Getting Started
with CyberSource Advanced

for the SCMP API

February 2017

CyberSource®

the power of payment

CyberSource Contact Information

For technical support questions, go to the Home page in the Business Center to see the contact information appropriate for your account.

Visit the Business Center, your central location for managing your online payment transactions, at https://businesscenter.cybersource.com.

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).

Copyright

Restricted Rights Legends

Trademarks

Contents

Recent Revisions to This Document

Release	Changes
February 2017	Added Ingenico ePayments information. See: • "Requesting a Follow-On Service," page 21 • "Working with Request Tokens," page 22. • "Request IDs and Request Tokens," page 26
May 2016	Added URLs for supported payment methods and integration methods. See page 8.
July 2013	This revision contains only editorial changes and no technical updates.
April 2013	This revision contains only editorial changes and no technical updates.
February 2013	Added section about going live. See page 11. Added note about security key separation in the Business Center. See "Installing and Testing the SCMP API," page 10.
January 2013	Added information about ampersands (&) in request fields for Moneris. See "Multi-Byte Characters and Special Characters," page 17.

About This Guide

Audience and Purpose

This guide is written for application developers who want to use the CyberSource SCMP API to integrate CyberSource services into their order management system. It describes the basic steps you must complete in order to get started with the SCMP API.

Implementing the CyberSource services requires software development skills. You must use the SCMP API request and reply fields to integrate the services into your existing order management system.

Conventions

Note and Important Statements

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

Note

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

Important

Text and Command Conventions

Convention	Usage
Bold	■ Field and service names in text; for example: Include the **ics_applications** field. ■ Items that you are instructed to act upon; for example: Click **Save**.
`Screen text`	■ XML elements. ■ Code examples and samples. ■ Text that you enter in an API environment; for example: Set the **ccAuthService_run** field to `true`.

Related Documents

- *Credit Card Services Using the SCMP API*
- *Electronic Check Services Using the SCMP API*
- *Getting Started with CyberSource Advanced for the SCMP API*
- *SCMP API Documentation and Downloads page*

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 at:

http://www.cybersource.com/support

Payment Processing with CyberSource

CyberSource Advanced is a payment solution that enables you to manage your payment transactions. CyberSource supports multiple payment methods and integration methods.

Supported payment methods:

http://www.cybersource.com/developers/documentation/global_payment_services/

Supported integration methods:

http://www.cybersource.com/developers/integration_methods/

Understanding the Payment Industry

In the e-commerce industry, multiple organizations work together to make online transactions possible. The following table describes some of the most important types of organizations in this industry.

Table 1   Types of Organizations in the Payment Industry

Type of Organization	Description
Merchant	A person or company that sells goods or services.
Merchant (acquiring) bank	A bank that provides businesses with accounts to accept credit card or check payments.
Card association	Organizations, such as Visa, Mastercard, and Discover, that have business relationships with the banks that issue your customers' cards.
Payment processor	An organization that processes payment requests, such as credit card authorizations and settlements, and routes them to the appropriate card associations according to their guidelines. Your merchant bank's processor relationship determines which payment processor you use.
Payment gateway	An organization, such as CyberSource, that enables merchants to securely send order information to and receive it from payment processors in the appropriate format.

Steps for Getting Started

	The SCMP API is CyberSource's older, legacy API. If you are starting your first implementation with CyberSource, use the Simple Order API instead of the SCMP API.
Note	

Registering and Logging In

To start using CyberSource services, register for a CyberSource account. After registering, you receive a confirmation email with your CyberSource username. Your password to the CyberSource Business Center is the one you associated with your username during registration.

A CyberSource partner can also provide you with a CyberSource account. If you register through one of these partners, you receive two confirmation emails: one containing your unique CyberSource username and the other containing your temporary password to the CyberSource Business Center. The first time you log in to the Business Center, the system prompts you to create a permanent password.

If you don't receive these emails, contact Customer Support for further assistance. If you have a CyberSource merchant account, the Customer Support phone number is included in your approval email.

Becoming Familiar with the Business Center

The CyberSource Business Center is a powerful and secure web portal designed to help you manage your customers' orders. It includes the Virtual Terminal should you choose to manually enter customers' orders. So, becoming familiar with the Business Center is crucial to managing your business payments efficiently.

The Business Center offers several options for processing order information and reducing fraud. In the Business Center, choose the **Virtual Terminal**, **Tools & Settings**, and **Account Management** tabs to access the settings pages. As you navigate the Business

Center, you can get additional information by clicking on the "Page help" link in the upper right area on each page.

Installing and Testing the SCMP API

Step 1   Generate security keys.

To ensure that you transmit information to CyberSource securely and to authenticate your transactions as belonging to your account, you need to generate security keys before you process transactions.

![!] **Important**   You must generate two transaction security keys—one for the CyberSource production environment and one for the test environment. For information about generating and using security keys, see *Creating and Using Security Keys* (PDF | HTML).

Step 2   Install an SCMP client.

a   Choose an SCMP client based on your platform and level of programming experience.

b   Learn how to use the API and client for running credit card orders by reading *Credit Card Services Using the SCMP API*. For information about processing electronic checks, see *Electronic Check Services Using the SCMP API*.

c   Download the client and its related documentation, which tells you how to install, test, and use the client.

d   Install the client by following the instructions in the documentation you downloaded with the client.

e   Run the samples included with the client to ensure that the connection with CyberSource is established. After you are comfortable with the samples, add code to integrate the client with your own application.

Step 3   Test your account.

To ensure that CyberSource successfully receives your order information, CyberSource strongly recommends that you run test transactions after implementing your chosen connection method. The test environment gives you the opportunity to troubleshoot and correct any connection issues. To verify that your implementation is correct, request test transactions, including authorizations, captures, and credits. You can test using your own credit card or, if you prefer to use test credit card numbers, use those provided in the following table with any future expiration date.

Table 2   Test Credit Card Numbers

Credit Card Type	Test Account Number[1]
Visa	4111 1111 1111 1111
Mastercard	5555 5555 5555 4444
American Express	3782 8224 6310 005
Discover	6011 1111 1111 1117
JCB	3566 1111 1111 1113
Diners Club	3800 000000 0006

1 remove spaces when sending to CyberSource.

Testing Information is available.

Going Live

After you have successfully tested your account and are ready to process real transactions, you can request to "go live". Because go-live requests must be in writing, you must submit a go-live request in an eTicket. For more information on submitting an eTicket, see "Submitting an eTicket."

In the eTicket, request that Customer Support enable your merchant ID in the production environment. Indicate which CyberSource services you would like to have enabled (for example, credit card processing, Decision Manager, or Payer Authentication). Be sure to include identifiers for your payment processor. If you are not sure who your payment processor is, contact your merchant acquirer.

Managing Your Orders

After you begin processing orders, you might need to review your transactions. For example, you might need to view all orders processed on a specific day, check order details, or verify whether orders were approved or declined. With the **Transaction Search** feature of the Business Center, you can:

■   Capture authorizations

■   Review, credit, or void sales

■   Create subscriptions from your customers' orders

Tracking and Reconciling Your Orders

The following table describes the values that you can use to track and reconcile your orders.

Table 3 Values for Tracking and Reconciling Orders

Value	Description
Request ID	The request ID is a unique identifier that CyberSource assigns to each request and returns in each reply message. You can use the request ID to do the following: ■ Identify a transaction in a CyberSource report ■ Search for a transaction in the Business Center ■ Discuss a specific request with Customer Support ■ Link a follow-on request to a primary request For specific field names, see the implementation guide or developer guide for the payment method you are using.
Merchant Reference Number	The merchant reference number is an order tracking number that you generate and send in your requests so that you can track orders as they move through the phases of processing with CyberSource. CyberSource recommends that you use a unique merchant reference number for each order and use the same merchant reference number for all the requests associated with the order. This enables you to efficiently track the order in the CyberSource reports and on the Transaction Search pages on the Business Center. For specific field names, see the implementation guide or developer guide for the payment method you are using.
Transaction Reference Number	For most CyberSource services, the reply message includes a unique transaction reference number that is assigned by CyberSource. For most payment processors, you can use this value to reconcile the transactions in your CyberSource reports with the transactions in your processor reports. For details, such as specific field names and information about processors that do not support reconciliation, see the implementation guide or developer guide for the payment method you are using.
Additional Tracking Values	A few services provide additional tracking values. See the order tracking information in the implementation guide or developer guide for the payment method you are using.

Accessing Reports

In addition to the Transaction Search feature in the Business Center, CyberSource generates pre-defined and on-demand reports to help you manage your orders. You can disable the generation of these reports at any time.

You can access your reports settings by logging in to the Business Center with your administrative login credentials. The following table describes the information required for your administrative login credentials.

Table 4   Information Required for Administrative Login Credentials

Value	Description
Merchant ID	Your regular merchant ID followed by **_acct**.
User Name	Your regular merchant ID followed by **_admin**.
Password	The password for this account should be the same as the original password that you chose for your merchant ID.

After you log in, click the **Account Management** tab, select **Report Subscriptions**, and click the **Edit** links on the basic and detail report headings to change your settings for reports. CyberSource recommends that you periodically download and save your reports for reference. Your reports remain available for approximately one year in the Business Center.

The reports that are the most useful for reconciliation are:
- Payment Batch Detail Report
- Payment Submission Detail Report
- Payment Events Report

For information about the formats of these reports and instructions for downloading them, see the *Reporting Developer Guide*.

Support Center

For more information about CyberSource services, log in to the Business Center and click the Support Center link at the top-left side of the page. At the Support Center, you can search the knowledge base, submit an eTicket, and browse for documentation.

Submitting an eTicket

To submit an eTicket:

Step 1   Log in to the CyberSource Business Center.

Step 2   Click **Support Center** near the top-left side of the page.

The Support Center appears.

Step 3   Click **Create eTicket**:

Step 4   Enter the following information on the Create eTicket screen:

- **First Name**: the first name of the person submitting the eTicket.

- **Last Name**: the last name of the person submitting the eTicket.

- **Phone Number**: the daytime phone number of the person submitting the eTicket.

- **Email Address**: the email address of the person submitting the eTicket.

- **Sensitive**: if you check this box, only the user submitting this eTicket and the Administrator on this account will be able to view this information.

> ⚠️ **Important**   Do not include personally identifiable information in your eTicket such as credit card numbers, card verification codes (CVV/CVC/CID), Social Security Numbers, or passwords.

- Issue Type: choose the most appropriate issue.

- **Summary**: enter a summary of the problem or request.

- **Description**: enter a detailed description of the problem or request.

Step 5   Click Next.

The eTicket is created.

SCMP API Basics

> ⚠ **Important**
>
> The SCMP API is CyberSource's older, legacy API. If you are starting your first implementation with CyberSource, you should use the Simple Order API instead of the SCMP API. See *Getting Started with CyberSource Advanced for the Simple Order API*.

Working with the Security Requirements

The SCMP API uses industry-standard Triple DES encryption, which guarantees the integrity and privacy of the messages that you use to access the CyberSource services.

Updating Your Client Software

The SCMP API clients include the following components:

- Client libraries for communicating with CyberSource services
- Security libraries that digitally sign the messages
- Sample code that shows how to digitally sign the messages and use the client libraries

To update your SCMP API client to the most recent version, see the SCMP API Clients page.

Constructing and Sending Requests

A request for a CyberSource service includes general information and information specific to the service that you are requesting. General information includes information about:

- You, the merchant
- The customer and the form of payment
- The items that the customer is buying

To indicate which service you are requesting, set the value of the **ics_applications** field to the name of the service. For example, to request the credit card authorization service, include the following line in your request message:

```
ics_applications=ics_auth
```

Multi-Byte Characters and Special Characters

CyberSource supports multi-byte characters for all services except Delivery Address Verification, Payment Tokenization, and Recurring Billing. Before implementing any of these services, contact Customer Support to discuss multi-byte character support. For the SCMP API, the Java client (version 3.7.7 or newer) and the .NET client support UTF-8. All of the other clients support ISO-8859-1.

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

> **Note**
>
> Request-level and offer-level field names and values must not contain carets (^) or colons (:). However, they can contain embedded spaces and any other printable characters. If you use more than one consecutive space, the extra spaces will be removed.
>
> **Atos**
> The **bill_** fields must not contain colons (:).
>
> **Moneris**
> Request-level and offer-level field names and values must not contain ampersands (&).

Data Types

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** 2016-08-11T224757Z equals August 11, 2016, 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

Using Offers or a Grand Total in a Request

For some services, you must specify the amount of the transaction. You can specify the amount either in a grand total for the entire transaction or in a separate amount for each product that the customer is purchasing.

Note If you are using Decision Manager, CyberSource recommends that you provide individual offer information instead of a grand total for the order. Decision Manager can be configured to use the individual offer information to assess the risk of the order and determine whether the purchaser is following your business rules. For more information about Decision Manager, see the *Decision Manager Developer Guide*.

Working with Offers

Offers are the products that your customers purchase from you. When you send a request for a service that requires an amount, you can send offer-specific information, such as the quantity of each offer ordered and the unit price for each offer. The offers are referred to as **offer0**, **offer1**, **offer2**, and so on. CyberSource uses the information you provide for each offer to calculate the grand total for the order.

Each offer line includes one or more offer-level fields that describe the product. Offer-level field names and values are separated by colons (:) and carets (^) in the following format:

```
offerN=<field name>:<field value>^<field name>:<field value>^...
```

The values of the offer-level fields cannot contain carets (^) or colons (:) because these characters indicate the start of the next field name or field value.

Required Offer-Level Fields

Which fields are required depends on the value you use for **product_code**. If **product_code** is one of the following values:

- ▪   default
- ▪   a value related to shipping and handling

or if you omit **product_code**, which causes it to default to the value default, then the only required field is **amount**. If you do not set **quantity**, it defaults to 1.

If you do not set **product_code** to one of the values in the previous list, the following fields are required:

- ▪   amount
- ▪   quantity
- ▪   product_name
- ▪   merchant_product_sku

The **tax_amount** field is always optional.

Specifying Tax

To include tax for an offer, use the **tax_amount** field. This value is the total tax for the entire quantity of that product. In other words, the value is not multiplied by **quantity**. For example:

```
offer0=amount:10.00^quantity:5^tax_amount:4.00
```

The grand total for this transaction is (10.00 * 5) + 4.00 = 54.00.

Specifying Freight Charges

To include a shipping and handling charge for the order, you must include an additional offer with **product_code** set to one of the following values:

- ▪   shipping_only
- ▪   handling_only
- ▪   shipping_and_handling

For example:

```
offer0=amount:10.00^quantity:5^tax_amount:4.00

offer1=amount:4.95^quantity:1^product_code:shipping_only
```

The grand total for this transaction is (10.00 * 5) + 4.00 + (4.95 * 1) = 58.95.

Grand Total

Instead of using offers, you can send a grand total for the order in the **grand_total_ amount** field. If you provide offer-level information in addition to the grand total:

■ CyberSource uses the grand total amount for the order total; CyberSource does not use the offer-level information to calculate the order total.

■ The offer-level information is displayed on the **Transaction Details** page on the Business Center.

> **!**
> **Important**
> If you include **grand_total_amount** in your request, you cannot include the tax calculation service in the request. See *Tax Calculation Service for the SCMP API.*

Coupons

You can offer your customers virtual coupons at your web store. CyberSource defines a coupon as a non-taxable, fixed amount deducted from an order total. Some examples of coupons you might offer are:

■ Register now and get $100 off your purchase!

■ Spring clearance! Get $10 off any order!

■ Thank you for ordering again within 30 days! We're taking $5 off your order!

How Coupons are Processed

This sequence summarizes how CyberSource processes a request that includes a coupon:

1 All offers are totaled and then the coupon amounts are deducted, resulting in an order subtotal.

2 If the request includes the tax calculation service, tax is calculated for all taxable offers to get an order tax total. The tax calculation service ignores coupon offers because they are not taxable.The order subtotal and order tax total are added to get an order grand total.

3 The order grand total is used by the services in your request.

For example, if you requested an electronic check debit in the request with the coupon, the electronic check debit service uses the order grand total as the amount to charge.

Coupon Constraints

You cannot use coupons to do the following:

■ Apply a discount to a specific item in a multi-offer order

■ Apply a discount to a specific offer before tax is calculated

■ Apply a percentage discount

The total coupon amount cannot be greater than the order grand total. Calculate your order totals before you send your requests to CyberSource so that you do not send orders with negative subtotals. CyberSource returns an error for orders with negative subtotals.

Including a Coupon in the Request

To request a coupon with an order, include in the request an offer with the product code set to `coupon`. For example, if your request contains two offers, **offer0** and **offer1**, request a coupon by adding **offer2**. The following example shows how to specify a 10 USD coupon. The **quantity**, **product_name**, and **merchant_product_sku** fields are required.

```
offer2=product_code:coupon^quantity:1^amount:10.00^product_name:Spring
Clearance^merchant_product_sku:349209.
```

Requesting a Follow-On Service

Request IDs and Request Tokens

> **! Important**
> Request tokens are required in follow-on request messages only for PayPal Express Checkout, China Processing, the Ingenico ePayments processor and the Atos processor. If you are using other payment methods and processors (see page 22), you are not required to include request tokens in your request messages.

Request IDs and request tokens are identifiers that CyberSource returns in the reply messages for all services. You need to store these values because you will need them when you send a request for a follow-on service. For the request ID, the field name depends on the names of the primary service and follow-on service.

> ⚠️ **Important** Although the name of the request token field that you receive is the same in each reply, the value for the field is different. Therefore, you must save each request token that you receive.

Alternative Payment Methods and Processors

For PayPal Express Checkout, China Processing, the Ingenico ePayments processor, and the Atos processor, a request for a follow-on service must include a request ID and a request token. Save the request ID from the reply for the primary service and send this value in the follow-on request.

Working with Request Tokens

> ⚠️ **Important** Request tokens are required in follow-on request messages for PayPal Express Checkout, China Processing, the Ingenico ePayments processor, and the Atos processor. If you are using other payment methods and processors (see page 22), you are not required to include request tokens in your request messages.

The request token is a unique identifier that CyberSource assigns to each request and returns to you in each reply. This field is an encoded string that does not contain any confidential information, such as account numbers or card verification numbers. For China Processing, the Ingenico ePayments processor and Atos, you need to store this value, which is a string of up to 256 characters. Depending on how you process follow-on requests, you might need to retrieve the request token value and include it in your follow-on service requests:

- If you process primary requests with an API, but process follow-on requests through the Business Center, you do not need to provide the request token data.

- If you process primary and follow-on requests with an API, you need to retrieve the request token from the primary reply message and include it in the follow-on request message:

  Primary reply: `request_token=AA4JUrWguaMUGwxSWVdPS5IM`

  Follow-on request: `order_request_token=AA4JUrWguaMUGwxSWVdPS5IM`

Merchants Who Have Not Implemented Request Tokens

If you were a CyberSource merchant before July 2008 and never implemented request tokens, you have a choice:

- You can implement the request token as described in this document.
- You can let CyberSource store the request token data for you and retrieve it for you as necessary when you send follow-on requests.

Merchants Who Have Implemented Request Tokens

If you were a CyberSource merchant before July 2008 and implemented request tokens, your implementation uses a different field name for the request token that is sent to each follow-on service. With the new implementation, you use the **order_request_token** field for all follow-on services. This approach makes it easier to manage the request token values. It also reduces the likelihood of submitting a duplicate request by accidentally sending in the wrong request token value. You have a choice:
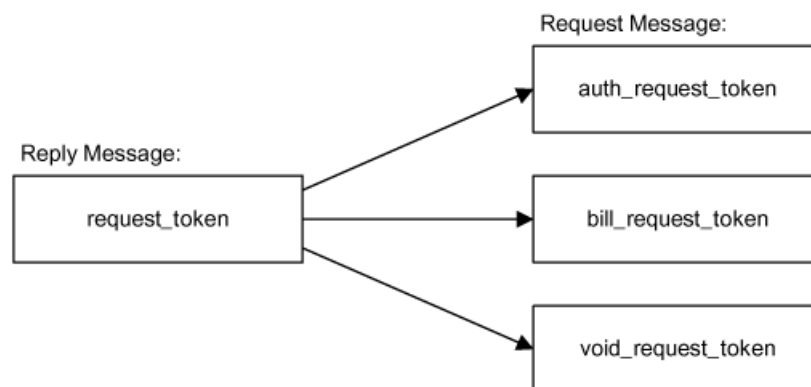
■ You can continue to use your current implementation at this time. It is still supported, but CyberSource recommends that you update your implementation to use the **order_request_token** field.

■ You can update your implementation to store the latest request token for a transaction in one database field to return with all follow-on services for the transaction:

Reply Message:

    request_token   →   Request Message: order_request_token

■ You can update your implementation without changing your database. Store the latest request token for a transaction in all of your existing request token database fields so that any follow-on request for the transaction will return the latest request token value:

> **Note** The following figure uses the request field names for the Credit Card services. If you are using a different set of services, substitute the request field names for the services you are using.

Request Message:

    Reply Message:
    request_token   →   auth_request_token
                    →   bill_request_token
                    →   void_request_token

Handling Replies

After receiving a request from you, CyberSource responds with a reply message containing the results of the request. You must integrate this into your system and any other system that uses it. This includes storing the data and passing it to any other systems that need it.

Write an error handler to interpret the information in the reply message. Do not show the reply information directly to your customers. Instead, present an appropriate response that provide customers with the results of their transactions.

⚠
Important

Because CyberSource can add reply fields, reply codes, and reply messages at any time, do the following.

■ Parse the reply data according to the names of the fields instead of their order in the reply. For more information about parsing reply fields, see the documentation for your client.

■ Program your error handler to use the reply flag value to determine the result if it receives a reply code that it does not recognize.

Reply Codes

Every reply message includes the **ics_rcode** field, which summarizes the overall result of your request, and one or more **<service>_rcode** fields, which provide the results for each service you requested. The following table describes the possible values for the reply codes. You are charged for all accepted and rejected requests. You are not charged for requests that result in errors

Reply Flags

Table 5   Possible Values for the Reply Codes

Reply Code Value	Description
1	*Success*—The request succeeded.
0	*Decline (Reject)*—One or more of the services were declined. Requests can be rejected by CyberSource, the payment processor, or the issuing bank. For example, CyberSource will reject a request if required data is missing or invalid. The issuing bank will reject a request if the card limit has been reached and funds are not available. To determine the reason for the reject decision, use the **ics_rflag** field.
-1	*Error*—There was a system error. Errors that are caused by system issues are usually unrelated to the content of the request itself. You must design your transaction management system to correctly handle CyberSource system errors. Depending on which payment processor is handling the transaction, the error could indicate a valid CyberSource system error or it could indicate a processor rejection because of invalid data. CyberSource recommends that you do not design your system to endlessly retry sending a transaction in the case of a system error. Use the value of the reply flag to determine the reason for the system error. For more information handling system errors and retries, see the documentation for your client.

Every reply message includes the **ics_rflag** field, which is a one-word value that provides information about your request, and one or more **<service>_rflag** fields, which provide information about each service you requested. The following table describes the reply flags that correspond to each reply code value.

Table 6   Possible Values for the Reply Flags

Reply Code Value	Corresponding Reply Flags
1	SOK.
0	The SPARTIALAPPROVAL value or a value starting with D such as DMISSINGFIELD.
-1	A value starting with E such as ESYSTEM. See the documentation for your CyberSource client for information about handling system errors and retries. **Note** If you receive the ESYSTEM flag in your reply along with the following error message, your system's clock is incorrect. You must adjust your system's clock for your time zone; otherwise your transactions will be rejected. Error message: The request ID generated by your client is incorrect because your system's clock does not match your local time. Please adjust your system's clock to your local time, and resend your request.

Reply Messages

The **ics_rmsg** value explains the **ics_rflag** value. The **<service>_rmsg** fields provide information about each service you requested.

Request IDs and Request Tokens

![Important] Request tokens are required in follow-on request messages for PayPal Express Checkout, China Processing, the Ingenico ePayments processor, and the Atos processor. If you are using other payment methods and processors (see page 26), you are not required to include request tokens in your request messages.

CyberSource returns a request ID and a request token in the reply for every service. You must store these values because you will need them when you send a request for a follow-on service as described in "Request IDs and Request Tokens," page 21.

![Important] Although the names of the request token and request ID fields are the same in each reply, the values for the fields are different in each reply. Therefore, you must save each request ID and request token that you receive.

Alternative Payment Methods and Processors

CyberSource returns a request ID in the reply for every service. You must store this value because you will need it when you send a request for a follow-on service as described in "Requesting a Follow-On Service," page 21.

![Important] Although the name of the request ID field is the same in each reply, the value for the field is different in each reply. Therefore, you must save each request ID that you receive.