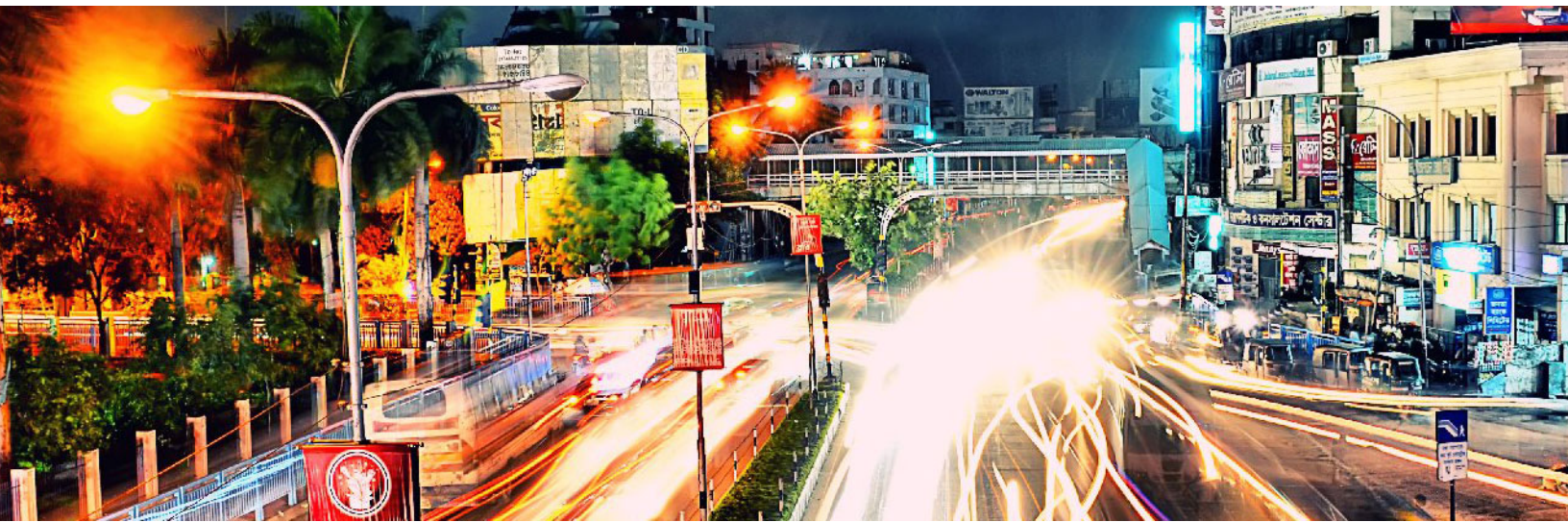


Samsung Pay

Using the Simple Order API



CyberSource[®]
A Visa Solution

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

© 2020. 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. Visa, Visa International, CyberSource, the Visa logo, and the CyberSource logo are the registered trademarks of Visa International in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Revision: July 2020

Contents

Recent Revisions to This Document 5

About This Guide 6

Audience and Purpose 6

Conventions 6

Notes and Important Statements 6

Text and Command Conventions 6

Related Documents 7

Customer Support 7

Chapter 1 Introduction 8

Requirements 8

Supported Processors, Acquirers, Card Types, and Optional Features 9

Transaction Endpoints 10

Chapter 2 Registration 11

Registering with Samsung 11

Registering with CyberSource 12

Chapter 3 Integrating the Samsung SDK 13

Creating a Project 13

Integrating the Samsung Pay SDK 13

Using the API Key 14

Chapter 4 Using the Samsung Pay SDK 15

Eligibility 15

Payment Request 16

Initiating a Payment 16

Requesting a Payment 18

| | | |
|------------------|---------------------------------|-----------|
| Chapter 5 | Authorizing a Payment | 20 |
| | Merchant Decryption | 20 |
| | Visa Transaction | 20 |
| | Mastercard Transaction | 22 |
| | American Express Transaction | 24 |
| | JCB Transaction | 26 |
| | CyberSource Decryption | 29 |
| | Visa Transaction | 29 |
| | Mastercard Transaction | 31 |
| | American Express Transaction | 34 |
| | JCB Transaction | 36 |
| | Additional CyberSource Services | 39 |

| | | |
|-------------------|---------------------------------------|-----------|
| Appendix A | API Fields | 40 |
| | Data Type Definitions | 40 |
| | Numbered Elements | 40 |
| | Relaxed Requirements for Address Data | 41 |
| | Request Fields | 42 |
| | Reply Fields | 49 |

Recent Revisions to This Document

| Release | Changes |
|----------------|---|
| July 2020 | Added endpoint and Business Center URLs for transactions in India. See " Transaction Endpoints ," page 10, and " Registering with CyberSource ," page 12. |
| May 2020 | Updated information about recurring payments. See " Supported Processors, Acquirers, Card Types, and Optional Features ," page 9. |
| January 2020 | Changed <i>payment network tokenization</i> to <i>authorizations with payment network tokens</i> throughout. Updated the Business Center procedure. See " Registering with CyberSource ," page 12. |
| September 2019 | This revision contains only editorial changes and no technical updates. |
| June 2019 | Changed the name of <i>Mastercard SecureCode</i> to <i>Mastercard Identity Check</i> . |
| May 2019 | This revision contains only editorial changes and no technical updates. |

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. See ["Using the Samsung Pay SDK," page 15](#), and ["Authorizing a Payment," page 20](#). 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

| Convention | Usage |
|-------------|---|
| bold | <ul style="list-style-type: none">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 | Code examples and samples. |

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](#))
- *Authorizations with Payment Network Tokens 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>

Introduction

Requirements



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

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

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

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

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, Acquirers, Card Types, and Optional Features](#)," page 9.
- A profile on the Samsung Pay Partner Portal, and you must obtain a partner ID. See "[Registration](#)," page 11.

Supported Processors, Acquirers, Card Types, and Optional Features

Merchant-initiated transactions, multiple partial captures, and subsequent authorizations are described in *Authorizations with Payment Network Tokens Using the Simple Order API* ([PDF](#) | [HTML](#)). Recurring payments and split shipments are described in *Credit Card Services Using the Simple Order API* ([PDF](#) | [HTML](#)).

Table 1 Supported Processors, Card Types, and Optional Features

| Processors | Card Types | Optional |
|--|---|--|
| American Express Direct | American Express | <ul style="list-style-type: none"> ■ Multiple partial captures ■ Recurring payments |
| Barclays | Visa, Mastercard, JCB, Maestro (International), Maestro (UK Domestic) If you support Maestro (UK Domestic), you must also support Maestro (International), and you must support Mastercard Identity Check for both card types. | <ul style="list-style-type: none"> ■ Multiple partial captures ■ Recurring payments |
| Chase Paymentech Solutions | Visa, Mastercard, American Express, Discover, Diners Club, JCB, Carte Blanche, Maestro (International) | <ul style="list-style-type: none"> ■ Multiple partial captures ■ Recurring payments |
| CyberSource through VisaNet. The supported acquirer is: <ul style="list-style-type: none"> ■ Vantiv CyberSource through VisaNet is a single processor with multiple acquirers. | Visa, Mastercard, American Express, Discover, JCB, Diners Club | <ul style="list-style-type: none"> ■ Recurring payments ■ Split shipments |
| Elavon Americas | Visa, Mastercard, American Express, JCB, Diners Club, Discover, China UnionPay | <ul style="list-style-type: none"> ■ Merchant-Initiated transactions ■ Multiple partial captures ■ Recurring payments |
| FDC Compass | Visa, Mastercard, American Express, Discover, Diners Club, JCB | <ul style="list-style-type: none"> ■ Multiple partial captures ■ Recurring payments |
| FDC Nashville Global | Visa, Mastercard, American Express, Discover, Diners Club, JCB, China UnionPay | <ul style="list-style-type: none"> ■ Multiple partial captures ■ Recurring payments |

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

| Processors | Card Types | Optional |
|---|--|--|
| GPN | Visa, Mastercard, American Express, Discover, Diners Club, JCB | Split shipments |
| JCN Gateway | Visa, Mastercard, American Express, Diners Club, JCB, NICOS house card, ORICO house card | Multiple partial captures |
| OmniPay Direct <ul style="list-style-type: none"> ■ Bank of America Merchant Services ■ First Data Merchant Solutions (Europe) ■ Global Payments International Acquiring | Visa, Mastercard, Discover, Diners Club, Maestro (UK Domestic), Maestro (International) | <ul style="list-style-type: none"> ■ Multiple partial captures ■ Recurring payments |
| Streamline | Visa, Mastercard | <ul style="list-style-type: none"> ■ Multiple partial captures ■ Recurring payments ■ Subsequent authorizations |
| TSYS Acquiring Solutions | Visa, Mastercard, American Express | Multiple partial captures |

Transaction Endpoints

Test transactions:

- Akamai endpoint:
<https://ics2wstesta.ic3.com/commerce/1.x/transactionProcessor>
- Non-Akamai endpoint:
<https://ics2wstest.ic3.com/commerce/1.x/transactionProcessor>

Live transactions:

- Akamai endpoint:
<https://ics2wsa.ic3.com/commerce/1.x/transactionProcessor>
- Non-Akamai endpoint:
<https://ics2ws.ic3.com/commerce/1.x/transactionProcessor>
- India endpoint:
<https://ics2ws.ic3.in.com/commerce/1.x/transactionProcessor>

Registration

Registering with Samsung

To register with Samsung:

- Step 1** Create a profile by completing the merchant application on the [Samsung Pay Partner Portal](#). Samsung will contact you if clarification is needed.
- Step 2** After your merchant application is approved, you receive a unique partner ID. Include this ID in your application.



You need the partner ID in order to generate the Certificate Signing Request (CSR) file in the CyberSource Business Center. See "[Registering with CyberSource](#)," page 12. 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 15.

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 14.

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.

- 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 test transactions: <https://ebctest.cybersource.com/ebc2/>
 - Create a CSR file for live transactions: <https://ebc2.cybersource.com/ebc2/>
 - Create a CSR file for live transactions in India: <https://ebc2.in.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 Samsung Pay Registration panel opens.
- Step 5** Enter your Samsung partner 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.



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

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

Integrating the Samsung SDK

Creating a Project

To create a 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 name of your application and the company domain.
 - Step 4** 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 5** Click **Next**.
 - Step 6** In the Target Android Devices settings, choose the required API levels.
 - Step 7** Click **Next**.
 - Step 8** 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.

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

Step 3 Import the package.

```
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 in "Registering with Samsung," page 11) 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 meta-data.

Example 1 Debug Mode

```
<meta-data
  android:name="debug_mode"
  android:value="Y" />
<meta-data
  android:name="spay_debug_api_key"
  android:value="asdfgkndkeiel7283094858" />
```

Example 2 Release Mode

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

Using the Samsung Pay SDK

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 `SsdKUnsupportedException` or `NullPointerException` error.

- `SsdKUnsupportedException`—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:



If the required fields are not included, you receive a `NullPointerException` error.

- 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

Example 4 Transaction Request Structure

```

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`—contains payment information.
- `PID`—the product ID created in the Samsung Pay Partner Portal. See ["Registration," page 11](#).
- `StatusListener`—the result of the payment request is delivered to `StatusListener`. This listener should be registered before you call the `startSamsungPay()` API method.

When you request the `startSamsungPay()` API method, the Samsung Pay online payment sheet is displayed on 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 19](#).
- `onFailure()`—this event is requested when the transaction fails. It returns an error code and error message.

Example 5 Request startSamsungPay() API Method

```

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 17.
    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

| Payment Credential | Description |
|---------------------------------|--|
| method | Payment protocol: 3D Secure. |
| merchant_ref | Merchant reference code. |
| billing_address.street | Number, street name. |
| billing_address.state_province | Two-letter state code. |
| billing_address.zip_postal_code | Five-character zip code. |
| billing_address.city | City name. |
| billing_address.county | Two letter country code. |
| 3ds.type | S for Samsung Pay. Encrypted. |
| 3ds.version | Current version 100. Encrypted. |
| 3ds.data | Base64-encoded payment data. Encrypted. |

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

<https://pay.samsung.com/developers>

Authorizing a Payment

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.

Merchant Decryption

Visa Transaction

See "[Request Fields](#)," [page 42](#), and "[Reply Fields](#)," [page 49](#), for detailed field descriptions.

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` 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.
- Step 6** Set the `ccAuthService_commerceIndicator` field to `internet`.
- Step 7** Set the `paymentSolution` field to `008`.

Example 6 Merchant Decryption Authorization Request (Visa)

```

<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>xxxx10000000xxxx</accountNumber>
    <expirationMonth>12</expirationMonth>
    <expirationYear>2020</expirationYear>
  </card>
  <ccAuthService run="true">
    <cavv>ABCDEFabcdefABCDEFabcdef0987654321234567</cavv>
    <commerceIndicator>internet</commerceIndicator>
  </ccAuthService>
  <paymentNetworkToken>
    <transactionType>1</transactionType>
  </paymentNetworkToken>
  <paymentSolution>008</paymentSolution>
</requestMessage>

```

Example 7 Merchant Decryption Authorization Reply (Visa)

```

<c:replyMessage>
  <c:merchantReferenceCode>demorefnum</c:merchantReferenceCode>
  <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>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>

```

Mastercard Transaction

See ["Request Fields," page 42](#), and ["Reply Fields," page 49](#), for detailed field descriptions.

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` fields to the payment network token expiration date values.
 - 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.

Step 7 Set the `ccAuthService_commerceIndicator` field to `spa`.

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

Example 8 Merchant Decryption Authorization Request (Mastercard)

```

<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)

```

<c:replyMessage>
  <c:merchantReferenceCode>demorefnum</c:merchantReferenceCode>
  <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>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>

```

American Express Transaction

See ["Request Fields," page 42](#), and ["Reply Fields," page 49](#), for detailed field descriptions.

To request an authorization for an American Express 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.



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.

- 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 `aesk`.

Step 7 Set the `paymentSolution` field to 008.

Example 10 Merchant Decryption Authorization Request (American Express)

```
<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)

```

<c:replyMessage>
  <c:merchantReferenceCode>demorefnum</c:merchantReferenceCode>
  <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

See ["Request Fields," page 42](#), and ["Reply Fields," page 49](#), for detailed field descriptions.

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.

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)

```

<c:replyMessage>
  <c:merchantReferenceCode>demorefnum</c:merchantReferenceCode>
  <c:requestID>446584034076500001541</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>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)

```

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_cvNumber=123
cardType=001
ccAuthService_cavv=ABCDEFabcdefABCDEFabcdef0987654321234567
ccAuthService_eciRaw=5
paymentNetworkToken_transactionType=1
paymentSolution=008

```

Example 15 Merchant Decryption NVP Reply (JCB)

```

merchantReferenceCode=demorefnum
requestID=4465840340765000001541
decision=accept
reasonCode=100
requestToken=Ahj/7wSR5C/4Icd2fdAKakGLadfg5535r/ghx3Z90AoBj3u
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

See ["Request Fields," page 42](#), and ["Reply Fields," page 49](#), for detailed field descriptions.

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. This format which includes the key reference ID (KID) value of your public key hash in the 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
RklEPUNPTU1PTi5TQU1TVU5HLk1OQVBQL1BBWU1FTlQ=.

Step 3 Set the **paymentNetworkToken_transactionType** field 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)

```
<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>RklEPUNPTU1PTi5TQU1TVU5HLk1OQVBQL1BBWU1FTlQ=</descriptor>
  </encryptedPayment>
  <paymentSolution>008</paymentSolution>
  <paymentNetworkToken>
    <transactionType>1</transactionType>
  </paymentNetworkToken>
</requestMessage>
```

Example 17 CyberSource Decryption Authorization Reply (Visa)

```

<c:replyMessage>
  <c:merchantReferenceCode>demorefnum</c:merchantReferenceCode>
  <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>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: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>

```

Mastercard Transaction

See ["Request Fields," page 42](#), and ["Reply Fields," page 49](#), for detailed field descriptions.

To request an authorization for a Mastercard 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. This format includes the key reference ID (KID) value of your public key hash in the 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
RklEPUNPTU1PTi5TQU1TVU5HLk1OQVBQL1BBWU1FTlQ=.

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)

```

<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>spa</commerceIndicator>
  </ccAuthService>
  <encryptedPayment>
    <data>ABCDEFabcdefABCDEFabcdef0987654321234567</data>
    <descriptor>RklEPUNPTU1PTi5TQU1TVU5HLklOQVBQLlBBWU1FTlQ=</descriptor>
  </encryptedPayment>
  <paymentSolution>008</paymentSolution>
  <paymentNetworkToken>
    <transactionType>1</transactionType>
  </paymentNetworkToken>
</requestMessage>

```

Example 19 CyberSource Decryption Authorization Reply (Mastercard)

```

<c:replyMessage>
  <c:merchantReferenceCode>demorefnum</c:merchantReferenceCode>
  <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>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: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>

```

American Express Transaction

See ["Request Fields," page 42](#), and ["Reply Fields," page 49](#), for detailed field descriptions.

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. This format which includes the key reference ID (KID) value of your public key hash in the 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
RklEPUNPTU1PTi5TQU1TVU5HLklOQVBQLlBBWU1FTlQ=.

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)

```
<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>RklEPUNPTU1PTi5TQU1TVU5HLklOQVBQLlBBWU1FTlQ=</descriptor>
  </encryptedPayment>
  <paymentSolution>008</paymentSolution>
  <paymentNetworkToken>
    <transactionType>1</transactionType>
  </paymentNetworkToken>
</requestMessage>
```

Example 21 CyberSource Decryption Authorization Reply (American Express)

```

<c:replyMessage>
  <c:merchantReferenceCode>demorefnum</c:merchantReferenceCode>
  <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: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>

```

JCB Transaction

See ["Request Fields," page 42](#), and ["Reply Fields," page 49](#), for detailed field descriptions.

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 `Rk1EPUNPTU1PTi5TQU1TVU5HLk1OQVBQL1BBWU1FT1Q=`.
 - 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>RklEPUNPTU1PTi5TQU1TVU5HLk1OQVBQL1BBWU1FTlQ= </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)

```
<c:replyMessage>
  <c:merchantReferenceCode>demorefnum</c:merchantReferenceCode>
  <c:requestID>4465840340765000001541</c:requestID>
  <c:decision>ACCEPT</c:decision>
  <c:reasonCode>100</c:reasonCode>
  <c:requestToken>Ahj/7wSR5C/4Icd2fdAKakGLadfg5535r/ghx3Z90AoBj3u</
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

| CyberSource Service | Description |
|----------------------------|--|
| Capture | 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. |
| Sale | A sale is a bundled authorization and capture. Request the authorization and capture services at the same time. CyberSource processes the capture immediately. |
| Authorization Reversal | 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. |

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

| Data Type | Description |
|---------------|---|
| Date and time | Format is YYYY-MM-DDThh:mm:ssZ, where: <ul style="list-style-type: none">■ T separates the date and the time■ Z indicates Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT) <p>Example 2020-01-11T22:47:57Z equals January 11, 2020, at 22:47:57 (10:47:57 p.m.).</p> |
| Integer | Whole number {..., -3, -2, -1, 0, 1, 2, 3, ...} |
| String | Sequence of letters, numbers, spaces, and special characters |

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 called `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**

| XML Schema Element Names | Corresponding Name-Value Pair Field Names |
|---|---|
| <pre><item id="0"> <unitPrice> <quantity> </item></pre> | <pre>item_0_unitPrice item_0_quantity</pre> |
| <pre><item id="1"> <unitPrice> <quantity> </item></pre> | <pre>item_1_unitPrice item_1_quantity</pre> |



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

Relaxed Requirements for Address Data

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.

Request Fields

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

Table 5 Request Fields

| Field | Description | Used By: Required (R) or Optional (O) | Data Type (Length) |
|------------------|--|---|-----------------------|
| billTo_city | <p>City of the billing address.</p> <p>Important It is your responsibility to determine whether a field is required for the transaction that you are requesting.</p> <p>See "Relaxed Requirements for Address Data," page 41.</p> | ccAuthService (See description) | String (50) |
| billTo_country | <p>Country of the billing address. Use the two-character ISO Standard Country Codes.</p> <p>Important It is your responsibility to determine whether a field is required for the transaction you are requesting.</p> <p>See "Relaxed Requirements for Address Data," page 41.</p> | ccAuthService (See description) | String (2) |
| billTo_email | <p>Customer's email address.</p> <p>Important It is your responsibility to determine whether a field is required for the transaction you are requesting.</p> <p>See "Relaxed Requirements for Address Data," page 41.</p> | ccAuthService (See description) | String (255) |
| billTo_firstName | <p>Customer's first name. For a credit card transaction, this name must match the name on the card.</p> <p>Important It is your responsibility to determine whether a field is required for the transaction you are requesting.</p> <p>See "Relaxed Requirements for Address Data," page 41.</p> | ccAuthService (See description) | String (60) |
| billTo_ipAddress | Customer's IP address. | ccAuthService (O) | String (15) |

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 Request Fields (Continued)

| Field | Description | Used By: Required (R) or Optional (O) | Data Type (Length) |
|--------------------|---|---|-----------------------|
| billTo_lastName | <p>Customer's last name. For a credit card transaction, this name must match the name on the card.</p> <p>Important It is your responsibility to determine whether a field is required for the transaction you are requesting.</p> <p>See "Relaxed Requirements for Address Data," page 41.</p> | ccAuthService (See description) | String (60) |
| billTo_phoneNumber | <p>Customer's phone number. CyberSource recommends that you include the country code when the order is from outside the U.S.</p> | ccAuthService (O) | String (15) |
| billTo_postalCode | <p>Postal code for the billing address. The postal code must consist of 5 to 9 digits.</p> <p>When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits]</p> <p>Example 12345-6789</p> <p>When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric]</p> <p>Example A1B 2C3</p> <p>Important It is your responsibility to determine whether a field is required for the transaction you are requesting.</p> <p>See "Relaxed Requirements for Address Data," page 41.</p> | ccAuthService (See description) | String (9) |
| billTo_state | <p>State or province of the billing address. For an address in the U.S. or Canada, use the State, Province, and Territory Codes for the United States and Canada.</p> <p>Important It is your responsibility to determine whether a field is required for the transaction you are requesting.</p> <p>See "Relaxed Requirements for Address Data," page 41.</p> | ccAuthService (See description) | String (2) |

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

Table 5 Request Fields (Continued)

| Field | Description | Used By: Required (R) or Optional (O) | Data Type (Length) |
|----------------------|--|---|--------------------------|
| billTo_street1 | <p>First line of the billing street address.</p> <p>Important It is your responsibility to determine whether a field is required for the transaction you are requesting.</p> <p>See "Relaxed Requirements for Address Data," page 41.</p> | ccAuthService (See description) | String (60) |
| billTo_street2 | <p>Additional address information.</p> <p>Example Attention: Accounts Payable</p> | ccAuthService (R) | String (60) |
| card_accountNumber | <p>Payment network token value.</p> <p>This value is obtained by decrypting the customer's encrypted payment data.</p> | ccAuthService (R) | Nonnegative integer (20) |
| card_expirationMonth | <p>Two-digit month in which the payment network token expires.</p> <p>Format: MM.</p> <p>Possible values: 01 through 12.</p> | ccAuthService (R) | String (2) |
| card_expirationYear | <p>Four-digit year in which the payment network token expires.</p> <p>Format: YYYY.</p> | ccAuthService (R) | Nonnegative integer (4) |
| ccAuthService_cavv | <p>Visa</p> <p>Cryptogram for payment network tokens transactions. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats.</p> <p>American Express</p> <p>For a 20-byte cryptogram, set this field to the cryptogram for payment network tokens transactions. For a 40-byte cryptogram, set this field to block A of the cryptogram for payment network tokens transactions. The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats.</p> | ccAuthService (R) | String (40) |

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

Table 5 Request Fields (Continued)

| Field | Description | Used By: Required (R) or Optional (O) | Data Type (Length) |
|--|--|---|-----------------------|
| ccAuthService_ commerceIndicator | For a payment network tokens transaction. Possible values: <ul style="list-style-type: none"> ■ <code>aesk</code> for the American Express card type ■ <code>spa</code> for the Mastercard card type ■ <code>internet</code> for the Visa card type | ccAuthService (R) | String (20) |
| ccAuthService_ directoryServerTrans actionID | Identifier generated during the authentication transaction by the Mastercard Directory Server and passed back with the authentication results. | ccAuthService (O) | String (36) |
| ccAuthService_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 (O) | String (40) |
| ccAuthService_ paSpecificationVersion | The 3D Secure version that you used for strong customer authentication (SCA); for example, 3D Secure 1.0.2 or 2.0.0. | ccAuthService (O) | String (20) |
| ccAuthService_run | Whether to include ccAuthService in your request. Possible values: <ul style="list-style-type: none"> ■ <code>true</code>: Include the service in your request. ■ <code>false</code> (default): Do not include the service in your request. | ccAuthService (R) | String (5) |
| ccAuthService_xid | American Express For a 20-byte cryptogram, set this field to the cryptogram for payment network tokens transactions. For a 40-byte cryptogram, set this field to block A of the cryptogram for payment network tokens transactions (see "Merchant Decryption," page 20). The value for this field must be 28-character Base64 or 40-character hex binary. All cryptograms use one of these formats. | ccAuthService (R) | String (40) |

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

Table 5 Request Fields (Continued)

| Field | Description | Used By: Required (R) or Optional (O) | Data Type (Length) |
|-----------------------------|---|---|-----------------------|
| 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 <i>3ds.data</i> 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 <code>default</code> . See "Numbered Elements," page 40 . | ccAuthService (O) | String (255) |
| item##_productName | Name of the product. This field is required when the item##_productCode value is not <code>default</code> or one of the values related to shipping and/or handling. See "Numbered Elements," page 40 . | ccAuthService (See description) | String (255) |
| item##_productSKU | Identification code for the product. This field is required when the item##_productCode value is not <code>default</code> or one of the values related to shipping and/or handling. See "Numbered Elements," page 40 . | ccAuthService (See description) | String (255) |
| item##_quantity | Default is 1. This field is required when the item##_productCode value is not <code>default</code> or one of the values related to shipping and/or handling. See "Numbered Elements," page 40 . | ccAuthService (See description) | Integer (10) |
| item##_taxAmount | Total tax to apply to the product. This value cannot be negative. See "Numbered Elements," page 40 . | ccAuthService (See description) | String (15) |

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 Request Fields (Continued)

| Field | Description | Used By: Required (R) or Optional (O) | Data Type (Length) |
|------------------------------------|--|---|-----------------------|
| item_#_unitPrice | 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 "Numbered Elements," page 40 . | ccAuthService (See description) | String (15) |
| merchantID | Your CyberSource merchant ID. Use the same merchant ID for evaluation, testing, and production. | ccAuthService (R) | String (30) |
| merchantReferenceCode | Merchant-generated order reference or tracking number. CyberSource recommends that you send a unique value for each transaction so that you can perform meaningful searches for the transaction. For information about tracking orders, see <i>Getting Started with CyberSource Advanced for the Simple Order API</i> (PDF HTML). | ccAuthService (R) | String (50) |
| paymentNetworkToken_assuranceLevel | Confidence level of the tokenization. This value is assigned by the token service provider. Note This field is supported only for FDC Nashville Global. | ccAuthService (O) | String (2) |
| paymentNetworkToken_deviceTechType | 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. Note This field is supported only for FDC Compass. | ccAuthService (O) | Integer (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 Request Fields (Continued)

| Field | Description | Used By: Required (R) or Optional (O) | Data Type (Length) |
|---|--|---|-----------------------|
| paymentNetworkToken_ requestorID | Value that identifies your business and indicates that the cardholder's account number is tokenized. This value is assigned by the token service provider and is unique within the token service provider's database. Note This field is supported only for FDC Nashville Global and Chase Paymentech Solutions. | ccAuthService (O) | String (11) |
| paymentNetworkToken_ transactionType | Type of transaction that provided the token data. This value does not specify the token service provider; it specifies the entity that provided you with information about the token. Set the value for this field to 1. | ccAuthService (R) | String (1) |
| paymentSolution | Identifies Samsung Pay as the payment solution that is being used for the transaction: Set the value for this field to 008. Note This unique ID differentiates digital solution transactions within the CyberSource platform for reporting purposes. | ccAuthService (R) | String (3) |
| purchaseTotals_ currency | Currency used for the order: USD | ccAuthService (R) | String (5) |
| purchaseTotals_ grandTotalAmount | Grand total for the order. This value cannot be negative. You can include a decimal point (.), but you cannot include any other special characters. CyberSource truncates the amount to the correct number of decimal places. | ccAuthService (R) | String (15) |
| surchargeAmount | The surcharge 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. | ccAuthService (O) | String (15) |
| ucaf_authenticationData | Cryptogram for payment network tokens transactions with Mastercard. | ccAuthService (R) | String (32) |

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 Request Fields (Continued)

| Field | Description | Used By: Required (R) or Optional (O) | Data Type (Length) |
|--------------------------|---|---|------------------------------|
| ucaf_collectionIndicator | Required field for payment network tokens transactions with Mastercard. Set the value for this field to 2. | ccAuthService (R) | String with numbers only (1) |

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

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 Reply Fields

| Field | Description | Returned By | Data Type & Length |
|--------------------------------|--|-------------|--------------------|
| card_suffix | Last four digits of the cardholder's account number. This field is returned only for tokenized transactions. You can use this value on the receipt that you give to the cardholder. This field is returned only for FDC Nashville Global. | ccAuthReply | String (4) |
| ccAuthReply_amount | Amount that was authorized. | ccAuthReply | String (15) |
| ccAuthReply_authorizationCode | Authorization code. Returned only when the processor returns this value. | ccAuthReply | String (7) |
| ccAuthReply_authorizedDateTime | Time of authorization. | ccAuthReply | Date and time (20) |

Table 6 Reply Fields (Continued)

| Field | Description | Returned By | Data Type & Length |
|---------------------------------------|--|-------------|--------------------|
| ccAuthReply_avsCode | AVS results. See <i>Credit Card Services Using the Simple Order API</i> (PDF HTML) for a detailed list of AVS codes. | ccAuthReply | String (1) |
| ccAuthReply_avsCodeRaw | AVS result code sent directly from the processor. Returned only when the processor returns this value. | ccAuthReply | String (10) |
| ccAuthReply_cvCode | CVN result code. See <i>Credit Card Services Using the Simple Order API</i> (PDF HTML) for a detailed list of CVN codes. | ccAuthReply | String (1) |
| ccAuthReply_cvCodeRaw | CVN result code sent directly from the processor. Returned only when the processor returns this value. | ccAuthReply | String (10) |
| ccAuthReply_processorResponse | For most processors, this is the error message sent directly from the bank. Returned only when the processor returns this value. | ccAuthReply | String (10) |
| ccAuthReply_reasonCode | Numeric value corresponding to the result of the credit card authorization request. See <i>Credit Card Services Using the Simple Order API</i> (PDF HTML) for a detailed list of reason codes. | ccAuthReply | Integer (5) |
| ccAuthReply_reconciliationID | Reference number for the transaction. This value is not returned for all processors. | ccAuthReply | String (60) |
| decision | Summarizes the result of the overall request. Possible values: <ul style="list-style-type: none"> ■ ACCEPT ■ ERROR ■ REJECT ■ REVIEW: Returned only when you use CyberSource Decision Manager. | ccAuthReply | String (6) |
| invalidField_0 through invalidField_N | Fields in the request that contained invalid data. For information about missing or invalid fields, see <i>Getting Started with CyberSource Advanced for the Simple Order API</i> (PDF HTML). | ccAuthReply | String (100) |
| merchantReferenceCode | Order reference or tracking number that you provided in the request. If you included multi-byte characters in this field in the request, the returned value might include corrupt characters. | ccAuthReply | String (50) |

Table 6 Reply Fields (Continued)

| Field | Description | Returned By | Data Type & Length |
|---------------------------------------|---|-------------|--------------------|
| missingField_0 through missingField_N | Required fields that were missing from the request. For information about missing or invalid fields, see <i>Getting Started with CyberSource Advanced for the Simple Order API</i> (PDF HTML). | ccAuthReply | String (100) |
| 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 <i>Credit Card Services Using the Simple Order API</i> (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 Reply Fields (Continued)

| Field | Description | Returned By | Data Type & Length |
|--------------|--|--------------------|-------------------------------|
| token_prefix | First 6 digits of token. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction. | ccAuthReply | String (6) |
| token_suffix | Last 4 digits of token. CyberSource includes this field in the reply message when it decrypts the payment blob for the tokenized transaction. | ccAuthReply | String (4) |