The payment network token value.	ccAuthService (R)	Nonnegative integer (20)
card_cardType	Type of card to authorize. Possible values: • `001`: Visa • `002`: Mastercard • `003`: American Express • `004`: Discover • `005`: Diners Club • `006`: Carte Blanche • `007`: JCB • `024`: Maestro (UK Domestic) • `036`: Cartes Bancaires • `042`: Maestro (International) • `054`: ELO • `062`: China UnionPay	ccAuthService (R)	String (3)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
card_cvNumber	CVN. See the *Credit Card Services Guide* for a list of processors that support CVN.	ccAuthService (O)	String with numbers only (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)
ccAuthService_cavv	Cardholder authentication verification value. The value for this field must be 28-character Base64 or 40-character hex binary. ***Transactions without 3D Secure Data*** Set to the value of the network token cryptogram. ***Visa and JCB Transactions with 3D Secure Data*** This value is a transaction identifier generated by the issuing bank during Visa Secure or JCB J/Secure payer authentication. 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 for in-app transactions with 3D Secure data.)	String (40)
ccAuthService_commerceIndicator	Type of transaction.	ccAuthService (R)	String (20)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	Possible values: • `aesk`: American Express card type • `dipb`: Discover card type • `internet`: Visa or JCB card type without 3D Secure data • `js`: J/Secure transaction • `recurring`: see Recurring Payments (on page 14). • `spa`: Mastercard card type • `vbv`: Visa Secure transaction **Important:** For Visa in-app transactions, the `internet` value is mapped to the Visa ECI value 7. For recurring payments, set this field to a value from the preceding list for the first payment and set this field to `recurring` for subsequent payments.		
ccAuthService_directoryServerTransactionID	Identifier generated during the authentication transaction by the Mastercard Directory Server and passed back with the authentication results.	ccAuthService (O)	String (36)
ccAuthService_firstRecurringPayment	Flag that indicates whether this transaction is the first in a series of recurring payments. See Recurring Payments (on page 14). ***OmniPay Direct***	ccAuthService (See description)	String (1)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	Possible values: • `Y:` Yes, the first payment in a series of recurring payments. • `N` (default): No, not the first payment in a series of recurring payments.		
ccAuthService_networkTokenCryptogram	Token authentication verification value. For token-based transactions with 3D Secure or Identity Check, you must submit both types of cryptograms: network token and 3D Secure/Identity Check. 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)
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)	String (5)
ccCaptureService_sequence	Capture number when requesting multiple partial captures for one authorization. Used along with **ccCaptureService_totalCount** to track which capture is being processed. For example, the second of five captures	ccCaptureService	Integer (2)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	would be passed to Cybersource as **ccCaptureService_sequence** = 2 and **ccCaptureService_totalCount** = 5. For the list of processors that support this field, see Special Request Fields for Multiple Partial Captures (on page 13).		
ccCaptureService_totalCount	Total number of captures when requesting multiple partial captures for one authorization. Used along with **ccCaptureService_sequence** to track which capture is being processed. For example, the second of five captures would be passed to Cybersource as **ccCaptureService_sequence** = 2 and **ccCaptureService_totalCount** = 5. For the list of processors that support this field, see Special Request Fields for Multiple Partial Captures (on page 13).	ccCaptureService (R)	Integer (2)
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)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
paymentNetworkToken_assuranceMethod	Confidence level of the tokenization, specified by the method used to verify the account or authenticate the cardholder. This field is supported for Visa Platform Connect only. The token service provider assigns the value of this field. Possible values: • `00`: No issuer identity and verification (ID&V). • `10`: Card issuer account verification. • `11`: Card issuer interactive, single-factor cardholder authentication. • `12`: Card issuer interactive, two-factor cardholder authentication. • `13`: Card issuer risk-oriented, non-interactive cardholder authentication. • `14`: Card issuer asserted authentication.	ccAuthService (O)	String (2)
paymentNetworkToken_deviceTechType	Type of technology used in the device to store token data. Possible values: • `001`: Secure element (SE) Smart card or memory with restricted access and strong encryption, which prevents tampering. To store payment credentials, an SE is tested against a set of requirements defined by the payment networks. Apple Pay uses this technology. • `002`: Host card emulation (HCE)	ccAuthService (O)	Integer (3)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	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. To store payment credentials, a database must meet very high level security requirements that exceed PCI DSS. Google Pay uses this technology.		
paymentNetworkToken_requestorID Writer's Note: This field is in: • Payment Network Tokenization Guides • CtV Beta versions of the PIN Debit Guides When you update the field description in one set of guides, you must also update it in the other set of guides.	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 field is supported only for and Chase Paymentech Solutions.	ccAuthService (R on ; otherwise, optional)	String (11)
paymentNetworkToken_transactionType	Type of transaction that provided the token data.	ccAuthService (R)	String (1)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	This value does not specify the token service provider; it specifies the entity that provided you with information about the token. Possible values: • `1`: In-app transaction. For Apple Pay, Google Pay, RuPay seamless flow, Samsung Pay, and Visa Safe Click (VSC). • `2`: Near-field communication (NFC) transaction. The customer's mobile device provided the token data for a contactless EMV transaction. For recurring transactions, use this value if the original transaction was a contactless EMV transaction. • `3`: Merchant-initiated transaction with stored customer credentials on Visa Platform Connect.		
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 .	ccAuthService (Optional for in-app transactions.) Writer's note: This field is in: • ENT and CtV versions of the Credit Card Guides • ENT Beta and CtV Beta	String (1)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	• 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 . • 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 . For Mastercard transactions, the only valid values are 2 and 4.	versions of the Retail Guides • ENT and CtV versions of the Tokenization Supplement When you update the field description in one set of guides, you must also update it in the other two sets of guides.	
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)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
subsequentAuth	Indicates whether the transaction is a merchant-initiated transaction or subsequent authorization. Possible values: • `true`: Merchant-initiated transaction or subsequent authorization • `false`: Not a merchant-initiated transaction or subsequent authorization This field is supported for: • All merchant-initiated transactions. • Subsequent authorizations on Streamline. The value for this field does not correspond to any data in the TC 33 capture file.53[1] ***Related Link*** Credit Card Services Guide	ccAuthService: • R for merchant-initiated transactions. • R for subsequent authorizations on Streamline. • Otherwise, not used.	String (5)
subsequentAuthFirst	Indicates whether the transaction is the first merchant-initiated transaction in a series, which means that the customer initiated the previous transaction. Possible values:	ccAuthService (R for merchant-initiated transactions; otherwise, not used.)	String (5)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	• `true`: First merchant-initiated transaction • `false`: Not the first merchant-initiated transaction • This field is supported only for merchant-initiated transactions. The value for this field corresponds to the following data in the TC 33 capture file53[1]: • Record: CP01 TCR1 • Position: 136 • Field: POS Environment ***Related Link*** Credit Card Services Guide		
subsequentAuthOriginalAmount	Amount of the original authorization. This field is supported only for the following kinds of transactions with Discover: • Merchant-initiated transactions • Subsequent authorizations on Streamline ***Related Link*** Credit Card Services Guide	ccAuthService (See description)	String (60)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
subsequentAuthReason	Reason for the merchant-initiated transaction or incremental authorization. Possible values: Reason for the merchant-initiated transaction. Possible values: • 1: Resubmission • 2: Delayed charge • 3: Reauthorization for split shipment • 4: No show • 5: Incremental authorization This field is supported only for: • The five kinds of merchant-initiated transactions in the preceding list. • Incremental authorization service. This field is supported only for the five kinds of merchant-initiated transactions in the preceding list. The value for this field corresponds to the following data in the TC 33 capture file53[1]: • Record: CP01 TCR0 • Position: 160-163 • Field: Message Reason Code	ccAuthService (See description)	String (1)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	Related Link Credit Card Services Guide		
subsequentAuthStoredCredential	Indicates whether you obtained the payment information from credentials on file (COF) instead of from the customer. Possible values: • `true`: Transaction uses COF • `false`: Transaction does not use COF • `Y`: Transaction uses COF • `N`: Transaction does not use COF When you use the Token Management Service, CyberSource sets this field to `true` for you. When you use the Token Management Service, Cybersource sets this field to `Y` for you. ***Related Link*** Credit Card Services Guide *Token Management Service Using the Simple Order API* (PDF | HTML)	ccAuthService (R for transactions that use COF information; otherwise, not used.)	String (5)
subsequentAuthTransactionID	Network transaction identifier that was returned in the **ccAuthReply_paymentNetworkTransactionID** field in the reply message for	ccAuthService:	String (15)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	either the original authorization in the series or the previous authorization in the series. Network transaction identifier that was returned in the **auth_payment_network_transaction_id** field in the reply message for either the original authorization in the series or the previous authorization in the series. The value for this field does not correspond to any data in the TC 33 capture file.53[1] FDI Australia This field is supported for installment payments. All Processors Other Than FDI Australia This field is supported for merchant-initiated transactions. ***Related Link*** Credit Card Services Guide	• R for merchant-initiated transactions. • Otherwise, not used.	
ucaf_authenticationData	Universal cardholder authentication field (UCAF) data. Set the value for this field to the Mastercard Identity Check cryptogram.	ccAuthService (R for in-app transactions with 3D Secure data)	String (32)
ucaf_collectionIndicator	Collection indicator for the universal cardholder authentication field for Mastercard. Set the value for this field to 2.	ccAuthService (R for in-app transactions with 3D Secure data)	String with numbers only (1)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
1—The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. 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 (on page 16). **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.			

Response Fields

Important: Because Cybersource can add response fields and reason codes at any time:

- You must parse the response data according to the names of the fields instead of the field order in the response. For more information about parsing response 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 response flag that it does not recognize.

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

Response 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. This field is returned only for .	ccAuthReply	String (4)

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
	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.		
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 Guide* for a detailed list of AVS codes.	ccAuthReply	String (1)
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 Guide* 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 This field is returned only for .	ccAuthReply	String (2)
ccAuthReply_paymentCardServiceResult	Result of the Mastercard card-on-file token service. Mastercard provides this value to Cybersource. Possible values:	ccAuthReply	String (1)

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
	• `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.		

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
	This field is returned only for .		
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. This field is returned only for .	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 This field is returned only for .	ccAuthReversalReply	String (2)
ccAuthReversalReply_paymentCardService Result	Result of the Mastercard card-on-file token service. Mastercard provides this value to Cybersource. Possible values:	ccAuthReversalReply	String (1)

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
	• `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 .		
decision	Summarizes the result of the overall request. Possible values:	ccAuthReply	String (6)

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
	• `ACCEPT` • `ERROR` • `REJECT` • `REVIEW`: Returned only when you use Cybersource Decision Manager.		
invalidField_0...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)
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...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 Writer's Note: This field is in:	Possible values: • `N`: Nonregulated • `R`: Regulated This field is returned only for .	ccAuthReply	String (1)

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
• Payment Network Tokenization Guides • CtV Beta versions of the PIN Debit Guides When you update the field description in one set of guides, you must also update it in the other set of guides.			

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
paymentNetworkToken_assuranceMethod	Confidence level of the tokenization, specified by the method used to verify the account or authenticate the cardholder. This field is supported for Visa Platform Connect only. The value of this field is assigned by the token service provider. Possible values: • `00`: No issuer identity and verification (ID&V). • `10`: Card issuer account verification. • `11`: Card issuer interactive, single-factor cardholder authentication. • `12`: Card issuer interactive, two-factor cardholder authentication. • `13`: Card issuer risk-oriented, non-interactive cardholder authentication. • `14`: Card issuer asserted authentication.	ccAuthReply	String (2)
paymentNetworkToken_originalCardCategory	Mastercard product ID associated with the primary account number (PAN). For the possible values, see Mastercard Product IDs in the Credit Card Services Guide. This field is returned only for Mastercard transactions on .	ccAuthReply	String (3)
paymentNetworkToken_requestorID Writer's Note: This field is in:	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. This field is supported only for .	ccAuthService	String (11)

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
• Payment Network Tokenization Guides • CtV Beta versions of the PIN Debit Guides When you update the field description in one set of guides, you must also update it in the other set of guides.			
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 Guide* for a detailed list of reason codes.	ccAuthReply	Integer (5)
requestID	Identifier for the request.	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.	ccAuthReply	String (2)

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
	Possible values: `01` through `12`.		
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 6 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 4 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. 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.			

Simple Order API Examples

Name-Value Pair Examples

In-App Authorization Request for Visa

```
merchantID=Foster_City_Flowers
merchantReferenceCode=12345678
billTo_firstName=Jane
billTo_lastName=Smith
billTo_street1=100 Main Street
billTo_street2=Suite 1234
billTo_city=Foster City
billTo_state=CA
billTo_postalCode=94404
billTo_country=US
billTo_email=jsmith@example.com
purchaseTotals_currency=USD
purchaseTotals_grandTotalAmount=16.00
card_accountNumber=4650100000000839
card_expirationMonth=12
card_expirationYear=2031
ccAuthService_run=true
ccAuthService_cavv=EHuWW9PiBkWvqE5juRwDzAUFBAk=
ccAuthService_commerceIndicator=vbv
ccAuthService_networkTokenCryptogram=qE5juRwDzAUFBAkEHuWW9PiBkWv=
paymentNetworkToken_transactionType=1
```

In-App Authorization Request for Mastercard

```
merchantID=Foster_City_Flowers
merchantReferenceCode=12345678
billTo_firstName=Jane
billTo_lastName=Smith
billTo_street1=100 Main Street
billTo_street2=Suite 1234
billTo_city=Foster City
billTo_state=CA
billTo_postalCode=94404
billTo_country=US
billTo_email=jsmith@example.com
purchaseTotals_currency=USD
purchaseTotals_grandTotalAmount=16.00
```

```
card_accountNumber=4650100000000839
card_expirationMonth=12
card_expirationYear=2031
ucaf_authenticationData=EHuWW9PiBkWvqE5juRwDzAUFBAk=
ucaf_collectionIndicator=2
ccAuthService_run=true
ccAuthService_commerceIndicator=spa
ccAuthService_networkTokenCryptogram=qE5juRwDzAUFBAkEHuWW9PiBkWv=
paymentNetworkToken_transactionType=1
```

In-App Authorization Request for American Express

```
merchantID=Foster_City_Flowers
merchantReferenceCode=12345678
billTo_firstName=Jane
billTo_lastName=Smith
billTo_street1=100 Main Street
billTo_street2=Suite 1234
billTo_city=Foster City
billTo_state=CA
billTo_postalCode=94404
billTo_country=US
billTo_email=jsmith@example.com
purchaseTotals_currency=USD
purchaseTotals_grandTotalAmount=16.00
card_accountNumber=4650100000000839
card_expirationMonth=12
card_expirationYear=2031
ccAuthService_run=true
ccAuthService_cavv=EHuWW9PiBkWvqE5juRwD
ccAuthService_commerceIndicator=aesk
ccAuthService_networkTokenCryptogram=qE5juRwDzAUFBAkEHuWW9PiBkWv=
paymentNetworkToken_transactionType=1
```

XML Examples

In-App Authorization Request for Visa

```
<requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.104">
      <merchantID>Foster_City_Flowers</merchantID>
      <merchantReferenceCode>12345678</merchantReferenceCode>
      <billTo>
            <firstName>Jane</firstName>
            <lastName>Smith</lastName>
```

```
            <street1>100 Main Street</street1>
            <street2>Suite 1234</street2>
            <city>Foster City</city>
            <state>CA</state>
            <postalCode>94404</postalCode>
            <country>US</country>
            <email>jsmith@example.com</email>
      </billTo>
      <purchaseTotals>
            <currency>USD</currency>
            <grandTotalAmount>16.00</grandTotalAmount>
      </purchaseTotals>
      <card>
            <accountNumber>4650100000000839</accountNumber>
            <expirationMonth>12</expirationMonth>
            <expirationYear>2031</expirationYear>
      </card>
      <ccAuthService run="true">
            <cavv>EHuWW9PiBkWvqE5juRwDzAUFBAk=</cavv>

 <networkTokenCryptogram>qE5juRwDzAUFBAkEHuWW9PiBkWv=</networkTokenCryptogram>
            <commerceIndicator>vbv</commerceIndicator>
      </ccAuthService>
      <paymentNetworkToken>
            <transactionType>1</transactionType>
      </paymentNetworkToken>
</requestMessage>
```

In-App Authorization Request for Mastercard

```
<requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.104">
      <merchantID>Foster_City_Flowers</merchantID>
      <merchantReferenceCode>12345678</merchantReferenceCode>
      <billTo>
            <firstName>Jane</firstName>
            <lastName>Smith</lastName>
            <street1>100 Main Street</street1>
            <street2>Suite 1234</street2>
            <city>Foster City</city>
            <state>CA</state>
            <postalCode>94404</postalCode>
            <country>US</country>
            <email>jsmith@example.com</email>
      </billTo>
      <purchaseTotals>
            <currency>USD</currency>
            <grandTotalAmount>16.00</grandTotalAmount>
      </purchaseTotals>
```

```
      <card>
            <accountNumber>4650100000000839</accountNumber>
            <expirationMonth>12</expirationMonth>
            <expirationYear>2031</expirationYear>
      </card>
      <ucaf>
            <authenticationData>EHuWW9PiBkWvqE5juRwDzAUFBAk=</authenticationData>
            <collectionIndicator>2</collectionIndicator>
      </ucaf>
      <ccAuthService run="true">

 <networkTokenCryptogram>qE5juRwDzAUFBAkEHuWW9PiBkWv=</networkTokenCryptogram>
            <commerceIndicator>spa</commerceIndicator>
      </ccAuthService>
      <paymentNetworkToken>
            <transactionType>1</transactionType>
      </paymentNetworkToken>
</requestMessage>
```

In-App Authorization Request for American Express

```
<requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.104">
      <merchantID>Foster_City_Flowers</merchantID>
      <merchantReferenceCode>12345678</merchantReferenceCode>
      <billTo>
            <firstName>Jane</firstName>
            <lastName>Smith</lastName>
            <street1>100 Main Street</street1>
            <street2>Suite 1234</street2>
            <city>Foster City</city>
            <state>CA</state>
            <postalCode>94404</postalCode>
            <country>US</country>
            <email>jsmith@example.com</email>
      </billTo>
      <purchaseTotals>
            <currency>USD</currency>
            <grandTotalAmount>16.00</grandTotalAmount>
      </purchaseTotals>
      <card>
            <accountNumber>4650100000000839</accountNumber>
            <expirationMonth>12</expirationMonth>
            <expirationYear>2031</expirationYear>
      </card>
      <ccAuthService run="true">

 <networkTokenCryptogram>qE5juRwDzAUFBAkEHuWW9PiBkWv=</networkTokenCryptogram>
            <commerceIndicator>aesk</commerceIndicator>
```

```
      </ccAuthService>
      <paymentNetworkToken>
            <transactionType>1</transactionType>
      </paymentNetworkToken>
</requestMessage>
```