Authorizations with Payment Network Tokens

SCMP API

Developer Guide

cybersource
A Visa Solution

© 2023. Cybersource Corporation. All rights reserved.

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

Restricted Rights Legends

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

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 Unpublished rights reserved under the copyright laws of the United States.

Trademarks

Authorize.Net, eCheck.Net, and The Power of Payment are registered trademarks of Cybersource Corporation. Cybersource and Cybersource Decision Manager are trademarks and/or service marks of Cybersource Corporation. Visa, Visa International, Cybersource, the Visa logo, the Cybersource logo, and 3-D Secure are the registered trademarks of Visa International in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Version: 23.01

Contents

Recent Revisions to This Document

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 **payment_network_token_assurance_level**, were replaced with new fields, both named **payment_network_token_assurance_method**.

See Request Fields (on page 20) and Response Fields (on page 33).

22.02

Visa Platform Connect

Updated the **payment_network_token_transaction_type** 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 **payment_network_token_assurance_level** request and response fields. See Request Fields (on page 20) and Response Fields (on page 33).

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 **payment_network_token_requestor_id**.

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 Tampa	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
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

In–App Transactions

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

bill_address1

bill_city

bill_country

bill_state

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

bill_zip

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

card_type

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.

cavv

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

currency

customer_cc_expmo

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

customer_cc_expyr

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

customer_cc_number

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

customer_email

customer_firstname

customer_lastname

e_commerce_indicator

grand_total_amount or offer0:amount

ics_applications

Set to `ics_auth`.

merchant_id

merchant_ref_number

network_token_cryptogram

payment_network_token_requestor_id

Required on

payment_network_token_transaction_type

Include 3D Secure data in the following fields:

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

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

See SCMP API Fields (on page 20) 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:

- **capture_sequence**
- **capture_total_count**

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
- **customer_cc_number**
- **merchant_ref_number**
- **grand_total_amount**

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 **cavv** field.
- Include **subsequent_auth**=Y.

API Fields

Formatting Restrictions

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

Data Type Definitions

Data Type	Description
Date and time	Format is yyyy-MM-DDThhmmssZ where: • T separates the date and the time. • Z indicates Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). **Example:** 2021-01-11T224757Z is January 11, 2021, at 22:47:57 (10:47:57 p.m.).
Decimal	Number that includes a decimal point. **Example:** 23.45, -0.1, 4.0, 90809.0468
Integer	Whole number {..., -3, -2, -1, 0, 1, 2, 3, ...}
Nonnegative integer	Whole number greater than or equal to zero {0, 1, 2, 3, ...}
Positive integer	Whole number greater than zero {1, 2, 3, ...}
String	Sequence of letters, numbers, spaces, and special characters

SCMP API Fields

Request Fields

Request Fields

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
auth_first_recurring_payment	Flag that indicates whether this transaction is the first in a series of recurring payments. Possible values: • `Y`: Yes, this is the first payment in a series of recurring payments. `N` (default): No, this is not the first payment in a series of recurring payments. See Recurring Payments (on page 14).	**ics_auth** (See description)	String (1)
bill_address1	First line of the billing street address.	**ics_auth** (R)[2]	: String (40) All other processors : String (60)
bill_address2	Additional address information. ***Example:*** Attention: Accounts Payable	**ics_auth** (R)	: String (40) All other processors : String (60)
bill_city	City of the billing address.	**ics_auth** (R)[2]	String (50)
bill_country	Country of the billing address. Use the two-character *ISO Standard Country Codes*.	**ics_auth** (R)[2]	String (2)
bill_state	State or province of the billing address. For an address in the U.S. or Canada, use the *State, Province, and Territory Codes for the United States and Canada*.	**ics_auth** (R)[2]	String (2)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
bill_zip	Postal code for the billing address. The postal code must consist of 5 to 9 digits. When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits] **Example:** 12345-6789 When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space][numeric][alpha][numeric] **Example:** A1B 2C3	**ics_auth** (R)[2]	: String (9) All other processors : String (10)
capture_sequence	Capture number when requesting multiple partial captures for one authorization. Used along with **capture_total_count** to track which capture is being processed. For example, the second of five captures would be passed to Cybersource as **capture_sequence** = 2 and **capture_total_count** = 5. For the list of processors that support this field, see (See Special Request Fields for Multiple Partial Captures.)	**ics_bill**	Integer (2)
capture_total_count	Total number of captures when requesting multiple partial captures for one authorization. Used along with **capture_sequence** to track which capture is being processed. For example, the second of five captures would be passed to Cybersource as **capture_sequence** = 2 and **capture_total_count** = 5. For the list of processors that support this field, see (See Special Request Fields for Multiple Partial Captures.)	**ics_bill**	Integer (2)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
card_type	Type of card to authorize. Possible values: • `001`: Visa • `002`: Mastercard • `003`: American Express • `004`: Discover • `005`: Diners Club • `006`: Carte Blanche • `007`: JCB • `024`: Maestro (UK Domestic) • `036`: Cartes Bancaires • `042`: Maestro (International) • `054`: ELO • `062`: China UnionPay	**ics_auth** (O)	String (3)
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. ***Visa Platform Connect***	**ics_auth** (R for in-app transactions with 3D Secure data.)	String (40)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	The value for this field corresponds to the following data in the TC 33 capture file1: • Record: CP01 TCR8 • Position: 77-78 • Field: CAVV version and authentication action.		
currency	Currency used for the order: USD	**ics_auth** (R)	String (5)
customer_cc_cv_number	CVN. See *Credit Card Services Using the SCMP API* for a list of processors that support CVN.	**ics_auth** (O)	Nonnegative integer (4)
customer_cc_expmo	Two-digit month in which the payment network token expires. Format: MM. Possible values: `01` through `12`.	**ics_auth** (R)	String (2)
customer_cc_expyr	Four-digit year in which the payment network token expires. Format: YYYY.	**ics_auth** (R)	Nonnegative integer (4)
customer_cc_number	The payment network token value.	**ics_auth** (R)	Nonnegative integer (20)
customer_email	Customer's email address.	**ics_auth** (R)[2]	String (255)
customer_firstname	Customer's first name. For a credit card transaction, this name must match the name on the card.	**ics_auth** (R)[2]	String (60)
customer_lastname	Customer's last name. For a credit card transaction, this name must match the name on the card.	**ics_auth** (R)[2]	String (60)
customer_phone	Customer's phone number. It is recommended that you include the country code when the order is from outside the U.S.	**ics_auth** (O)	String (15)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
directory_server_transaction_id	Identifier generated during the authentication transaction by the Mastercard Directory Server and passed back with the authentication results.	**ics_auth** (O)	String (36)
e_commerce_indicator	Type of transaction. 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.	**ics_auth** (R)	String (20)
grand_total_amount	Grand total for the order. This value cannot be negative. You can include a decimal point (.), but you cannot include any other special characters. Cybersource truncates the amount to the correct number of decimal places.	**ics_auth** (R)	Decimal (15)
ics_applications	Cybersource service to process for the request:	**ics_auth** (R)	String (255)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	`ics_auth`		
merchant_id	Your Cybersource merchant ID. Use the same merchant ID for evaluation, testing, and production.	**ics_auth** (R)	String (30)
merchant_ref_number	Merchant-generated order reference or tracking number. Cybersource recommends that you send a unique value for each transaction so that you can perform meaningful searches for the transaction. For information about tracking orders, see *Getting Started with Cybersource Advanced for the SCMP API*.	**ics_auth** (R)	String (50)
network_token_cryptogram	Token authentication verification value cryptogram. For token-based transactions with 3D Secure or 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.	**ics_auth** (O)	String (40)
pa_specification_version	The 3D Secure version that you used for strong customer authentication (SCA); for example, 3D Secure 1.0.2 or 2.0.0.	**ics_auth** (O)	String (20)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
payment_network_token_assurance_method	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.	**ics_auth** (O)	String (2)
payment_network_token_device_tech_type	Type of technology used in the device to store token data. Possible value: • `001`: Secure Element (SE)	**ics_auth** (O)	Integer (3)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	Smart card or memory with restricted access and encryption to prevent data tampering. For storing payment credentials, a SE is tested against a set of requirements defined by the payment networks. This technology is used by Apple Pay. • `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. To store payment credentials, a database must meet very high level security requirements that exceed PCI DSS. This technology is used by Google Pay.		
payment_network_token_requestor_id	Value that identifies your business and indicates that the cardholder's account number is tokenized. This value is assigned by the token service provider and is unique within the token service provider's database. This field is supported only for and Chase Paymentech Solutions.	**ics_auth** (R on ; otherwise, optional)	Integer (1)
payment_network_token_transaction_type	Type of transaction that provided the token data. This value does not specify the token service provider; it specifies the entity that provided you with information about the token. Possible values:	**ics_auth** (R)	String (1)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	• `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 . • `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 .	**ics_auth** (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 versions of the Retail Guides • ENT and CtV versions	String (1)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	• `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`.	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.	
subsequent_auth	Indicates whether the transaction is a merchant-initiated transaction or subsequent authorization. Possible values: • `N`: Merchant-initiated transaction or subsequent authorization • `Y`: 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]	**ics_auth**: • R for merchant-initiated transactions. • R for subsequent authorizations on Streamline. • Otherwise, not used.	String (5)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	Related Link Credit Card Services Guide		
subsequent_auth_first	Indicates whether the transaction is the first merchant-initiated transaction in a series, which means that the customer initiated the previous transaction. Possible values: • `Y`: First merchant-initiated transaction • `N`: 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	**ics_auth** (R for merchant-initiated transactions; otherwise, not used.)	String (5)
subsequent_auth_original_amount	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***	**ics_auth** (See description)	String (60)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	Credit Card Services Guide		
subsequent_auth_reason	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 ***Related Link*** Credit Card Services Guide	**ics_auth** (See description)	String (1)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
subsequent_auth_stored_credential	Indicates whether you obtained the payment information from credentials on file (COF) instead of from the customer. Possible values: • `Y`: Transaction uses COF • `N`: Transaction does not use COF 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 SCMP API* (PDF | HTML)	**ics_auth** (R for transactions that use COF information; otherwise, not used.)	String (5)
subsequent_auth_transaction_id	Network transaction identifier that was returned in the **ccAuthReply_paymentNetworkTransactionID** field in the reply message for 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.	**ics_auth**: • R for merchant-initiated transactions. • Otherwise, not used.	String (15)

Request Fields (continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
	All Processors Other Than FDI Australia This field is supported for merchant-initiated transactions. ***Related Link*** Credit Card Services Guide		
ucaf_authentication_data	Universal cardholder authentication field (UCAF) data. Set the value for this field to the Mastercard Identity Check cryptogram.	**ics_auth** (R for in-app transactions with 3D Secure data)	String (32)
ucaf_collection_indicator	Collection indicator for the universal cardholder authentication field for Mastercard. Set the value for this field to 2.	**ics_auth** (R for in-app transactions with 3D Secure data)	String with numbers only (1)
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, response codes, and response flags 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 response codes and response flags without problems.
- Your error handler should use the **ics_rcode** 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 SCMP API* for detailed descriptions of additional API response fields.

Response Fields

Field	Description	Returned By	Data Type & Length
auth_auth_amount	Amount that was authorized.	**ics_auth**	Decimal (15)
auth_auth_avs	AVS result code. See *Credit Card Services Using the SCMP API* for a detailed list of AVS values.	**ics_auth**	String (1)
auth_auth_code	Authorization code. Returned only when the processor returns this value.	**ics_auth**	String (7)
auth_auth_response	For most processors, this value is the error message sent directly from the bank. Returned only when the processor returns this value.	**ics_auth**	String (10)
auth_avs_raw	AVS result code sent directly from the processor. Returned only when the processor returns this value.	**ics_auth**	String (10)
auth_payment_card_service	Mastercard service that was used for the transaction. Mastercard provides this value to Cybersource. Possible value: `53`: Mastercard card-on-file token service The value for this field corresponds to the following data in the TC 33 capture file[1]: • Record: CP01 TCR6 • Position: 133-134 • Field: Mastercard Merchant on-behalf service.	**ics_auth**	String (2)

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
	This field is returned only for .		
auth_payment_card_service_result	Result of the Mastercard card-on-file token service. Mastercard provides this value to Cybersource. Possible values: • `C`: Service completed successfully. • `F`: One of the following: ◦ Incorrect Mastercard POS entry mode. The Mastercard POS entry mode should be 81 for an authorization or authorization reversal. ◦ Incorrect Mastercard POS entry mode. The Mastercard POS entry mode should be 01 for a tokenized request. ◦ Token requestor ID is missing or formatted incorrectly. • `I`: One of the following: ◦ Invalid token requestor ID. ◦ Suspended or deactivated token. ◦ Invalid token (not in mapping table). • `T`: Invalid combination of token requestor ID and token. • `U`: Expired token. • `W`: Primary account number (PAN) listed in electronic warning bulletin.This field is returned only for . This field is returned only for .	**ics_auth**	String (1)
auth_rcode	Indicates whether the service request was successful. Possible values:	**ics_auth**	Integer (1)

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
	• `-1`: An error occurred. • `0`: The request was declined. • `1`: The request was successful.		
auth_reversal_payment_card_service	Mastercard service that was used for the transaction. Mastercard provides this value to Cybersource. Possible value: `53`: Mastercard card-on-file token service The value for this field corresponds to the following data in the TC 33 capture file1: • Record: CP01 TCR6 • Position: 133-134 • Field: Mastercard Merchant on-behalf service. This field is returned only for .	**ics_auth_reversal**	String (2)

auth_reversal_payment_card_service_result	Result of the Mastercard card-on-file token service. Mastercard provides this value to Cybersource. Possible values:
	
	• `C`: Service completed successfully.
	• `F`: One of the following:
	  ◦ Incorrect Mastercard POS entry mode. The Mastercard POS entry mode should be 81 for an authorization or authorization reversal.
	  ◦ Incorrect Mastercard POS entry mode. The Mastercard POS entry mode should be 01 for a tokenized request.
	  ◦ Token requestor ID is missing or formatted incorrectly.
		ics_auth_reversal	String (1)

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
	• `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 . This field is returned only for .		
auth_rflag	One-word description of the result of the entire request. See *Credit Card Services Using the SCMP API* for a detailed list of rflag values.	**ics_auth**	String (50)
auth_rmsg	Message that explains the response flag auth_rflag. Do not display this message to the customer, and do not use this field to write an error handler.	**ics_auth**	String (255)
auth_trans_ref_no	Reference number for the transaction. This value is not returned for all processors.	**ics_auth**	String (60)
auth_transaction_qualification	Type of authentication for which the transaction qualifies as determined by the Mastercard authentication service, which confirms the identity of the cardholder. Mastercard provides this value to Cybersource. Possible values: • `1`: Transaction qualifies for Mastercard authentication type 1.	**ics_auth**	String (1)

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
	• `2`: Transaction qualifies for Mastercard authentication type 2. The value for this field corresponds to the following data in the TC 33 capture file1: • Record: CP01 TCR6 • Position: 132 • Field: Mastercard Member Defined service. This field is returned only for .		
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 . 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.	**ics_auth**	String (4)
currency	Currency used for the order. For the possible values, see the *ISO Standard Currency Codes*.	**ics_auth**	String (5)
ics_rcode	Indicates whether the service request was successful. Possible values: • `-1`: An error occurred. • `0`: The request was declined. • `1`: The request was successful.	**ics_auth**	Integer (1)

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
ics_rflag	One-word description of the result of the entire request. See *Credit Card Services Using the SCMP API* for a detailed list of rflag values.	**ics_auth**	String (50)
ics_rmsg	Message that explains the reply flag **ics_rflag**. Do not display this message to the customer, and do not use this field to write an error handler.	**ics_auth**	String (255)
merchant_ref_number	Order reference or tracking number that you provided in the request. If you included multi-byte characters in this field in the request, the returned value might include corrupted characters.	**ics_auth**	String (50)
payment_network_token_account_status 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.	Possible values: • N: Nonregulated • R: Regulated This field is returned only for .	**ics_auth**	String (1)

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
payment_network_token_assurance_method	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. This field is returned only for Visa Platform Connect.	**ics_auth**	String (2)

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
payment_network_token_original_card_category	Mastercard product ID associated with the primary account number (PAN). For the possible values, see Mastercard Product IDs in *Credit Card Services Using the SCMP API*. This field is returned only for Mastercard transactions on .	**ics_auth**	String (3)
payment_network_token_requestor_id 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 value is returned only if the processor provides it. This field is supported only for and Chase Paymentech Solutions.	**ics_auth**	Integer (11)
request_id	Identifier for the request.	**ics_auth**	String (26)
request_token	Request token data created by Cybersource for each response. The field is an encoded string that contains no confidential information such as an account or card verification number. The string can contain a maximum of 256 characters.	**ics_auth**	String (256)

Response Fields (continued)

Field	Description	Returned By	Data Type & Length
token_expiration_month	Month in which the token expires. Cybersource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction. Format: MM. Possible values: `01` through `12`.	**ics_auth**	String (2)
token_expiration_year	Year in which the token expires. Cybersource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction. Format: YYYY.	**ics_auth**	String (4)
token_prefix	First 6 digits of token. Cybersource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction.	**ics_auth**	String (6)
token_suffix	Last 4 digits of token. Cybersource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction.	**ics_auth**	String (4)
1—The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to Cybersource. 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.			

SCMP API Examples

In-App Authorization Request for Visa

```
merchant_id=Foster_City_Flowers
merchant_ref_number=12345678
customer_firstname=Jane
customer_lastname=Smith
bill_address1=100 Main Street
bill_address2=Suite 1234
bill_city=Foster City
bill_state=CA
bill_zip=94404
bill_country=US
customer_email=jsmith@example.com
currency=USD
grand_total_amount=16.00
customer_cc_number=4650100000000839
customer_cc_expmo=12
customer_cc_expyr=2031
ics_applications=ics_auth
cavv=EHuWW9PiBkWvqE5juRwDzAUFBAk=
e_commerce_indicator=vbv
network_token_cryptogram=qE5juRwDzAUFBAkEHuWW9PiBkWv=
payment_network_token_transaction_type=1
```

In-App Authorization Request for Mastercard

```
merchant_id=Foster_City_Flowers
merchant_ref_number=12345678
customer_firstname=Jane
customer_lastname=Smith
bill_address1=100 Main Street
bill_address2=Suite 1234
bill_city=Foster City
bill_state=CA
bill_zip=94404
bill_country=US
customer_email=jsmith@example.com
currency=USD
grand_total_amount=16.00
customer_cc_number=4650100000000839
customer_cc_expmo=12
customer_cc_expyr=2031
```

```
ics_applications=ics_auth
e_commerce_indicator=spa
network_token_cryptogram=qE5juRwDzAUFBAkEHuWW9PiBkWv=
ucaf_authentication_data=EHuWW9PiBkWvqE5juRwDzAUFBAk=
ucaf_collection_indicator=2
payment_network_token_transaction_type=1
```

In-App Authorization Request for American Express

```
merchant_id=Foster_City_Flowers
merchant_ref_number=12345678
customer_firstname=Jane
customer_lastname=Smith
bill_address1=100 Main Street
bill_address2=Suite 1234
bill_city=Foster City
bill_state=CA
bill_zip=94404
bill_country=US
customer_email=jsmith@example.com
currency=USD
grand_total_amount=16.00
customer_cc_number=4650100000000839
customer_cc_expmo=12
customer_cc_expyr=2031
ics_applications=ics_auth
e_commerce_indicator=aesk
network_token_cryptogram=qE5juRwDzAUFBAkEHuWW9PiBkWv=
payment_network_token_transaction_type=1
```