Apple Pay
Using the SCMP API

November 2019
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

© 2019 CyberSource Corporation. All rights reserved. CyberSource Corporation ("CyberSource") furnishes this document and the software described in this document under the applicable agreement between the reader of this document ("You") and CyberSource ("Agreement"). You may use this document and/or software only in accordance with the terms of the Agreement. Except as expressly set forth in the Agreement, the information contained in this document is subject to change without notice and therefore should not be interpreted in any way as a guarantee or warranty by CyberSource. CyberSource assumes no responsibility or liability for any errors that may appear in this document. The copyrighted software that accompanies this document is licensed to You for use only in strict accordance with the Agreement. You should read the Agreement carefully before using the software. Except as permitted by the Agreement, You may not reproduce any part of this document, store this document in a retrieval system, or transmit this document, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written consent of CyberSource.

Restricted Rights Legends

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

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 Unpublished rights reserved under the copyright laws of the United States.

Trademarks


CyberSource, CyberSource Payment Manager, CyberSource Risk Manager, CyberSource Decision Manager, and CyberSource Connect are trademarks and/or service marks of CyberSource Corporation.

All other brands and product names are trademarks or registered trademarks of their respective owners.
## Contents

**Recent Revisions to This Document** 5

**About This Guide** 7
- Audience and Purpose 7
- Conventions 7
  - Note and Important Statements 7
  - Text and Command Conventions 8
- Related Documents 8
- Customer Support 8

### Chapter 1 Apple Pay Integrations 9

**In-App Transactions Using the CyberSource API** 9
- Merchant Decryption 9
- CyberSource Decryption 10

**Web Transactions** 11
- Merchant Decryption 11
- CyberSource Decryption 11

**Requirements** 12

**Apple Pay JavaScript** 13
- Apple Pay Button 13
- ApplePaySession Class 13
- Create ApplePaySession Object 14
- Merchant Validation 14
- Payment Confirmation 14
- Merchant Decryption 14
- CyberSource Decryption 15
# Contents

## Chapter 2  Getting Started 16
- Requirements 16
- Supported Processors, Card Types, and Optional Features 17
- Enrolling in Apple Pay 18
  - Generating a New CSR 19
- Transaction Reports 20

## Chapter 3  Requesting the Authorization Service 21
- Option 1: Merchant Decryption 21
  - Visa Transaction 21
  - Mastercard Transaction 23
  - American Express Transaction 25
  - Discover Transaction 27
  - JCB Transaction 28
- Option 2: CyberSource Decryption 30
  - Visa Transaction 30
  - Mastercard Transaction 31
  - American Express Transaction 33
  - Discover Transaction 35
  - JCB Transaction 36
- Additional CyberSource Services 38

## Appendix A  SCMP API Fields 39
- Data Type Definitions 39
- Relaxed Requirements for Address Data and Expiration Date 39
- API Request Fields 40
- Offer-Level Fields 46
- API Reply Fields 47
Recent Revisions to This Document

<table>
<thead>
<tr>
<th>Release</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 2019</td>
<td>Changed <em>payment network tokenization</em> to <em>authorizations with payment network tokens</em> throughout.</td>
</tr>
<tr>
<td></td>
<td>SIX: added an important note. See SIX, page 18.</td>
</tr>
<tr>
<td>September 2019</td>
<td>This revision contains only editorial changes and no technical updates.</td>
</tr>
<tr>
<td>May 2019</td>
<td>This revision contains only editorial changes and no technical updates.</td>
</tr>
<tr>
<td>Release</td>
<td>Changes</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Added the following request fields that support tokenized transactions using a network token with 3D Secure or SecureCode (see &quot;API Request Fields,&quot; page 40):</td>
</tr>
<tr>
<td></td>
<td>▪ directory_server_transaction_id</td>
</tr>
<tr>
<td></td>
<td>▪ network_token_cryptogram</td>
</tr>
<tr>
<td></td>
<td>▪ pa_specification_version</td>
</tr>
<tr>
<td></td>
<td>Added the <strong>directory_server_transaction_id</strong> reply field that supports tokenized transactions using a network token with 3D Secure or SecureCode (see &quot;API Reply Fields,&quot; page 47).</td>
</tr>
<tr>
<td></td>
<td>Added support for the processor <strong>Elavon Americas</strong>. See &quot;Supported Processors, Card Types, and Optional Features,&quot; page 17.</td>
</tr>
<tr>
<td></td>
<td>Added support for merchant-initiated transactions as an optional feature for the following processors (see &quot;Supported Processors, Card Types, and Optional Features,&quot; page 17):</td>
</tr>
<tr>
<td></td>
<td>▪ Chase Paymentech Solutions</td>
</tr>
<tr>
<td></td>
<td>▪ CyberSource through VisaNet</td>
</tr>
<tr>
<td></td>
<td>▪ Elavon Americas</td>
</tr>
<tr>
<td></td>
<td>Added support for subsequent authorizations as an optional feature for the following processors (see &quot;Supported Processors, Card Types, and Optional Features,&quot; page 17):</td>
</tr>
<tr>
<td></td>
<td>▪ FDC Nashville Global</td>
</tr>
<tr>
<td></td>
<td>▪ JCN Gateway</td>
</tr>
<tr>
<td></td>
<td>Added support for the following optional features by Elavon Americas (see &quot;Supported Processors, Card Types, and Optional Features,&quot; page 17):</td>
</tr>
<tr>
<td></td>
<td>▪ Multiple partial captures</td>
</tr>
<tr>
<td></td>
<td>▪ Recurring payments</td>
</tr>
<tr>
<td>March 2019</td>
<td>Added support for the processor <strong>Credit Mutuel-CIC</strong>. See &quot;Supported Processors, Card Types, and Optional Features,&quot; page 17.</td>
</tr>
<tr>
<td></td>
<td>Added support for recurring payments as an optional feature for the processors <strong>Credit Mutuel-CIC</strong> and <strong>SIX</strong>. See &quot;Supported Processors, Card Types, and Optional Features,&quot; page 17.</td>
</tr>
</tbody>
</table>
About This Guide

Audience and Purpose

This document is written for merchants who want to use Apple Pay in an iOS application and use information from Apple to process payments through CyberSource. This document provides an overview for integrating Apple and CyberSource services into an order management system.

Conventions

Note and Important Statements

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

An Important statement contains information essential to successfully completing a task or learning a concept.
Text and Command Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Usage</th>
</tr>
</thead>
</table>
| Bold       | ■ Field and service names in text; for example: Include the **card_accountNumber** 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

CyberSource Documents:  
■ *Business Center User Guide* (PDF | HTML)  
■ *Business Center Reporting User Guide* (PDF | HTML)  
■ *Credit Card Services Using the SCMP API* (PDF | HTML)  
■ *Authorizations with Payment Network Tokens Using the SCMP API* (PDF | HTML)

Apple Documents:  
■ *PassKit Framework Reference*

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
In-App Transactions Using the CyberSource API

Merchant Decryption

1. When the customer chooses to pay with Apple Pay, you use the Apple PassKit Framework to request the encrypted payment data from Apple.

2. Apple uses the Secure Element to create a payment token (the PKPaymentToken structure) and encrypt the token’s payment data (the paymentData field of the PKPaymentToken structure) before it sends it to your application.

3. You forward the encrypted payment data to your e-commerce back-end system to decrypt. For information on decryption, see:

   https://developer.apple.com/library/ios/documentation/PassKit/Reference/PaymentTokenJSON/PaymentTokenJSON.html#//apple_ref/doc/uid/TP40014929-CH8-SW1

4. Using the CyberSource API, you submit the authorization request and include the decrypted payment data. See "Option 1: Merchant Decryption," page 21.
5 CyberSource forwards the information to the payment network, including your processor and the relevant payment card company.

---

Important

You must use the Business Center or one of the CyberSource API services to capture, credit, or void the authorization. See Credit Card Services Using the SCMP API.

---

**CyberSource Decryption**

1. When the customer chooses to pay with Apple Pay, you use the Apple PassKit Framework to request the encrypted payment data from Apple.

2. Apple uses the Secure Element to create a payment token (the `PKPaymentToken` structure) and encrypt the token’s payment data (the `paymentData` field of the `PKPaymentToken` structure) before it sends it to your application.

3. You forward the encrypted payment data to your e-commerce back-end system.

4. Using the CyberSource API, you submit the authorization request. In the `encrypted_payment_data` field include the Base64 encoded value obtained from the `paymentData` field of the `PKPaymentToken` structure. See "Option 2: CyberSource Decryption," page 30.

5. CyberSource decrypts the payment data and forwards the information to the payment network, including your processor and the relevant payment card company.

---

Important

You must use the Business Center or one of the CyberSource API services to capture, credit, or void the authorization. See Credit Card Services Using the SCMP API.
Web Transactions

Merchant Decryption

1. When the customer chooses to pay with Apple Pay, you use the Apple Pay JavaScript to request the encrypted payment data from Apple.

2. Apple uses the Secure Element to create a payment token (the `PKPaymentToken` structure) and encrypt the token’s payment data (the `paymentData` field of the `PKPaymentToken` structure) before it sends it your application using the `onpaymentauthorized` callback function.

3. You forward the encrypted payment data to your e-commerce back-end system to decrypt. For information on decryption, see:

   https://developer.apple.com/library/ios/documentation/PassKit/Reference/PaymentTokenJSON/PaymentTokenJSON.html#//apple_ref/doc/uid/TP40014929-CH8-SW1

4. Using the CyberSource API, you submit the authorization request and include the decrypted payment data. See "Option 2: CyberSource Decryption," page 30.

5. CyberSource forwards the information to the payment network, including your processor and the relevant payment card company.

   ---
   **Important**
   You must use the Business Center or one of the CyberSource API services to capture, credit, or void the authorization. See Credit Card Services Using the SCMP API.
   ---

CyberSource Decryption

1. When the customer chooses to pay with Apple Pay, you use the Apple Pay JavaScript to request the encrypted payment data from Apple.

2. Apple uses the Secure Element to create a payment token (the `PKPaymentToken` structure) and encrypt the token’s payment data (the `paymentData` field of the `PKPaymentToken` structure) before it sends it your application via the `onpaymentauthorized` callback function.

3. You forward the encrypted payment data to your e-commerce back-end system.

4. Using the CyberSource API, you submit the authorization request. In the `encrypted_payment_data` field include the Base64 encoded value obtained from the `paymentData` field of the `PKPaymentToken` structure. See "Option 2: CyberSource Decryption," page 30.
5 CyberSource decrypts the payment data and forwards the information to the payment network, including your processor and the relevant payment card company.

---

**Important**

You must use the Business Center or one of the CyberSource API services to capture, credit, or void the authorization. See *Credit Card Services Using the SCMP API.*

---

### Requirements

You must be an *Admin* or *Team Agent* user of your Apple Developer Program account.

For details on each requirement below, see:


**To configure your requirements:**

**Step 1** Register your merchant ID.

If you are currently processing In-App transactions, you can use the same merchant ID for processing Web transactions.

**Step 2** Create or upload a Certificate Signing Request (CSR), which is used to encrypt the payment information during the payment process.

If you are using the merchant decryption method (see "Option 1: Merchant Decryption," page 21), create a CSR.

If you are using the CyberSource decryption method (see "Option 2: CyberSource Decryption," page 30), upload the CSR that you created in the Business Center (see "Enrolling in Apple Pay," page 18).

If you are currently processing In-App transactions, you can use the same CSR for processing Web transactions.

**Step 3** Register your domain. Registration is required in order to use Apple Pay on your web site.

**Step 4** Create a Merchant Identity Certificate. This certificate is required in order to connect to the Apple servers.
Apple Pay JavaScript

Use the Apple Pay JavaScript to accept Apple Pay payments on your web site. The Apple Pay JavaScript tests that Apple Pay exists on your web site, displays the Apple Pay sheet, and receives the payment token.

Apple Pay Button

When a customer clicks or taps an Apple Pay button, it must invoke the Apple Pay payment sheet.

For information on how to use Apple Pay buttons and the button styles, see:


You can use CSS templates provided by Apple to display the Apple Pay button on your web site. There are two templates: logo only button and buy with button. For more information, see Displaying the Apple Pay Button.

ApplePaySession Class

The ApplePaySession class manages the payment process on your web site. The ApplePaySession object is the entry point for Apple Pay on your web site.

Before displaying the Apple Pay button (see "Apple Pay Button," page 13) or creating an Apple Pay session (see "Create ApplePaySession Object," page 14), ensure that the Apple Pay JavaScript API is available and enabled on the device.

To enable the Apple Pay JavaScript API:

Step 1 Verify that the window.ApplePaySession class exists.

Step 2 Call its canMakePayments or canMakePaymentsWithActiveCard method:

- canMakePayments—verifies that the device is enabled for Apple Pay.

- canMakePaymentsWithActiveCard—verifies that the device is enabled for Apple Pay and the customer has a card stored on the device. You can call this method only if Apple Pay is the default payment method during your checkout flow, or if you want to add the Apple Pay button to your product detail page.

Note All optional features are described in Authorizations with Payment Network Tokens Using the SCMP API (PDF | HTML).

Important When a customer clicks or taps an Apple Pay button, it must invoke the Apple Pay payment sheet.
Create ApplePaySession Object

There are two required arguments when creating an ApplePaySession object:

- Version number—the API version is 1.
- Payment request—the PaymentRequest dictionary contains the information required in order to display the payment form.

When the session is created, call its begin method to display the payment form. This method can be called only when invoked by a user’s request.

Merchant Validation

When the payment form is displayed, the onvalidatemerchant callback function is called and provides a URL to pass to your server for validating the merchant session. Refer to the Merchant Validation section.

Payment Confirmation

When the customer confirms the payment by clicking or tapping the Apple Pay button, the onpaymentauthorized callback function is called and provides the payment token.

Merchant Decryption

Forward the encrypted payment data to your e-commerce back-end system to decrypt. For information on decryption, see: https://developer.apple.com/library/ios/documentation/PassKit/Reference/PaymentTokenJSON/PaymentTokenJSON.html#//apple_ref/doc/uid/TP40014929-CH8-SW1

Using the CyberSource API, submit the authorization request and include the decrypted payment data. See "Option 1: Merchant Decryption," page 21.
CyberSource Decryption

Forward the encrypted payment data to your e-commerce back-end system.

Using the CyberSource API, submit the authorization request. In the `encrypted_payment_data` field include the Base64 encoded value obtained from the `paymentData` object. Example 1 shows the JavaScript for obtaining this value. See "Option 2: CyberSource Decryption," page 30.

Example 1  JavaScript for Obtaining a Base64-Encoded Value

```javascript
session.onpaymentauthorized = function (event) {

    var paymentDataString = JSON.stringify(event.payment.token.paymentData);

    var paymentDataBase64 = btoa(paymentDataString);

    ...

}
```
Getting Started

Requirements

- CyberSource account. If you do not already have a CyberSource account, contact your local CyberSource sales representative. You can find your local Sales office here: http://www.cybersource.com/locations/

- Merchant account with a supported processor (see Table 1, “Processors, Card Types, and Optional Features,” on page 17).

- You must have an Admin or Team Agent user of the Apple Pay Developer account.

---

Important

Apple Pay relies on authorizations with payment network tokens. You can sign up for Apple Pay only when both of the following statements are true:

- Your processor supports payment network tokens.
- CyberSource supports payment network tokens with your processor.

If one or both of the preceding statements are not true, you must take one of the following actions before you can sign up for Apple Pay:

- Obtain a new merchant account with a processor that supports payment network tokens.
- Wait until your processor supports payment network tokens.
## Supported Processors, Card Types, and Optional Features

All optional features, except split shipments, are described in *Authorizations with Payment Network Tokens Using the SCMP API* (PDF | HTML). Split shipments are described in *Credit Card Services Using the SCMP API* (PDF | HTML).

### Table 1  Processors, Card Types, and Optional Features

<table>
<thead>
<tr>
<th>Processor</th>
<th>Card Types</th>
<th>Optional Features</th>
</tr>
</thead>
</table>
| American Express Direct | American Express | - Multiple partial captures  
| | | - Recurring payments |
| Barclays | Visa, Mastercard, Maestro (International), Maestro (UK Domestic) | - Multiple partial captures  
| | | - Recurring payments |
| Chase Paymentech Solutions | Visa, Mastercard, American Express, Discover, Maestro (International) | - Merchant-Initiated transactions  
| | | - Multiple partial captures  
| | | - Recurring payments |
| Credit Mutuel-CIC | Visa, Mastercard, Cartes Bancaires | Recurring Payments |
| 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 | - Merchant-Initiated transactions  
| | | - Recurring payments  
| | | - Split shipments |
| Elavon Americas | Visa, Mastercard, American Express, JCB, Discover | - Merchant-Initiated transactions  
| | | - Multiple partial captures  
| | | - Recurring payments |
| FDC Compass | Visa, Mastercard, American Express | - Multiple partial captures  
| | | - Recurring payments |
| FDC Nashville Global | Visa, Mastercard, American Express, Discover | - Multiple partial captures  
| | | - Recurring payments  
| | | - Subsequent authorizations |
| GPN | Visa, Mastercard, American Express | - Recurring payments  
| | | - Split shipments |
Chapter 2  Getting Started

Enrolling in Apple Pay

To enroll in Apple Pay:

**Step 1** Log in to the Business Center:
- Test transactions: https://ebctest.cybersource.com/ebc2/
- Live transactions: https://ebc2.cybersource.com/ebc2/

**Step 2** On the left navigation pane, click the **Payment Configuration** icon.

**Step 3** Click **Digital Payment Solutions**. The Digital Payments page appears.

---

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

<table>
<thead>
<tr>
<th>Processor</th>
<th>Card Types</th>
<th>Optional Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>JCN Gateway</td>
<td>JCB</td>
<td>Multiple partial captures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subsequent authorizations</td>
</tr>
<tr>
<td>OmniPay Direct. The supported acquirers are:</td>
<td>Visa, Mastercard, Maestro (UK Domestic), Maestro (International)</td>
<td>Multiple partial captures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recurring payments</td>
</tr>
<tr>
<td>Bank of America Merchant Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>First Data Merchant Solutions (Europe)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Global Payments International Acquiring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIX</td>
<td>Visa, Mastercard, Maestro (UK Domestic), Maestro (International)</td>
<td>Recurring Payments</td>
</tr>
<tr>
<td><strong>Important</strong> SIX is supported only for card-present processing.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Streamline</td>
<td>Visa, Mastercard, Maestro (UK Domestic), Maestro (International)</td>
<td>Multiple partial captures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recurring payments</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subsequent authorizations</td>
</tr>
<tr>
<td>TSYS Acquiring Solutions</td>
<td>Visa, Mastercard, American Express</td>
<td>Multiple partial captures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recurring payments</td>
</tr>
<tr>
<td>Worldpay VAP</td>
<td>Visa, Mastercard</td>
<td>Recurring Payments</td>
</tr>
</tbody>
</table>

Worldpay VAP was previously called Litle. Litle was purchased by Vantiv, which was then purchased by Worldpay VAP. If you have any questions about this situation, contact your account manager at Worldpay VAP.
**Step 4**  Click **Configure**. The Apple Pay Registration panel opens.

**Step 5**  Enter your Apple Merchant ID.

**Step 6**  Click **Generate New CSR**.

**Step 7**  To download your CSR, click the **Download** icon next to the key.

**Step 8**  Follow your browser’s instructions to save and open the file.

**Step 9**  Complete the enrollment process by submitting your CSR to Apple.

**Step 10**  For information about adding certificates to your Apple Merchant ID, refer to the Apple Pay PassKit:

https://developer.apple.com/documentation/passkit

**Step 11**  Test your software. See "Requesting the Authorization Service," page 21.

---

If you are using a CyberSource test account, you must connect to the Apple developer system and not to the Apple production system.

---

**Important**

After you complete your testing, you must create a new CSR for the CyberSource production system, and you must use that CSR for the Apple production system. Until you perform these steps, you cannot enable payments in your iOS application.

---

**Step 12**  Repeat Steps 1 through 10 with your CyberSource production account and the Apple production account.

---

**Generating a New CSR**

**To generate a new CSR:**

**Step 1**  Log in to the Business Center:

- Test transactions: https://ebctest.cybersource.com/ebc2/
- Live transactions: https://ebc2.cybersource.com/ebc2/

**Step 2**  On the left navigation pane, click the **Payment Configuration** icon.

**Step 3**  Click **Digital Payment Solutions**. The Digital Payments page appears.
Step 4 Click **Configure**. The Apple Pay Registration panel opens.

Step 5 To download your CSR, click the **Download** icon next to the key.

Step 6 Follow your browser's instructions to save and open the file.

Step 7 To edit your Apple Merchant ID, click the **Edit** icon. The Edit CSR panel opens.

Step 8 Modify your merchant ID as necessary and click **Update**.

---

**Transaction Reports**

Go to the Business Center and use the Transaction Request Report to obtain information about your transactions:

- In the Business Center, use the Transaction Search page to identify Apple transactions. You can search for transactions by date, application type, customer name, and other transaction identifiers.

- For information about the Transaction Request Report, see the *Business Center Reporting User Guide (PDF | HTML)*
Option 1: Merchant Decryption

Visa Transaction

To request an authorization for a Visa transaction:

- **Step 1** Set the `customer_cc_number` field to the payment network token value.
- **Step 2** Set the `customer_cc_expmo` and `customer_cc_expyr` fields to the values from the payment network token expiration date.
- **Step 3** Set the `cavv` field to the 3D Secure cryptogram of the payment network token.
- **Step 4** Set the `network_token_cryptogram` field to the network token cryptogram.
- **Step 5** Set the `payment_network_token_transaction_type` field to 1.
- **Step 6** Set the `e_commerce_indicator` field to the ECI value contained in the Apple Pay response payload (5=vvb and 7=internet).
- **Step 7** Set the `payment_solution` field to 001.

See the Relaxed Requirements for Address Data and Expiration Date page and "API Request Fields," page 40, for details and field descriptions.
Example 2  Authorization Request (Visa)

```
bill_address1=123 Main Street
bill_address2=Suite 12345
bill_city=Small Town
bill_country=US
bill_state=CA
bill_zip=98765
card_type=001
cavv=EHuWW9PiBkWvqE5juRwDzAUFBAk=
currency=USD
customer_cc_expno=12
customer_cc_expyr=2031
customer_cc_number=4111111111111111
customer_email=js@example.com
customer_firstname=Jane
customer_lastname=Smith
customer_phone=999-999-9999
e_commerce_indicator=internet
grand_total_amount=100.00
ics_applications=ics_auth
merchant_id=mid123
merchant_ref_number=ref123
payment_network_token_transaction_type=1
payment_solution=001
```
**Mastercard Transaction**

To request an authorization for a Mastercard transaction:

---

**Note** See the Relaxed Requirements for Address Data and Expiration Date page and "API Request Fields," page 40, for details and field descriptions.

**Step 1** Set the `customer_cc_number` field to the payment network token value.

**Step 2** Set the `customer_cc_expmo` and `customer_cc_expyr` fields to the values from the payment network token expiration date.

**Step 3** Set the `ucaf_authentication_data` field to the 3D Secure cryptogram of the payment network token.

**Step 4** Set the `network_token_cryptogram` field to the network token cryptogram.

**Step 5** Set the `ucaf_collection_indicator` field to 2.

**Step 6** Set the `payment_network_token_transaction_type` field to 1.

**Step 7** Set the `e_commerce_indicator` field to spa.

**Step 8** Set the `payment_solution` field to 001.
Example 4  Authorization Request (Mastercard)

```
bill_address1=123 Main Street
bill_address2=Suite 12345
bill_city=Small Town
bill_country=US
bill_state=CA
bill_zip=98765
card_type=002
currency=USD
customer_cc_expmo=12
customer_cc_expyr=2031
customer_cc_number=5432543254325432
customer_email=js@example.com
customer_firstname=Jane
customer_lastname=Smith
customer_phone=999-999-9999
e_commerce_indicator=spa
grand_total_amount=100.00
ics_applications=ics_auth
merchant_id=med123
merchant_ref_number=ref123
ucaf_authentication_data=ABCDEFabcdefABCDEFabcdef0987654321234567
ucaf_collection_indicator=2
payment_network_token_transaction_type=1
payment_solution=001
```

Example 5  Authorization Reply (Mastercard)

```
auth_auth_amount=100.00
auth_auth_avs=X
auth_auth_code=888888
auth_auth_response=100
auth_avs_raw=I1
auth_rcode=1
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_trans_ref_no=15356268CR2XF23X
currency=USD
ics_rcode=1
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
merchant_ref_number=ref123
request_id=4697369268106124601541
request_token=Ahj/7wSR/UoVmlbMmziHSZjMECTh+h+KjMHSB04gwGA2dDjQoxQAAA6xdr
```
American Express Transaction

To request an authorization for an American Express transaction:

See the Relaxed Requirements for Address Data and Expiration Date page and "API Request Fields," page 40, for details and field descriptions.

Step 1  Set the customer_cc_number field to the payment network token value.

Step 2  Set the customer_cc_expmo and customer_cc_expyr fields to the values from the payment network token expiration date.

Step 3  Set the cavv field to the 3D Secure cryptogram of the payment network token.

Include the whole 20-byte cryptogram in the cavv field. For a 40-byte cryptogram, split the cryptogram into two 20-byte binary values (block A and block B). Set the cavv field to the block A value and set the xid field to the block B value.

Step 4  Set the network_token_cryptogram field to the network token cryptogram.

Step 5  Set the payment_network_token_transaction_type field to 1.

Step 6  Set the e_commerce_indicator field to aesk.
Step 7  Set the `payment_solution` field to 001.

Example 6  Authorization Request (American Express)

```
bill_address1=123 Main Street
bill_address2=Suite 12345
bill_city=Small Town
bill_country=US
bill_state=CA
bill_zip=98765
card_type=003
cavv=EHuWW9PiBkWvqE5juRwDzAUFBaK=
currency=USD
customer_cc_expmo=12
customer_cc_expyr=2031
customer_cc_number=37828224631xxxx
customer_email=js@example.com
customer_firstname=Jane
customer_lastname=Smith
customer_phone=999-999-9999
e_commerce_indicator=aesk
grand_total_amount=100
ics_applications=ics_auth
merchant_id=mid123
merchant_ref_number=ref123
payment_network_token_transaction_type=1
payment_solution=001
```

Example 7  Authorization Reply (American Express)

```
auth_auth_amount=100.00
auth_auth_avs=X
auth_auth_code=888888
auth_auth_response=100
auth_avs_raw=11
auth_rcode=1
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_trans_ref_no=15356269CR2XF23Y
currency=USD
ics_rcode=1
ics_return_code=1000000
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
merchant_ref_number=ref123
request_id=4697369273896124701541
request_token=Ahj/7wSR/UowJcJsefb4e64b4e64756hjrd8/P61GBLhJRpb2QAAAPxNY
```
Discover Transaction

To request an authorization for a Discover transaction:

- **Step 1** Set the `customer_cc_number` field to the payment network token value.
- **Step 2** Set the `customer_cc_expmo` and `customer_cc_expyr` fields to the values from the payment network token expiration date.
- **Step 3** Set the `cavv` field to the 3D Secure cryptogram of the payment network token.
- **Step 4** Set the `network_token_cryptogram` field to the network token cryptogram.
- **Step 5** Set the `payment_network_token_transaction_type` field to 1.
- **Step 6** Set the `e_commerce_indicator` field to `dipb`.
- **Step 7** Set the `payment_solution` field to 001.

Example 8  Authorization Request (Discover)

```
bill_address1=123 Main Street
bill_address2=Suite 12345
bill_city=Small Town
bill_country=US
bill_state=CA
bill_zip=98765
card_type=004
cavv=EHuWW9PiBkWvqE5juRwDzAUFBAk=
currency=USD
customer_cc_expmo=12
customer_cc_expyr=2031
customer_cc_number=601111111111xxxx
customer_email=js@example.com
customer_firstname=Jane
customer_lastname=Smith
customer_phone=999-999-9999
e_commerce_indicator=dipb
grand_total_amount=100
ics_applications=ics_auth
merchant_id=mid123
merchant_ref_number=ref123
payment_network_token_transaction_type=1
payment_solution=001
```
Chapter 3  Requesting the Authorization Service

Example 9  Authorization Reply (Discover)

```
auth_auth_amount=100.00
auth_auth_avs=X
auth_auth_code=888888
auth_auth_response=100
auth_avs_raw=II
auth_rcode=1
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_trans_ref_no=15356269CR2XF23Y
currency=USD
ics_rcode=1
ics_return_code=1000000
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
merchant_ref_number=ref123
request_id=4697369273896124701541
request_token=Ahj/7wSR/UowJcJsefb4e64b4e64756hjrd8/P61GBLhJRpZQAAAPxNY
```

JCB Transaction

To request an authorization for a JCB transaction:

**Step 1** Set the `customer_cc_number` field to the payment network token value.

**Step 2** Set the `customer_cc_expmo` and `customer_cc_expyr` fields to the values from the payment network token expiration date field.

**Step 3** Set the `cavv` field to the 3D Secure cryptogram of the payment network token.

**Step 4** Set the `payment_network_token_transaction_type` field to 1.

**Step 5** Set the `eci_raw` field to the ECI value contained in the Apple Pay response payload.

**Step 6** Set the `payment_solution` field to 001.

Note: See the Relaxed Requirements for Address Data and Expiration Date page and "API Request Fields," page 40, for details and field descriptions.
Example 10  Authorization Request (JCB)

```plaintext
bill_address1=123 Main Street
bill_address2=Suite 12345
bill_city=Small Town
bill_country=US
bill_state=CA
bill_zip=98765
card_type=007
currency=USD
customer_cc_expmo=12
customer_cc_expyr=2031
customer_cc_number=356611111111xxxx
customer_email=js@example.com
customer_firstname=Jane
customer_lastname=Smith
customer_phone=999-999-9999
eci_raw=05
grand_total_amount=100.00
ics_applications=ics_auth
merchant_id=med123
cavv=EHuWW9PiWtvqE5juRwDzAUFBAk=
payment_network_token_transaction_type=1
payment_solution=001
```

Example 11  Authorization Reply (JCB)

```plaintext
auth_auth_amount=100.00
auth_auth_avs=X
auth_auth_code=888888
auth_auth_response=100
auth_avs_raw=I1
auth_rcode=1
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_trans_ref_no=15356268CR2XF23X
currency=USD
ics_rcode=1
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
merchant_ref_number=ref123
request_id=4697369268106124601541
request_token=Ahj/7wSR/UoVmibMmziHS2jMECT/h+KjMHSB04gwGA2dDjQoxQAAA6xdr
```
Chapter 3  Requesting the Authorization Service

Option 2: CyberSource Decryption

Visa Transaction

To request an authorization for a Visa transaction:

Step 1  Set the encrypted_payment_data field to the Base64-encoded value obtained from the paymentData property of the PKPaymentToken object. See “CyberSource Decryption,” page 10.

Step 2  Set the encrypted_payment_descriptor field to Rk1EPUNPTU1PTi5BUFBMRS5JTkFQUC5QQV1NRU5U

Step 3  Set the payment_solution field to 001.

Example 12  Authorization Request (Visa)

```plaintext
bill_address1=123 Main Street
bill_address2=Suite 12345
bill_city=Small Town
bill_country=US
bill_state=CA
bill_zip=98765
currency=USD
customer_email=js@example.com
customer_firstname=Jane
customer_lastname=Smith
card_type=001
encrypted_payment_data=eyJkYXRhW5FINWZqVjfkak1NdVNSaE96dWF2ZGVyb2c9PSJ9
encrypted_payment_descriptor=Rk1EPUNPTU1PTi5BUFBMRS5JTkFQUC5QQV1NRU5U
encrypted_payment_encoding=Base64
grand_total_amount=100.00
ics_applications=ics_auth
merchant_id=mid123
merchant_ref_number=ref123
payment_solution=001
```

Note  See the Relaxed Requirements for Address Data and Expiration Date page and “API Request Fields,” page 40, for details and field descriptions.
Chapter 3  Requesting the Authorization Service

Example 13  Authorization Reply (Visa)

```
auth_auth_amount=100.00
auth_auth_avs=X
auth_auth_code=888888
auth_auth_response=100
auth_avs_raw=I1
auth_rcode=1
auth_rflag=SOK
auth_rmsg=Request was processed successfully.
auth_trans_ref_no=35363393DQME5FP
currency=USD
ics_rcode=1
ics_rflag=SOK
ics_rmsg=Request was processed successfully.
merchant_ref_number=ref123
request_id=46973020687653080154
request_token=Ahj/7BT/w1nwRbsB04gwhQybdU2yMTRCrwJyP6kJUeh0S27iQAAA/wTV
token_expiration_month=07
token_expiration_year=2025
token_prefix=411111
token_suffix=1111
```

**Mastercard Transaction**

To request an authorization for a Mastercard transaction:

- **Step 1** Set the `encrypted_payment_data` field to the Base64-encoded value obtained from the `paymentData` property of the `PKPaymentToken` object. See "CyberSource Decryption," page 10.

- **Step 2** Set the `encrypted_payment_descriptor` field to `Rk1EPUNPTU1PTi5BFMBR5JTkFQUC5QV1NRU5U`.

- **Step 3** Set the `payment_solution` field to 001.

Note: See the Relaxed Requirements for Address Data and Expiration Date page and "API Request Fields," page 40, for details and field descriptions.
Chapter 3  Requesting the Authorization Service

Example 14  Authorization Request (Mastercard)

```
bbill_address1=123 Main Street
bill_address2=Suite 12345
bill_city=Small Town
bill_country=US
bill_state=CA
bill_zip=98765
card_type=002
currency=USD
customer_email=js@example.com
customer_firstname=Jane
customer_lastname=Smith
encrypted_payment_data=eyJkYXRhV5FINW2qVjfkak1NdVNSaE96dWF2ZGVyb2c9PSJ9
encrypted_payment_descriptor=RklEPUNPTU1PTi5BUFBMRS5JTkFQUC5QQVlNRU5U
encrypted_payment_encoding=Base64
grand_total_amount=100.00
ics_applications=ics_auth
merchant_id=mid123
merchant_ref_number=ref123
payment_solution=001
```

Example 15  Authorization Reply (Mastercard)

```
request_token=Ahj/7wSR5C/p6oJEy1gKIkGLNkwsMrW8HlU5tGHST/hHzdACT/hVB3c
currency=USD
request_id=4465838340055000001541
auth_rflag=SOK
ics_rmsg=Request was processed successfully.
auth_auth_amount=100.00
auth_rcode=1
auth_trans_ref_no=13209255CGJSMQCR
auth_auth_code=888888
auth_rmsg=Request was processed successfully.
ics_rflag=SOK
auth_auth_response=100
auth_avs_raw=11
auth_auth_time=2015-11-03T205035Z
merchant_ref_number=ref123
ics_rcode=1
token_prefix=128945
token_suffix=2398
token_expirationMonth=08
token_expirationYear=2021
```
American Express Transaction

To request an authorization for an American Express transaction:

**Step 1** Set the `encrypted_payment_data` field to the Base64-encoded value obtained from the `paymentData` property of the `PKPaymentToken` object. See "CyberSource Decryption," page 10.

**Step 2** Set the `encrypted_payment_descriptor` field to
Rk1EPUNPTU1PTi5BUFBMRS5JTkFQUC5QQV1NRU5U

**Step 3** Set the `payment_solution` field to 001.

Example 16 Authorization Request (American Express)

```
bill_address1=123 Main Street
bill_address2=Suite 12345
bill_city=Small Town
bill_country=US
bill_state=CA
bill_zip=98765
card_type=003
currency=USD
customer_email=js@example.com
customer_firstname=Jane
customer_lastname=Smith
encrypted_payment_data=eyJkYXRhW5FINWZqVjfkak1NdVNSaE96dWF2ZGVyb2c9PSJ9
encrypted_payment_descriptor=Rk1EPUNPTU1PTi5BUFBMRS5JTkFQUC5QQV1NRU5U
encrypted_payment_encoding=Base64
grand_total_amount=100.00
ics_applications=ics_auth
merchant_id=mid123
merchant_ref_number=ref123
payment_solution=001
```
### Example 17  Authorization Reply (American Express)

```plaintext
request_token=Ahj/7wSR5C/wGXKw1xAKIkGLNkwsmraHH1U5tGHaT/hHgzecDT/h6BBL
currency=USD
request_id=4465839210285000001541
auth_rflag=SOK
ics_rmsg=Request was processed successfully.
auth_auth_amount=100.00
auth_rcode=1
auth_trans_ref_no=13209256CGJSMQCZ
auth_auth_code=888888
auth_rmsg=Request was processed successfully.
ics_rflag=SOK
auth_auth_response=100
auth_avs_raw=I1
auth_auth_time=2015-11-03T205202Z
merchant_ref_number=ref123
ics_rcode=1
token_prefix=593056
token_suffix=0842
token_expirationMonth=08
token_expirationYear=2021
```
Discover Transaction

To request an authorization for a Discover transaction:

**Step 1** Set the `encrypted_payment_data` field to the Base64-encoded value obtained from the `paymentData` property of the `PKPaymentToken` object. See "CyberSource Decryption," page 10.

**Step 2** Set the `encrypted_payment_descriptor` field to `Rk1EPUNPTU1PTi5BUFBMRS5JTkFQUC5QQV1NRU5U`.

**Step 3** Set the `payment_network_token_transaction_type` field to 1.

**Step 4** Set the `payment_solution` field to 001.

**Example 18 Authorization Request (Discover)**

```
bill_address1=123 Main Street
bill_address2=Suite 12345
bill_city=Small Town
bill_country=US
bill_state=CA
bill_zip=98765
card_type=004
currency=USD
customer_email=js@example.com
customer_firstname=Jane
customer_lastname=Smith
encrypted_payment_data=eyJkYXRhW5FINWZqVjfkak1NdVNSaE96dWF2ZGVyb2c9PSJ9
encrypted_payment_descriptor=RRk1EPUNPTU1PTi5BUFBMRS5JTkFQUC5QQV1NRU5U
encrypted_payment_encoding=Base64
grand_total_amount=100.00
ics_applications=ics_auth
merchant_id=mid123
merchant_ref_number=ref123
payment_network_token_transaction_type=1
payment_solution=001
```
Example 19  Authorization Reply (Discover)

```
request_token=Ahj/7wSR5C/wGKw1xAKiGLNkwcsmraHH1U5tgH4aT/hHgZcDT/h6BBL
currency=USD
request_id=4465839210285000001541
auth_rflag=SOK
ics_rmsg=Request was processed successfully.
auth_auth_amount=100.00
auth_rcode=1
auth_trans_ref_no=13209256CGJSMQClZ
auth_auth_code=888888
auth_rmsg=Request was processed successfully.
ics_rflag=SOK
auth_auth_response=100
auth_avs_raw=II
auth_auth_time=2015-11-03T205202Z
merchant_ref_number=ref123
ics_rcode=1
token_prefix=601111
token_suffix=1117
token_expirationMonth=08
token_expirationYear=2021
```

**JCB Transaction**

To request an authorization for a JCB transaction:

---

**Note**

See the [Relaxed Requirements for Address Data and Expiration Date](#) page and "API Request Fields," page 40, for details and field descriptions.

---

**Step 1** Set the `encrypted_payment_data` field to the Base64-encoded value obtained from the `paymentData` property of the `PKPaymentToken` object.

**Step 2** Set the `encrypted_payment_decryptor` field to `Rk1EPUNPTU1PTi5BUFBMRS5JTkFQUC5QQV1NRU5U`.

**Step 3** Set the `payment_solution` field to `001`.
Example 20  Authorization Request (JCB)

```
bill_address1=123 Main Street
bill_address2=Suite 12345
bill_city=Small Town
bill_country=US
bill_state=CA
bill_zip=98765
card_type=007
currency=USD
customer_cc_expmo=12
customer_cc_expyr=2031
customer_cc_number=555555555555xxxx
customer_email=js@example.com
customer_firstname=Jane
customer_lastname=Smith
customer_phone=999-999-9999
eci_raw=05
grand_total_amount=100.00
ics_applications=ics_auth
merchant_id=med123
cavv=EHuWW9PiKuwq5juRwDzAUFBAk=
payment_network_token_transaction_type=1
payment_solution=001
```

Example 21  Authorization Reply (JCB)

```
request_token=Ahj/?wSR5C/p6oJExIgKIkGLNkwcsmrWHH1U5tGHST/hHgzdACT/hVB3c
currency=USD
request_id=4465838340055000001541
auth_rflag=SOK
ics_rmsg=Request was processed successfully.
auth_auth_amount=100.00
auth_rcode=1
auth_trans_ref_no=13209255CGJSMQCR
auth_auth_code=888888
auth_rmsg=Request was processed successfully.
ics_rflag=SOK
auth_auth_response=100
auth_avs_raw=I1
auth_auth_time=2015-11-03T205035Z
merchant_ref_number=ref123
ics_rcode=1
token_prefix=128945
token_suffix=2398
token_expirationMonth=08
token_expirationYear=2021
```
Additional CyberSource Services

Refer to the *Credit Card Services Using the SCMP API* for information on how to request these follow-on services.

**Table 2 CyberSource Services**

<table>
<thead>
<tr>
<th>CyberSource Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture</td>
<td>A follow-on service that uses the request ID returned from the previous authorization. The request ID links the capture to the authorization. This service transfers funds from the customer’s account to your bank and usually takes two to four days to complete.</td>
</tr>
<tr>
<td>Sale</td>
<td>A sale is a bundled authorization and capture. Request the authorization and capture services at the same time. CyberSource processes the capture immediately.</td>
</tr>
<tr>
<td>Auth Reversal</td>
<td>A follow-on service that uses the request ID returned from the previous authorization. An auth reversal releases the hold that the authorization placed on the customer’s credit card funds. Use this service to reverse an unnecessary or undesired authorization.</td>
</tr>
</tbody>
</table>
Data Type Definitions

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and time</td>
<td>Format is YYYY-MM-DDThhmmssZ, where:</td>
</tr>
<tr>
<td></td>
<td>T separates the date and the time.</td>
</tr>
<tr>
<td>Decimal</td>
<td>Number that includes a decimal point</td>
</tr>
<tr>
<td></td>
<td>Examples: 23.45, -0.1, 4.0, 90809.0468</td>
</tr>
<tr>
<td>Integer</td>
<td>Whole number {..., -3, -2, -1, 0, 1, 2, 3, ...}</td>
</tr>
<tr>
<td>Nonnegative integer</td>
<td>Whole number greater than or equal to zero {0, 1, 2, 3, ...}</td>
</tr>
<tr>
<td>Positive integer</td>
<td>Whole number greater than zero {1, 2, 3, ...}</td>
</tr>
<tr>
<td>String</td>
<td>Sequence of letters, numbers, spaces, and special characters</td>
</tr>
</tbody>
</table>

Relaxed Requirements for Address Data and Expiration Date

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

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

### Table 3 Request Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type (Length)</th>
</tr>
</thead>
<tbody>
<tr>
<td>bill_address1</td>
<td>First line of the billing street address.</td>
<td>ics_auth (R)²</td>
<td>CyberSource through VisaNet: String (40) All other processors: String (60)</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> It is your responsibility to determine whether a field is required for the transaction you are requesting.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bill_address2</td>
<td>Additional address information.</td>
<td>ics_auth (O)</td>
<td>CyberSource through VisaNet: String (40) All other processors: String (60)</td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong> Attention: Accounts Payable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bill_city</td>
<td>City of the billing address.</td>
<td>ics_auth (R)²</td>
<td>String (50)</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> It is your responsibility to determine whether a field is required for the transaction you are requesting.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bill_country</td>
<td>Country of the billing address. Use the two-character ISO Standard Country Codes.</td>
<td>ics_auth (R)²</td>
<td>String (2)</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> It is your responsibility to determine whether a field is required for the transaction you are requesting.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

2. This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See “Relaxed Requirements for Address Data and Expiration Date,” page 39. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 3 Request Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type (Length)</th>
</tr>
</thead>
<tbody>
<tr>
<td>bill_state</td>
<td>State or province of the billing address. For an address in the U.S. or Canada, use the <em>State, Province, and Territory Codes for the United States and Canada</em>.</td>
<td>ics_auth (R)²</td>
<td>String (2)</td>
</tr>
</tbody>
</table>

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

| bill_zip | Postal code for the billing address. The postal code must consist of 5 to 9 digits. When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits]  
*Example* 12345-6789  
When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric]  
*Example* A1B 2C3 | ics_auth (R)² | CyberSource through VisaNet:  
String (9)  
All other processors:  
String (10) |

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

| card_type | Type of card to authorize. Possible values:  
- 001: Visa  
- 002: Mastercard  
- 003: American Express  
- 004: Discover | ics_auth (O) | String (3) |

---

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

2. This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See “Relaxed Requirements for Address Data and Expiration Date,” page 39. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 3 Request Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type (Length)</th>
</tr>
</thead>
<tbody>
<tr>
<td>cavv</td>
<td>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.</td>
<td>ics_auth (R)</td>
<td>String (40)</td>
</tr>
<tr>
<td></td>
<td><strong>American Express</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>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 (see <strong>American Express Transaction,</strong> page 25). The value for this field must be 28-character base64 or 40-character hex binary. All cryptograms use one of these formats.</td>
<td>ics_auth (R)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Discover</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cryptogram for payment network tokenization transactions. The value for this field can be a 20 or 40-character hex binary. All cryptograms use one of these formats.</td>
<td>ics_auth (R)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>CyberSource through VisaNet</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The value for this field corresponds to the following data in the TC 33 capture file:</td>
<td>ics_auth (R)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Record: CP01 TCR8</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Position: 77-78</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Field: CAVV version and authentication action.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>currency</td>
<td>Currency used for the order: USD</td>
<td>ics_auth (R)</td>
<td>String (5)</td>
</tr>
</tbody>
</table>
| customer_cc_expmo | Two-digit month in which the payment network token expires.  
Format: MM.  
Possible values: 01 through 12. | ics_auth (R)                          | String (2)         |
| customer_cc_expyr | Four-digit year in which the payment network token expires.  
Format: YYYY. | ics_auth (R)                          | Nonnegative integer (4) |
| customer_cc_number | The payment network token value.                                           | ics_auth (R)                          | Nonnegative integer (20) |

---

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

2 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 39. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 3  Request Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type (Length)</th>
</tr>
</thead>
<tbody>
<tr>
<td>customer_email</td>
<td>Customer’s email address.</td>
<td>ics_auth (R)^2</td>
<td>String (255)</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> It is your responsibility to determine whether a field is required for the transaction you are requesting.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>customer_firstname</td>
<td>Customer’s first name. For a credit card transaction, this name must match the name on the card.</td>
<td>ics_auth (R)^2</td>
<td>String (60)</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> It is your responsibility to determine whether a field is required for the transaction you are requesting.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>customer_lastname</td>
<td>Customer’s last name. For a credit card transaction, this name must match the name on the card.</td>
<td>ics_auth (R)^2</td>
<td>String (60)</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> It is your responsibility to determine whether a field is required for the transaction you are requesting.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>customer_phone</td>
<td>Customer’s phone number. CyberSource recommends that you include the country code when the order is from outside the U.S.</td>
<td>ics_auth (O)</td>
<td>String (15)</td>
</tr>
<tr>
<td>e_commerce_indicator</td>
<td>For a payment network tokenization transaction. The values are required for the merchant decryption method (see &quot;Option 1: Merchant Decryption,&quot; page 21). Possible values:</td>
<td>ics_auth (See description)</td>
<td>String (20)</td>
</tr>
<tr>
<td></td>
<td>■ aesk: American Express card type</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ spa: Mastercard card type</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ internet: Visa card type</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ dipb: Discover card type</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong> For Visa in-app transactions, the internet value is mapped to the Visa ECI value 7.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eci_raw</td>
<td>Raw electronic commerce indicator (ECI).</td>
<td>ics_auth</td>
<td>String (2)</td>
</tr>
</tbody>
</table>

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

2 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 39. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 3  Request Fields  (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type (Length)</th>
</tr>
</thead>
<tbody>
<tr>
<td>encrypted_payment_data</td>
<td>The encrypted payment data value. Populates this field with the encrypted payment data obtained from the paymentData field of the PKPaymentToken structure. See the PassKit Framework Reference.</td>
<td>ics_auth (R)</td>
<td>String (3072)</td>
</tr>
<tr>
<td>encrypted_payment_descriptor</td>
<td>Format of the encrypted payment data. The value for Apple Pay is: Rk1EPUNPTU1PTi5BUFBMRS5JTkFQUC5QQV1NR5U</td>
<td>ics_auth (R)</td>
<td>String (128)</td>
</tr>
<tr>
<td>encrypted_payment_encoding</td>
<td>Encoding method used to encrypt the payment data: Base64</td>
<td>ics_auth (R)</td>
<td>String (6)</td>
</tr>
<tr>
<td>grand_total_amount</td>
<td>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.</td>
<td>ics_auth (R)</td>
<td>Decimal (60)</td>
</tr>
<tr>
<td>ics_applications</td>
<td>CyberSource service to process for the request: ics_auth</td>
<td>ics_auth (R)</td>
<td>String (255)</td>
</tr>
<tr>
<td>merchant_id</td>
<td>Your CyberSource merchant ID. Use the same merchant ID for evaluation, testing, and production.</td>
<td>ics_auth (R)</td>
<td>String (30)</td>
</tr>
<tr>
<td>merchant_ref_number</td>
<td>Merchant-generated order reference or tracking number. CyberSource recommends that you send a unique value for each transaction so that you can perform meaningful searches for the transaction. For information about tracking orders, see Getting Started with CyberSource Advanced for the SCMP API.</td>
<td>ics_auth (R)</td>
<td>String (50)</td>
</tr>
<tr>
<td>payment_network_token_assurance_level</td>
<td>Confidence level of the transaction. This value is assigned by the token service provider.</td>
<td>ics_auth (O)</td>
<td>String (2)</td>
</tr>
</tbody>
</table>

**Note** This field is supported only for CyberSource through VisaNet and FDC Nashville Global.

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

2. This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 39. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 3 Request Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type (Length)</th>
</tr>
</thead>
<tbody>
<tr>
<td>payment_network_token_device_tech_type</td>
<td>Type of technology used in the device to store token data. Possible value:</td>
<td>ics_auth (O)</td>
<td>Integer (3)</td>
</tr>
<tr>
<td></td>
<td>001: Secure Element (SE)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Smart card or memory with restricted access and encryption to prevent data tampering. For storing payment credentials, a SE is tested against a set of requirements defined by the payment networks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This field is supported only for FDC Compass.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>payment_network_token_requestor_id</td>
<td>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.</td>
<td>ics_auth (O)</td>
<td>Integer (1)</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This field is supported only for CyberSource through VisaNet, FDC Nashville Global, and Chase Paymentech Solutions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>payment_network_token_transaction_type</td>
<td>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. An application on the customer’s mobile device provided the token data.</td>
<td>ics_auth (R)</td>
<td>String (1)</td>
</tr>
<tr>
<td>payment_solution</td>
<td>Identifies Apple Pay as the payment solution that is being used for the transaction: Set the value for this field to 001.</td>
<td>ics_auth (R)</td>
<td>String (3)</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This unique ID differentiates digital solution transactions within the CyberSource platform for reporting purposes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ucaf_authentication_data</td>
<td>Cryptogram for payment network tokenization transactions with Mastercard.</td>
<td>ics_auth (R)</td>
<td>String (32)</td>
</tr>
<tr>
<td>ucaf_collection_indicator</td>
<td>Required field for payment network tokenization transactions with Mastercard. Set the value for this field to 2.</td>
<td>ics_auth (R)</td>
<td>String with numbers only (1)</td>
</tr>
</tbody>
</table>

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

2 This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 39. **Important** It is your responsibility to determine whether a field is required for the transaction you are requesting.
### Table 3  Request Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type (Length)</th>
</tr>
</thead>
<tbody>
<tr>
<td>xid</td>
<td>Visa</td>
<td>ics_auth (R)</td>
<td>String (40)</td>
</tr>
<tr>
<td></td>
<td>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 (see &quot;American Express Transaction,&quot; page 25). The value for this field must be 28-character base64 or 40-character hex binary. All cryptograms use one of these formats.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

2. This field is optional if your CyberSource account is configured for relaxed requirements for address data and expiration date. See "Relaxed Requirements for Address Data and Expiration Date," page 39. Important It is your responsibility to determine whether a field is required for the transaction you are requesting.

---

## Offer-Level Fields

### Table 4  Offer-Level Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By: Required (R) or Optional (O)</th>
<th>Data Type (Length)</th>
</tr>
</thead>
<tbody>
<tr>
<td>amount</td>
<td>Per-item price of the product. This value cannot be negative. You can include a decimal point (.), but you cannot include any other special characters.</td>
<td>ics_auth (See description)</td>
<td>Decimal (15)</td>
</tr>
<tr>
<td>merchant_product_sku</td>
<td>Identification code for the product. This field is required when the <strong>product_code</strong> value is not <strong>default</strong> or one of the values related to shipping and/or handling.</td>
<td>ics_auth (See description)</td>
<td>String (255)</td>
</tr>
<tr>
<td>product_code</td>
<td>Type of product. This value is used to determine the product category: electronic, handling, physical, service, or shipping. The default is <strong>default</strong>.</td>
<td>ics_auth (See description)</td>
<td>String (255)</td>
</tr>
<tr>
<td>product_name</td>
<td>Name of the product. This field is required when the <strong>product_code</strong> value is not <strong>default</strong> or one of the values related to shipping and/or handling.</td>
<td>ics_auth (See description)</td>
<td>String (255)</td>
</tr>
</tbody>
</table>
### Appendix A  SCMP API Fields

#### Table 4  Offer-Level Fields  (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Used By:</th>
<th>Data Type (Length)</th>
</tr>
</thead>
<tbody>
<tr>
<td>quantity</td>
<td>The default is 1. This field is required when the product_code value is not default or one of the values related to shipping and/or handling.</td>
<td>ics_auth (See description)</td>
<td>Integer (10)</td>
</tr>
<tr>
<td>tax_amount</td>
<td>Total tax to apply to the product. This value cannot be negative.</td>
<td>ics_auth (See description)</td>
<td>String (15)</td>
</tr>
</tbody>
</table>

#### API Reply Fields

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

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

#### Table 5  Reply Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Returned By</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth_auth_amount</td>
<td>Amount that was authorized.</td>
<td>ics_auth</td>
<td>Decimal (15)</td>
</tr>
<tr>
<td>auth_auth_avs</td>
<td>AVS result code. See <em>Credit Card Services Using the SCMP API</em> for a detailed list of AVS values.</td>
<td>ics_auth</td>
<td>String (1)</td>
</tr>
<tr>
<td>auth_auth_code</td>
<td>Authorization code. Returned only when the processor returns this value.</td>
<td>ics_auth</td>
<td>String (7)</td>
</tr>
<tr>
<td>auth_auth_response</td>
<td>For most processors, this value is the error message sent directly from the bank. Returned only when the processor returns this value.</td>
<td>ics_auth</td>
<td>String (10)</td>
</tr>
</tbody>
</table>

¹ The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.
Table 5  Reply Fields  (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Returned By</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth_avs_raw</td>
<td>AVS result code sent directly from the processor. Returned only when the processor returns this value.</td>
<td>ics_auth</td>
<td>String (10)</td>
</tr>
<tr>
<td>auth_payment_card_service</td>
<td>Mastercard service that was used for the transaction. Mastercard provides this value to CyberSource. Possible value: 53: Mastercard card-on-file token service This field is returned only for CyberSource through VisaNet.</td>
<td>ics_auth</td>
<td>String (2)</td>
</tr>
</tbody>
</table>

*CyberSource through VisaNet*

The value for this field corresponds to the following data in the TC 33 capture file:\footnote{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.}

- Record: CP01 TCR6
- Position: 133-134

Field: Mastercard Merchant on-behalf service.

*Note*  This field is returned only for CyberSource through VisaNet.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Returned By</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
</table>
| auth_payment_card_service_result | Result of the Mastercard card-on-file token service. Mastercard provides this value to CyberSource. Possible values:  
- **C**: Service completed successfully.  
- **F**: One of the following:  
  - Incorrect Mastercard POS entry mode. The Mastercard POS entry mode should be 81 for an authorization or authorization reversal.  
  - Incorrect Mastercard POS entry mode. The Mastercard POS entry mode should be 01 for a tokenized request.  
  - Token requestor ID is missing or formatted incorrectly.  
- **I**: One of the following:  
  - Invalid token requestor ID.  
  - Suspended or deactivated token.  
  - Invalid token (not in mapping table).  
- **T**: Invalid combination of token requestor ID and token.  
- **U**: Expired token.  
- **W**: Primary account number (PAN) listed in electronic warning bulletin. This field is returned only for CyberSource through VisaNet.  |
| ics_auth | Indicates whether the service request was successful. Possible values:  
- **-1**: An error occurred.  
- **0**: The request was declined.  
- **1**: The request was successful.  |

**Note** This field is returned only for CyberSource through VisaNet.

---

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.
### Table 5  Reply Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Returned By</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth_reversal_payment_card_service</td>
<td>Mastercard service that was used for the transaction. Mastercard provides this value to CyberSource. Possible value:  53: Mastercard card-on-file token service This field is returned only for CyberSource through VisaNet. <strong>CyberSource through VisaNet</strong>  The value for this field corresponds to the following data in the TC 33 capture file¹:  - Record: CP01 TCR6  - Position: 133-134  Field: Mastercard Merchant on-behalf service. <strong>Note</strong> This field is returned only for CyberSource through VisaNet.</td>
<td>ics_auth_reversal</td>
<td>String (2)</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Returned By</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
</table>
| auth_reversal_payment_card_service_result | Result of the Mastercard card-on-file token service. Mastercard provides this value to CyberSource. Possible values:  
- C: Service completed successfully.  
- F: One of the following:  
  - Incorrect Mastercard POS entry mode. The Mastercard POS entry mode should be 81 for an authorization or authorization reversal.  
  - Incorrect Mastercard POS entry mode. The Mastercard POS entry mode should be 01 for a tokenized request.  
  - Token requestor ID is missing or formatted incorrectly.  
- I: One of the following:  
  - Invalid token requestor ID.  
  - Suspended or deactivated token.  
  - Invalid token (not in mapping table).  
- T: Invalid combination of token requestor ID and token.  
- U: Expired token.  
- W: Primary account number (PAN) listed in electronic warning bulletin. This field is returned only for CyberSource through VisaNet. |
|                                           |                                                                              | ics_auth_reversal | String (1)        |
| auth_rflag                                | One-word description of the result of the entire request. See Credit Card Services Using the SCMP API for a detailed list of rflag values.  
|                                           |                                                                              | ics_auth      | String (50)       |
| auth_rmsg                                 | Message that explains the reply flag auth_rflag. Do not display this message to the customer, and do not use this field to write an error handler.  
|                                           |                                                                              | ics_auth      | String (255)      |
| auth_trans_ref_no                         | Reference number for the transaction.  
This value is not returned for all processors.  
|                                           |                                                                              | ics_auth      | String (60)       |

Note This field is returned only for CyberSource through VisaNet.

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.
### SCMP API Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Returned By</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
</table>
| auth_transaction_qualification | Type of authentication for which the transaction qualifies as determined by the Mastercard authentication service, which confirms the identity of the cardholder. Mastercard provides this value to CyberSource. Possible values:  
  - 1: Transaction qualifies for Mastercard authentication type 1.  
  This field is returned only for CyberSource through VisaNet.  
  **CyberSource through VisaNet**  
  The value for this field corresponds to the following data in the TC 33 capture file¹:  
  - Record: CP01 TCR6  
  - Position: 132  
  Field: Mastercard Member Defined service.  
  **Note** This field is returned only for CyberSource through VisaNet. | ics_auth | String (1) |
| 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 file¹:  
  - Record: CP01 TCRB  
  - Position: 85  
  Field: American Express last 4 PAN return indicator. | ics_auth | String (4) |
| currency                      | Currency used for the order. For the possible values, see the ISO Standard Currency Codes. | ics_auth | String (5) |

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.
### SCMP API Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Returned By</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
</table>
| ics_rcode | Indicates whether the service request was successful. Possible values:  
- -1: An error occurred.  
- 0: The request was declined.  
- 1: The request was successful. | ics_auth | Integer (1) |
| ics_rflag | One-word description of the result of the entire request. See *Credit Card Services Using the SCMP API* for a detailed list of rflag values. | ics_auth | String (50) |
| ics_rmsg | Message that explains the reply flag ics_rflag. Do not display this message to the customer, and do not use this field to write an error handler. | ics_auth | String (255) |
| merchant_ref_number | Order reference or tracking number that you provided in the request. If you included multi-byte characters in this field in the request, the returned value might include corrupted characters. | ics_auth | String (50) |
| payment_network_token_account_status | Possible values:  
- N: Nonregulated  
- R: Regulated  
This field is returned only for CyberSource through VisaNet.  
**Note** This field is returned only for CyberSource through VisaNet. | ics_auth | String (1) |
| payment_network_token_assurance_level | 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 CyberSource through VisaNet and FDC Nashville Global. | ics_auth | String (2) |
| payment_network_token_original_card_category | Mastercard product ID associated with the primary account number (PAN). For the possible values, see "MasterCard Product IDs" in *Credit Card Services Using the SCMP API*. For the possible values, see "Mastercard Product IDs" in *Credit Card Services for CyberSource through VisaNet Using the SCMP API*.  
**Note** This field is returned only for Mastercard transactions on CyberSource through VisaNet on CyberSource through VisaNet. | ics_auth | String (3) |

---

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant's acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.
### Table 5  Reply Fields  (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Returned By</th>
<th>Data Type &amp; Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>payment_network_token_requestor_id</td>
<td>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. <strong>Note</strong> This field is supported only for CyberSource through VisaNet and FDC Nashville Global. <strong>Note</strong> This field is returned only for CyberSource through VisaNet. and CyberSource through VisaNet and FDC Nashville Global.</td>
<td>ics_auth</td>
<td>Integer (11)</td>
</tr>
<tr>
<td>request_id</td>
<td>Identifier for the request.</td>
<td>ics_auth</td>
<td>String (26)</td>
</tr>
<tr>
<td>request_token</td>
<td>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.</td>
<td>ics_auth</td>
<td>String (256)</td>
</tr>
<tr>
<td>token_expiration_month</td>
<td>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.</td>
<td>ics_auth</td>
<td>String (2)</td>
</tr>
<tr>
<td>token_expiration_year</td>
<td>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.</td>
<td>ics_auth</td>
<td>String (4)</td>
</tr>
<tr>
<td>token_prefix</td>
<td>First 6 digits of token. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction.</td>
<td>ics_auth</td>
<td>String (6)</td>
</tr>
<tr>
<td>token_suffix</td>
<td>Last 4 digits of token. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction.</td>
<td>ics_auth</td>
<td>String (4)</td>
</tr>
</tbody>
</table>

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.