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 Unpublished rights reserved under the copyright laws of the United States.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

Authorize.Net, eCheck.Net, and The Power of Payment are registered trademarks of CyberSource Corporation. 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
  - Notes and Important Statements 7
  - Text and Command Conventions 8
- Related Documents 8
- Customer Support 8

---

### Chapter 1  Introduction 9
- Requirements 9
- Supported Processors, Card Types, and Optional Features 10
- Transaction Endpoints 12

---

### Chapter 2  Registration 13
- Registering with Samsung 13
- Registering with CyberSource 14

---

### Chapter 3  Integrating the Samsung SDK 16
- Creating a Project 16
- Integrating the Samsung Pay SDK 17
- Using the API Key 17
Chapter 4  Using the Samsung Pay SDK  18
   Eligibility  18
   Payment Request  19
      Initiating a Payment  19
      Requesting a Payment  21

Chapter 5  Authorizing a Payment  23
   Merchant Decryption  23
      Visa Transaction  23
      Mastercard Transaction  25
      American Express Transaction  27
      JCB Transaction  29
   CyberSource Decryption  32
      Visa Transaction  32
      Mastercard Transaction  34
      American Express Transaction  37
      JCB Transaction  40
   Additional CyberSource Services  43

Appendix A  API Fields  44
   Data Type Definitions  44
   Numbered Elements  44
   Relaxed Requirements for Address Data  45
   API Request Fields  46
   API Reply Fields  54
**Recent Revisions to This Document**

<table>
<thead>
<tr>
<th>Release</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 2019</td>
<td>Changed the name of <em>Mastercard SecureCode</em> to <em>Mastercard Identity Check</em>.</td>
</tr>
</tbody>
</table>
| May 2019 | Removed the following request fields that were erroneously added in the April 2019 release:  
- `ccSaleService_directoryServerTransactionID`  
- `ccSaleService_networkTokenCryptogram`  
- `ccSaleService_paSpecificationVersion`  
  Removed the following reply fields that were erroneously added in the April 2019 release:  
- `payerAuthEnrollReply_directoryServerTransactionID`  
- `payerAuthValidateReply_directoryServerTransactionID` |
<table>
<thead>
<tr>
<th>Release</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2019</td>
<td>Added support for tokenized transactions using a network token with 3D Secure or Identity Check. See &quot;Merchant Decryption,&quot; page 23.</td>
</tr>
<tr>
<td></td>
<td>Added the following request fields that support tokenized transactions using a network token with 3D Secure or Identity Check (see &quot;API Request Fields,&quot; page 46):</td>
</tr>
<tr>
<td></td>
<td>■ ccAuthService_directoryServerTransactionID</td>
</tr>
<tr>
<td></td>
<td>■ ccAuthService_networkTokenCryptogram</td>
</tr>
<tr>
<td></td>
<td>■ ccAuthService_paSpecificationVersion</td>
</tr>
<tr>
<td></td>
<td>■ ccSaleService_directoryServerTransactionID</td>
</tr>
<tr>
<td></td>
<td>■ ccSaleService_networkTokenCryptogram</td>
</tr>
<tr>
<td></td>
<td>■ ccSaleService_paSpecificationVersion</td>
</tr>
<tr>
<td></td>
<td>Added the following reply fields that support tokenized transactions using a network token with 3D Secure or Identity Check (see &quot;API Reply Fields,&quot; page 54):</td>
</tr>
<tr>
<td></td>
<td>■ payerAuthEnrollReply_directoryServerTransactionID</td>
</tr>
<tr>
<td></td>
<td>■ payerAuthValidateReply_directoryServerTransactionID</td>
</tr>
<tr>
<td></td>
<td>Added support for the processor Elavon Americas. See &quot;Supported Processors, Card Types, and Optional Features,&quot; page 10.</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 10):</td>
</tr>
<tr>
<td></td>
<td>■ Merchant-Initiated transactions</td>
</tr>
<tr>
<td></td>
<td>■ Multiple partial captures</td>
</tr>
<tr>
<td></td>
<td>■ Recurring payments</td>
</tr>
<tr>
<td></td>
<td>fieldname, and payment descriptor.</td>
</tr>
<tr>
<td></td>
<td>Updated &quot;Supported Processors, Card Types, and Optional Features,&quot; page 10 to remove erroneous content regarding Vantiv.</td>
</tr>
<tr>
<td></td>
<td>Updated URLs for the following:</td>
</tr>
<tr>
<td></td>
<td>■ Samsung Pay Partner Portal (see &quot;Related Documents,&quot; page 8)</td>
</tr>
<tr>
<td></td>
<td>■ Transaction Endpoints (see &quot;Transaction Endpoints,&quot; page 12)</td>
</tr>
<tr>
<td></td>
<td>■ Samsung Pay registration (see &quot;Registering with Samsung,&quot; page 13)</td>
</tr>
<tr>
<td></td>
<td>■ Decrypting payment credentials (see &quot;Encrypted Payment Credential,&quot; page 22)</td>
</tr>
</tbody>
</table>
About This Guide

Audience and Purpose

This document is written for merchants who want to enable customers to use Samsung Pay to pay for in-app purchases. This document provides an overview of integrating the Samsung Pay SDK and describes how to request the CyberSource API to process an authorization.

This document describes the Samsung Pay SDK and the CyberSource API. See "Using the Samsung Pay SDK," page 18, and "Authorizing a Payment," page 23. Merchants must use the Samsung Pay SDK to receive the customer’s encrypted payment data before requesting the CyberSource API to process the transaction.

Conventions

Notes 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>
<tbody>
<tr>
<td>bold</td>
<td>Field and service names in text; for example: Include the <strong>card_accountNumber</strong> field.</td>
</tr>
<tr>
<td></td>
<td>Items that you are instructed to act upon; for example: Click <strong>Save</strong>.</td>
</tr>
<tr>
<td>Screen text</td>
<td>Code examples and samples.</td>
</tr>
</tbody>
</table>

Related Documents

CyberSource Documents:
- **Getting Started with CyberSource Advanced for the Simple Order API** (PDF | HTML)
- Simple Order API and SOAP Toolkit API Documentation and Downloads page
- **Credit Card Services Using the Simple Order API** (PDF | HTML)
- **Payment Network Tokenization Using the Simple Order API** (PDF | HTML)

Samsung Pay documents:
- Samsung Pay Partner Portal

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
Requirements

**Important**

ProductName relies on payment network tokenization. You can sign up for ProductName only if both of the following statements are true:

- Your processor supports payment network tokenization.
- CyberSource supports payment network tokenization 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 ProductName:

- Obtain a new merchant account with a processor that supports payment network tokenization.
- Wait until your processor supports payment network tokenization.

You must create:

- A CyberSource account. If you do not already have a CyberSource account, contact your local CyberSource sales representative:  
  http://www.cybersource.com/locations/
- A merchant account with a supported processor. See "Supported Processors, Card Types, and Optional Features," page 10.

All optional features are described in *Payment Network Tokenization Using the Simple Order API.*
## Supported Processors, Card Types, and Optional Features

All optional features, except split shipments, are described in *Payment Network Tokenization Using the Simple Order API* (PDF | HTML). Split shipments are described in *Credit Card Services Using the Simple Order API* (PDF | HTML).

<table>
<thead>
<tr>
<th>Processors</th>
<th>Card Types</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Express Direct</td>
<td>American Express</td>
<td>• Multiple partial captures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Recurring Payments</td>
</tr>
<tr>
<td>Barclays</td>
<td>Visa, Mastercard, JCB, Maestro (International), Maestro (UK Domestic)</td>
<td>• Multiple partial captures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Recurring Payments</td>
</tr>
<tr>
<td></td>
<td>If you support Maestro (UK Domestic), you must also support Maestro (International), and you must support Mastercard Identity Check for both card types.</td>
<td></td>
</tr>
<tr>
<td>Chase Paymentech Solutions</td>
<td>Visa, Mastercard, American Express, Discover, Diners Club, JCB, Carte Blanche, Maestro (International)</td>
<td>• Multiple partial captures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Recurring Payments</td>
</tr>
<tr>
<td>CyberSource through VisaNet.</td>
<td>Visa, Mastercard, American Express, Discover, JCB, Diners Club</td>
<td>• Split shipments.</td>
</tr>
<tr>
<td>The supported acquirer is:</td>
<td></td>
<td>• Recurring Payments</td>
</tr>
<tr>
<td>Vantiv</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CyberSource through VisaNet</td>
<td>is a single processor with multiple acquirers.</td>
<td></td>
</tr>
<tr>
<td>Elavon Americas</td>
<td>Visa, Mastercard, American Express, JCB, Diners Club, Discover, China UnionPay</td>
<td>• Merchant-Initiated transactions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Multiple partial captures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Recurring payments</td>
</tr>
<tr>
<td>FDC Compass</td>
<td>Visa, Mastercard, American Express, Discover, Diners Club, JCB</td>
<td>• Multiple partial captures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Recurring Payments</td>
</tr>
</tbody>
</table>
Table 1  Supported Processors, Card Types, and Optional Features (Continued)

<table>
<thead>
<tr>
<th>Processors</th>
<th>Card Types</th>
<th>Optional</th>
</tr>
</thead>
</table>
| FDC Nashville Global        | Visa, Mastercard, American Express, Discover, Diners Club, JCB, China UnionPay | • Multiple partial captures.  
                              |                                                | • Recurring Payments                        |
| GPN                         | Visa, Mastercard, American Express, Discover, Diners Club, JCB | • Split shipments  
                              |                                                | • Recurring Payments                        |
| JCN Gateway                 | Visa, Mastercard, American Express, Diners Club, JCB | Multiple partial captures                     |
| OmniPay Direct              | Visa, Mastercard, Discover, Diners Club, Maestro (UK Domestic), Maestro (International) | • Multiple partial captures  
                              |                                                | • Recurring Payments                        |
| Streamline                  | Visa, Mastercard                                  | • Multiple partial captures  
                              |                                                | • Recurring Payments                        |
| TSYS Acquiring Solutions    | Visa, Mastercard, American Express                | • Multiple partial captures  
                              |                                                | • Recurring Payments                        |
Transaction Endpoints

CAS (test transactions):
- Akamai endpoints:
  
  https://ics2wstesta.ic3.com/commerce/1.x/transactionProcessor

- Non-Akamai endpoints:
  
  https://ics2wstest.ic3.com/commerce/1.x/transactionProcessor

Production (live transactions):
- Akamai endpoints:

  https://ics2wsa.ic3.com/commerce/1.x/transactionProcessor

- Non-Akamai endpoints

  https://ics2ws.ic3.com/commerce/1.x/transactionProcessor
Registering with Samsung

To register with Samsung:

**Step 1** Create a profile by completing the merchant application on the Samsung Pay Partner Portal.

---

Note

Samsung will contact you if clarifications are required.

---

**Step 2** After your merchant application is approved, you receive a unique partner ID. Include this ID in your application.

---

Important

You need the partner ID in order to generate the Certificate Signing Request (CSR) file in using the CyberSource Business Center. See "Registering with CyberSource," page 14. Samsung requires the CSR file in order to encrypt sensitive payment data; it contains an identifier and public key.

---

**Step 3** Using the Samsung Pay Partner Portal, upload the CSR file.

**Step 4** Enter an application name and a package name.

**Step 5** When you associate the CSR file with the application, Samsung generates a product ID.

**Step 6** Create login details for application developers on the Samsung Pay Partner Portal.

**Step 7** Download and integrate the Samsung Pay SDK into your application. See "Using the Samsung Pay SDK," page 18.

The SDK contains:

- A Javadoc
- The Samsung Pay SDK files *samsungpay.jar* and *sdk-v1.0.0.jar*
- A sample app
- The branding guide
- Image files

**Step 8** Register a Samsung account ID and request a `debug-api-key` file using the Samsung Pay Partner Portal. The `debug-api-key` file is valid for three months. See "Using the API Key," page 17.

---

**Note**

The Samsung account ID, the `debug-api-key`, and the product ID are used to validate your application so that you can use the Samsung Pay SDK for testing purposes.

---

**Step 9** Submit your application for approval using the Samsung Pay Partner Portal. Upload the final version of the Android Application Package (APK) file using the Samsung Pay Partner Portal and include screenshots of your checkout page displaying the Samsung Pay logo.

---

## Registering with CyberSource

**To register with CyberSource:**

**Step 1** Log in to the Business Center:
- Create a CSR file for live transactions: [https://ebc.cybersource.com](https://ebc.cybersource.com)
- Create a CSR file for test transactions: [https://ebctest.cybersource.com](https://ebctest.cybersource.com)

**Step 2** Under Account Management in the left navigation panel, click Digital Payment Solutions.

**Step 3** Click **Sign Up**. Follow the steps to verify your account information and accept the ProductName Merchant Services Agreement.
Step 4 Register with CyberSource:

a Enter your Samsung partner ID that you obtained in Step 2.

b Click Generate CSR to generate a Certificate Signing Request (CSR) file that is associated with your Samsung partner ID.

Important

Only one CSR is permitted for each unique Samsung partner ID. If you modify your Samsung partner ID you must generate a new CSR.

c Submit the CSR file to Samsung.
Creating a Project

To create a new project using Android Studio:

**Step 1** Download Android Studio.

**Step 2** Open Android Studio and click **Start a new Android Studio project**.

**Step 3** In the New Project settings, enter the following:
- The name of your application.
- The company domain.
- To change the package name, click **Edit**. By default, Android Studio sets the last element of the project's package name to the name of your application.

**Step 4** Click **Next**.

**Step 5** In the Target Android Devices settings, choose the required API levels.

**Step 6** Click **Next**.

**Step 7** Choose the required activity and click **Finish**.
Integrating the Samsung Pay SDK

To integrate the Samsung Pay SDK:

**Step 1** Add the `samsungpay.jar` and `sdk-v1.0.0.jar` files to the `libs` folder of your Android project.

**Step 2** Choose **Gradle Scripts > build.gradle** and enter the dependencies shown below.

```java
dependencies {
    compile files('libs/samsungpay.jar')
    compile files('libs/sdk-v1.0.0.jar')
}
```

**Step 3** Import the package.

```java
import com.samsung.android.sdk.samsungpay;
```

Using the API Key

The API key is used to verify that your app (in debug mode or release mode) can use the Samsung Pay SDK APIs with the Samsung Pay application. To get the API key, you must create a `debug-api-key` file (Step 8) and include it in the `manifest` file.

To use the API key:

**Step 1** Include the API key in the `manifest` file with a custom tag. This enables the merchant app `android manifest` file to provide the `DebugMode`, `spay_debug_api_key` values as metadata.

**Example 1** Debug Mode

```xml
<meta-data
    android:name="debug_mode"
    android:value="Y" />
<meta-data
    android:name="spay_debug_api_key"
    android:value="asdfggkndkeie17283094858" />
```

**Example 2** Release Mode

```xml
<meta-data
    android:name="debug_mode"
    android:value="N" />
```
Eligibility

Initialize the SSamsungPay class to verify that your application is eligible for Samsung Pay and to display the Samsung Pay button to the customer (refer to branding guidelines).

The SSamsungPay class provides the following API methods:

- `initialize()` — initializes the Samsung Pay SDK and verifies eligibility for Samsung Pay, including the device, software, and business area.

  Request the `initialize()` API method of the SSamsungPay class before using the Samsung Pay SDK.

- `getVersionCode()` — retrieves the version number of the Samsung Pay SDK as an integer.

- `getVersionName()` — retrieves the version name of the Samsung Pay SDK as a string.

After the `initialize()` API method request is successful, display the Samsung Pay button to the customer.

If the `initialize()` API method request fails, the method displays a `SdkUnsupportedException` or `NullPointerException` error.

- `SdkUnsupportedException` — the device is not a Samsung device or does not support the Samsung Pay package.

- `NullPointerException` — the context passed is null.
Example 3  Samsung Pay Class

SSamsungPay spay = new SSamsungPay();
try {
    spay.initialize(mContext);
} catch (SsdkUnsupportedException e1) {
    e1.printStackTrace();
    pay_button.setVisibility(View.INVISIBLE);
}

Payment Request

Initiating a Payment

To initiate a payment:

Step 1  Include the following fields in the PaymentInfo class:

- Merchant Name—the merchant name as it appears on the payment sheet of Samsung Pay and customer’s bank statement. This field is required.
- Amount—this field is required.
- Payment Protocol—3D Secure. This field is required.
- Permitted Card Brands—specify the card brands that are supported such as Visa, Mastercard, or American Express. This field is required.
- Merchant ID
- Order Number
- Shipping Address—this field is required if SEND_SHIPPING or NEED_BILLING_AND_SEND_SHIPPING is set for AddressVisibilityOption.
- Address Visibility Option
- Card Holder Name
- Recurring Option

Important
If the required fields are not included, you receive a NullPointerException error.
Example 4  Transaction Request Structure

```java
private PaymentInfo makeTransactionDetails() {
    // Supported card brands
    ArrayList<CardInfo.Brand> brandList = new ArrayList<CardInfo.Brand>();
    if (visaBrand.isChecked())
        brandList.add(CardInfo.Brand.VISA);
    if (mcBrand.isChecked())
        brandList.add(CardInfo.Brand.Mastercard);
    if (amexBrand.isChecked())
        brandList.add(CardInfo.Brand.AMERICANEXPRESS);

    // Basic payment information
    PaymentInfo paymentReq = new PaymentInfo.Builder()
        .setMerchantId("merchantID")
        .setMerchantName("Test")
        .setAmount(getAmount())
        .setShippingAddress(getShippingAddressInfo())
        .setOrderNumber(orderNoView.getText().toString())
        .setPaymentProtocol(PaymentProtocol.PROTOCOL_3DS)
        .setAddressInPaymentSheet(AddressInPaymentSheet.DO_NOT_SHOW)
        .setAllowedCardBrands(brandList)
        .setRecurringEnabled(isRecurring)
        .setCardHolderNameEnabled(isCardHolderNameRequired)
        .build();
    return paymentReq;
}

// Add shipping address details
private Address getShippingAddressInfo() {
    Address address = new Address.Builder()
        .setAddressee(name.getText().toString())
        .setAddressLine1(addLine1.getText().toString())
        .setAddressLine2(addLine2.getText().toString())
        .setCity(city.getText().toString())
        .setState(state.getText().toString())
        .setCountryCode(country.getSelectedItem().toString())
        .setPostalCode(zip.getText().toString()).build();
    return address;
}

// Add amount details private Amount getAmount() {
    Amount amount = new Amount.Builder()
        .setCurrencyCode(currencyType.getSelectedItem().toString())
        .setItemTotalPrice(productPrice.getText().toString())
        .setShippingPrice(shippingPrice.getText().toString())
        .setTax(taxPrice.getText().toString())
        .setTotalPrice(totalAmount.getText().toString()).build();
    return amount;
}
```
## Requesting a Payment

**To request a payment:**

**Step 1** Use the `startSamsungPay()` API method in the `PaymentManager` class.

The `PaymentManager` class includes the following API methods:

- `startSamsungPay()` — requests to initiate payment with Samsung Pay.
- `updateAmount()` — updates the transaction amount if shipping address or card information is updated by Samsung Pay.
- `updateAmountFailed()` — returns an error code when the new amount cannot be updated because of a wrong address.

**Step 2** Request the `startSamsungPay()` API method and include the following data:

- `PaymentInfo` — the `paymentInfo` structure, which contains payment information.
- `StatusListener` — the result of the payment request is delivered to `StatusListener`. This listener should be registered before calling the `startSamsungPay()` API method.

When you request the `startSamsungPay()` API method, the Samsung Pay online payment sheet is displayed on the screen of your application. The customer selects a registered card for payment and can also update the billing and shipping address.

The payment reply is delivered as one of the following events to `StatusListener`:

- `onSuccess()` — this event is requested when Samsung Pay confirms the payment. It includes `encryptedPaymentCredential` in JSON format. See Table 2, "Encrypted Payment Credential," on page 22.
- `onFailure()` — this event is requested when the transaction fails. It returns an error code and error message.
Example 5 Request startSamsungPay() API Method

```java
public void onPayButtonClicked(View v) {
    // Call startSamsungPay() method of PaymentManager class.
    // To create a transaction request for makeTransactionDetails() in
    // the following code, see Example 4, "Transaction Request Structure,"
    // on page 20.
    try {
        mPaymentManager.startSamsungPay(makeTransactionDetails(), "enter
        product ID",
        mStatusListener);
    } catch (NullPointerException e) {
        e.printStackTrace();
    }
}

private PaymentManager.StatusListener mStatusListener = new
PaymentManager.StatusListener() {
    @Override
    public void onFailure(int errCode, String msg) {
        Log.d(TAG, " onFailed ");
    }
    @Override
    public void onSuccess(PaymentInfo arg0, String result) {
        Log.d(TAG, "onSuccess ");
    }
};
```

Table 2 Encrypted Payment Credential

<table>
<thead>
<tr>
<th>Payment Credential</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>method</td>
<td>Payment protocol: 3D Secure.</td>
</tr>
<tr>
<td>merchant_ref</td>
<td>Merchant reference code.</td>
</tr>
<tr>
<td>billing_address.street</td>
<td>Number, street name.</td>
</tr>
<tr>
<td>billing_address.state_province</td>
<td>Two letter state code.</td>
</tr>
<tr>
<td>billing_address.zip_postal_code</td>
<td>Five character zip code.</td>
</tr>
<tr>
<td>billing_address.city</td>
<td>City name.</td>
</tr>
<tr>
<td>billing_address.county</td>
<td>Two letter country code.</td>
</tr>
<tr>
<td>3ds.type</td>
<td>S for Samsung Pay.</td>
</tr>
<tr>
<td>3ds.version</td>
<td>Current version 100.</td>
</tr>
<tr>
<td>3ds.data</td>
<td>Base64 encoded payment data.</td>
</tr>
</tbody>
</table>

For information on how to decrypt the encrypted payment credential, see:

https://pay.samsung.com/developers
Authorizing a Payment

Merchant Decryption

Visa Transaction

To request an authorization for a Visa transaction:

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

**Step 2** Set the `card_expirationMonth` and `card_expirationYear` values to the payment network token expiration date fields.

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

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

**Step 5** Set the `paymentNetworkToken_transactionType` field to 1.

**Step 6** Set the `ccAuthService_commerceIndicator` field to `internet`.

**Step 7** Set the `paymentSolution` field to 008.

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

Note: See "API Request Fields," page 46, and "API Reply Fields," page 54, for detailed field descriptions.
Example 6  Merchant Decryption Authorization Request (Visa)

```xml
<requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.121">
  <merchantID>demomerchant</merchantID>
  <merchantReferenceCode>demorefnnum</merchantReferenceCode>
  <billTo>
    <firstName>James</firstName>
    <lastName>Smith</lastName>
    <street1>1295 Charleston Road</street1>
    <city>Test City</city>
    <state>CA</state>
    <postalCode>99999</postalCode>
    <country>US</country>
    <email>demo@example.com</email>
  </billTo>
  <purchaseTotals>
    <currency>USD</currency>
    <grandTotalAmount>5.00</grandTotalAmount>
  </purchaseTotals>
  <card>
    <accountNumber>xxxx1000000xxxx</accountNumber>
    <expirationMonth>12</expirationMonth>
    <expirationYear>2020</expirationYear>
  </card>
  <ccAuthService run="true">
    <cavv>ABCDEFabcdefABCDEFabcdef0987654321234567</cavv>
    <commerceIndicator>internet</commerceIndicator>
    <xid>1234567890987654321ABCDEFabcdefABCDEF123</xid>
  </ccAuthService>
  <paymentNetworkToken>
    <transactionType>1</transactionType>
  </paymentNetworkToken>
  <paymentSolution>008</paymentSolution>
</requestMessage>
```
Example 7    Merchant Decryption Authorization Reply (Visa)

```xml
<c:replyMessage>
  <c:requestID>4465840340765000001541</c:requestID>
  <c:decision>ACCEPT</c:decision>
  <c:requestToken>Ahj/7wSR5C/4Icd2fdAKakGLadfg5535r/ghx3Z90AoBj3u</c:requestToken>
  <c:purchaseTotals>
    <c:currency>USD</c:currency>
  </c:purchaseTotals>
  <c:ccAuthReply>
    <c:reasonCode>100</c:reasonCode>
    <c:amount>5.00</c:amount>
    <c:avsCode>X</c:avsCode>
    <c:authorizedDateTime>2015-11-03T20:53:54Z</c:authorizedDateTime>
    <c:processorResponse>100</c:processorResponse>
    <c:reconciliationID>11267051CGJSMQDC</c:reconciliationID>
  </c:ccAuthReply>
</c:replyMessage>
```

**Mastercard Transaction**

To request an authorization for a Mastercard transaction:

- **Step 1** Set the `card_accountNumber` field to the payment network token value.
- **Step 2** Set the `card_expirationMonth` and `card_expirationYear` values to the payment network token expiration date fields.
- **Step 3** Set the `ucaf_authenticationData` field to the 3D Secure cryptogram of the payment network token.
- **Step 4** Set the `ccAuthService_networkTokenCryptogram` field to the network token cryptogram.
- **Step 5** Set the `ucaf_collectionIndicator` field to 2.
- **Step 6** Set the `paymentNetworkToken_transactionType` field to 1.

Note: See "API Request Fields," page 46, and "API Reply Fields," page 54, for detailed field descriptions.
**Step 7**  Set the `ccAuthService_commerceIndicator` field to `spa`.

**Step 8**  Set the `paymentSolution` field to `008`.

---

**Example 8  Merchant Decryption Authorization Request (Mastercard)**

```xml
<requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.121">
  <merchantID>demomerchant</merchantID>
  <merchantReferenceCode>demorefnum</merchantReferenceCode>
  <billTo>
    <firstName>James</firstName>
    <lastName>Smith</lastName>
    <street1>1295 Charleston Road</street1>
    <city>Test City</city>
    <state>CA</state>
    <postalCode>99999</postalCode>
    <country>US</country>
    <email>demo@example.com</email>
  </billTo>
  <purchaseTotals>
    <currency>USD</currency>
    <grandTotalAmount>5.00</grandTotalAmount>
  </purchaseTotals>
  <card>
    <accountNumber>xxxx55555555xxxx</accountNumber>
    <expirationMonth>12</expirationMonth>
    <expirationYear>2020</expirationYear>
  </card>
  <ucaf>
    <authenticationData>ABCDEFabcdefABCDscdef0987654321234567</authenticationData>
    <collectionIndicator>2</collectionIndicator>
  </ucaf>
  <ccAuthService run="true">
    <commerceIndicator>spa</commerceIndicator>
  </ccAuthService>
  <paymentNetworkToken>
    <transactionType>1</transactionType>
  </paymentNetworkToken>
  <paymentSolution>008</paymentSolution>
</requestMessage>
```
Example 9  Merchant Decryption Authorization Reply (Mastercard)

```xml
<c:replyMessage>
  <c:requestID>4465840340765000001541</c:requestID>
  <c:decision>ACCEPT</c:decision>
  <c:reasonCode>100</c:reasonCode>
  <c:requestToken>Ahj/7wSR5C/4Icd2fdAKakGLadfg5535r/ghx3Z90AoBj3u</c:requestToken>
  <c:purchaseTotals>
    <c:currency>USD</c:currency>
  </c:purchaseTotals>
  <c:ccAuthReply>
    <c:reasonCode>100</c:reasonCode>
    <c:amount>5.00</c:amount>
    <c:authorizationCode>888888</c:authorizationCode>
    <c:avsCode>X</c:avsCode>
    <c:avsCodeRaw>II</c:avsCodeRaw>
    <c:authorizedDateTime>2015-11-03T20:53:54Z</c:authorizedDateTime>
    <c:processorResponse>100</c:processorResponse>
    <c:reconciliationID>11267051CGJSMQDC</c:reconciliationID>
  </c:ccAuthReply>
</c:replyMessage>
```

American Express Transaction

To request an authorization for an American Express transaction:

1. Set the `card_accountNumber` field to the payment network token value.
2. Set the `card_expirationMonth` and `card_expirationYear` values to the payment network expiration date fields.
3. Set the `ccAuthService_cavv` field to the 3D Secure cryptogram of the payment network token.

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

4. Set the `ccAuthService_networkTokenCryptogram` field to the network token cryptogram.

---

See "API Request Fields," page 46, and "API Reply Fields," page 54, for detailed field descriptions.
Step 5  Set the paymentNetworkToken_transactionType field to 1.

Step 6  Set the ccAuthService_commerceIndicator field to aesk.

Step 7  Set the paymentSolution field to 008.

Example 10  Merchant Decryption Authorization Request (American Express)

```xml
<requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.121">
    <merchantID>demomerchant</merchantID>
    <merchantReferenceCode>demorefnum</merchantReferenceCode>
    <billTo>
        <firstName>James</firstName>
        <lastName>Smith</lastName>
        <street1>1295 Charleston Road</street1>
        <city>Test City</city>
        <state>CA</state>
        <postalCode>99999</postalCode>
        <country>US</country>
        <email>demo@example.com</email>
    </billTo>
    <purchaseTotals>
        <currency>USD</currency>
        <grandTotalAmount>5.00</grandTotalAmount>
    </purchaseTotals>
    <card>
        <accountNumber>xxxx8224631xxxx</accountNumber>
        <expirationMonth>12</expirationMonth>
        <expirationYear>2020</expirationYear>
    </card>
    <ccAuthService run="true">
        <cavv>ABCDEFabcdefABCDEFabcdef0987654321234567</cavv>
        <commerceIndicator>aesk</commerceIndicator>
        <xid>1234567890987654321ABCDEFabcdefABCDEF123</xid>
    </ccAuthService>
    <paymentNetworkToken>
        <transactionType>1</transactionType>
    </paymentNetworkToken>
    <paymentSolution>008</paymentSolution>
</requestMessage>
```
Example 11  Merchant Decryption Authorization Reply (American Express)

```xml
<c:replyMessage>
  <c:requestID>4465840340765000001541</c:requestID>
  <c:decision>ACCEPT</c:decision>
  <c:reasonCode>100</c:reasonCode>
  <c:requestToken>Ahj/7wSR5C/4Icd2fdAKakGLadfg5535r/ghx3Z90AoBj3u</c:requestToken>
  <c:purchaseTotals>
    <c:currency>USD</c:currency>
  </c:purchaseTotals>
  <c:ccAuthReply>
    <c:reasonCode>100</c:reasonCode>
    <c:amount>5.00</c:amount>
    <c:authorizationCode>888888</c:authorizationCode>
    <c:avsCode>V</c:avsCode>
    <c:avsCodeRaw>I1</c:avsCodeRaw>
    <c:authorizedDateTime>2015-11-03T20:53:54Z</c:authorizedDateTime>
    <c:processorResponse>100</c:processorResponse>
    <c:reconciliationID>11267051CGJSMQDC</c:reconciliationID>
  </c:ccAuthReply>
</c:replyMessage>
```

**JCB Transaction**

To request an authorization for a JCB transaction:

- **Step 1**: Set the `card_accountNumber` field to the payment network token value.
- **Step 2**: Set the `card_expirationMonth` and `card_expirationYear` fields to the payment network token expiration date values.
- **Step 3**: Set the `ccAuthService_cavv` field to the 3D Secure cryptogram of the payment network token.
- **Step 4**: Set the `ccAuthService_networkTokenCryptogram` field to the network token cryptogram.
- **Step 5**: Set the `paymentNetworkToken_transactionType` field to 1.

See "API Request Fields," page 46, and "API Reply Fields," page 54, for detailed field descriptions.
**Step 6**  Set the `ccAuthService_eciRaw` field to the ECI value contained in the Samsung Pay response payload.

**Step 7**  Set the `PaymentSolution` field to 008.

---

**Example 12  Merchant Decryption Authorization Request (JCB)**

```
<requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.121">
  <merchantID>demomerchant</merchantID>
  <merchantReferenceCode>demorefnum</merchantReferenceCode>
  <billTo>
    <firstName>Jane</firstName>
    <lastName>Smith</lastName>
    <street1>123 Main Street</street1>
    <city>Small Town</city>
    <state>CA</state>
    <postalCode>98765</postalCode>
    <country>US</country>
    <email>jsmith@example.com</email>
  </billTo>
  <purchaseTotals>
    <currency>USD</currency>
    <grandTotalAmount>5.00</grandTotalAmount>
  </purchaseTotals>
  <card>
    <accountNumber>xxxx11111111xxxx</accountNumber>
    <expirationMonth>12</expirationMonth>
    <expirationYear>2020</expirationYear>
    <cvNumber>123</cvNumber>
    <cardType>001</cardType>
  </card>
  <ccAuthService run="true">
    <cavv>ABCDEFabcdefABCDEFabcdef0987654321234567</cavv>
    <eciRaw>5</eciRaw>
  </ccAuthService>
  <paymentNetworkToken>
    <transactionType>1</transactionType>
  </paymentNetworkToken>
  <paymentSolution>008</paymentSolution>
</requestMessage>
```
Example 13  Merchant Decryption Authorization Reply (JCB)

```xml
<c:replyMessage>
  <c:requestID>4465840340765000001541</c:requestID>
  <c:decision>ACCEPT</c:decision>
  <c:reasonCode>100</c:reasonCode>
  <c:requestToken>
    Ahj/7wSR5C/4Icd2fdAKakGLadfg5535r/ghx3290AcBj3u
  </c:requestToken>
  <c:purchaseTotals>
    <c:currency>USD</c:currency>
  </c:purchaseTotals>
  <c:ccAuthReply>
    <c:reasonCode>100</c:reasonCode>
    <c:amount>5.00</c:amount>
    <c:authorizationCode>888888</c:authorizationCode>
    <c:avsCode>X</c:avsCode>
    <c:avsCodeRaw>I1</c:avsCodeRaw>
    <c:authorizedDateTime>2015-11-03T20:53:54Z</c:authorizedDateTime>
    <c:processorResponse>100</c:processorResponse>
    <c:reconciliationID>11267051CGJSMQDC</c:reconciliationID>
  </c:ccAuthReply>
</c:replyMessage>
```

Example 14  Merchant Decryption NVP Request (JCB)

```xml
merchantID=demomerchant
merchantReferenceCode=demorefnum
billTo_firstName=Jane
billTo_lastName=Smith
billTo_street1=123 Main Street
billTo_city=Small Town
billTo_state=CA
billTo_postalCode=98765
billTo_country=US
billTo_email=jsmith@example.com
purchaseTotals_currency=USD
purchaseTotals_grandTotalAmount=5.00
card_accountNumber=xxxx00202036xxxx
card_expirationYear=2020
card_cvnNumber=123
cardType=001
ccAuthService_cavv=ABCDEFabcdefABCDEFabcdef0987654321234567
ccAuthService_eciRaw=5
paymentNetworkToken_transactionType=1
paymentSolution=008
```
Example 15  Merchant Decryption NVP Reply (JCB)

```plaintext
merchantsReferenceCode=demorefnum
requestID=4465840340765000001541
decision=accept
reasonCode=100
requestToken=Ahj/7wSR5C/4Icd2fdAKakGLadfg5535r/ghx3290AoBj3u
purchaseTotals_currency=USD
ccAuthReply_reasonCode=100
ccAuthReply_amount=5.00
ccAuthReply_authorizationCode=888888
ccAuthReply_avsCode=X
ccAuthReply_avsCodeRaw=I1
ccAuthReply_authorizedDateTime=2015-11-03T20:53:54Z
ccAuthReply_processorResponse=100
ccAuthReply_reconciliationID=11267051CGJSMQDC
```

CyberSource Decryption

Visa Transaction

To request an authorization for a Visa transaction:

- **Step 1**  Set the `encryptedPayment_data` field to the value that was returned from Samsung Pay in the `3ds.data` block.

  - **a**  Retrieve the payment data from Samsung Pay in JSON Web Encryption (JWE) format, which includes the key reference ID (KID) value of your public key hash in the JWE header.

  - **b**  Encode it in Base64.

  - **c**  Set the values in this structure:

    ```json
    {
      "publicKeyHash": "enter the encrypted KID value here",
      "version": "100",
      "data": "enter the encoded data from step b here"
    }
    ```

Note

See "API Request Fields," page 46, and "API Reply Fields," page 54, for detailed field descriptions.
d  Encode the structure in Base64.

e  Add the value to the **encryptedPayment_data** field.

**Step 2**  Set the **encryptedPayment_descriptor** field to
Rk1EPUNPTU1PTi5TQU1TVU5HLk1OQVBL1BBWU1FT1Q=.

**Step 3**  Set the **paymentNetworkToken_transactionType** to 1.

**Step 4**  Set the **ccAuthService_commerceIndicator** field to internet.

**Step 5**  Set the **paymentSolution** field to 008.

---

**Example 16  CyberSource Decryption Authorization Request (Visa)**

```xml
<requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.121">
  <merchantID>demomerchant</merchantID>
  <merchantReferenceCode>demorefnum</merchantReferenceCode>
  <billTo>
    <firstName>James</firstName>
    <lastName>Smith</lastName>
    <street1>1295 Charleston Road</street1>
    <city>Test City</city>
    <state>CA</state>
    <postalCode>99999</postalCode>
    <country>US</country>
    <email>demo@example.com</email>
  </billTo>
  <purchaseTotals>
    <currency>USD</currency>
    <grandTotalAmount>5.00</grandTotalAmount>
  </purchaseTotals>
  <ccAuthService run="true">
    <commerceIndicator>internet</commerceIndicator>
  </ccAuthService>
  <encryptedPayment>
    <data>ABCDEFabcdefABCDEFabcdef0987654321234567</data>
    <descriptor>Rk1EPUNPTU1PTi5TQU1TVU5HLk1OQVBL1BBWU1FT1Q=</descriptor>
  </encryptedPayment>
  <paymentSolution>008</paymentSolution>
  <paymentNetworkToken>
    <transactionType>1</transactionType>
  </paymentNetworkToken>
</requestMessage>
```
Example 17   CyberSource Decryption Authorization Reply (Visa)

```xml
<c:replyMessage>
  <c:requestID>4465840340765000001541</c:requestID>
  <c:decision>ACCEPT</c:decision>
  <c:reasonCode>100</c:reasonCode>
  <c:requestToken>Ahj/7wSR5C/4Icd2fdAKakGLadfg5535r/ghx3Z90AoBj3u</c:requestToken>
  <c:purchaseTotals>
    <c:currency>USD</c:currency>
  </c:purchaseTotals>
  <c:ccAuthReply>
    <c:reasonCode>100</c:reasonCode>
    <c:amount>5.00</c:amount>
    <c:authorizationCode>888888</c:authorizationCode>
    <c:avsCode>X</c:avsCode>
    <c:avsCodeRaw>II</c:avsCodeRaw>
    <c:authorizedDateTime>2015-11-03T20:53:54Z</c:authorizedDateTime>
    <c:processorResponse>100</c:processorResponse>
    <c:reconciliationID>11267051CGJSMQDC</c:reconciliationID>
  </c:ccAuthReply>
  <c:token>
    <c:prefix>294672</c:prefix>
    <c:suffix>4397</c:suffix>
    <c:expirationMonth>08</c:expirationMonth>
    <c:expirationYear>2021</c:expirationYear>
  </c:token>
</c:replyMessage>
```

Note
See "API Request Fields," page 46, and "API Reply Fields," page 54, for detailed field descriptions.

Mastercard Transaction

To request an authorization for a Mastercard transaction:

See "API Request Fields," page 46, and "API Reply Fields," page 54, for detailed field descriptions.

Step 1 Set the `<encryptedPayment_data>` field to the value that was returned from Samsung Pay in the `<3ds.data>` block.

a Retrieve the payment data from Samsung Pay in JSON Web Encryption (JWE) format, which includes the key reference ID (KID) value of your public key hash in the JWE header.

b Encode it in Base64.
c  Set the values in this structure:

```
{
   "publicKeyHash": "enter the encrypted KID value here",
   "version": "100",
   "data": "enter the encoded data from step b here"
}
```

d  Encode the structure in Base64.

e  Add the value to the `encryptedPayment_data` field.

**Step 2**  Set the `encryptedPayment_descriptor` field to `Rk1EPUNPTU1PTi5TQU1TVU5HLk1QVBQL1BBWU1PT1Q=`.

**Step 3**  Set the `ccAuthService_commerceIndicator` field to `spa`.

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

**Step 5**  Set the `paymentSolution` field to `008`. 
Example 18  CyberSource Decryption Authorization Request (Mastercard)

```xml
<requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.121">
  <merchantID>demosmerchant</merchantID>
  <merchantReferenceCode>demosrefnum</merchantReferenceCode>
  <billTo>
    <firstName>James</firstName>
    <lastName>Smith</lastName>
    <street1>1295 Charleston Road</street1>
    <city>Test City</city>
    <state>CA</state>
    <postalCode>99999</postalCode>
    <country>US</country>
    <email>demo@example.com</email>
  </billTo>
  <purchaseTotals>
    <currency>USD</currency>
    <grandTotalAmount>5.00</grandTotalAmount>
  </purchaseTotals>
  <ccAuthService run="true">
    <commerceIndicator>spa</commerceIndicator>
  </ccAuthService>
  <encryptedPayment>
    <data>ABCDEFabcdefABCDEFabcdef0987654321234567</data>
    <descriptor>RklEPUNPTU1PTi5TQU1TVU5HLk1OQVBQLlBBWU1FTlQ=</descriptor>
  </encryptedPayment>
  <paymentSolution>008</paymentSolution>
  <paymentNetworkToken>
    <transactionType>1</transactionType>
  </paymentNetworkToken>
</requestMessage>
```
Example 19  CyberSource Decryption Authorization Reply (Mastercard)

```xml
<c:replyMessage>
    <c:requestID>4465840340765000001541</c:requestID>
    <c:decision>ACCEPT</c:decision>
    <c:reasonCode>100</c:reasonCode>
    <c:requestToken>Ahj/7wSR5C/4Icd2fdAKakGLadfg5535r/ghx3Z90AoBj3u</c:requestToken>
    <c:purchaseTotals>
        <c:currency>USD</c:currency>
    </c:purchaseTotals>
    <c:ccAuthReply>
        <c:reasonCode>100</c:reasonCode>
        <c:amount>5.00</c:amount>
        <c:authorizationCode>888888</c:authorizationCode>
        <c:avsCode>X</c:avsCode>
        <c:avsCodeRaw>II</c:avsCodeRaw>
        <c:authorizedDateTime>2015-11-03T20:53:54Z</c:authorizedDateTime>
        <c:processorResponse>100</c:processorResponse>
        <c:reconciliationID>11267051CGJSMQDC</c:reconciliationID>
    </c:ccAuthReply>
    <c:token>
        <c:prefix>128945</c:prefix>
        <c:suffix>2398</c:suffix>
        <c:expirationMonth>08</c:expirationMonth>
        <c:expirationYear>2021</c:expirationYear>
    </c:token>
</c:replyMessage>
```

Note  
See "API Request Fields," page 46, and "API Reply Fields," page 54, for detailed field descriptions.

### American Express Transaction

To request an authorization for an American Express transaction:

**Step 1**  
Set the `encryptedPayment_data` field to the value that was returned from Samsung Pay in the `3ds.data` block.

- **a**  
  Retrieve the payment data from Samsung Pay in JSON Web Encryption (JWE) format, which includes the key reference ID (KID) value of your public key hash in the JWE header.

- **b**  
  Encode it in Base64.
Chapter 5  Authorizing a Payment

**c** Set the values in this structure:

```json
{
    "publicKeyHash": "enter the encrypted KID value here",
    "version": "100",
    "data": "enter the encoded data from step b here"
}
```

**d** Encode the structure in Base64.

**e** Add the value to the `encryptedPayment_data` field.

**Step 2** Set the `encryptedPayment_descriptor` field to `Rk1EPUNPTU1PTi5TQU1TVU5HLk1OQVBQL1BBWU1FTIQ=`.

**Step 3** Set the `ccAuthService_commerceIndicator` field to `spa`.

**Step 4** Set the `paymentSolution` field to `008`. 
Example 20  CyberSource Decryption Authorization Request (American Express)

```xml
:requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.121">
  <merchantID>demomerchant</merchantID>
  <merchantReferenceCode>demorefnum</merchantReferenceCode>
  <billTo>
    <firstName>James</firstName>
    <lastName>Smith</lastName>
    <street1>1295 Charleston Road</street1>
    <city>Test City</city>
    <state>CA</state>
    <postalCode>99999</postalCode>
    <country>US</country>
    <email>demo@example.com</email>
  </billTo>
  <purchaseTotals>
    <currency>USD</currency>
    <grandTotalAmount>5.00</grandTotalAmount>
  </purchaseTotals>
  <ccAuthService run="true">
    <commerceIndicator>aesk</commerceIndicator>
  </ccAuthService>
  <encryptedPayment>
    <data>ABCDEFabcdefABCDEFabcdef0987654321234567</data>
    <descriptor>RklEPUNPTU1PTi5TQU1TVU5HLk1OQVQLlBBWU1FTlQ=</descriptor>
  </encryptedPayment>
  <paymentSolution>008</paymentSolution>
  <paymentNetworkToken>
    <transactionType>1</transactionType>
  </paymentNetworkToken>
</requestMessage>
```
Chapter 5  Authorizing a Payment

Example 21  CyberSource Decryption Authorization Reply (American Express)

```xml
<c:replyMessage>
  <c:requestID>446584034076500001541</c:requestID>
  <c:decision>ACCEPT</c:decision>
  <c:reasonCode>100</c:reasonCode>
  <c:requestToken>Ahj/7wSR5C/4Icd2fdAKaKLaedfg5535r/ghx3Z90AoBj3u</c:requestToken>
  <c:purchaseTotals>
    <c:currency>USD</c:currency>
  </c:purchaseTotals>
  <c:ccAuthReply>
    <c:reasonCode>100</c:reasonCode>
    <c:amount>5.00</c:amount>
    <c:authorizationCode>888888</c:authorizationCode>
    <c:avsCode>V</c:avsCode>
    <c:avsCodeRaw>II</c:avsCodeRaw>
    <c:authorizedDateTime>2015-11-03T20:53:54Z</c:authorizedDateTime>
    <c:processorResponse>100</c:processorResponse>
    <c:reconciliationID>11267051CGJSMQDC</c:reconciliationID>
  </c:ccAuthReply>
  <c:token>
    <c:prefix>593056</c:prefix>
    <c:suffix>0842</c:suffix>
    <c:expirationMonth>08</c:expirationMonth>
    <c:expirationYear>2021</c:expirationYear>
  </c:token>
</c:replyMessage>
```

Note  See "API Request Fields," page 46, and "API Reply Fields," page 54, for detailed field descriptions.

JCB Transaction

To request an authorization for a JCB transaction:

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

- **Step 2**  Set the `encryptedPaymentDescriptor` field to `Rk1EPUNPTU1PTi5TQU1TVU5HLk1OQBQLlBBWU1PTiQ=`.

- **Step 3**  Set the `paymentSolution` field to `008`.  
Example 22  CyberSource Decryption Authorization Request (JCB)

```
<requestMessage xmlns="urn:schemas-cybersource-com:transaction-data-1.121">
  <merchantID>demomerchant</merchantID>
  <merchantReferenceCode>demorefnum</merchantReferenceCode>
  <billTo>
    <firstName>Jane</firstName>
    <lastName>Smith</lastName>
    <street1>123 Main Street</street1>
    <city>Small Town</city>
    <state>CA</state>
    <postalCode>98765</postalCode>
    <country>US</country>
    <email>jsmith@example.com</email>
  </billTo>
  <purchaseTotals>
    <currency>USD</currency>
    <grandTotalAmount>5.00</grandTotalAmount>
  </purchaseTotals>
  <encryptedPayment>
    <descriptor>RklEPUNPTU1PTi5TQU1TVU5HLklOQVBQLlBWWU1FTlQ=</descriptor>
    <data>ABCDEFabcdefABCDEFabcdef0987654321234567</data>
    <encoding>Base64</encoding>
  </encryptedPayment>
  <card>
    <cardType>001</cardType>
  </card>
  <ccAuthService run="true"/>
  <paymentSolution>008</paymentSolution>
</requestMessage>
```
Example 23  CyberSource Decryption Authorization Reply (JCB)

```xml
<c:replyMessage>
  <c:requestID>4465840340765000001541</c:requestID>
  <c:decision>ACCEPT</c:decision>
  <c:reasonCode>100</c:reasonCode>
  <c:requestToken>Ahj/7wSR5c/4Icd2fdAKakGLadfg5535r/ghx3290AoBj3u</c:requestToken>
  <c:token>
    <c:expirationMonth>07</c:expirationMonth>
    <c:expirationYear>2025</c:expirationYear>
    <c:prefix>239845</c:prefix>
    <c:suffix>2947</c:suffix>
  </c:token>
  <c:purchaseTotals>
    <c:currency>USD</c:currency>
  </c:purchaseTotals>
  <c:ccAuthReply>
    <c:reasonCode>100</c:reasonCode>
    <c:amount>5.00</c:amount>
    <c:authorizationCode>888888</c:authorizationCode>
    <c:avsCode>X</c:avsCode>
    <c:avsCodeRaw>I1</c:avsCodeRaw>
    <c:processorResponse>100</c:processorResponse>
    <c:reconciliationID>11267051CGJSMQDC</c:reconciliationID>
  </c:ccAuthReply>
</c:replyMessage>
```
Additional CyberSource Services

Refer to Credit Card Services Using the Simple Order API (PDF | HTML) for information on how to request these follow-on services.

Table 3 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>Authorization Reversal</td>
<td>A follow-on service that uses the request ID returned from the previous authorization. An authorization 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>
API Fields

Data Type Definitions

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

Table 4  Data Type Definitions

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integer</td>
<td>Whole number {..., -3, -2, -1, 0, 1, 2, 3, ...}</td>
</tr>
<tr>
<td>String</td>
<td>Sequence of letters, numbers, spaces, and special characters</td>
</tr>
</tbody>
</table>

Numbered Elements

The CyberSource XML schema includes several numbered elements. You can include these complex elements more than once in a request. For example, when a customer order includes more than one item, you must include multiple <item> elements in your request. Each item is numbered, starting with 0. The XML schema uses an id attribute in the item’s opening tag to indicate the number. For example:

    <item id="0"/>

As a name-value pair field name, this tag is represented as item_0. In this portion of the field name, the underscore before the number does not indicate hierarchy in the XML schema. The item fields are generically referred to as item_<element name> in the documentation.
Below is an example of the numbered `<item>` element and the corresponding name-value pair field names. If you are using the Simple Object Access Protocol (SOAP), the client contains a corresponding `Item` class.

**Example 24  Numbered XML Schema Element Names and Name-Value Pair Field Names**

<table>
<thead>
<tr>
<th>XML Schema Element Names</th>
<th>Corresponding Name-Value Pair Field Names</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;item id=&quot;0&quot;&gt;</code></td>
<td><code>item_0_unitPrice</code></td>
</tr>
<tr>
<td><code>&lt;unitPrice&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;quantity&gt;</code></td>
<td><code>item_0_quantity</code></td>
</tr>
<tr>
<td><code>&lt;/item&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;item id=&quot;1&quot;&gt;</code></td>
<td></td>
</tr>
<tr>
<td><code>&lt;unitPrice&gt;</code></td>
<td><code>item_1_unitPrice</code></td>
</tr>
<tr>
<td><code>&lt;quantity&gt;</code></td>
<td><code>item_1_quantity</code></td>
</tr>
<tr>
<td><code>&lt;/item&gt;</code></td>
<td></td>
</tr>
</tbody>
</table>

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

---

**Relaxed Requirements for Address Data**

Contact CyberSource Customer Support to have your account enabled for relaxed requirements for address data and expiration date. For more information, see the Relaxed Requirements for Address Data and Expiration Date page.
### API Request Fields

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

#### Table 5  API 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>billTo_city</td>
<td>City of the billing address.</td>
<td>ccAuthService (See description)</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></td>
<td>See &quot;Relaxed Requirements for Address Data,&quot; page 45.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>billTo_country</td>
<td>Country of the billing address. Use the two-character ISO Standard Country Codes.</td>
<td></td>
<td></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></td>
<td>See &quot;Relaxed Requirements for Address Data,&quot; page 45.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>billTo_email</td>
<td>Customer’s email address.</td>
<td>ccAuthService (See description)</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></td>
<td>See &quot;Relaxed Requirements for Address Data,&quot; page 45.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>billTo_firstName</td>
<td>Customer’s first name. For a credit card transaction, this name must match the name on the card.</td>
<td></td>
<td></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></td>
<td>See &quot;Relaxed Requirements for Address Data,&quot; page 45.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>billTo_ipAddress</td>
<td>Customer’s IP address.</td>
<td>ccAuthService (O)</td>
<td>String (15)</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  API 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>billTo_lastName</td>
<td>Customer's last name. For a credit card transaction, this name must match the name on the card.</td>
<td>ccAuthService (See description)</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></td>
<td>See &quot;Relaxed Requirements for Address Data,&quot; page 45.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>billTo_phoneNumber</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>ccAuthService (O)</td>
<td>String (15)</td>
</tr>
<tr>
<td>billTo_postalCode</td>
<td>Postal code for the billing address. The postal code must consist of 5 to 9 digits.</td>
<td>ccAuthService (See description)</td>
<td>String (9)</td>
</tr>
<tr>
<td></td>
<td>When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong> 12345-6789</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example</strong> A1B 2C3</td>
<td></td>
<td></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></td>
<td>See &quot;Relaxed Requirements for Address Data,&quot; page 45.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>billTo_state</td>
<td>State or province of the billing address. For an address in the U.S. or Canada, use the <a href="index.html#state-province-and-territory-codes-for-the-united-states-and-canada">State, Province, and Territory Codes for the United States and Canada.</a></td>
<td>ccAuthService (See description)</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>
<tr>
<td></td>
<td>See &quot;Relaxed Requirements for Address Data,&quot; page 45.</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.
Table 5  API Request 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>billTo_street1</td>
<td>First line of the billing street address.</td>
<td>ccAuthService (See description)</td>
<td>String (60)</td>
</tr>
<tr>
<td>billTo_street2</td>
<td>Additional address information.</td>
<td>ccAuthService (R)</td>
<td>String (60)</td>
</tr>
<tr>
<td>card_accountNumber</td>
<td>Payment network token value.</td>
<td>ccAuthService (R)</td>
<td>Nonnegative integer (20)</td>
</tr>
<tr>
<td>card_expirationMonth</td>
<td>Two-digit month in which the payment network token expires. Format: MM. Possible values: 01 through 12.</td>
<td>ccAuthService (R)</td>
<td>String (2)</td>
</tr>
<tr>
<td>card_expirationYear</td>
<td>Four-digit year in which the payment network token expires. Format: YYYY.</td>
<td>ccAuthService (R)</td>
<td>Nonnegative integer (4)</td>
</tr>
<tr>
<td>ccAuthService_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. <strong>American Express</strong> For a 20-byte cryptogram, set this field to the cryptogram for payment network tokenization transactions. For a 40-byte cryptogram, set this field to block A of the cryptogram for payment network tokenization transactions. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats.</td>
<td>ccAuthService (R)</td>
<td>String (40)</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  API 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>
</table>
| ccAuthService_commerceIndicator | For a payment network tokenization transaction. Possible values:  
- aesk for the American Express card type  
- spa for the Mastercard card type  
- internet for the Visa card type | ccAuthService (R)                                                        | String (20) |
| ccAuthService_directoryServerTransactionActionID | Identifier generated during the authentication transaction by the Mastercard Directory Server and passed back with the authentication results. | ccAuthService (O)                                                               | String (36) |
| ccAuthService_eciRaw | Raw electronic commerce indicator (ECI).                                                                           | ccAuthService                                                                   | String (2) |
| ccAuthService_networkTokenCryptogram | Token authentication verification value cryptogram. For token-based transactions with 3D Secure or Identity Check, you must submit both types of cryptograms: network token and 3D Secure/Identity Check. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats. | ccAuthService                                                                   | String (40) |
| ccAuthService_paSpecificationVersion | The 3D Secure version that you used for Secured Consumer Authentication (SCA); for example, 3D Secure 1.0.2 or 2.0.0. | ccAuthService                                                                   | String (20) |
| ccAuthService_run            | Whether to include ccAuthService in your request. Possible values:  
- true: Include the service in your request.  
- false (default): Do not include the service in your request. | ccAuthService (R)                                                               | String (5) |

---

1 The TC 33 Capture file contains information about the purchases and refunds that a merchant submits to CyberSource. CyberSource through VisaNet creates the TC 33 Capture file at the end of the day and sends it to the merchant’s acquirer, who uses this information to facilitate end-of-day clearing processing with payment card companies.
### Appendix A  API 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>
</table>
| ccAuthService_xid   | Visa
- Cryptogram for payment network tokenization transactions. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats.|
|                     | American Express
- For a 20-byte cryptogram, set this field to the cryptogram for payment network tokenization transactions. For a 40-byte cryptogram, set this field to block A of the cryptogram for payment network tokenization transactions (see "Merchant Decryption," page 23). The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats.|
|                     | ccAuthService (R) String (40)                                                                                                                                                                               |                                      |                    |
| encryptedPayment_data | Encrypted payment data value. If you are using the CyberSource Decryption option, populate this field with the encrypted payment data value returned from Samsung Pay in the 3ds.data block.                                                                 | ccAuthService (R)                     |                    |
| encryptedPayment_descriptor | Format of the encrypted payment data. The value for Samsung Pay is Rk1EPUNPTU1PTi5TQU1TVU5HLk1O QVBQL1BBWU1FT1Q=                                                                                                           | ccAuthService (R)                     |                    |
| item_#_productCode   | Type of product. This value is used to determine the product category: electronic, handling, physical, service, or shipping. The default is default.
- See "Numbered Elements," page 44.                                                                                                                                                     | ccAuthService (O)                     | String (255)       |
| item_#_productName   | Name of the product.
- This field is required when the item_#_productCode value is not default or one of the values related to shipping and/or handling.
- See "Numbered Elements," page 44.                                                                                                                                                   | ccAuthService (See description)       | String (255)       |

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  API 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>item_#_productSKU</td>
<td>Identification code for the product. This field is required when the item_#_productCode value is not default or one of the values related to shipping and/or handling. See &quot;Numbered Elements,&quot; page 44.</td>
<td>ccAuthService (See description)</td>
<td>String (255)</td>
</tr>
<tr>
<td>item_#_quantity</td>
<td>Default is 1. This field is required when the item_#_productCode value is not default or one of the values related to shipping and/or handling. See &quot;Numbered Elements,&quot; page 44.</td>
<td>ccAuthService (See description)</td>
<td>Integer (10)</td>
</tr>
<tr>
<td>item_#_taxAmount</td>
<td>Total tax to apply to the product. This value cannot be negative. See &quot;Numbered Elements,&quot; page 44.</td>
<td>cc AuthService (See description)</td>
<td>String (15)</td>
</tr>
<tr>
<td>item_#_unitPrice</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. See &quot;Numbered Elements,&quot; page 44.</td>
<td>ccAuthService (See description)</td>
<td>String (15)</td>
</tr>
<tr>
<td>merchantID</td>
<td>Your CyberSource merchant ID. Use the same merchant ID for evaluation, testing, and production.</td>
<td>cc AuthService (R)</td>
<td>String (30)</td>
</tr>
<tr>
<td>merchantReferenceCode</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 Simple Order API (PDF</td>
<td>HTML).</td>
<td>cc AuthService (R)</td>
</tr>
<tr>
<td>paymentNetworkToken_</td>
<td>Confidence level of the tokenization. This value is assigned by the token service provider. Note: This field is supported only for FDC Nashvill e Global.</td>
<td>cc AuthService (O)</td>
<td>String (2)</td>
</tr>
<tr>
<td>assuranceLevel</td>
<td></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.
### Table 5 API 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>paymentNetworkToken_deviceTechType</td>
<td>Type of technology used in the device to store token data. Possible value: 002: Host card emulation (HCE) Emulation of a smart card by using software to create a virtual and exact representation of the card. Sensitive data is stored in a database that is hosted in the cloud. For storing payment credentials, a database must meet very stringent security requirements that exceed PCI DSS. <strong>Note</strong> This field is supported only for FDC Compass.</td>
<td>ccAuthService (O)</td>
<td>Integer (3)</td>
</tr>
<tr>
<td>paymentNetworkToken_requestorID</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. <strong>Note</strong> This field is supported only for FDC Nashville Global and Chase Paymentech Solutions.</td>
<td>ccAuthService (O)</td>
<td>String (11)</td>
</tr>
<tr>
<td>paymentNetworkToken_transactionType</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.</td>
<td>ccAuthService (R)</td>
<td>String (1)</td>
</tr>
<tr>
<td>paymentSolution</td>
<td>Identifies Samsung Pay as the payment solution that is being used for the transaction: Set the value for this field to 008. <strong>Note</strong> This unique ID differentiates digital solution transactions within the CyberSource platform for reporting purposes.</td>
<td>ccAuthService (R)</td>
<td>String (3)</td>
</tr>
<tr>
<td>purchaseTotals_currency</td>
<td>Currency used for the order: USD</td>
<td>ccAuthService (R)</td>
<td>String (5)</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  API 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>purchaseTotals_grandTotalAmount</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>ccAuthService (O)</td>
<td>String (15)</td>
</tr>
<tr>
<td>surchargeAmount</td>
<td>Amount is included in the total transaction amount but is passed in a separate field to the issuer and acquirer for tracking. The issuer can provide information about the surcharge amount to the customer. This field is supported only for CyberSource through VisaNet.</td>
<td>ccAuthService (O)</td>
<td>String (15)</td>
</tr>
<tr>
<td>ucaf_authenticationData</td>
<td>Cryptogram for payment network tokenization transactions with Mastercard.</td>
<td>ccAuthService (R)</td>
<td>String (32)</td>
</tr>
<tr>
<td>ucaf_collectionIndicator</td>
<td>Required field for payment network tokenization transactions with Mastercard.</td>
<td>ccAuthService (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.
API Reply Fields

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

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

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

Table 6  API 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>card_suffix</td>
<td>Last four digits of the cardholder’s account number. This field is returned only for tokenized transactions. You can use this value on the receipt that you give to the cardholder. This field is returned only for FDC Nashville Global.</td>
<td>ccAuthReply</td>
<td>String (4)</td>
</tr>
<tr>
<td>ccAuthReply_amount</td>
<td>Amount that was authorized.</td>
<td>ccAuthReply</td>
<td>String (15)</td>
</tr>
<tr>
<td>ccAuthReply_authorizationCode</td>
<td>Authorization code. Returned only when the processor returns this value.</td>
<td>ccAuthReply</td>
<td>String (7)</td>
</tr>
<tr>
<td>ccAuthReply_avsCode</td>
<td>AVS results. See Credit Card Services Using the Simple Order API (PDF</td>
<td>HTML) for a detailed list of AVS codes.</td>
<td>ccAuthReply</td>
</tr>
<tr>
<td>ccAuthReply_avsCodeRaw</td>
<td>AVS result code sent directly from the processor. Returned only when the processor returns this value.</td>
<td>ccAuthReply</td>
<td>String (10)</td>
</tr>
<tr>
<td>ccAuthReply_cvCode</td>
<td>CVN result code. See Credit Card Services Using the Simple Order API (PDF</td>
<td>HTML) for a detailed list of CVN codes.</td>
<td>ccAuthReply</td>
</tr>
</tbody>
</table>
### Table 6 API 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>ccAuthReply_cvCodeRaw</td>
<td>CVN result code sent directly from the processor. Returned only when the processor returns this value.</td>
<td>ccAuthReply</td>
<td>String (10)</td>
</tr>
<tr>
<td>ccAuthReply_processorResponse</td>
<td>For most processors, this is the error message sent directly from the bank. Returned only when the processor returns this value.</td>
<td>ccAuthReply</td>
<td>String (10)</td>
</tr>
<tr>
<td>ccAuthReply_reasonCode</td>
<td>Numeric value corresponding to the result of the credit card authorization request. See Credit Card Services Using the Simple Order API (PDF</td>
<td>HTML) for a detailed list of reason codes.</td>
<td>ccAuthReply</td>
</tr>
<tr>
<td>ccAuthReply_reconciliationID</td>
<td>Reference number for the transaction. This value is not returned for all processors.</td>
<td>ccAuthReply</td>
<td>String (60)</td>
</tr>
<tr>
<td>decision</td>
<td>Summarizes the result of the overall request. Possible values:</td>
<td>ccAuthReply</td>
<td>String (6)</td>
</tr>
<tr>
<td></td>
<td>- ACCEPT</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- ERROR</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- REJECT</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- REVIEW: Returned only when you use CyberSource Decision Manager.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>invalidField_0 through invalidField_N</td>
<td>Fields in the request that contained invalid data. For information about missing or invalid fields, see Getting Started with CyberSource Advanced for the Simple Order API (PDF</td>
<td>HTML).</td>
<td>ccAuthReply</td>
</tr>
<tr>
<td>merchantReferenceCode</td>
<td>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.</td>
<td>ccAuthReply</td>
<td>String (50)</td>
</tr>
</tbody>
</table>
Table 6  API 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>missingField_0 through missingField_N</td>
<td>Required fields that were missing from the request. For information about missing or invalid fields, see Getting Started with CyberSource Advanced for the Simple Order API (PDF</td>
<td>HTML).</td>
<td>ccAuthReply String (100)</td>
</tr>
</tbody>
</table>
| paymentNetworkToken_assuranceLevel | Confidence level of the tokenization. This value is assigned by the token service provider.  

**Note**  This field is returned only for FDC Nashville Global. | ccAuthReply | String (2) |
| purchaseTotals_currency | Currency used for the order. For the possible values, see the ISO Standard Currency Codes.                                                      | ccAuthReply | String (5) |
| reasonCode | Numeric value corresponding to the result of the overall request. See Credit Card Services Using the Simple Order API (PDF | HTML) for a detailed list of reason codes. | ccAuthReply | Integer (5) |
| requestID | Identifier for the request generated by the client.                                                                                                             | ccAuthReply | String (26) |
| requestToken | Request token data created by CyberSource for each reply. The field is an encoded string that contains no confidential information such as an account or card verification number. The string can contain a maximum of 256 characters. | ccAuthReply | String (256) |
| token_expirationMonth | Month in which the token expires. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction.  

Format: MM.  
Possible values: 01 through 12. | ccAuthReply | String (2) |
| token_expirationYear | Year in which the token expires. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction.  

Format: YYYY. | ccAuthReply | String (4) |
### Table 6  API 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>token_prefix</td>
<td>First six digits of token. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction.</td>
<td>ccAuthReply</td>
<td>String (6)</td>
</tr>
<tr>
<td>token_suffix</td>
<td>Last four digits of token. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction.</td>
<td>ccAuthReply</td>
<td>String (4)</td>
</tr>
</tbody>
</table>