Payment Network Tokenization Using the Simple Order API

Supplement to *Credit Card Services Using the Simple Order API*

May 2019

CyberSource®
the power of payment

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

CyberSource Contact Information

For general information about our company, products, and services, go to http://www.cybersource.com.

For sales questions about any CyberSource Service, email sales@cybersource.com or call 650-432-7350 or 888-330-2300 (toll free in the United States).

For support information about any CyberSource Service, visit the Support Center: http://www.cybersource.com/support

Copyright

Restricted Rights Legends

Trademarks

Contents

Recent Revisions to This Document

Release	Changes
May 2019	Removed the following request fields that were erroneously added in the April 2019 release: ■ ccSaleService_directoryServerTransactionID ■ ccSaleService_networkTokenCryptogram ■ ccSaleService_paSpecificationVersion Removed the following reply fields that were erroneously added in the April 2019 release: ■ payerAuthEnrollReply_directoryServerTransactionID ■ payerAuthValidateReply_directoryServerTransactionID

Release	Changes
April 2019	Added support for tokenized transactions using a network token with 3D Secure or SecureCode. See "In-App Transactions," page 12. Added the following request fields that support tokenized transactions using a network token with 3D Secure or SecureCode (see "API Request Fields," page 34): ■ ccAuthService_directoryServerTransactionID ■ ccAuthService_networkTokenCryptogram ■ ccAuthService_paSpecificationVersion ■ ccSaleService_directoryServerTransactionID ■ ccSaleService_networkTokenCryptogram ■ ccSaleService_paSpecificationVersion Added the following reply fields that support tokenized transactions using a network token with 3D Secure or SecureCode (see "API Reply Fields," page 45): ■ payerAuthEnrollReply_directoryServerTransactionID ■ payerAuthValidateReply_directoryServerTransactionID Added support for the processor *Elavon Americas*. See "Supported Processors and Card Types," page 11. Added support for the following optional features by Elavon Americas: ■ Merchant-Initiated transactions (see page 15) ■ Multiple partial captures (see page 23) ■ Recurring payments (see page 25) ■ Replacement expiration dates for recurring payments (see page 28) Added support for recurring payments as an optional feature for the following by the processor *WorldPay VAP* (see "Recurring Payments," page 25): ■ Apple Pay ■ Google Pay
March 2019	Added support for the processor *Credit Mutuel-CIC*. See "Supported Processors and Card Types," page 11. Added support for recurring payments as an optional feature by the following processors (see "Recurring Payments," page 25): ■ Credit Mutuel-CIC ■ SIX
September 2018	Added support for subsequent authorizations on FDC Nashville Global. See "Recurring Payments," page 25, and "Subsequent Authorizations," page 32. Added **subsequentAuthOriginalAmount**. See "API Request Fields," page 34. All processors that support special request fields for multiple partial captures: updated the Required/Optional information for **ccCaptureService_sequence** and **ccCaptureService_totalCount**. See "API Request Fields," page 34. FDC Nashville Global: updated the information in Table 5, "Processors that Support Multiple Partial Captures."

Release	Changes
August 2018	This revision contains only editorial changes and no technical updates.
July 2018	Added support for the processor *Worldpay VAP*. See "Supported Processors and Card Types," page 11. Added a new chapter: "Optional Features," page 15. Changed JCB request payer authentication field setting for ccAuthService_commerceIndicator from `vbv` to `JS`. See page 37.

About This Guide

Audience and Purpose

This document is written for application developers who want to add payment network tokenization functionality to 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 *Credit Card Services Using the Simple Order API*.

Updating the CyberSource credit card services requires software development skills. You must write code that uses the API request and reply fields to integrate the payment network tokenization functionality into your existing order management system.

Conventions

The following special statement is used in this document:

Note

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

The following text conventions are used in this document:

Table 1 Text Conventions

Convention	Meaning
bold	Field and service names in text; for example: Include the **ccAuthService_run** field.
`Screen text`	▪ XML elements. ▪ Code examples. ▪ Values for API fields; for example: Set the **ccAuthService_run** field to `true`.

Related Documents

- *Google Pay Using the Simple Order API* (PDF | HTML)
- *Apple Pay Using the Simple Order API* (PDF | HTML)
- *Card-Present Processing Using the Simple Order API* (PDF | HTML)
- *Credit Card Services Using the Simple Order API* (PDF | HTML)
- *Credit Card Services for CyberSource through VisaNet Using the Simple Order API*—contact CyberSource Customer Support to obtain this guide.
- *Getting Started with CyberSource Advanced for the Simple Order API* (PDF | HTML)
- *Samsung Pay Using the Simple Order API* (PDF | HTML)

Refer to the Support Center for complete CyberSource technical documentation:

http://www.cybersource.com/support_center/support_documentation

Customer Support

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

http://www.cybersource.com/support

CHAPTER 1

Payment Network Tokenization

Payment network tokenization (PNT) enables you to request an authorization with a token instead of a primary account number (PAN). This guide explains how to use payment network tokenization in credit card transactions.

Note This Payment Network Tokenization 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.

Note *Payment network tokenization* and CyberSource *payment tokenization* are not the same feature.

- With payment network tokenization, the token is created by a token service provider and can be used throughout the financial network.
- With CyberSource payment tokenization, the token is created by CyberSource and can be used only with CyberSource services.

Note For an incremental authorization, you don't 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

Table 2 Processors and Card Types

Processor	Credit Card Types
American Express Direct	American Express
Barclays	Visa, Mastercard, JCB, Maestro (International), Maestro (UK Domestic) **Note** If you support Maestro (UK Domestic), you must also support Maestro (International), and you must support Mastercard SecureCode for both card types.
Chase Paymentech Solutions	Visa, Mastercard, American Express, Discover, Diners Club, JCB, Carte Blanche, Maestro (International)
Credit Mutuel-CIC	Visa, Mastercard, Cartes Bancaires
CyberSource through VisaNet. The supported acquirers are: ■ Australia and New Zealand Banking Group Ltd. (ANZ) ■ CitiBank Singapore Ltd. ■ Global Payments Asia Pacific ■ Vantiv ■ Westpac	Visa, Mastercard, American Express, Discover, JCB, Diners Club
Elavon Americas	Visa, Mastercard, American Express, JCB, Diners Club, Discover, China UnionPay
FDC Compass	Visa, Mastercard, American Express, Discover, Diners Club, JCB
FDC Nashville Global	Visa, Mastercard, American Express, Discover, Diners Club, JCB, China UnionPay
GPN	Visa, Mastercard, American Express, Discover, Diners Club, JCB
JCN Gateway	JCB
Moneris	Visa, Mastercard, American Express
OmniPay Direct. The supported acquirers are: ■ First Data Merchant Solutions (Europe) ■ Global Payments International Acquiring	Visa, Mastercard, Discover, Diners Club, Maestro (UK Domestic), Maestro (International)
SIX	Visa, Mastercard

Table 2 Processors and Card Types (Continued)

Processor	Credit Card Types
Streamline	Visa, Mastercard
TSYS Acquiring Solutions	Visa, Mastercard, American Express
Worldpay VAP	Visa, Mastercard

In-App Transactions

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

In the authorization request:

- Set the account number field to the token value instead of to the customer's PAN. Obtain the token value from the token service provider. The account number field is **card_accountNumber**.
- Set the expiration date fields to the token expiration date instead of to the credit card expiration date. Obtain the token expiration date from the token service provider. The expiration date fields are **card_expirationMonth** and **card_expirationYear**.
- Include the transaction type field, which is **paymentNetworkToken_transactionType**.
- On CyberSource through VisaNet, you can choose to include the requestor ID field, which is **paymentNetworkToken_requestorID**.
- Include the following payer authentication fields:

  For Visa requests:

  - ccAuthService_commerceIndicator—set to `vbv` or `internet`
  - ccAuthService_cavv—set to the 3D Secure cryptogram
  - ccAuthService_xid—set to the network token cryptogram

Note

For transactions with the **ccAuthService_commerceIndicator** field set to `internet`, set the **ccAuthService_cavv** field to the 3D Secure cryptogram.

For transactions with the **ccAuthService_commerceIndicator** field set to `vbv`:

- Set the **ccAuthService_cavv** field to the 3D Secure cryptogram.
- Set the **ccAuthService_xid** field to the network token cryptogram.

For Verified by Visa transactions without payment network tokenization, set the **ccAuthService_cavv** field to the 3D Secure cryptogram.

For Mastercard requests:

- ccAuthService_commerceIndicator—set to `spa`
- ucaf_authenticationData—set to the SecureCode cryptogram or the network token cryptogram if the SecureCode cryptogram is not provided.
- ucaf_collectionIndicator—set to 2


Note

If a SecureCode cryptogram is not provided, set the **ucaf_authenticationData** field to the network token cryptogram.

For JCB requests:

- ccAuthService_commerceIndicator—set to `JS` or `internet`
- ccAuthService_cavv—set to cryptogram

For American Express requests:

For the American Express card type, the cryptogram is a 20-byte or 40-byte binary value.


Note

On some processors, American Express SafeKey is not supported, but you can use the American Express SafeKey fields for payment network tokenization.

For a 20-byte cryptogram, send the cryptogram in the cardholder authentication verification value (CAVV) field.

- ccAuthService_commerceIndicator—set to `aesk`
- ccAuthService_cavv—set to block A of the cryptogram

For a 40-byte cryptogram, split the cryptogram into two 20-byte binary values (block A and block B). Send the first 20-byte value (block A) in the cardholder authentication verification value (CAVV) field. Send the second 20-byte value (block B) in the transaction ID (XID) field.

- ccAuthService_commerceIndicator—set to `aesk`
- ccAuthService_cavv—set to block A of the cryptogram
- ccAuthService_xid—set to block B of the cryptogram

- Include the basic fields required for every 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_cardType
- 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.
- ccAuthService_run
- merchantID
- merchantReferenceCode
- purchaseTotals_currency
- purchaseTotals_grandTotalAmount or item_#_unitPrice

For descriptions of these fields, see "API Request Fields," page 34.

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

CHAPTER 2

Optional Features

Merchant-Initiated Transactions

Service:

Authorization

Card type:

Visa

Processors:

- See the following table.

Table 3 Processors that Support Merchant-Initiated Transactions

Processors	Supported Digital Payments
Chase Paymentech Solutions	PNT, Apple Pay, Google Pay, Samsung Pay **Note** The only scenarios supported on Chase Paymentech Solutions are reauthorizations and unscheduled card-on-file transactions.
CyberSource through VisaNet	PNT, Apple Pay, Google Pay, Samsung Pay
Elavon Americas	PNT, Apple Pay, Google Pay, Samsung Pay

Most authorizations are initiated by a cardholder in person, on the phone, or on a web site. A *merchant-initiated transaction* (MIT) is an authorization that you initiate when the cardholder is not present.

Terminology

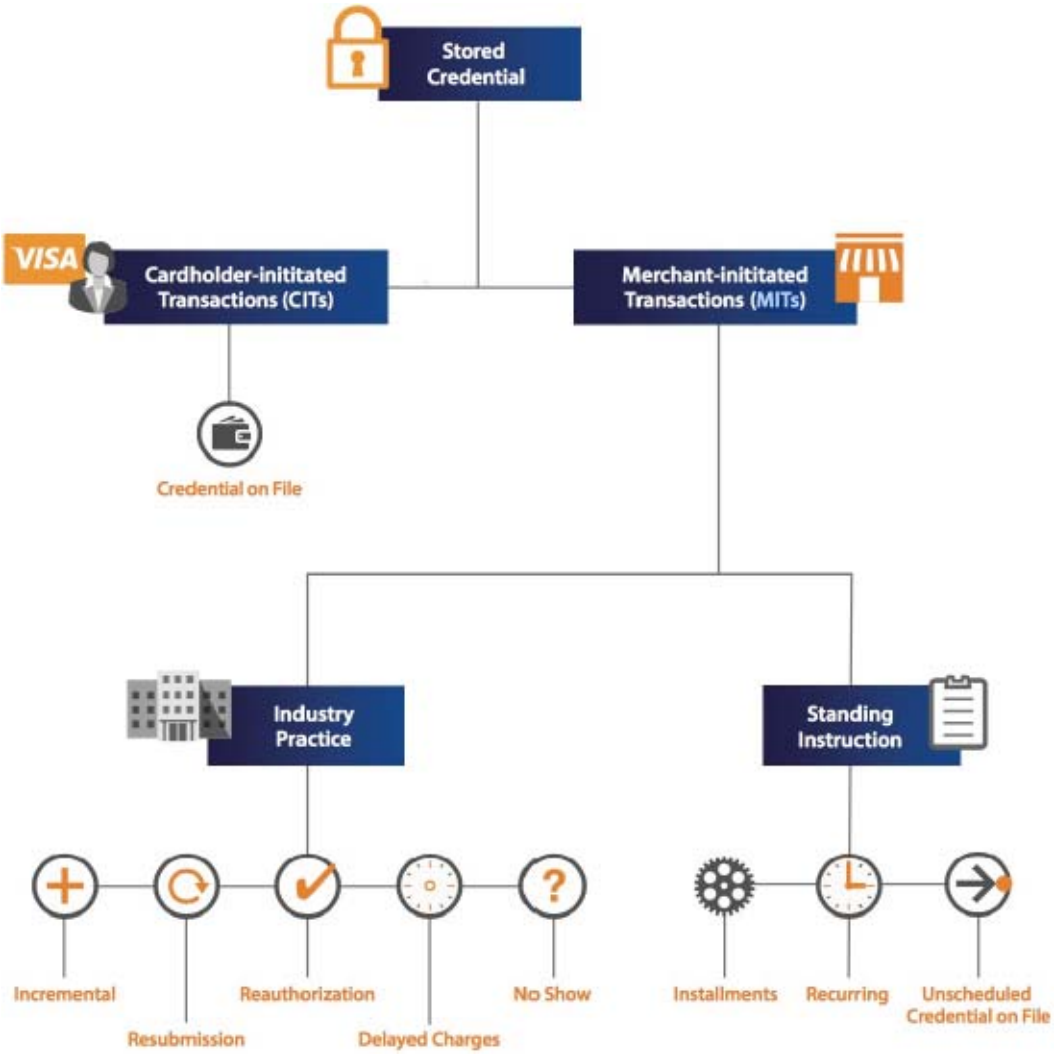
Table 4 Terminology for Merchant-Initiated Transactions

Term	Description
Cardholder-initiated transaction (CIT)	Transaction that uses payment information provided by the cardholder. A CIT can be any of the following kinds of transactions: ■ Card present: cardholder goes to a brick-and-mortar store in person to make a purchase and provides payment information in the store. ■ Card-on-file or Credential-on-file (COF): cardholder orders an item online and instructs you to use the payment information that is saved in your system. ■ E-commerce: cardholder orders an item online and provides payment information during checkout. ■ Mail order or telephone order (MOTO): cardholder orders an item over the telephone and provides payment information to the person who is taking the order.
COF transaction	Transaction that uses payment information that you saved in your system.

Overview

Figure 1 illustrates the relationships between stored credentials, CITs, and MITs.

Figure 1 Stored Credentials and Merchant-Initiated Transactions



There are two main types of MITs:

- An *industry practice* transaction: a one-time MIT that derives payment information from a CIT.
- A standing instruction: one transaction in a series of repeated transactions or a one-time, unscheduled transaction that uses COF payment information.

Descriptions

- Account top-up—is the result of instructions between you and the cardholder to charge a specific or variable amount at specified or variable intervals. An account top-up is an unscheduled COF transaction.

- Delayed charge—is associated with an agreement between you and the cardholder for services rendered. Delayed charges are typical for lodging transactions and auto rental transactions.


Note

The CyberSource delayed charge feature is not available on FDC Compass.

- Final authorization—occurs when you need to authorize the final amount after an estimated authorization.

- Incremental authorization—is a continuation of a purchase when the originally approved amount is modified to accommodate additional services. Incremental authorizations are typical for lodging transactions and auto rental transactions.


Note

The CyberSource incremental authorization feature is not available on these processors:

- FDC Compass
- FDC Nashville Global
- OmniPay Direct

- Installment payment—is the result of instructions governed by a contract between you and a cardholder. The instructions enable you to charge a specific amount at specified intervals. To find out whether your processor is supported for installment payments, see “Installment Payments” in the *Credit Card Guide*.

- No-show transaction—occurs when you and a cardholder have an agreement for a purchase, but the cardholder does not meet the terms of the agreement. No-show transactions are typically used in hotels and motels for a single-night stay.


Note

The CyberSource no-show transaction feature is not available on FDC Compass.

- Reauthorization for split shipment—a split shipment occurs when multiple goods purchased in a single transaction are shipped at separate times. When the goods become available to ship, either you or CyberSource perform a new authorization for the portion of the transaction being delivered. This ensures that the cardholder's funds are still available. The reauthorization is performed in one of the following scenarios:

  - Before requesting a capture, you request an authorization using the saved cardholder credentials.

  - You use the CyberSource split-shipment feature. To find out whether your processor is supported for split shipments, see the "Split Shipments" section in this guide.

- Recurring payment—is the result of instructions governed by a contract between you and a cardholder. The instructions enable you to charge a specific or variable amount at specified intervals. To find out whether your processor is supported for recurring payments, see the "Recurring Payments" section in this guide.

- Resubmission—occurs when a cardholder-initiated purchase occurred, but you could not obtain an authorization at that time. A resubmission is valid only when the original authorization was declined for insufficient funds and only for a limited number of days after the original purchase.

Scenarios

Delayed Charge

A delayed charge is associated with an agreement between you and the cardholder for services rendered. Merchants might use delayed charges after providing services such as lodging, travel, or auto rental.

To create a delayed charge authorization request:

Step 1 Include the following required fields in the authorization request:

- subsequentAuth—set the value for this field to `true`.
- subsequentAuthReason—set the value for this field to `2`.
- subsequentAuthTransactionID—set the value for this field to the network transaction identifier.

Step 2 If the payment information is COF information, include the following field in the authorization request:

- subsequentAuthStoredCredential—set the value for this field to `true`.

Installment Payment

An installment payment is a COF transaction. A series of installment payments consists of multiple transactions that you bill to a cardholder over a period of time agreed to by you and the cardholder for a single purchase of goods or services. The agreement enables you to charge a specific amount at specified intervals.

To create an installment payment authorization request:

Step 1 Cardholder consents to terms and establishes service or obtains goods.

Step 2 You charge the first installment payment as a CIT. Include the following field in the authorization request:

- subsequentAuthFirst—set the value for this field to `true`.

Step 3 You charge subsequent installment payments on a regular basis. Include the following fields in each authorization request:

- ccAuthService_commerceIndicator—set the value for this field to `install`.
- subsequentAuthTransactionID—set the value for this field to the network transaction identifier.

No-Show Transaction

A no-show transaction occurs when you and a cardholder have an agreement for a purchase, but the cardholder does not meet the terms of the agreement. No-show transactions are typically used in hotels and motels for a single-night stay.

To create a no-show transaction authorization request:

Step 1 Include the following required fields in the authorization request:

- subsequentAuth—set the value for this field to `true`.
- subsequentAuthReason—set the value for this field to `4`.
- subsequentAuthTransactionID—set the value for this field to the network transaction identifier.

Step 2 If the payment information is COF information, include the following field in the authorization request:

- subsequentAuthStoredCredential—set the value for this field to `true`.

Reauthorization

A reauthorization is a purchase made after an original purchase that can reflect a number of specific conditions. Common instances that require reauthorizations include delayed shipments, split shipments, extended stays, and extended rentals.

To create a reauthorization request:

Step 1 Include the following required fields in the authorization request:

- subsequentAuth—set the value for this field to `true`.
- subsequentAuthReason—set the value for this field to 3.
- subsequentAuthTransactionID—set the value for this field to the network transaction identifier.

Step 2 If the payment information is COF information, include the following field in the authorization request:

- subsequentAuthStoredCredential—set the value for this field to `true`.

Recurring Payment

A recurring payment is a COF transaction. A series of recurring payments consists of multiple transactions that you bill to a cardholder at fixed, regular intervals not to exceed one year between transactions. The series of recurring payments is the result of an agreement between you and the cardholder.

To create a recurring payment authorization request:

Step 1 Cardholder consents to terms and establishes service or obtains goods.

Step 2 You charge the first recurring payment as a CIT. Include the following field in the authorization request:

- subsequentAuthFirst—set the value for this field to `true`.

Step 3 You charge subsequent recurring payments on a regular basis. Include the following fields in each authorization request:

- ccAuthService_commerceIndicator—set the value for this field to `recurring`.
- subsequentAuthTransactionID—set the value for this field to the network transaction identifier.

Resubmission

A resubmission occurs when you cannot obtain an authorization for a cardholder-initiated purchase. A resubmission is valid only when the original authorization was declined for insufficient funds and only for a limited number of days after the original purchase.

To create a resubmission authorization request:

Step 1 Include the following required fields in the authorization request:

- subsequentAuth—set the value for this field to `true`.
- subsequentAuthReason—set the value for this field to `1`.
- subsequentAuthTransactionID—set the value for this field to the network transaction identifier.

Step 2 If the payment information is COF information, include the following field in the authorization request:

- subsequentAuthStoredCredential—set the value for this field to `true`.

Unscheduled COF Transaction

An unscheduled COF transaction uses stored payment information for a fixed or variable amount that does not occur on a scheduled or regular basis.

To create an unscheduled COF transaction authorization request:

Step 1 Cardholder consents to terms and establishes service or obtains goods.

Step 2 You charge the first payment. Include the following field in the authorization request:

- subsequentAuthFirst—set the value for this field to `true`.

Step 3 You charge subsequent payments. Include the following fields in each authorization request:

- subsequentAuth—set the value for this field to `true`.
- subsequentAuthTransactionID—set the value for this field to the network transaction identifier.

API Field Descriptions

For descriptions of the fields in the preceding scenarios, see Appendix A, "API Fields," on page 33.

Multiple Partial Captures

Processors:

- See the following table.

Table 5 Processors that Support Multiple Partial Captures

Processors	Supported Digital Payments
American Express Direct	PNT, Apple Pay, Samsung Pay
Barclays	PNT, Apple Pay, Google Pay, Samsung Pay
Chase Paymentech Solutions	PNT, Apple Pay, Samsung Pay
Elavon Americas	PNT, Apple Pay, Google Pay, Samsung Pay
FDC Compass	PNT, Apple Pay, Samsung Pay
FDC Nashville Global	PNT, Apple Pay, Google Pay, Samsung Pay **Note** Multiple partial captures are supported only for card-not-present transactions; they are not supported for card-present transactions.
JCN Gateway	PNT, Apple Pay, Google Pay, Samsung Pay
Omnipay Direct. The supported acquirers are: ■ Bank of America Merchant Services ■ First Data Merchant Solutions (Europe) ■ Global Payments International Acquiring	 ■ Apple Pay, Google Pay, Samsung Pay ■ PNT, Apple Pay, Google Pay, Samsung Pay ■ PNT, Apple Pay, Google Pay, Samsung Pay
Streamline	PNT, Apple Pay, Samsung Pay **Note** See "Multiple Partial Captures on Streamline," page 25.
TSYS Acquiring Solutions	PNT, Apple Pay, Samsung Pay
Worldpay VAP	PNT **Note** Worldpay VAP was previously called *Litle*.

Note

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," page 31.

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.
- FDC Compass. To avoid a downgrade for a Visa transaction, the special request fields are required. For other card types, CyberSource strongly recommends that you include the special request fields.
- FDC Nashville Global. The special request fields are required for Visa and Mastercard transactions. They are not supported for other card types.
- 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. The supported acquirers are:
  - Bank of America Merchant Services
  - Cardnet International
  - First Data Merchant Solutions (Europe)
  - Global Payments International Acquiring
- 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 is the same for a merchant ID. You must ensure that you do not submit duplicate transaction information when using multiple partial captures; otherwise Streamline may reject the transaction.

- transaction date
- card_accountNumber
- merchantReferenceCode
- purchaseTotals_grandTotalAmount

Recurring Payments

Service:

- Authorization

Processors:

- See the following table.

Table 6 Processors That Support Recurring Payments

Processors	Credit Card Types	Supported Digital Payments
American Express Direct	American Express	PNT, Apple Pay, Google Pay, Samsung Pay
Barclays	Visa, Mastercard, JCB	PNT, Apple Pay, Google Pay, Samsung Pay
Chase Paymentech Solutions	Visa, Mastercard, American Express, Discover	PNT, Apple Pay, Chase Pay, Google Pay, Samsung Pay
Credit Mutuel-CIC	Visa, Mastercard, Cartes Bancaires	PNT, Apple Pay, Google Pay
CyberSource through VisaNet	Visa, Mastercard, American Express, Diners Club, JCB, Discover	Australia and New Zealand Banking Group Ltd.—PNT, Apple Pay, Google Pay CitiBank Singapore Ltd.—PNT, Apple Pay Global Payments Asia Pacific—PNT, Apple Pay Vantiv—PNT, Apple Pay, Google Pay, Samsung Pay Westpac—PNT, Apple Pay, Google Pay
Elavon Americas	Visa, Mastercard, American Express, JCB, Diners Club, Discover, China UnionPay	PNT, Apple Pay, Google Pay, Samsung Pay
FDC Compass	Visa, Mastercard, American Express, Discover, Diners Club, JCB	PNT, Apple Pay, Google Pay, Samsung Pay

Table 6 Processors That Support Recurring Payments (Continued)

Processors	Credit Card Types	Supported Digital Payments
FDC Nashville Global	Visa, Mastercard, American Express, Discover, China UnionPay	PNT, Apple Pay, Google Pay, Samsung Pay
GPN	Visa, Mastercard, American Express, Discover, Diners Club, JCB	PNT, Apple Pay, Google Pay, Samsung Pay
OmniPay Direct	Visa, Mastercard Visa, Mastercard, Discover, Diners Club Visa, Mastercard	Bank of America Merchant Services—Apple Pay, Google Pay, Samsung Pay First Data Merchant Solutions (Europe)—PNT, Apple Pay, Google Pay, Samsung Pay Global Payments International Acquiring—PNT, Apple Pay, Google Pay, Samsung Pay
SIX	Visa, Mastercard, Discover, Diners Club, JCB, Maestro (International), Maestro (UK Domestic), China UnionPay, Visa Electron	PNT, Apple Pay, Google Pay
Streamline **Note** To process recurring payments with Streamline, contact the CyberSource European office. For the European office's phone number, go to the CyberSource web site and click the **Contact Us** link: www.cybersource.com		PNT, Apple Pay, Google Pay, Samsung Pay
TSYS Acquiring Solutions	Visa, Mastercard, American Express, Discover	PNT, Apple Pay, Google Pay, Samsung Pay
Worldpay VAP Worldpay VAP was previously called *Litle*.	Visa, Mastercard, American Express, Discover, Diners Club, JCB	PNT, Apple Pay, Google Pay

American Express and Discover have programs that you must register for if you want to process recurring payments. Contact American Express and Discover for details about their programs.

Depending on the types of products and services you sell, you might want to process recurring payments for a customer. For example, you might want to charge a customer 19.95 USD each month to use a service that you offer.

A customer's recurring payment does not have to be the same amount each time.

You must disclose clearly to customers when they make a purchase what the amount will be for the recurring payments. If the amount varies based on usage, make it clear.

To create a recurring payment:

Step 1 For the first payment, the type of request you need to send depends on which processor and card type you are using.

- For Mastercard and American Express transactions on FDC Nashville Global, include the following fields and values in the request for the first payment:

  ccAuthService_commerceIndicator=`recurring`

  ccAuthService_firstRecurringPayment=TRUE

  card_cvNumber

- For all card types on OmniPay Direct, request a non-recurring transaction and include the following field and value in the request for the first payment:

  ccAuthService_firstRecurringPayment=Y

- For all other processors and card types, request a non-recurring transaction for a credit card authorization.

If the first authorization is successful, you can submit subsequent authorizations for recurring payments using that card. If the first authorization is not successful, do not submit subsequent authorizations using that card.

Important You must perform Step 1 once per year to verify the account.

Step 2 For each subsequent recurring payment, send an authorization request using the e-commerce indicator to indicate that the payment is a recurring payment:

ccAuthService_commerceIndicator=`recurring`

For Discover card transactions on FDC Nashville Global, **subsequentAuthOriginalAmount** is a required field. See the description for the **subsequentAuthOriginalAmount** field in Table 11, "API Request Fields."

If your processor supports merchant-initiated transactions, your authorization request must include subsequent authorization fields as described in "Merchant-Initiated Transactions," page 15.

CyberSource also offers services that enable you to create a subscription or customer profile for a customer in the CyberSource system and then use that subscription or customer profile later to manually or automatically bill the customer. The CyberSource system eliminates the need for you to handle or store the customer's sensitive credit card information or create your own system for billing the customer on a regular basis. For more information, see *Token Management Service Using the Simple Order API* and *Recurring Billing Using the Simple Order API*.

AVS and Recurring Payments


Note

FDMS Nashville does not support AVS for recurring payments.

If AVS is supported for your processor and card type, AVS is run for every authorization request that you submit. For recurring payments, verify the AVS result for the first payment to ensure that the payment information is accurate and to reduce the risk of fraud.

You must decide what to do with the AVS results for subsequent payments. You might want to ignore the AVS results for these payments because you already confirmed with the first payment that the credit card number is valid and not fraudulent.

When you need to change the credit card number used for a series of recurring payments, follow Step 1 in creating a recurring payment to verify the new account number. Closely evaluate the AVS results. If the first authorization is successful, you can submit subsequent authorizations for recurring payments using that card. If the first authorization is not successful, do not submit subsequent authorizations using that card. For subsequent payments, follow Step 2 in creating a recurring payment. You can choose to ignore the AVS results.

CVN and Recurring Payments


Note

FDMS Nashville does not support CVN for recurring payments.

Replacement Expiration Dates for Recurring Payments

Service:

- Authorization

Processors and card types:

- See the following table.

Table 7 Processors That Support Replacement Expiration Dates for Recurring Payments

Processors	Credit Card Types	Supported Digital Payments
American Express Direct	American Express	PNT, Apple Pay, Google Pay, Samsung Pay
Barclays	Visa, Mastercard, JCB	PNT, Apple Pay, Google Pay, Samsung Pay

Table 7 Processors That Support Replacement Expiration Dates for Recurring Payments (Continued)

Processors	Credit Card Types	Supported Digital Payments
Chase Paymentech Solutions	Visa, Mastercard	PNT, Apple Pay, Google Pay, Samsung Pay
CyberSource through VisaNet	Visa, Mastercard, American Express, Discover, Diners Club, JCB **Note** Not all card types are supported for all acquirers. If an acquirer is supported for recurring payments, the acquirer is also supported for replacement expiration dates for recurring payments. For the list of supported acquirers, see the entry for CyberSource through VisaNet in Table 6, "Processors That Support Recurring Payments," on page 25.	Australia and New Zealand Banking Group Ltd.—PNT, Apple Pay, Google Pay CitiBank Singapore Ltd.—PNT, Apple Pay Global Payments Asia Pacific—PNT, Apple Pay Vantiv—PNT, Apple Pay, Google Pay, Samsung Pay Westpac—PNT, Apple Pay, Google Pay
Elavon Americas	Visa, Mastercard, American Express, JCB, Diners Club, Discover, China UnionPay	PNT, Apple Pay, Google Pay, Samsung Pay
FDC Compass	Visa, Mastercard, American Express, Discover, Diners Club	PNT, Apple Pay, Google Pay, Samsung Pay
Streamline **Note** To process recurring payments with Streamline, contact the CyberSource European office. For the European office's phone number, go to the CyberSource web site and click the **Contact Us** link: www.cybersource.com		PNT, Apple Pay, Google Pay, Samsung Pay

Normally when you request a credit card authorization, you must provide a valid expiration date for the credit card. If you are processing a recurring payment, and the credit card that you have on file for the customer has expired, you might still be able to request the authorization depending on which processor you use. Instead of sending the out-of-date expiration date, you can include a replacement expiration date in your request.

Important

Do not use a replacement expiration date for cards that are not expired. Use a replacement expiration date only for cards that are expired and only for recurring payments.

Using a replacement expiration date for a recurring payment does not guarantee that the authorization will be successful. The issuing bank determines whether a card is authorized; some issuing banks do not accept an expiration date that does not match the expiration date in the bank's database.

Important

Effective October 17, 2014, an issuing bank can decline an authorization request for a recurring transaction with a Visa Europe card if the expiration date is incorrect, invalid, or missing. If you do not provide the correct expiration date for a recurring transaction, the authorization request might be declined.

The replacement expiration date that CyberSource supports is 12/2099. To use this date, include these fields and values in your authorization request:

card_expirationMonth=`12`

card_expirationYear=`2099`

Relaxed Requirements for Address Data and Expiration Date

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

Split Shipments

Note

For details about split shipments, see *Credit Card Services Using the Simple Order API*.

Services:

- Authorization
- Capture

Processors:

- See the following table.

Table 8 Processors that Support Split Shipments

Processors	Supported Digital Payments
CyberSource through VisaNet	PNT, Apple Pay, Samsung Pay **Important** Split shipments are not available for Mastercard transactions in the IDR currency on CyberSource through VisaNet.
GPN	PNT, Apple Pay, Google Pay, Samsung Pay

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

Note

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," page 23.
- The split-shipment 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.

Table 9 Processors that Support Subsequent Authorizations

Processors	Card Types	Supported Digital Payments
FDC Nashville Global	Discover	Apple Pay
JCN Gateway	JCB	Apple Pay
Streamline	Visa, Mastercard	Apple Pay, Samsung 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.

To request a subsequent authorization:

Step 1 Request the authorization for the first item.

Step 2 In each subsequent authorization request:

- Do not include the **ccAuthService_cavv** field.
- Include **subsequentAuth**=`true`.
- On FDC Nashville Global, include **subsequentAuthOriginalAmount**=`true`.

APPENDIX A

API Fields

Formatting Restrictions

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

Note

The values of the **item_#_** fields must not contain carets (^) or colons (:) because these characters are reserved for use by the CyberSource services.

Values for request-level and item-level fields must not contain new lines or carriage returns. However, they can contain embedded spaces and any other printable characters. CyberSource removes all leading and trailing spaces.

Data Type Definitions

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

Table 10 Data Type Definitions

Data Type	Description
Integer	Whole number {..., -3, -2, -1, 0, 1, 2, 3, ...}
String	Sequence of letters, numbers, spaces, and special characters

API Request Fields


Note

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

Table 11 API Request Fields

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
billTo_city	City of the billing address. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.	ccAuthService (See description)	String (50)
billTo_country	Country of the billing address. Use the two-character *ISO Standard Country Codes*. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.	ccAuthService (See description)	String (2)
billTo_email	Customer's email address. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.	ccAuthService (See description)	String (255)
billTo_firstName	Customer's first name. For a credit card transaction, this name must match the name on the card. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.	ccAuthService (See description)	String (60)
billTo_lastName	Customer's last name. For a credit card transaction, this name must match the name on the card. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.	ccAuthService (See description)	String (60)

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

Table 11 API Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
billTo_phoneNumber	Customer's phone number. CyberSource recommends that you include the country code when the order is from outside the U.S.	ccAuthService (O)	String (15)
billTo_postalCode	Postal code for the billing address. The postal code must consist of 5 to 9 digits. When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits] **Example** 12345-6789 When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric] **Example** A1B 2C3 **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.	ccAuthService (See description)	String (9)
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*. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.	ccAuthService (See description)	String (2)
billTo_street1	First line of the billing street address. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.	ccAuthService (See description)	String (60)
billTo_street2	Additional address information. **Example** Attention: Accounts Payable	ccAuthService (R)	String (60)

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

Table 11 API Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
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 ■ `007`: JCB	ccAuthService (R)	String (3)
card_cvNumber	CVN. See *Credit Card Services Using the Simple Order API* 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	***Visa*** Cryptogram for payment network tokenization transactions. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats. ***American Express*** For a 20-byte cryptogram, set this field to the cryptogram for payment network tokenization transactions. For a 40-byte cryptogram, set this field to block A of the cryptogram for payment network tokenization transactions. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats. ***CyberSource through VisaNet*** The value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCR8 ■ Position: 77-78 ■ Field: CAVV version and authentication action.	ccAuthService (R)	String (40)

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

Table 11 API Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
ccAuthService_ commerceIndicator	Type of transaction. Possible values: ■ `aesk`: American Express card type ■ `spa`: Mastercard card type ■ `install`: for subsequent installment payments. See "Merchant-Initiated Transactions," page 15. ■ `internet`: Visa card type ■ `dipb`: Discover card type ■ `recurring`: see "Recurring Payments," page 25. **Important** For Visa in-app transactions, the `internet` value is mapped to the Visa ECI value 7. **Note** 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 (See description)	String (20)
ccAuthService_ directoryServerTrans actionID	Identifier generated during the authentication transaction by the Mastercard Directory Server and passed back with the authentication results.	ccAuthService (O)	String (36)
ccAuthService_ firstRecurringPayment	Flag that indicates whether this transaction is the first in a series of recurring payments. See "Recurring Payments," page 25. ***FDC Nashville Global*** Possible values: ■ `true`: Yes, this is the first payment in a series of recurring payments. ■ `false` (default): No, this is not the first payment in a series of recurring payments. ***OmniPay Direct*** 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.	ccAuthService (See description)	String (1)

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

Table 11 API Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
ccAuthService_ networkTokenCryptogram	Token authentication verification value. For token-based transactions with 3D Secure or SecureCode, you must submit both types of cryptograms: network token and 3D Secure/SecureCode. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats.	ccAuthService (O)	String (40)
ccAuthService_ paSpecificationVersion	The 3D Secure version that you used for Secured Consumer 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)
ccAuthService_xid	***Visa*** Cryptogram for payment network tokenization transactions. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats. ***American Express*** For a 20-byte cryptogram, set this field to the cryptogram for payment network tokenization transactions. For a 40-byte cryptogram, set this field to block A of the cryptogram for payment network tokenization transactions. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats.	ccAuthService (R)	String (40)

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

Table 11 API Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
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 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," page 24.	ccCaptureService (See "Special Request Fields for Multiple Partial Captures," page 24.)	Integer (2)
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," page 24.	ccCaptureService (See "Special Request Fields for Multiple Partial Captures," page 24.)	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)
paymentNetworkToken_ assuranceLevel	Confidence level of the tokenization. This value is assigned by the token service provider. **Note** This field is supported only for CyberSource through VisaNet and FDC Nashville Global.	ccAuthService (O)	String (2)

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

Table 11 API Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
paymentNetworkToken_ deviceTechType	Type of technology used in the device to store token data. Possible 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) 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. **Note** This field is supported only for FDC Compass.	ccAuthService (O)	Integer (3)
paymentNetworkToken_ requestorID	Value that identifies your business and indicates that the cardholder's account number is tokenized. This value is assigned by the token service provider and is unique within the token service provider's database. **Note** This field is supported only for CyberSource through VisaNet, FDC Nashville Global, and Chase Paymentech Solutions.	ccAuthService (O)	String (11)
paymentNetworkToken_ transactionType	Type of transaction that provided the token data. This value does not specify the token service provider; it specifies the entity that provided you with information about the token. Set the value for this field to `1`.	ccAuthService (R)	String (1)

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

Table 11 API Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
pos_environment	Operating environment. Possible values: ■ 0: No terminal used or unknown environment. ■ 1: On merchant premises, attended. ■ 2: On merchant premises, unattended, or cardholder terminal. Examples: oil, kiosks, self-checkout, home computer, mobile telephone, personal digital assistant (PDA). Cardholder terminal is supported only for Mastercard transactions on CyberSource through VisaNet. ■ 3: Off merchant premises, attended. Examples: portable POS devices at trade shows, at service calls, or in taxis. ■ 4: Off merchant premises, unattended, or cardholder terminal. Examples: vending machines, home computer, mobile telephone, PDA. Cardholder terminal is supported only for Mastercard transactions on CyberSource through VisaNet. ■ 5: On premises of cardholder, unattended. ■ 9: Unknown delivery mode. ■ S: Electronic delivery of product. Examples: music, software, or eTickets that are downloaded over the internet. ■ T: Physical delivery of product. Examples: music or software that is delivered by mail or by a courier. **Note** This field is supported only for American Express Direct and CyberSource through VisaNet. ***CyberSource through VisaNet*** For Mastercard transactions, the only valid values are 2 and 4.	ccAuthService (Optional for in-app payment network tokenization transactions.)	String (1)
purchaseTotals_currency	Currency used for the order: USD	ccAuthService (R)	String (5)
purchaseTotals_ grandTotalAmount	Grand total for the order. This value cannot be negative. You can include a decimal point (.), but you cannot include any other special characters. CyberSource truncates the amount to the correct number of decimal places.	ccAuthService (R)	Decimal (60)

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

Table 11 API 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. Possible values: ■ `true`: Merchant-initiated transaction ■ `false`: Not a merchant-initiated transaction This field is supported for: ■ All merchant-initiated transactions. ■ Subsequent authorizations on FDC Nashville Global and Streamline only. ***CyberSource through VisaNet*** The value for this field does not correspond to any data in the TC 33 capture file.[1] ***All Processors*** See "Merchant-Initiated Transactions," page 15, and "Subsequent Authorizations," page 32.	ccAuthService (R for merchant-initiated transactions; 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: ■ `true`: First merchant-initiated transaction ■ `false`: Not the first merchant-initiated transaction This field is supported only for merchant-initiated transactions. ***CyberSource through VisaNet*** The value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCR1 ■ Position: 136 ■ Field: POS Environment ***All Processors*** See "Merchant-Initiated Transactions," page 15.	ccAuthService (R for merchant-initiated transactions; otherwise, not used)	String (5)
subsequentAuthOriginalAmount	Amount of the original authorization. This field is supported only for Apple Pay, Google Pay, and Samsung Pay transactions with Discover on FDC Nashville Global. See "Recurring Payments," page 25, and "Subsequent Authorizations," page 32.	ccAuthService (R)	String (60)

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

Table 11 API 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: ■ 1: Resubmission ■ 2: Delayed charge ■ 3: Reauthorization for split shipment ■ 4: No show ■ 5: Account top up This field is required only for the five kinds of transactions in the preceding list. This field is supported only for merchant-initiated transactions and incremental authorizations. ***CyberSource through VisaNet*** The value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCR0 ■ Position: 160-163 ■ Field: Message Reason Code ***All Processors*** See "Merchant-Initiated Transactions," page 15.	ccAuthService (See description)	String (1)
subsequentAuthStored Credential	Indicates whether the transaction uses card-on-file (COF) payment information for a merchant-initiated transaction. Possible values: ■ `true`: Transaction uses COF information ■ `false`: Transaction does not use COF information This field is supported only for merchant-initiated transactions. See "Merchant-Initiated Transactions," page 15.	ccAuthService (R for merchant-initiated transactions; otherwise, not used)	String (5)

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

Table 11 API Request Fields (Continued)

Field	Description	Used By: Required (R) or Optional (O)	Data Type (Length)
subsequentAuthTransactionID	Network transaction identifier that was returned in the **ccAuthReply_paymentNetworkTransactionID** field in the reply message for either the original merchant-initiated authorization in the series or the previous merchant-initiated authorization in the series. This field is supported only for merchant-initiated transactions. ***CyberSource through VisaNet*** The value for this field does not correspond to any data in the TC 33 capture file.[1] ***All Processors*** See "Merchant-Initiated Transactions," page 15.	ccAuthService (R for merchant-initiated transactions; otherwise, not used)	String (15)
ucaf_authenticationData	Cryptogram for payment network tokenization transactions with Mastercard.	ccAuthService (R)	String (32)
ucaf_collectionIndicator	Required field for payment network tokenization transactions with Mastercard. Set the value for this field to 2.	ccAuthService (R)	String with numbers only (1)

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

API Reply Fields

Important

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

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

Note

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

Table 12 API Reply Fields

Field	Description	Returned By	Data Type & Length
card_suffix	Last four digits of the cardholder's account number. This field is returned only for tokenized transactions. You can use this value on the receipt that you give to the cardholder. **Note** This field is returned only for CyberSource through VisaNet and FDC Nashville Global. ***CyberSource through VisaNet*** The value for this field corresponds to the following data in the TC 33 capture file[1]: ■ Record: CP01 TCRB ■ Position: 85 ■ Field: American Express last 4 PAN return indicator.	ccAuthReply	String (4)
ccAuthReply_amount	Amount that was authorized.	ccAuthReply	String (15)
ccAuthReply_ authorizationCode	Authorization code. Returned only when the processor returns this value.	ccAuthReply	String (7)
ccAuthReply_ authorizedDateTime	Time of authorization. Format: YYYY-MM-DDThh:mm:ssZ Example: 2018-08-11T22:47:57Z equals August 11, 2018, at 22:47 (10:47:57 p.m.). The T separates the date and the time. The Z indicates UTC.	ccAuthReply	String (20)

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

Table 12 API Reply Fields (Continued)

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

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

Table 12 API Reply Fields (Continued)

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

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

Table 12 API Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
ccAuthReply_ transactionQualification	Type of authentication for which the transaction qualifies as determined by the Mastercard authentication service, which confirms the identity of the cardholder. Mastercard provides this value to CyberSource. Possible values: ■ 1: Transaction qualifies for Mastercard authentication type 1. ■ 2: Transaction qualifies for Mastercard authentication type 2. **Note** This field is returned only for CyberSource through VisaNet.	ccAuthReply	String (1)
ccAuthReversalReply_ paymentCardService	Mastercard service that was used for the transaction. Mastercard provides this value to CyberSource. Possible value: 53: Mastercard card-on-file token service **Note** This field is returned only for CyberSource through VisaNet.	ccAuthReversal Reply	String (2)

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

Table 12 API Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
ccAuthReversalReply_paymentCardServiceResult	Result of the Mastercard card-on-file token service. Mastercard provides this value to CyberSource. Possible values: ■ C: Service completed successfully. ■ F: One of the following: • Incorrect Mastercard POS entry mode. The Mastercard POS entry mode should be 81 for an authorization or authorization reversal. • Incorrect Mastercard POS entry mode. The Mastercard POS entry mode should be 01 for a tokenized request. • Token requestor ID is missing or formatted incorrectly. ■ I: One of the following: • Invalid token requestor ID. • Suspended or deactivated token. • Invalid token (not in mapping table). ■ T: Invalid combination of token requestor ID and token. ■ U: Expired token. ■ W: Primary account number (PAN) listed in electronic warning bulletin. **Note** This field is returned only for CyberSource through VisaNet.	ccAuthReversalReply	String (1)
decision	Summarizes the result of the overall request. Possible values: ■ ACCEPT ■ ERROR ■ REJECT ■ REVIEW: Returned only when you use CyberSource Decision Manager.	ccAuthReply	String (6)
invalidField_0...N	Fields in the request that contained invalid data. For information about missing or invalid fields, see *Getting Started with CyberSource Advanced for the Simple Order API*.	ccAuthReply	String (100)

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

Table 12 API Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
merchantReferenceCode	Order reference or tracking number that you provided in the request. If you included multi-byte characters in this field in the request, the returned value might include corrupted characters.	ccAuthReply	String (50)
missingField_0...N	Required fields that were missing from the request. For information about missing or invalid fields, see *Getting Started with CyberSource Advanced for the Simple Order API*.	ccAuthReply	String (100)
paymentNetworkToken_ accountStatus	Possible values: ■ N: Nonregulated ■ R: Regulated **Note** This field is returned only for CyberSource through VisaNet.	ccAuthReply	String (1)
paymentNetworkToken_ assuranceLevel	Confidence level of the tokenization. This value is assigned by the token service provider. **Note** This field is returned only for CyberSource through VisaNet and FDC Nashville Global.	ccAuthReply	String (2)
paymentNetworkToken_ originalCardCategory	Mastercard product ID associated with the primary account number (PAN). For the possible values, see "Mastercard Product IDs" in *Credit Card Services Using the Simple Order API*. **Note** This field is returned only for Mastercard transactions on CyberSource through VisaNet.	ccAuthReply	String (3)
paymentNetworkToken_ requestorID	Value that identifies your business and indicates that the cardholder's account number is tokenized. This value is assigned by the token service provider and is unique within the token service provider's database. This value is returned only if the processor provides it. **Note** This field is supported only for CyberSource through VisaNet and FDC Nashville Global.	ccAuthService	String (11)
purchaseTotals_currency	Currency used for the order. For the possible values, see the *ISO Standard Currency Codes*.	ccAuthReply	String (5)
reasonCode	Numeric value corresponding to the result of the overall request. See *Credit Card Services Using the Simple Order API* for a detailed list of reason codes.	ccAuthReply	Integer (5)
requestID	Identifier for the request generated by the client.	ccAuthReply	String (26)

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

Table 12 API Reply Fields (Continued)

Field	Description	Returned By	Data Type & Length
requestToken	Request token data created by CyberSource for each reply. The field is an encoded string that contains no confidential information such as an account or card verification number. The string can contain a maximum of 256 characters.	ccAuthReply	String (256)
token_expirationMonth	Month in which the token expires. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction. Format: MM. Possible values: `01` through `12`.	ccAuthReply	String (2)
token_expirationYear	Year in which the token expires. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction. Format: YYYY.	ccAuthReply	String (4)
token_prefix	First six digits of token. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction.	ccAuthReply	String (6)
token_suffix	Last four digits of token. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction.	ccAuthReply	String (4)

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

APPENDIX B

Examples

Name-Value Pair Examples

Example 1 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_xid=EHuWW9PiBkWvqE5juRwDzAUFBAk=
paymentNetworkToken_transactionType=1
```

Example 2 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
paymentNetworkToken_transactionType=1
```

Example 3 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_xid=BkWvqE5juRwDzAUFBAk=
paymentNetworkToken_transactionType=1
```

XML Examples

Example 4 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>
      <commerceIndicator>vbv</commerceIndicator>
      <xid>EHuWW9PiBkWvqE5juRwDzAUFBAk=</xid>
   </ccAuthService>
   <paymentNetworkToken>
      <transactionType>1</transactionType>
   </paymentNetworkToken>
</requestMessage>
```

Example 5 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">
      <commerceIndicator>spa</commerceIndicator>
   </ccAuthService>
   <paymentNetworkToken>
      <transactionType>1</transactionType>
   </paymentNetworkToken>
</requestMessage>
```

Example 6 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">
      <cavv>EHuWW9PiBkWvqE5juRwD</cavv>
      <commerceIndicator>aesk</commerceIndicator>
      <xid>BkWvqE5juRwDzAUFBAk=</xid>
   </ccAuthService>
   <paymentNetworkToken>
      <transactionType>1</transactionType>
   </paymentNetworkToken>
</requestMessage>
```