CyberSource Secure Acceptance Web/Mobile

Configuration Guide

August 2013

CyberSource®
the power of payment

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

CyberSource Contact Information

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

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

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

Copyright

Restricted Rights Legends

Trademarks

Contents

Recent Revisions to This Document

Release Date	Changes
August 2013	■ Updated the “Customizing the Appearance and Branding” section. See page 28. ■ Updated the “Localization” section. See page 31. ■ Added “Standalone Payment Token” section. See page 37. ■ Updated the “Examples” appendix. See page 81.
June 2013	■ Added the “Enabling eChecks” section. See page 18. ■ Added the following API request fields (see page 51): • company_tax_id • driver_license_number • driver_license_state • echeck_account_number • echeck_account_type • echeck_check_number • echeck_routing_number • echeck_sec_code ■ Added the following API reply fields (see page page 63): • req_company_tax_id • req_driver_license_number • req_driver_license_state • req_echeck_account_number • req_echeck_account_type • req_echeck_check_number • echeck_debit_ref_no • echeck_debit_submit_time • req_echeck_routing_number • req_echeck_sec_code • service_fee_amount • service_fee_return_url ■ Updated the “Reason Codes” table. See page 80.
May 2013	■ Added the “Enabling the Service Fee” section. See page 18. ■ Updated the “Reason Codes” section. See page 80.

Release Date	Changes
March 2013	■ Updated the “Viewing Transactions in the Business Center” section. See page 42.
February 2013	■ Updated the "Creating a Security Key" chapter. See page 19. ■ Updated the "Configuring Payer Authentication" section. See page 16. ■ Added the **bill_payment** API request field. See page 53. ■ Added the **req_bill_payment** API reply field. See page 63. ■ Updated the **bill_to_address_state** API request field. See page 53. ■ Updated the **req_bill_to_address_state** API reply field. See page 63.
January 2013	■ Reorganized the document: • Removed the “Payment Tokenization” chapter. • Added the "one-click Checkout" section. See page 12. • Added the "Creating a Payment Token" chapter. See page 13. • Added the "Using a Payment Token" chapter. See page 41. • Added the "Updating a Payment Token" chapter. See page 44. • Created the “Using Decision Manager” chapter. See page 47. ■ Updated the following API request fields: • transaction_type • reference_number • signed_date_time ■ Added the **allow_payment_token_update** field. See "API Fields," page 50. ■ Added the one-click checkout endpoint. See "Invoking Secure Acceptance," page 33. ■ Updated the “Examples” appendix. See page 81.

About This Guide

Audience

This guide is written for merchants who want to accept payments on a secure checkout hosted by CyberSource but who don't want to handle or store sensitive payment information on their own servers.

Using Secure Acceptance Web/Mobile requires minimal scripting skills. You must create a security script and modify your HTML form to invoke Secure Acceptance. You will also use the Business Center to review and manage orders.

Purpose

This guide describes tasks you must complete to create, customize, and invoke Secure Acceptance You will use the Business Center to customize the appearance and branding of Secure Acceptance, providing a seamless customer checkout experience from your web site to Secure Acceptance.

Conventions

Note

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

Important

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

A *Warning* contains information or instructions, which, if not heeded, can result in a security risk, irreversible loss of data, or significant cost in time or revenue or both.

Related Documentation

- *Payer Authentication Using the SCMP API* describes how to use the payer authentication services.
- *Reporting Developer Guide* describes how to view and configure Business Center reports.
- *Secure Acceptance Silent Order POST Development Guide* describes how to create and integrate your checkout with the Secure Acceptance Silent Order POST.
- *Payment Tokenization Using the Business Center* describes how to create and use payment tokens.
- *Decision Manager Developer Guide Using the SCMP API* describes how to integrate and use the Decision Manager services.
- Payment Card Industry Data Security Standard (PCI DSS) web site offers standards and supporting materials to enhance payment card data security.

CHAPTER 1

Using Secure Acceptance Web/Mobile

CyberSource Secure Acceptance Web/Mobile is your secure hosted customer checkout experience. It consists of securely managed payment forms for processing transactions enabling you to decrease your Payment Card Industry Data Security Standard (PCI DSS) obligations reducing any risks associated with handling or storing sensitive payment information. You, the merchant, out-source payments to Secure Acceptance, which is designed to accept card payments.

To create your customer's Secure Acceptance experience, you take these steps:

1. Create and configure Secure Acceptance profiles.
2. Update the code on your web site to invoke Secure Acceptance and immediately process card transactions. Sensitive card data bypasses your network and is accepted by Secure Acceptance directly from the customer. CyberSource processes the transaction on your behalf by sending an approval request to your payment processor in real time.
3. Use the reply information to display an appropriate transaction response page to the customer. You can view and manage all orders in the Business Center.

Secure Acceptance Profile

A Secure Acceptance profile consists of settings that you configure to create a customer checkout experience. You can create and edit multiple profiles, each offering a custom checkout experience. For example, you might need multiple profiles for localized branding of your web sites.You can display a multi-step checkout process to the customer as well as configure the appearance and branding, payment options, languages, and customer notifications.

Payment Tokens

Important Contact CyberSource Customer Support to activate your merchant account for the use of the payment tokenization services. You cannot use payment tokenization services until your account is activated and you have enabled payment tokenization for Secure Acceptance (see page 13.)

Payment Tokenization replaces sensitive credit card information with a unique identifier that cannot be mathematically reversed. CyberSource securely stores all the card information, replacing it with the payment token, also known as a *subscription ID*, which you store on your server.

The payment token identifies the card and retrieves the associated billing, shipping, and card information. No sensitive card information is stored on your servers, therefore reducing your PCI DSS obligations.

The payment tokenization solution is compatible with the Visa and MasterCard Account Updater service. All payment information stored with CyberSource is automatically updated by participating banks, thereby reducing payment failures. See the *Account Updater User Guide*.

There are three types of payment tokens:

- 16 digit—displays the last 4 digits of the primary account number (PAN) and passes Luhn mod-10 checks.
- 16 digit—displays 99 as the two leading digits and passes Luhn mod-10 checks. If your business rules prohibit using 99 as the leading digits, you must modify your system to accept the other 16-digit payment token.
- 22 digit—this is the default payment token.

Note The billing, shipping, and card information is displayed on the Order Review page of Secure Acceptance.

one-click Checkout

With *one-click Checkout*, customers can buy products with a single click. Before a customer can use one-click Checkout, he or she must create a payment token during the first transaction on the merchant web site. See "Payment Token for a one-click Checkout Transaction," page 38. The payment token is an identifier for the payment details; therefore, no further purchases require entering any information. When the payment token is included in a payment request, it retrieves the card, billing, and shipping information related to the original payment request from the CyberSource database.

To use one-click Checkout, you must include the one-click Checkout endpoint to process the transaction. See "Invoking Secure Acceptance," page 33.

Subscription Payments

A customer subscription contains information that you store in the CyberSource database and use for future billing. At any time, you can send a request to bill the customer for an amount you specify, and CyberSource uses the payment token to retrieve the card, billing, and shipping information to process the transaction. You can also view the customer subscription in the CyberSource Business Center. See "Viewing Transactions in the Business Center," page 42.

A customer subscription includes:

- Customer contact information, such as billing and shipping information.
- Customer payment information, such as card type, masked account number, and expiration date.
- Customer order information, such as the transaction reference number and merchant-defined data fields.

Type of Subscription	Description
Recurring	A recurring billing service with no specific end date. You must specify the amount and frequency of each payment and the start date for processing the payments. CyberSource creates a schedule based on this information and automatically bills the customer according to the schedule. For example, you can offer an online service that the customer subscribes to and can charge a monthly fee for this service. See "Payment Token for Recurring Payments," page 39.
Installment	A recurring billing service with a fixed number of scheduled payments. You must specify the number of payments, the amount and frequency of each payment, and the start date for processing the payments. CyberSource creates a schedule based on this information and automatically bills the customer according to the schedule. For example, you can offer a product for 75 USD and let the customer pay in three installments of 25 USD. See "Payment Token for Installment Payments," page 40.

CHAPTER 2

Creating a Web/Mobile Profile

Important This chapter is written for first-time users of Secure Acceptance. If you have already created a Web/Mobile profile, see "Updating a Secure Acceptance Profile." Contact CyberSource Customer Support to enable your account for Secure Acceptance.

To create a Web/Mobile profile:

Step 1 Log in to the Business Center:

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

Step 2 In the left navigation panel, choose **Tools & Settings > Secure Acceptance > Profiles**.

Step 3 Enter a profile name. The profile name is required and cannot exceed 20 alphanumeric characters.

Step 4 Enter a profile ID. The profile ID is case sensitive and must be exactly 7 alphanumeric characters. This field is required. It is used in each transaction to identify and display the Secure Acceptance profile.

Step 5 Enter a profile description. The description cannot exceed 255 characters.

Step 6 Check **Web/Mobile**.

Step 7 Enter a company name. The company name is required and cannot exceed 40 alphanumeric characters.

Step 8 Enter company contact information: name, email, and phone number.

Step 9 Check **Payment Tokenization.** For more information, see page 37.

Step 10 Check **Decision Manager**. For more information, see page 47.

Step 11 Check **Enable Verbose Data**. For more information, see page 47.

Step 12 Click **Create**. The Profile Settings page appears.

Profile Settings

Configure the profile settings to create your customer checkout experience.

Important

*****You must activate a profile in order to use it. You must configure these required fields before activating a profile:

- Configuring Payment Settings
- Creating a Security Key
- Displaying a Customer Response Page

Creating a Web/Mobile Profile

- Profile name, ID, description
- Integration method
- Company information
- Value added services

Note You completed this task on page 13.

Configuring Notifications

- Merchant POST URL
- Merchant POST email
- Merchant receipt email
- Customer receipt email

Configuring Payment Settings*****

- Payment types, currencies
- CVN, payer authentication
- Auto authorization reversal

Displaying a Customer Response Page*****

- CyberSource response pages
- Custom response page URL
- Custom return page URL

Creating a Security Key*****

- Signature version and method
- Access key, secret key
- Key activation

Customizing the Appearance and Branding

- Customize header and footer
- Customize main body

Upload logos and images

Configuring the Payment Form

- Billing and shipping information
- Tax amount display
- Order review display

Localization

- Supported languages
- Locale codes

Additional Options for a Profile

- Deactivate—deactivates the active profile. The profile is now listed in the inactive profile list. Available only for an active profile.
- Create Editable Version—duplicates the active profile. The editable version is listed in the inactive profile list. Available only for an active profile.
- Promote to Active—activates the inactive profile. Available only for an inactive profile.

Configuring Payment Settings

You must select the card types to offer to the customer as payment methods. For each card type you select you can also manage currencies, CVNs, and payer authentication options. Select only the types of credit cards and currencies that your merchant account provider authorizes.


Note

The Card Verification Number (CVN) is a three- or four-digit number printed on the back or front of a credit card. This number helps ensure that the customer has possession of the card at the time of the transaction.

Adding a Card Type

To add a card type and enable the CVN:

Step 1 On the Profile Settings page, click **Payment Settings**. The Payment Settings page appears.

Step 2 Click **Add/Edit Card Types**. The Add/Edit Card Types window appears.

Step 3 Check each card type that you want to offer to the customer as a payment method.

Step 4 Click **Update**.

Step 5 Click the pencil icon in the column for each card type. The Edit Card Settings page appears.

Step 6 Check **CVN Display** to display the CVN field on Secure Acceptance. The customer decides whether to enter the CVN.

Step 7 Check **CVN Required**. The CVN Display option must also be checked. If this option is checked, the customer is required to enter the CVN.

Step 8 Click **Update**. The card types are added as an accepted payment type.

Step 9 Click **Save**.

Configuring Payer Authentication

Important

Before you can use CyberSource Payer Authentication, you must contact CyberSource Customer Support to provide information about your company and your acquiring bank so that CyberSource may configure your account. Your merchant ID must be enabled for payer authentication. See *Payer Authentication Using the SCMP API*.

Payer authentication enables you to add support for Verified by Visa, MasterCard SecureCode, and American Express SafeKey without running additional software on your own server. The payer authentication services deter unauthorized card use and provide added protection from fraudulent chargeback activity.

For each transaction, you receive detailed information in the replies and in the transaction details page of the Business Center. You can store this information for up to 12 months. CyberSource recommends that you store the payer authentication data because you may be required to display this information as proof of enrollment verification for any payer authentication transaction that you re-present because of a chargeback. Your account provider may require that you provide all data in human-readable format. Make sure that you can decode the PAReq and PARes.

Note

The language used on each Payer Authentication page is determined by your issuing bank and overrides the locale you have specified. If you use the test card numbers for testing purposes the default language used on the Payer Authentication page is English, and overrides the locale you have specified. See "Testing Transactions," page 49.

To configure payer authentication:

Step 1 On the Profile Settings page, click **Payment Settings**. The Payment Settings page appears.

Step 2 Click the pencil icon in the column for each card type. The **Edit Card Settings** page appears.

Step 3 Check **Payer Authentication** for each card type that you want to offer to the customer as a payment method. The card types that support payer authentication are:

- Amex
- MasterCard
- Maestro (UK Domestic or International)
- Visa

Step 4 Click **Update**.

Adding a Currency

Important By default, all currencies are listed as disabled. You must select at least one currency. Contact your merchant account provider for a list of supported currencies.

To add a supported currency for each card type:

Step 1 On the Profile Settings page, click **Payment Settings**. The Payment Settings page appears.

Step 2 Click the pencil icon in the column for each card type. The Edit Card Settings page appears.

Step 3 Click **Select All** or select a currency and use the arrow to move it from the Disabled list to the Enabled list.

Step 4 Click **Update**.

Enabling Automatic Authorization Reversals

For transactions that fail to return an Address Verification System (AVS) or a Card Verification Number (CVN) match, you can enable Secure Acceptance to perform an automatic authorization reversals. An automatic reversal releases the reserved funds held against a customer's card.

To enable automatic authorization reversals:

Step 1 On the Profile Settings page, click **Payment Settings**. The Payment Settings page appears.

Step 2 Check **Fails AVS check**. Authorization is automatically reversed on a transaction that fails an AVS check.

Step 3 Check **Fails CVN check**. Authorization is automatically reversed on a transaction that fails a CVN check.

Step 4 Click **Save**.

Enabling eChecks

An eCheck is a payment made directly from your customer's U.S. or Canadian bank account. As part of the checkout process, you must display a terms and conditions statement for eChecks. Within the terms and conditions statement it is recommended to include a link to the table of returned item fees. The table lists by state the amount that your customer has to pay when a check is returned.

To enable the eCheck payment option:

Step 1 On the Profile Settings page, click **Payment Settings**. The Payment Settings page appears.

Step 2 Check **eCheck payments enabled**.

Step 3 Click the pencil icon in the currencies table. The Electronic Check Settings page appears.

Step 4 Click **Select All** or select a currency and use the arrow to move it from the Disabled list to the Enabled list.

Step 5 Click **Update**.

Step 6 Click **Save**. You must configure the eCheck information fields. See "Displaying eCheck Information Fields," page 24.

Enabling the Service Fee

Important Contact CyberSource Customer Support to have your CyberSource account configured for this feature. Service fees are supported only if Wells Fargo is your acquiring bank and FDC Nashville is your payment processor.

As part of the checkout process, you must display a terms and conditions statement for the service fee. A customer must accept the terms and conditions before submitting an order.

To enable the service fee:

Step 1 On the Profile Settings page, click **Payment Settings**. The Payment Settings page appears.

Step 2 Check **Service Fee applies on transactions using this profile**. The service fee terms and conditions URL and the service fee amount are added to the customer review page.

Warning

Transactions will fail if you disable this feature. Do not disable this feature unless instructed to do so by your account manager.

Step 3 Click **Save**.

Important

After you save the profile you cannot disable the service fee functionality for that profile. All transactions using the profile will include the service fee amount.

Creating a Security Key

The security script signs the request fields using the secret key and the HMAC SHA256 algorithm. To verify data, the security script generates a signature to compare with the signature returned from the Secure Acceptance server. You must have an active security key to activate a profile. A security key expires after 2 years. The security key protects each transaction from data tampering.

Important

You cannot use the same security key for both test and live transactions. You must download a security key for both versions of Secure Acceptance:

- For live transactions: https://ebc.cybersource.com
- For test transactions: https://ebctest.cybersource.com

To create and activate a security key:

Step 1 On the Profile Settings page, click **Security**. The Security Keys page appears.

Step 2 Click **Create New Key**. The Create New Key page appears.

Step 3 Enter a key name (required).

Step 4 Choose signature version **Version 1**.

Step 5 Choose signature method **HMAC-SHA256**.

Step 6 Click **Generate Key**. The Create New Key window expands and displays the new access key and secret key. This window closes after 30 seconds.

Step 7 Copy and save the access key and secret key.

- Access key: Secure Sockets Layer (SSL) authentication with Secure Acceptance. You can have many access keys per profile. See page 33.
- Secret key: signs the transaction data and is required for each transaction. Copy and paste this secret key into your security script. See page 33.

By default, the new security key is active. The other options for each security key are:

- Deactivate: deactivates the security key. The security key is inactive.
- Activate: activates an inactive security key.
- View: displays the access key and security key.

Note When you create a security key, it is displayed in the security keys table. You can select a table row to display the access key and the secret key for that specific security key.

Step 8 Click **Return to Profile home**. The Profile Settings page appears.

Configuring the Payment Form

The payment form is the customer's checkout experience. It consists of a series of windows in which the customer enters or reviews information before submitting a transaction. Select the fields that you want displayed on each screen of the checkout process: billing, shipping, payment, and order review. The customer enters or reviews information in the order.

Displaying the Tax Amount

Follow these steps to display the total tax amount of the transaction as a separate line on each window of the checkout process. The total tax amount must be included in each transaction.

To display the tax amount:

Step 1 On the Profile Settings page, click **Payment Form**. The Payment Form page appears.

Step 2 Check **Display the total tax amount in each step of the checkout process**.

Important

Calculate and include the total tax amount in the **tax_amount** API field. See "Invoking Secure Acceptance," page 33.

Note

Do not click **Save** until you have selected the billing or shipping fields, or both.

Step 3 Click **Save**. The Profile Settings page appears.

Displaying Billing Information Fields

Select the customer billing information fields that you want displayed on Secure Acceptance.

To display and edit billing information fields:

Step 1 On the Profile Settings page, click **Payment Form**. The Payment Form page appears.

Step 2 Check **Billing Information.** The billing information fields appear.

Step 3 Check the billing information fields to be included in Secure Acceptance. The options for each field are:

- Display: the customer can view the information contained in this field. Choose this option if you want to populate the fields before invoking Secure Acceptance.
- Edit: the customer can view and edit the information contained in this field.
- Require: the customer is required to enter information in this field to submit the transaction. When you select this option, all other options are automatically selected.

Note Do not click **Save** until you have selected the shipping and order review fields.

Step 4 Click **Save**. The Profile Settings page appears.

Displaying Shipping Information Fields

Select the customer shipping information fields that you want displayed on Secure Acceptance. These fields are optional. If you do not add these fields, the shipping information step is removed from Secure Acceptance.

To display and edit shipping information fields:

Step 1 On the Profile Settings page, click **Payment Form**. The Payment Form page appears.

Step 2 Check **Shipping Information.**

Step 3 Check the shipping information fields to be included in Secure Acceptance. The options for each field are:

- Display: the customer can view the information contained in this field. Choose this option if you want to populate the fields before invoking Secure Acceptance.
- Edit: the customer can view and edit the information contained in this field.
- Require: the customer is required to enter information in this field to submit the transaction. When you select this option, all other options are automatically selected.

Note Do not click **Save** until you have selected the billing and order review fields.

Step 4 Click **Save**. The Profile Settings page appears.

Displaying eCheck Information Fields

Select the customer eCheck information fields that you want displayed on Secure Acceptance.

To display and edit eCheck information fields:

Step 1 On the Profile Settings page, click **Payment Form**. The Payment Form page appears.

Step 2 Check the eCheck information fields to be included in Secure Acceptance. The options for each field are:

- Display: the customer can view the information contained in this field. Choose this option if you want to populate the fields before invoking Secure Acceptance.
- Edit: the customer can view and edit the information contained in this field.
- Require: the customer is required to enter information in this field to before submitting the transaction. When you select this option, all other options are automatically selected.

Note Do not click **Save** until you have selected the billing and order review fields.

Step 3 Click **Save**. The Profile Settings page appears.

Customizing Order Review

Select the fields that you want displayed on the Order Review page of Secure Acceptance. The customer reviews this information before submitting the transaction.

To display and edit order review fields:

Step 1 On the Profile Settings page, click **Payment Form**. The Payment Form page appears.

Step 2 Check the fields that you want displayed on the Order Review page of Secure Acceptance. The options for each field are:

- Display: the customer can view the information contained in this field. Available only for billing and shipping information.
- Edit: the customer can view and edit the information contained in this field.

Step 3 Click **Save**. The Profile Settings page appears.

Configuring Notifications

Secure Acceptance sends merchant and customer notifications in response to transactions.

Configuring Merchant Notifications

You can receive a merchant notification by email or as an HTTP POST to a URL for each transaction processed. Both notifications contain the same transaction result data. Choose the card number digits that you want displayed in each notification. Parse or process the transaction data contained in each notification.

To configure merchant notifications:

Step 1 On the Profile Settings page, click **Notifications**. The Notifications page appears.

Step 2 Choose a merchant notification in one of two ways:

- Check Merchant POST URL. Enter the **URL**. CyberSource sends transaction information to this URL. For more information, see "API Fields," page 50.

Important Use ports 80, 443, or 8080 in the URL. Contact CyberSource Customer Support if you encounter problems using an HTTPS-based URL.

- Check Merchant POST Email. Enter your email address.

Note CyberSource sends transaction response information to this email address including payment information, return codes, and all relevant order information.

Step 3 Choose the card number digits that you want displayed in the merchant or customer receipt:

- Return credit card BIN: displays the card's Bank Identification Number (BIN), which is the first six digits of the card number. All other digits are masked: 123456xxxxxxxxxx
- Return last 4 digits of credit card number: displays the last four digits of the card number. All other digits are masked: xxxxxxxxxxxx1234
- Return BIN and last 4 digits of credit card number: displays the BIN and the last four digits of the card number. All other digits are masked: 123456xxxxxx1234

Step 4 Continue to configure the customer notifications (see page 26) or click **Save**. The Profile Settings page appears.

Configuring Customer Notifications

You can send a purchase receipt email to your customer and a copy to your own email address. Both are optional. Customers may reply with questions regarding their purchases, so use an active email account. The email format is HTML unless your customer email is rich text format (RTF).

To configure customer notifications:

Step 1 On the Profile Settings page, click **Notifications**. The Notifications page appears.

Step 2 Check **Email Receipt to Customer.**

Step 3 Enter the email address to be displayed on the customer receipt. The customer will reply to this email with any queries.

Step 4 Enter the name of your business. It is displayed on the customer receipt.

Step 5 Check **Send a copy to**. This setting is optional.

Step 6 Enter your email address to receive a copy of the customer's receipt.

Note

Your copy of the customer receipt will contain additional transaction response information.

Step 7 Click **Save**. The Profile Settings page appears.

Company Logo

You can upload a company logo to display on customer notifications.

To add a logo to the customer receipt and email:

Step 1 On the Profile Settings page, click **Appearance and Branding**. The Appearance and Branding window appears.

Step 2 Check **Display Notification Logo**.

Step 3 Click **Upload Company Logo**. Find and upload the image that you want to display on the customer receipt and email.

Important

For preview, an image must not exceed 200 (w) x 60 (h) pixels. The image file type must be GIF, JPEG, or PNG.

Step 4 Click **Save**.

Displaying a Customer Response Page

You can choose to display a response page to the customer at the end of the checkout process. Enter a URL for your own customer response page or use the CyberSource hosted response pages. Depending upon the transaction result, the CyberSource hosted response pages are Accept, Decline, or Error. Review declined orders as soon as possible because you may be able to correct problems related to address or card verification, or you may be able to obtain a verbal authorization. You can also choose to display a web page to the customer after the checkout process is completed.

CyberSource Hosted Response Page

To display a CyberSource hosted response page:

Step 1 On the Profile Settings page, click **Customer Response Pages**. The Customer Response Pages page appears.

Step 2 Check **Hosted by CyberSource**.

Step 3 Choose a number from the **Decline Retry Limit** drop-down list. The maximum number of times a customer can retry a declined transaction is 5.

Step 4 Enter the redirect URL of the web page. This web page is displayed to the customer after the checkout process is completed.

Step 5 Click **Save**. The Profile Settings page appears.

Custom Response Page

To display your custom response page:

Step 1 On the Profile Settings page, click **Customer Response Pages**. The Customer Response Pages page appears.

Step 2 Check **Hosted by you**.

Step 3 Enter the URL for your customer response page. Use port 80, 443, or 8080 in the URL.


Note

Parse the transaction results from the URL according to the reason code, and redirect your customer to the appropriate response page. For more information, see "API Fields," page 50.

Step 4 Click **Save**. The Profile Settings page appears.

Customizing the Appearance and Branding

Customize the appearance and branding of Secure Acceptance. Choose a background color, font, and text color. Upload a logo or image, and align it within the header or footer.


Important

If you customize the appearance and branding of the payment form CyberSource strongly recommends that you preview your changes in the Image Preview window. For preview, the image must not exceed 200 (w) x 60 (h) pixels.

To change the header color and upload an image:

Step 1 On the Profile Settings page, click **Appearance and Branding**. The Appearance and Branding page appears.

Step 2 Check **Display Header**. Checked by default.

Step 3 Choose a color in one of two ways:

- Enter a hexadecimal value for the header color of the payment form.
- Click within the header color palette to choose a color. Click the icon at the bottom right to confirm your selection.

Step 4 Click **Upload Header Image**. Find and upload the image to display as the header banner or as a logo within the header banner.

Important To display an image as the header banner of the payment form, the image size must not exceed 840 (w) x 60 (h) pixels. To display a small logo within the header banner, the logo height must not exceed 60 pixels. The image file type must be GIF, JPEG, or PNG.

Step 5 Check an alignment option for the image or logo: left-aligned, centered, or right-aligned.

Step 6 Click **Save**.

Step 7 Click **Set to Default** to set all the default settings on this page.

To change the main body color and font settings:

Step 1 On the Profile Settings page, click **Appearance and Branding**. The Appearance and Branding window appears.

Step 2 Choose a color in one of two ways:

- Enter a hexadecimal value for the background color of the payment form.
- Click within the background color palette to choose a color. Click the icon at the bottom right to confirm your selection.

Step 3 Choose the style of text to be displayed.

Step 4 Choose a color in one of two ways:

- Enter a hexadecimal value for the text color of the payment form.
- Click within the text color palette and select a color. Click the icon at the bottom right to confirm your selection.

Step 5 Click **Save**.

Step 6 Click **Set to Default** to set all the default settings on this page.

To change the background color and font color of the total amount:

Step 1 On the Profile Settings page, click **Appearance and Branding**. The Appearance and Branding window appears.

Step 2 Choose a background color in one of two ways:

- Enter a hexadecimal value for the background color of the total amount box.
- Click within the background color palette to choose a color. Click the icon at the bottom right to confirm your selection.

Step 3 Choose a text color in one of two ways:

- Enter a hexadecimal value for the text color of the total amount.
- Click within the text color palette and select a color. Click the icon at the bottom right to confirm your selection.

Step 4 Click **Save**.

Step 5 Click **Set to Default** to set all the default settings on this page.

To change the footer color and upload a small logo or image:

Step 1 On the Profile Settings page, click **Appearance and Branding**. The Appearance and Branding window appears.

Step 2 Check **Display Footer**.

Step 3 Choose a color in one of two ways:

- Enter a hexadecimal value for the footer color of the payment form.
- Click within the footer color palette to choose a color. Click the icon at the bottom right to confirm your selection.

Step 4 Click **Upload Footer Image**. Find and upload the image that you want to display within the footer.

Important To display a small logo in the footer of the payment form, the logo height must not exceed 60 pixels. The image file type must be GIF, JPEG, or PNG.

Step 5 Check an alignment option for the image or logo: left-aligned, centered, or right-aligned.

Important For preview, an image must not exceed 200 (w) x 60 (h) pixels.

Step 6 Click **Save**.

Step 7 Click **Set to Default** to set all the default settings on this page.

Localization

Secure Acceptance supports 27 languages for localization purposes. The table below lists all the supported languages and the locale code you must include in your HTML form. Click **Return to Profile home**. The Profile Settings page appears.

To specify and display the local language on Secure Acceptance:

Step 1 Include the **locale** API field in your HTML form.

Step 2 Enter the locale code in the API field. See "Invoking Secure Acceptance," page 33.

Example American English

```
<input type="hidden" name="locale" value="en-us">
```

Step 3 Click **Return to Profile home**. The Profile Settings page appears.

Table 1 Locale Codes

Language	Locale Code
Arabic	ar-XN
Cambodia	km-KH
Chinese - Hong Kong	zh-HK
Chinese - Maco	zh-MO
Chinese - Mainland	zh-CN
Chinese - Singapore	zh-SG
Chinese - Taiwan	zh-TW
Czech	cz-CZ
Dutch	nl-nl
English - American	en-US
English - Australia	en-AU
English - Britain	en-GB
English - Canada	en-CA
English - Ireland	en-IE
English - New Zealand	en-NZ

Table 1 Locale Codes (Continued)

Language	Locale Code
French	fr-FR
French - Canada	fr-CA
German	de-DE
German - Austria	de-AT
Hungary	hu-HU
Indonesian	id-ID
Italian	it-IT
Japanese	ja-JP
Korean	ko-KR
Lao People's Democratic Republic	lo-LA
Malaysian Bahasa	ms-MY
Philippines Tagalog	tl-PH
Polish	pl-PL
Portuguese - Brazil	pt-BR
Russian	ru-RU
Slovakian	sk-SK
Spanish	es-ES
Spanish - Argentina	es-AR
Spanish - Chile	es-CL
Spanish - Colombia	es-CO
Spanish - Mexico	es-MX
Spanish - Peru	es-PE
Spanish - American	es-US
Thai	th-TH
Turkish	tr-TR
Vietnamese	vi-VN

Activating a Profile

Important

You must configure these required fields before activating a profile:

- Configuring Payment Settings
- Creating a Security Key
- Displaying a Customer Response Page

To activate a profile:

Step 1 On the Profile Settings page, click **Promote to Active**. The profile is now active and listed as an active profile on the Manage Profiles page.

Note

The All Profiles link appears on the Profile Settings page. Click **All Profiles** to view the Manage Profiles list. See "Updating a Secure Acceptance Profile," page 35.

Invoking Secure Acceptance

Important

Secure Acceptance can support any dynamic scripting language that supports HMAC256 hashing algorithms. The available downloads are samples, and each sample consists of a security script, a payment form, a payment confirmation page, and a receipt page.

Depending on the scripting language that you use, the following samples are available for download:

- JSP
- ASP.NET (C#)
- Ruby
- PHP
- Perl
- VB

To invoke and display Secure Acceptance:

Step 1 In the security script sample, enter your security key into the **SECRET_KEY** field. See "Creating a Security Key," page 19.

Step 2 In the payment form, paste your access key and profile ID into their respective fields. See "Creating a Security Key." Additional API fields can be added to this form if you want the fields pre-populated when Secure Acceptance is invoked. See "Optional API Request Fields," page 53.

Step 3 In the payment confirmation page, enter the endpoint for processing either test or live transactions:

Standard transaction endpoints (non-token based):

- Test transactions: https://testsecureacceptance.cybersource.com/pay
- Live transactions: https://secureacceptance.cybersource.com/pay

One-click transaction endpoints:

- Test transactions: https://testsecureacceptance.cybersource.com/oneclick/pay
- Live transactions: https://secureacceptance.cybersource.com/oneclick/pay

Create standalone token endpoints:

- Test transactions: https://testsecureacceptance.cybersource.com/token/create
- Live transactions: https://secureacceptance.cybersource.com/token/create

CHAPTER 3

Updating a Secure Acceptance Profile

Profile status can be active or inactive:

- Active: the live Secure Acceptanceprofile. This is your current profile, and it is read-only. You can have more than one active profile.
- Inactive: the version of a new profile before activation, or the editable version of an active profile. Update and activate this profile to replace the current active profile.

Important If you have multiple profiles the Manage Profiles page appears by default when you log in to the Business Center.

To update a profile:

Step 1 Log in to the Business Center:

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

Step 2 In the left navigation panel, choose **Tools & Settings > Secure Acceptance > Profiles**.

Step 3 Check the active or inactive profile.

The options for an active profile are:

- Deactivate: deactivates the active profile. The profile is then listed in the inactive profile list.
- Edit: select edit and update the active profile. An editable version of the active profile appears in the inactive profile list. To activate this inactive profile, click **Promote to Active**.
- Copy: duplicates the active profile. The duplicate profile (editable version) is listed in the inactive profile list.

The options for an inactive profile are:

- Promote to Active: promotes the inactive profile to the active profile list. It replaces the current active profile, and it is removed from the inactive profile list.
- Delete: deletes the inactive profile.
- Copy: duplicates the inactive profile. The duplicate profile (editable version) is listed in the inactive profile list.

Note You can also click the pencil icon to edit an inactive profile.

Step 4 Click **Continue**. The Profile Settings page appears.

Step 5 Update the inactive profile (editable version). See "Creating a Web/Mobile Profile," page 13.

Step 6 Activate the inactive profile. See "Activating a Profile," page 33**.**

Important When you activate an inactive profile, it replaces the current active profile and is removed from the inactive profile list on the Manage Profiles page.

Step 7 Click **All Profiles** to view the active and inactive profiles you have created.

Important If you have multiple profiles the Manage Profiles page appears by default when you log in to the Business Center and choose **Tools & Settings > Secure Acceptance > Profiles**.

CHAPTER 4

Creating a Payment Token

Standalone Payment Token

For an eCheck Customer

To create a standalone payment token for an eCheck customer:

Step 1 Set the endpoint to:

- Test transactions: https://testsecureacceptance.cybersource.com/token/create
- Live transactions: https://secureacceptance.cybersource.com/token/create

Step 2 Set the **transaction_type** field to **create_payment_token**.

Step 3 Include the following fields in the request:

- access_key
- profile_id
- currency
- amount
- locale
- bill_to_forename
- bill_to_surname
- bill_to_email
- bill_to_address_line1
- bill_to_address_city
- bill_to_address_state
- bill_to_address_postal_code
- bill_to_address_country
- payment_method
- echeck_account_number
- echeck_routing_number
- echeck_account_type

- echeck_sec_code
- company_tax_id
- driver_license_number
- driver_license_state
- date_of_birth
- reference_number
- transaction_uuid
- signed_date_time
- signed_field_names

For detailed descriptions of all request and reply fields, see "API Fields," page 50.

Payment Token for a one-click Checkout Transaction

To create a payment token for a one-click Checkout transaction:

Step 1 Set the endpoint to:

- Test transactions: https://testsecureacceptance.cybersource.com/oneclick/pay
- Live transactions: https://secureacceptance.cybersource.com/oneclick/pay

Step 2 Set the **transaction_type** field to **authorization,create_payment_token** or **sale,create_payment_token**.

Step 3 Include the following fields in the request:

- access_key—required field.
- transaction_uuid—required field.
- signed_field_names—required field.
- unsigned_field_names—required field.
- signed_date_time—required field.
- signature—required field.
- profile_id—required field.
- reference_number—required field.
- currency—required field.
- amount—required field.
- locale—required field.
- payment_token_comments—optional field.

- payment_token_title—optional field.
- payment_token_consumer_id—optional field.
- merchant_secure_data1—optional field.
- merchant_secure_data2—optional field.
- merchant_secure_data3—optional field.
- merchant_secure_data4—optional field.

Important If no optional fields are included in the request, the customer enters the data into each field on the checkout screen.

For detailed descriptions of all request and reply fields, see "API Fields," page 50.

Payment Token for Recurring Payments

You must specify the amount and frequency of each payment and the start date for processing the payments. CyberSource creates a schedule based on this information and automatically bills the customer according to the schedule.

To create a payment token for a recurring payment:

Step 1 Set the endpoint to:

- Test transactions: https://testsecureacceptance.cybersource.com/pay
- Live transactions: https://secureacceptance.cybersource.com/pay

Step 2 Include the same request fields that you send for creating a payment token with a transaction. See "Payment Token for a one-click Checkout Transaction," page 36.

Important The **amount** field is an optional field that indicates the setup fee for processing recurring payments. To charge this fee, include the **amount** field and ensure that the **transaction_type** field is set to **authorization,create_payment_token** or **sale,create_payment_token**.

Step 3 Include the additional recurring subscription fields in the request:

- recurring_amount—the amount of each payment.
- recurring_frequency—the frequency of payments for the subscription.
- recurring_start_date—the first payment date for the subscription.

For detailed descriptions of all request and reply fields, see "API Fields," page 50.

Payment Token for Installment Payments

You must specify the number of payments, the amount and frequency of each payment, and the start date for processing the payments. CyberSource creates a schedule based on this information and automatically bills the customer according to the schedule.

To create a payment token for an installment payment:

Step 1 Set the endpoint to:

- Test transactions: https://testsecureacceptance.cybersource.com/pay
- Live transactions: https://secureacceptance.cybersource.com/pay

Step 2 Include the same request fields that you send for creating a payment token with a transaction. See "Payment Token for a one-click Checkout Transaction," page 36.

Important The **amount** field is an optional field that indicates the setup fee for processing recurring payments. To charge this fee, include the **amount** field and ensure the **transaction_type** field is set to **authorization,create_payment_token** or **sale,create_payment_token**.

Step 3 Include the following additional installment subscription fields in the request:

- recurring_amount—the amount of each payment.
- recurring_frequency—the frequency of payments for the subscription.
- recurring_start_date—the first payment date for the subscription.
- recurring_number_of_installments—total number of payments for the subscription.

For detailed descriptions of all request and reply fields, see "API Fields," page 50.

CHAPTER 5

Using a Payment Token

Processing a one-click Checkout Transaction

Important

one-click checkout supports card and eCheck transactions.

To process a one-click Checkout transaction with a payment token:

Step 1 Set the endpoint to:

- Test transactions: https://testsecureacceptance.cybersource.com/oneclick/pay
- Live transactions: https://secureacceptance.cybersource.com/oneclick/pay

Step 2 Include the one-click Checkout endpoint on your payment confirmation page. See "Invoking Secure Acceptance," page 33.

Step 3 Include the following fields in the request:

- access_key—required field.
- transaction_uuid—required field.
- signed_field_names—required field.
- unsigned_field_names—required field.
- signed_date_time—required field.
- signature—required field.
- profile_id—required field.
- reference_number—required field.
- transaction_type—set to **authorization** or **sale**. Required field.
- amount—required field.
- currency—required field.
- locale—required field.
- payment_token—required field.

- allow_payment_token_update—set to **true** to enable customers to update their billing, shipping, and payment details on the order review page. This field is optional and available only if the payment method is card.

Important If you do not include the **allow_payment_token_update** field in the request and the customer updates a billing, shipping, or card field, no updates are saved for subsequent transactions.

Note If you enabled the service fee feature, the terms and conditions are displayed on the customer review page. See "Enabling the Service Fee," page 18. A customer must accept the terms and conditions before submitting an order.

For detailed descriptions of all request and reply fields, see "API Fields," page 50. For an example of this transaction, see page 81.

Viewing Transactions in the Business Center

To view a transaction in the Business Center:

Step 1 Log in to the Business Center:

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

Step 2 In the left navigation panel, choose **Transaction Search > Secure Acceptance Search**. The Secure Acceptance Search page appears. The search options are:

- Account suffix
- Cardholder's surname
- Merchant reference number
- Request ID

Step 3 Select the date range for your search. The dates can range from the current day to a maximum of 6 months past.

Step 4 Select the number of results to be displayed, from 10 to 100 transactions per page.

Step 5 Click **Search**. The Secure Acceptance Transaction Search Results page appears.

Important If a transaction has missing or invalid data, it is displayed in the Secure Acceptance Transaction Search Results page without a request ID link.

Step 6 The additional search options for each transaction are:

- Click the **request ID** link of the transaction. The Transaction Search Details page appears.
- Click the magnifying glass icon in the Log column for each transaction. The Secure Acceptance Transaction Search Details page appears. The search results are:
  - Summary information—includes the merchant ID, request ID, profile ID, the transaction decision, and the message for the transaction.
  - Request log—includes all the request API fields for the transaction.
  - Reply log—includes all the reply API fields for the transaction.

CHAPTER 6

Updating a Payment Token

Payment Token for a one-click Checkout Transaction

To update a payment token for a one-click Checkout transaction:

Important

one-click checkout supports card and eCheck transactions.

Step 1 Set the endpoint:

- Test transactions: https://testsecureacceptance.cybersource.com/oneclick/pay
- Live transactions: https://secureacceptance.cybersource.com/oneclick/pay

Step 2 Set the **transaction_type** field to **authorization,update_payment_token** or **sale,update_payment_token**.

Step 3 Include the following fields in the request:

- access_key—required field.
- transaction_uuid—required field.
- signed_field_names—required field.
- unsigned_field_names—required field.
- signed_date_time—required field.
- signature—required field.
- profile_id—required field.
- reference_number—required field.
- amount—required field.
- currency—required field.
- locale—required field.
- payment_token—required field.
- payment_token_comments—optional field.

- payment_token_title—optional field.
- allow_payment_token_update—set to **true** to enable customers to update their billing, shipping, and payment details on the order review page. Optional field.

For detailed descriptions of all request and reply fields, see "API Fields," page 50.

Payment Token for Recurring Payments

To update a payment token for a recurring payment:

Step 1 Set the endpoint:

- Test transactions: https://testsecureacceptance.cybersource.com/pay
- Live transactions: https://secureacceptance.cybersource.com/pay

Step 1 Set the **transaction_type** field to **authorization,update_payment_token** or **sale,update_payment_token**.

Step 2 Include the same request fields that you send for processing an on-demand transaction. See "Payment Token for a one-click Checkout Transaction," page 44.

Step 3 Update the relevant request fields.

You cannot update the following recurring payment fields in the request:

- recurring_amount—the amount of each payment.
- recurring_frequency—the frequency of payments for the subscription.
- recurring_start_date—the first payment date for the subscription.

For detailed descriptions of all request and reply fields, see "API Fields," page 50.

Payment Token for Installment Payments

To update a payment token for an installment subscription:

Step 1 Set the endpoint:

- Test transactions: https://testsecureacceptance.cybersource.com/pay
- Live transactions: https://secureacceptance.cybersource.com/pay

Step 2 Set the **transaction_type** field to **authorization,update_payment_token** or **sale,update_payment_token**.

Step 3 Include the same request fields that you send for processing an on-demand transaction. See "Payment Token for a one-click Checkout Transaction," page 44.

Step 4 Update the relevant request fields.

You cannot update the following installment payment fields in the request:

- recurring_amount—the amount of each payment.
- recurring_frequency—the frequency of payments for the subscription.
- recurring_start_date—the first payment date for the subscription.
- recurring_number_of_installments—total number of payments for the subscription.

For detailed descriptions of all request and reply fields, see "API Fields," page 50.

CHAPTER 7

Using Decision Manager

Important Contact CyberSource Customer Support to enable the Decision Manager verbose data mode for your merchant account and for detailed information regarding the device fingerprint.

Decision Manager is a hosted fraud management tool that enables you to identify legitimate orders quickly and that reduces the need to manually intervene in your order review process. You can accurately identify and review potentially risky transactions while minimizing the rejection of valid orders. With Secure Acceptance, you can use Decision Manager to screen orders containing travel data. Include the complete route or the individual legs of the trip, or both. For more information, see page 89. If you include both, the value for the complete route is used.

Decision Manager also obtains data about the geographical location of a customer by linking the IP address extracted from the customer's browser to the country and the credit card. Add the customer's IP address to the **customer_ip_address** field and include it in the request. See "Processing a one-click Checkout Transaction," page 89.

Verbose mode returns detailed information about the order, and it returns the decision of each rule that the order triggered. Rules that are evaluated as true are returned with the appropriate results and field names, but rules that are evaluated as false are not returned.

Include the following fields in the request:

- consumer_id
- complete_route
- customer_cookies_accepted
- customer_gift_wrap
- customer_ip_address
- departure_time
- date_of_birth
- device_fingerprint_id
- journey_leg#_orig
- journey_leg#_dest
- journey_type
- merchant_defined_data#

- returns_accepted

For detailed descriptions of all request fields, see "API Fields," page 50. For detailed descriptions of all the Decision Manager reply fields, see the *Decision Manager Developer Guide Using the SCMP API*.

CHAPTER 8

Testing Transactions

Important You must create a profile in both the test and live versions of Secure Acceptance. You cannot copy a profile from the test version to the live version. You must recreate the profile.

To test Secure Acceptance transactions:

Step 1 Log in to the Test Business Center: https://ebctest.cybersource.com

Step 2 Create a Secure Acceptanceprofile. See "Creating a Web/Mobile Profile," page 13

Step 3 Invoke Secure Acceptance. See page 33.

Important Include the test transactions endpoint in your HTML form. See "Invoking Secure Acceptance," page 33.

Step 4 You may use the following test credit card numbers for transactions:

Credit Card Type	Test Account Number
Visa	4111111111111111
MasterCard	5555555555554444
American Express	378282246310005
Discover	6011111111111117
JCB	3566111111111113
Diners Club	38000000000006
Maestro International (16 digits)	6000340000009859
Maestro Domestic (16 digits)	6759180000005546

To simulate processor-specific error messages, choose your payment processor here:
http://www.cybersource.com/developers/test_and_manage/testing/legacy_scmp_api/

CHAPTER 9

API Fields

Data Type Definitions

Data Type	Description
Date and time	Format is YYYY-MM-DDThhmmssZ, where: ■ T separates the date and the time ■ Z indicates Coordinated Universal Time (UTC), which is also known as Greenwich Mean Time Example: 2012-08-11T224757Z equals 10:47:57 P.M. on August 11, 2012
Decimal	Number that includes a decimal point Examples: 23.45, -0.1, 4.0, 90809.0468
Integer	Whole number {..., -3, -2, -1, 0, 1, 2, 3, ...}
Nonnegative integer	Whole number greater than or equal to zero {0, 1, 2, 3, ...}
Positive integer	Whole number greater than zero {1, 2, 3, ...}
String	Sequence of letters, numbers, spaces, and special characters

Request-Level Fields

Required API Request Fields

Important These API request fields are required in order to process each transaction. Add each one to the HTML form that invokes and displays Secure Acceptance. See Invoking Secure Acceptance, page 33.

Table 2 Required API Fields

Field Name	Description	Data Type & Length
access_key	Required for authentication with Secure Acceptance. See Creating a Security Key, page 19.	String (32)
amount	Total amount for the order. Must be greater than or equal to zero and must equal the total amount of each line item including the tax amount.	String (15)
currency	Currency used for the order. For the possible values, see the ISO currency codes.	String (5)
locale	Indicates the language to use for customer-facing content. Possible value: en-us. See Activating a Profile, page 33.	String (5)
profile_id	Identifies the profile to use with each transaction. See Creating a Security Key, page 19.	String (7)
reference_number	Unique merchant-generated order reference or tracking number for each transaction.	String (50)
signature	Merchant-generated Base64 signature. This is generated using the signing method for the access_key field supplied.	
signed_date_time	The date and time that the signature was generated. Must be in UTC Date & Time format. This field is used to check for duplicate transaction attempts. **Important** Your system time must be accurate to avoid payment processing errors related to the signed_date_time field.	String (20)

Table 2 Required API Fields (Continued)

Field Name	Description	Data Type & Length
signed_field_names	A comma-separated list of request fields that are signed. This field is used to generate a signature that is used to verify the content of the transaction to protect it from tampering. **Important** All request fields should be signed to prevent data tampering, with the exception of the card_number field and the signature field.	Variable
transaction_type	The type of transactions: ■ authorization ■ sale ■ create_payment_token ■ authorization,create_payment_token ■ sale,create_payment_token ■ authorization,update_payment_token ■ sale,update_payment_token	String (60)
transaction_uuid	Unique merchant-generated identifier. Include with the access_key field for each transaction. This identifier must be unique for each transaction. This field is used to check for duplicate transaction attempts.	String (50)
unsigned_field_names	A comma-separated list of request fields that are not signed.	Variable

Optional API Request Fields

Important These API request fields are optional for processing each transaction. The data contained in each API field populates the corresponding fields within Secure Acceptance. Add each one to your HTML form that invokes and displays Secure Acceptance. See Invoking Secure Acceptance, page 33.

Table 3 Optional API Fields

Field Name	Description	Data Type & Length
allow_payment_token_ update	Indicates whether the customer can update the billing, shipping, and payment information on the order review page. This field can contain one of the following values: ■ true: customer can update details. ■ false: customer cannot update details.	String (5)
bill_payment	Flag that indicates a payment for a bill or for an existing contractual loan.Visa provides a Bill Payment program that enables customers to use their Visa cards to pay their bills. Possible values: ■ true: Bill payment or loan payment. ■ false (default): Not a bill payment or loan payment.	String (5)
bill_to_address_city	City in the billing address.	String (50)
bill_to_address_country	Country code for the billing address. Use the two-character ISO country codes.	String (2)
bill_to_address_line1	First line of the billing address.	String (60)
bill_to_address_line2	Second line of the billing address.	String (60)
bill_to_address_postal_code	Postal code for the billing address.	String (10)
bill_to_address_state	State or province in the billing address. Use the two-character ISO state and province code. **Important** This field is required for U.S. and Canada.	String (2)
bill_to_company_name	Name of the customer's company.	String (40)
bill_to_email	Customer's email address, including the full domain name.	String (255)
bill_to_forename	Customer's first name. This name must be the same as the name on the card.	String (60)
bill_to_phone	Customer's phone number. CyberSource recommends that you include the country code if the order is from outside the U.S.	String (15)

Table 3 Optional API Fields (Continued)

Field Name	Description	Data Type & Length
bill_to_surname	Customer's last name. This name must be the same as the name on the card.	String (60)
card_cvn	Card verification number. Can be configured to optional.	String (4)
card_expiry_date	Card expiration date. Format: MM-YYYY	String (7)
card_number	Card number.	String (20)
card_type	Type of card to authorize. Use one of these values: ■ 001: Visa ■ 002: MasterCard ■ 003: American Express ■ 004: Discover ■ 005: Diners Club ■ 006: Carte Blanche ■ 007: JCB ■ 014: EnRoute ■ 021: JAL ■ 024: Maestro (UK Domestic) ■ 031: Delta ■ 033: Visa Electron ■ 034: Dankort ■ 035: Laser ■ 036: Carte Bleue ■ 037: Carta Si ■ 042: Maestro (International) ■ 043: GE Money UK card	String (3)
company_tax_id	Company's tax identifier.	String (9)

Table 3 Optional API Fields (Continued)

Field Name	Description	Data Type & Length
complete_route	Concatenation of individual travel legs in the format for example: SFO-JFK:JFK-LHR:LHR-CDG. For a complete list of airport codes, see IATA's City Code Directory. **Note** In your request, send either the complete route or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the value of **complete_route** takes precedence over that of the **journey_leg#** fields.	String (255)
consumer_id	Identifier for the customer's account. This field is defined when you create a subscription.	String (50)
customer_cookies_accepted	Indicates whether the customer's browser accepts cookies. This field can contain one of the following values: ■ true: customer's browser accepts cookies. ■ false: customer's browser does not accept cookies.	String (5)
customer_gift_wrap	Indicates whether the customer requested gift wrapping for this purchase. This field can contain one of the following values: ■ true: customer requested gift wrapping. ■ false: customer did not request gift wrapping.	String (5)
customer_ip_address	Customer's IP address reported by your web server via socket information.	String (15)
date_of_birth	Date of birth of the customer. Use the format: YYYYMMDD.	String (8)
debt_indicator	Flag that indicates a payment for an existing contractual loan under the VISA Debt Repayment program. Contact your processor for details and requirements. Possible formats: ■ false (default): Not a loan payment ■ true: Loan payment	String (5)

Table 3 Optional API Fields (Continued)

Field Name	Description	Data Type & Length
departure_time	Departure data and time of the first leg of the trip. Use one of the following formats: ■ yyyy-MM-dd HH:mm z ■ yyyy-MM-dd hh:mm a z ■ yyyy-MM-dd hh:mma z HH = 24-hour format hh = 12-hour format a = am or pm (case insensitive) z = time zone of the departing flight, for example: If the airline is based in city A, but the flight departs from city B, z is the time zone of city B at the time of departure.	DateTime (25)
device_fingerprint_id	Field that contains the session ID for the fingerprint. The string can contain uppercase and lowercase letters, digits, and these special characters: hyphen (-) and underscore (_) However, do not use the same uppercase and lowercase letters to indicate different session IDs. The session ID must be unique for each merchant ID. You can use any string that you are already generating, such as an order number or web session ID.	String (88)
driver_license_number	Driver's license number of the customer.	String (30)
driver_license_state	State or province where the customer's driver's license was issued. Use the two-character *State, Province, and Territory Codes for the United States and Canada*.	String (2)
echeck_account_number	Account number.	Non-negative integer (17)
echeck_account_type	Account type. Possible values: ■ C: Checking ■ S: Savings (USD only) ■ X: Corporate checking (USD only)	String (1)
echeck_check_number	Check number.	Integer (8)
echeck_routing_number	Bank routing number. This is also called the transit number.	Non-negative integer (9)

Table 3 Optional API Fields (Continued)

Field Name	Description	Data Type & Length
echeck_sec_code	The authorization method for the transaction. Possible values: ■ CCD: Corporate cash disbursement—A charge or credit against a business checking account. You can use one-time or recurring CCD transactions to transfer funds to or from a corporate entity. A standing authorization is required for recurring transactions. ■ PPD: Prearranged payment and deposit entry—A charge or credit against a personal checking or savings account. You can originate a PPD entry only when the payment and deposit terms between you and the customer are prearranged. A written authorization from the customer is required for one-time transactions and a written standing authorization is required for recurring transactions. ■ TEL: Telephone-initiated entry—A one-time charge against a personal checking or savings account. You can originate a TEL entry only when there is a business relationship between you and the customer or when the customer initiates a telephone call to you. For a TEL entry, you must obtain a payment authorization from the customer over the telephone. ■ WEB: Internet-initiated entry—A charge against a personal checking or savings account. You can originate a one-time or recurring WEB entry when the customer initiates the transaction over the Internet. For a WEB entry, you must obtain payment authorization from the customer over the Internet.	String (3)
ignore_avs	Ignore the results of AVS verification. Possible values: ■ true ■ false **Important** To prevent data tampering CyberSource recommends signing this field. See signed_field_names, page 52.	String (5)

Table 3 Optional API Fields (Continued)

Field Name	Description	Data Type & Length
ignore_cvn	Ignore the results of CVN verification. Possible values: ■ true ■ false **Important** To prevent data tampering CyberSource recommends signing this field. See signed_field_names, page 52.	String (5)
item_#_code	Type of product. If it is supplied, the item code must be one of the following values: • default • adult_content • coupon • electronic_good • electronic_software • gift_certificate • service • subscription • handling_only • service • shipping_and_handling • shipping_only • subscription # can range from 0 to 49.	
item_#_name	Name of the item. # can range from 0 to 49.	String (255)
item_#_quantity	Quantity of line items. **Important** Required field if one of the following product codes is used: • adult_content • coupon • electronic_good • electronic_software • gift_certificate • service • subscription # can range from 0 to 49.	String (10)

Table 3 Optional API Fields (Continued)

Field Name	Description	Data Type & Length
item_#_sku	Identification code for the product. **Important** Required field if one of the following product codes is used: • adult_content • coupon • electronic_good • electronic_software • gift_certificate • service • subscription # can range from 0 to 49.	String (255)
item_#_tax_amount	Tax amount to apply to the line item. # can range from 0 to 49. This value cannot be negative. The tax amount and the offer amount must be in the same currency.	String (15)
item_#_unit_price	Price of the line item. # can range from 0 to 49. This value cannot be negative.	String (15)
journey_leg#_dest	Airport code for the origin of the leg of the trip designated by the pound (#) symbol in the field name. A maximum of 30 legs can be included in the request. This code is usually three digits long, for example: SFO = San Francisco. Do not use the colon (:) or the hyphen (-). For a complete list of airport codes, see IATA's City Code Directory. **Note** In your request, send either the **complete_route** field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the complete route takes precedence over the individual legs.	String (3)
journey_leg#_orig	Airport code for the origin of the leg of the trip designated by the pound (#) symbol in the field name. A maximum of 30 legs can be included in the request. This code is usually three digits long, for example: SFO = San Francisco. Do not use the colon (:) or the hyphen (-). For a complete list of airport codes, see IATA's City Code Directory. **Note** In your request, send either the **complete_route** field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the complete route takes precedence over the individual legs.	String (3)
journey_type	Type of travel, such as: one way or round trip.	String (32)

Table 3 Optional API Fields (Continued)

Field Name	Description	Data Type & Length
line_item_count	Total number of line items. Maximum number is 49.	String (2)
merchant_defined_data#	Optional fields that you can use to store information. # can range from 1 to 100. **Note** Merchant defined data fields 1 to 4 are stored against the payment token and are used for subsequent token based transactions. Merchant defined data fields 5 to 100 are passed trough to Decision Manager as part of the initial payment request and are not stored against the payment token. **Important** Merchant-defined data fields are not intended to and MUST NOT be used to capture personally identifying information. Accordingly, merchants are prohibited from capturing, obtaining, and/or transmitting any personally identifying information in or via the merchant-defined data fields. Personally identifying information includes, but is not limited to, card number, bank account number, social security number, driver's license number, state-issued identification number, passport number, and card verification numbers (CVV, CVC2, CVV2, CID, CVN). In the event CyberSource discovers that a merchant is capturing and/or transmitting personally identifying information via the merchant-defined data fields, whether or not intentionally, CyberSource WILL immediately suspend the merchant's account, which will result in a rejection of any and all transaction requests submitted by the merchant after the point of suspension.	String (100)
merchant_secure_data1 merchant_secure_data2 merchant_secure_data3	Optional fields that you can use to store information. CyberSource encrypts the data before storing it in the database.	String (100)
merchant_secure_data4	Optional field that you can use to store information. CyberSource encrypts the data before storing it in the database.	String (2000)
override_custom_receipt_page	Overrides the custom receipt profile setting with your own URL. **Important** To prevent data tampering CyberSource recommends signing this field. See signed_field_names, page 52.	String (255)

Table 3 Optional API Fields (Continued)

Field Name	Description	Data Type & Length
payment_method	Method of payment. Possible values: ■ card ■ echek	String (30)
payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the CyberSource database. When this field is included in the request, the card data, and billing and shipping information are optional. **Important** You must be currently using CyberSource Payment Tokenization services. Populate this field with the customer subscription ID.	String (26)
payment_token_comments	Optional comments you have for the customer subscription.	String (255)
payment_token_title	Name or title for the customer subscription.	String (60)
recurring_amount	Payment amount for each installment or recurring subscription payment.	String (15)
recurring_frequency	Frequency of payments for an installment or recurring subscription. Possible values: ■ weekly ■ monthly ■ quarterly ■ annually ■ bi-weekly ■ semi-monthly ■ quad-weekly ■ semi-annually	String (20)
recurring_number_of_ installments	Total number of payments set up for an installment subscription. The range of installments is from 1 to 156.	String (3)
recurring_start_date	First payment date for an installment or recurring subscription payment. Date must use the format YYYYMMDD. If a date in the past is supplied, the start date defaults to the day after the date was entered.	String (8)

Table 3 Optional API Fields (Continued)

Field Name	Description	Data Type & Length
returns_accepted	Indicates whether product returns are accepted. This field can contain one of the following values: ■ true ■ false	String (5)
ship_to_address_city	City of shipping address.	String (50)
ship_to_address_country	Country code for the shipping address. Use the two-character ISO country codes.	String (2)
ship_to_address_line1	First line of shipping address.	String (60)
ship_to_address_line2	Second line of shipping address.	String (60)
ship_to_address_postal_code	Postal code for the shipping address.	String (10)
ship_to_address_state	State or province of shipping address. Use the two-character ISO state and province codes. **Important** This field is required for U.S. and Canada.	String (2)
ship_to_company_name	Name of the company receiving the product.	String (40)
ship_to_forename	First name of the person receiving the product.	String (60)
ship_to_phone	Phone number of the shipping address.	String (15)
ship_to_surname	Last name of the person receiving the product.	String (60)
shipping_method	Shipping method for the product. Possible values: ■ sameday: Courier or same-day service ■ oneday: Next day or overnight service ■ twoday: Two-day service ■ threeday: Three-day service ■ lowcost: Lowest-cost service ■ pickup: Store pick-up ■ other: Other shipping method ■ none: No shipping method	String (10)
skip_decision_manager	Indicates whether to skip Decision Manager when creating a subscription. This field can contain one of the following values: ■ true ■ false	String (5)

Table 3 Optional API Fields (Continued)

Field Name	Description	Data Type & Length
tax_amount	Total tax amount to apply to the order. This value cannot be negative. **Important** To prevent data tampering CyberSource recommends signing this field. See signed_field_names, page 52.	String (15)

API Reply Fields

Important

If configured, these API reply fields are sent back to your Merchant POST URL or email. See Configuring Merchant Notifications, page 25.

Because CyberSource may add reply fields and reason codes at any time, proceed as follows:

- You should parse the reply data according to the names of the fields instead of their order in the reply. For more information on parsing reply fields, see the documentation for your scripting language.
- Your error handler should use the **decision** field to obtain the result if it receives a reason code that it does not recognize.

Table 4 API Reply Fields

Field Name	Description	Data Type and Length
auth_amount	Amount that was authorized.	String (15)
auth_avs_code	AVS result code. See "AVS Codes."	String (1)
auth_avs_code_raw	AVS result code sent directly from the processor. Returned only if a value is returned by the processor.	String (10)
auth_code	Authorization code. Returned only if a value is returned by the processor.	String (7)
auth_cv_result	CVN result code. See "CVN Codes."	String (1)
auth_cv_result_raw	CVN result code sent directly from the processor. Returned only if a value is returned by the processor.	String (10)
auth_response	For most processors, this is the error message sent directly from the bank. Returned only if a value is returned by the processor.	String (10)
auth_time	Time of authorization in UTC.	String (20)

Table 4 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
auth_trans_ref_no	Reference number that you use to reconcile your CyberSource reports with your processor reports.	String (60)
bill_trans_ref_no	Reference number that you use to reconcile your CyberSource reports with your processor reports.	String (60)
decision	The result of your request. Possible values: ■ ACCEPT ■ DECLINE ■ REVIEW ■ ERROR See "Reason Codes."	String (7)
echeck_debit_ref_no	Reference number for the transaction.	String (60)
echeck_debit_submit_time	Time when the debit was requested in UTC.	Date and Time (20)
invalid_fields	Indicates which request fields were invalid.	Variable
message	Reply message from the payment gateway.	String (255)
payer_authentication_cavv	Cardholder authentication verification value (CAVV). Transaction identifier generated by the issuing bank. This field is used by the payer authentication validation service.	String (50)

Table 4 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
payer_authentication_eci	Electronic commerce indicator (ECI). Numeric indicator returned only for Verified by Visa transactions. This field is used by payer authentication validation and enrollment services. Possible values: Enrollment Service: ■ 06: Card can be enrolled. You are protected. ■ 07: Card cannot be enrolled. You are not protected. Validation Service: ■ 00: Failed authentication ■ 05: Successful authentication. ■ 06: Authentication attempted. ■ 07: Failed authentication.	String (3)
payer_authentication_proof_xml	XML element containing proof of enrollment checking. For cards not issued in the U.S. or Canada, your bank may require this data as proof of enrollment validation for any payer authentication transaction that you re-present because of a chargeback. For cards issued in the U.S. or Canada, Visa may require this data for specific merchant category codes.	String (1024)
payer_authentication_uad	MasterCard SecureCode UCAF authentication data. Returned only for MasterCard SecureCode transactions.	String (32)

Table 4 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
payer_authentication_uci	MasterCard SecureCode UCAF collection indicator. This field indicates whether authentication data is collected at your web site. Possible values: ■ 0: Authentication data was not collected and customer authentication not completed. ■ 1: Authentication data was not collected because customer authentication not completed. ■ 2: Authentication data was collected. Customer completed authentication.	String (1)
payer_authentication_xid	Transaction identifier generated by CyberSource Payer Authentication. Used to match an outgoing PA request with an incoming PA response.	String (28)
reason_code	Numeric value corresponding to the result of the credit card authorization request. See "Reason Codes."	String (5)
req_access_key	Authenticates the merchant with the application.	String (32)
req_allow_payment_token_update	Indicates whether the customer can update the billing, shipping, and payment information on the order review page. This field can contain one of the following values: ■ true: customer can update details. ■ false: customer cannot update details.	String (5)
req_amount	Total amount for the order. Must be greater than or equal to zero.	String (15)
req_bill_payment	Flag that indicates a payment for a bill or for an existing contractual loan.Visa provides a Bill Payment program that enables customers to use their Visa cards to pay their bills. Possible values: ■ true: Bill payment or loan payment. ■ false (default): Not a bill payment or loan payment.	String (1)

Table 4 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_bill_to_address_city	City in the billing address.	String (50)
req_bill_to_address_country	Country code for the billing address. Use the two-character ISO country codes.	String (2)
req_bill_to_address_line1	First line of the street address in the billing address.	String (60)
req_bill_to_address_line2	Second line of the street address in the billing address.	String (60)
req_bill_to_address_postal_code	Postal code for the billing address.	String (10)
req_bill_to_address_state	State or province in the billing address. The two-character ISO state and province code. **Important** This field is required for U.S and Canada.	String (2)
req_bill_to_company_name	Name of the customer's company.	String (40)
req_bill_to_email	Customer's email address.	String (255)
req_bill_to_forename	Customer's first name.	String (60)
req_bill_to_phone	Customer's phone number.	String (15)
req_bill_to_surname	Customer's last name.	String (60)
req_card_cvn	Card verification number.	String (4)
req_card_expiry_date	Card expiration date.	String (7)
req_card_number	Card number.	String (20)
req_card_type	Type of card. See Configuring Merchant Notifications, page 25.	String (3)
req_company_tax_id	Company's tax identifier. The the last four digits are not masked.	String (9)
req_consumer_id	Identifier for the customer account. This value is defined when creating a customer subscription.	String (50)

Table 4 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_complete_route	Concatenation of individual travel legs in the format: SFO-JFK:JFK-LHR:LHR-CDG. For a complete list of airport codes, see IATA's City Code Directory. **Note** In your request, send either the complete route field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the value of **complete_route** takes precedence over that of the **journey_leg#** fields.	String (255)
req_currency	Currency used for the order. See ISO currency codes.	String (5)
req_customer_cookies_accepted	Indicates whether the customer's browser accepts cookies. This field can contain one of the following values: ■ true: customer's browser accepts cookies. ■ false: customer's browser does not accept cookies.	String (5)
req_customer_gift_wrap	Indicates whether the customer requested gift wrapping for this purchase. This field can contain one of the following values: ■ true: customer requested gift wrapping. ■ false: customer did not request gift wrapping.	String (5)
req_customer_ip_address	Customer's IP address reported by your web server using socket information.	
req_date_of_birth	Date of birth of the customer. Use the format: YYYYMMDD.	String (8)
req_debt_indicator	Flag that indicates a payment for an existing contractual loan under the VISA Debt Repayment program. Contact your processor for details and requirements. Possible formats: ■ false (default): Not a loan payment ■ true: Loan payment	String (5)

Table 4 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_departure_time	Departure date and time of the first leg of the trip. Use one of the following formats: ■ yyyy-MM-dd HH:mm z ■ yyyy-MM-dd hh:mm a z ■ yyyy-MM-dd hh:mma z HH = 24-hour format hh = 12-hour format a = am or pm (case insensitive) z = time zone of the departing flight, for example: If the airline is based in city A, but the flight departs from city B, z is the time zone of city B at the time of departure.	String (25)
req_device_fingerprint_id	Field that contains the session ID for the fingerprint. The string can contain uppercase and lowercase letters, digits, and these special characters: hyphen (-) and underscore (_) However, do not use the same uppercase and lowercase letters to indicate different sessions IDs. The session ID must be unique for each merchant ID. You can use any string that you are already generating, such as an order number or web session ID.	String (88)
req_driver_license_number	Driver's license number of the customer. The the last four digits are not masked.	String (30)
req_driver_license_state	State or province from which the customer's driver's license was issued. Use the two-character *State, Province, and Territory Codes for the United States and Canada*.	String (2)
req_echeck_account_number	Account number. This number is masked.	Non-negative integer (17)
req_echeck_account_type	Account type. Possible values: ■ C: Checking ■ S: Savings (USD only) ■ X: Corporate checking (USD only)	String (1)
req_echeck_check_number	Check number.	Integer (8)

Table 4 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_echeck_routing_number	Bank routing number. It is also called the transit number.	Non-negative integer (9)
req_echeck_sec_code	The authorization method for the transaction. Possible values: ■ CCD ■ PPD ■ TEL ■ WEB See echeck_sec_code, page 57.	String (3)
req_ignore_avs	Ignore the results of AVS verification. Possible values: ■ true ■ false	String (5)
req_ignore_cvn	Ignore the results of CVN verification. Possible values: ■ true ■ false	String (5)
req_item_#_code	Type of product. # can range from 0 to 49.	
req_item_#_name	Name of the item. # can range from 0 to 49.	String (255)
req_item_#_quantity	Quantity of line items. # can range from 0 to 49.	String (10)
req_item_#_sku	Identification code for the product. # can range from 0 to 49.	String (255)
req_item_#_tax_amount	Tax amount to apply to the line item. # can range from 0 to 49. This value cannot be negative. The tax amount and the offer amount must be in the same currency.	String (15)
req_item_#_unit_price	Price of the line item. # can range from 0 to 49. This value cannot be negative.	String (15)

Table 4 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_journey_leg#_dest	Airport code for the origin of the leg of the trip designated by the pound (#) symbol in the field name. A maximum of 30 legs can be included in the request. This code is usually three digits long, for example: SFO = San Francisco. Do not use the colon (:) or the hyphen (-). For a complete list of airport codes, see IATA's City Code Directory. In your request, send either the **complete_route** field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the complete route takes precedence over the individual legs.	String (3)
req_journey_leg#_orig	Airport code for the origin of the leg of the trip designated by the pound (#) symbol in the field name. A maximum of 30 legs can be included in the request. This code is usually three digits long, for example: SFO = San Francisco. Do not use the colon (:) or the hyphen (-). For a complete list of airport codes, see IATA's City Code Directory. In your request, send the **complete_route** field or the individual legs (**journey_leg#_orig** and **journey_leg#_dest**). If you send all the fields, the complete route takes precedence over the individual legs.	String (3)
req_journey_type	Type of travel, such as: one way or round trip.	String (32)
req_line_item_count	Total number of line items. Maximum amount is 50.	String (2)
req_locale	Indicates the language to use for customer content. See "Activating a Profile."	String (5)

Table 4 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_merchant_defined_data#	Optional fields that you can use to store information. # can range from 1 to 100. **Note** Merchant defined data fields 1 to 4 are stored against the payment token and are used for subsequent token based transactions. Merchant defined data fields 5 to 100 are passed trough to Decision Manager as part of the initial payment request and are not stored against the payment token. **Important** Merchant-defined data fields are not intended to and MUST NOT be used to capture personally identifying information. Accordingly, merchants are prohibited from capturing, obtaining, and/or transmitting any personally identifying information in or via the merchant-defined data fields. Personally identifying information includes, but is not limited to, card number, bank account number, social security number, driver's license number, state-issued identification number, passport number, and card verification numbers (CVV, CVC2, CVV2, CID, CVN). In the event CyberSource discovers that a merchant is capturing and/or transmitting personally identifying information via the merchant-defined data fields, whether or not intentionally, CyberSource WILL immediately suspend the merchant's account, which will result in a rejection of any and all transaction requests submitted by the merchant after the point of suspension.	String (100)
req_merchant_secure_data1 req_merchant_secure_data2 req_merchant_secure_data3	Optional fields that you can use to store information. CyberSource encrypts the data before storing it in the database.	String (100)

Table 4 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_merchant_secure_data4	Optional field that you can use to store information. CyberSource encrypts the data before storing it in the database.	String (2000)
req_override_custom_receipt_page	Overrides the custom receipt profile setting with your own URL.	String (255)
req_payment_method	Method of payment. Possible values: ■ card ■ echeck	String (30)
req_payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the CyberSource database. When this field is included in the request, the card data and billing and shipping information are optional. **Important** You must be currently using CyberSource Payment Tokenization services. Populate this field with the customer subscription ID.	String (26)

Table 4 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the CyberSource database. This payment token super cedes the previous payment token and is returned if: ■ the merchant is configured for a 16 digit payment token which displays the last 4 digits of the primary account number (PAN) and passes Luhn mod-10 check. See Payment Tokens, page 11. ■ the consumer has updated the card number on their payment token. This payment token super cedes the previous payment token and should be used for subsequent transactions. **Important** You must be currently using CyberSource Payment Tokenization services. Populate this field with the customer subscription ID.	String (26)
req_payment_token_comments	Optional comments about the customer subscription.	String (255)
req_payment_token_title	Name of the customer subscription.	String (60)
req_profile_id	Identifies the profile to use with each transaction.	String (7)
req_recurring_amount	Payment amount for each installment or recurring subscription payment.	String (15)
req_recurring_frequency	Frequency of payments for an installment or recurring subscription.	String (20)
req_recurring_number_of_ installments	Total number of payments set up for an installment subscription. Installments range from 1 to 156.	String (3)
req_recurring_start_date	First payment date for an installment or recurring subscription payment. Date must use the format YYYYMMDD. If a date in the past is supplied, the start date defaults to the day after the date was entered.	String (8)

Table 4 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_reference_number	Unique merchant-generated order reference or tracking number for each transaction.	String (50)
req_returns_accepted	Indicates whether product returns are accepted. This field can contain one of the following values: ■ true ■ false	String (5)
req_ship_to_address_city	City of shipping address.	String (50)
req_ship_to_address_country	The two-character country code.	String (2)
req_ship_to_address_line1	First line of shipping address.	String (60)
req_ship_to_address_line2	Second line of shipping address.	String (60)
req_ship_to_address_postal_code	Postal code for the shipping address.	String (10)
req_ship_to_address_state	The two-character ISO state and province code.	String (2)
req_ship_to_company_name	Name of the company receiving the product.	String (40)
req_ship_to_forename	First name of person receiving the product.	String (60)
req_ship_to_phone	Phone number for the shipping address.	String (15)
req_ship_to_surname	Last name of person receiving the product.	String (60)
req_shipping_method	Shipping method for the product. Possible values: ■ sameday: Courier or same-day service ■ oneday: Next day or overnight service ■ twoday: Two-day service ■ threeday: Three-day service ■ lowcost: Lowest-cost service ■ pickup: Store pick-up ■ other: Other shipping method ■ none: No shipping method	String (10)

Table 4 API Reply Fields (Continued)

Field Name	Description	Data Type and Length
req_skip_decision_manager	Indicates whether to skip decision manager when creating a subscription. This field can contain one of the following values: ■ true ■ false	String (5)
req_tax_amount	Total tax to apply to the product.	String (15)
req_transaction_type	The type of transaction requested.	String (60)
req_transaction_uuid	Unique merchant-generated identifier. Include with the access_key field for each transaction.	String (50)
required_fields	Indicates which of the request fields were required but not provided.	Variable
service_fee_amount	The service fee amount for the order.	String (15)
signature	The Base64 signature returned by the server.	String (44)
signed_date_time	The date and time of when the signature was generated by the server. UTC date and time format: 2011-12-31T11:59:59Z	String (20)
signed_field_names	A comma-separated list of response data that was signed by the server. All fields within this list should be used to generate a signature that can then be compared to the response signature to verify the response.	Variable
transaction_id	The transaction identifier returned from the payment gateway.	String (26)

AVS Codes

An issuing bank uses the AVS code to confirm that your customer is providing the correct billing address. If the customer provides incorrect data, the transaction might be fraudulent. The international and U.S. domestic Address Verification Service (AVS) codes are the Visa standard AVS codes, except for codes 1 and 2, which are CyberSource AVS codes. The standard AVS return codes for other types of credit cards (including American Express cards) are mapped to the Visa standard codes. You receive the code in the **auth_avs_code** reply field. See API Reply Fields, page 63.

Important When you populate billing street address 1 and billing street address 2, CyberSource through VisaNet concatenates the two values. If the concatenated value exceeds 40 characters, CyberSource through VisaNet truncates the value at 40 characters before sending it to Visa and the issuing bank. Truncating this value affects AVS results and therefore might impact risk decisions and chargebacks.

International AVS Codes

These codes are returned only for Visa cards issued outside the U.S.

Table 5 International AVS Codes

Code	Response	Description
B	Partial match	Street address matches, but postal code is not verified.
C	No match	Street address and postal code do not match.
D & M	Match	Street address and postal code match.
I	No match	Address not verified.
P	Partial match	Postal code matches, but street address not verified.

U.S. Domestic AVS Codes

Table 6 U.S. Domestic AVS Codes

Code	Response	Description
A	Partial match	Street address matches, but 5-digit and 9-digit postal codes do not match.
B	Partial match	Street address matches, but postal code is not verified.
C	No match	Street address and postal code do not match.
D & M	Match	Street address and postal code match.
E	Invalid	AVS data is invalid or AVS is not allowed for this card type.
F	Partial match	Card member's name does not match, but billing postal code matches. Returned only for the American Express card type.

Table 6 U.S. Domestic AVS Codes (Continued)

Code	Response	Description
G		Not supported.
H	Partial match:	Card member's name does not match, but street address and postal code match. Returned only for the American Express card type.
I	No match	Address not verified.
J	Match	Card member's name, billing address, and postal code match. Shipping information verified and chargeback protection guaranteed through the Fraud Protection Program. Returned only if you are signed up to use AAV+ with the American Express Phoenix processor.
K	Partial match	Card member's name matches, but billing address and billing postal code do not match. Returned only for the American Express card type.
L	Partial match	Card member's name and billing postal code match, but billing address does not match. Returned only for the American Express card type.
M	Match	Street address and postal code match.
N	No match	One of the following: ■ Street address and postal code do not match. ■ Card member's name, street address, and postal code do not match. Returned only for the American Express card type.
O	Partial match	Card member's name and billing address match, but billing postal code does not match. Returned only for the American Express card type.
P	Partial match	Postal code matches, but street address not verified.
Q	Match	Card member's name, billing address, and postal code match. Shipping information verified but chargeback protection not guaranteed (Standard program). Returned only if you are signed to use AAV+ with the American Express Phoenix processor.
R	System unavailable	System unavailable.
S	Not supported	U.S.-issuing bank does not support AVS.
T	Partial match	Card member's name does not match, but street address matches. Returned only for the American Express card type.
U	System unavailable	Address information unavailable for one of these reasons: ■ The U.S. bank does not support non-U.S. AVS. ■ The AVS in a U.S. bank is not functioning properly.
V	Match	Card member's name, billing address, and billing postal code match. Returned only for the American Express card type.
W	Partial match	Street address does not match, but 9-digit postal code matches.
X	Match	Street address and 9-digit postal code match.

Table 6 U.S. Domestic AVS Codes (Continued)

Code	Response	Description
Y	Match	Street address and 5-digit postal code match.
Z	Partial match	Street address does not match, but 5-digit postal code matches.
1	Not supported	AVS is not supported for this processor or card type.
2	Unrecognized	The processor returned an unrecognized value for the AVS response.
3	Match	Address is confirmed. Returned only for PayPal Express Checkout.
4	No match	Address is not confirmed. Returned only for PayPal Express Checkout.

CVN Codes

Table 7 CVN Codes

Code	Description
D	The transaction was considered to be suspicious by the issuing bank.
I	The CVN failed the processor's data validation.
M	The CVN matched.
N	The CVN did not match.
P	The CVN was not processed by the processor for an unspecified reason.
S	The CVN is on the card but was not included in the request.
U	Card verification is not supported by the issuing bank.
X	Card verification is not supported by the card association.
1	Card verification is not supported for this processor or card type.
2	An unrecognized result code was returned by the processor for the card verification response.
3	No result code was returned by the processor.

Reason Codes

The **reasonCode** field contains additional data regarding the decision response of the transaction. Depending on the decision of a transaction request, the CyberSource's default receipt page or your receipt page is displayed to the customer. Both you and your customer may also receive an email receipt. See "Configuring Notifications."

Table 8 Reason Codes

Decision	Reason Code	Type of Notification
ACCEPT	100, 110	■ Customer receipt page ■ Customer receipt email ■ Merchant POST URL ■ Merchant receipt email
REVIEW	200, 201, 230, 520	■ Customer receipt page
DECLINE	102, 200, 202, 203, 204, 205, 207, 208, 210, 211, 221, 222, 230, 231, 232, 233, 234, 236, 240, 475, 476	■ Customer receipt page (1) ■ Merchant POST URL (1) ■ Merchant receipt email (1)
ERROR	Reason code depends on the specific reason for the error.	■ Customer receipt page
CANCEL	The consumer did not accept the service fee conditions.	■ Customer receipt page

(1) The customer receives the decline message "Your order was declined. Please verify your information" twice, before the merchant receives the decline message. The decline message relates to either the processor declining the transaction, or a payment processing error, or the customer entered their 3D Secure credentials incorrectly.

APPENDIX A

Examples

Creating a Payment Token

eCheck Standalone Payment Token

Endpoint:

- Test transactions: https://testsecureacceptance.cybersource.com/token/create
- Live transactions: https://secureacceptance.cybersource.com/token/create

Example eCheck standalone Create Payment Token Request

```
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p1
profile_id=ECP0001
currency=USD
transaction_type=create_payment_token
amount=100.00
locale=en
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_city=San Francisco
bill_to_address_state=CA
bill_to_address_postal_code=94043
bill_to_address_country=US
payment_method=echeck
echeck_account_number=222234100
echeck_routing_number=121042882
echeck_account_type=c
echeck_sec_code=WEB
company_tax_id=123456789
driver_license_number=10-12234-123
driver_license_state=NY
date_of_birth=19901001
reference_number=173056001373554202429468 3
transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2013-07-11T15:16:54Z
signed_field_names=comma separated list of signed field
```

Example eCheck standalone Create Payment Token Reply

```
req_bill_to_address_country=US
req_driver_license_state=NY
req_driver_license_number=xx-xxxxx-xxx
req_date_of_birth=19901001
decision=ACCEPT
req_bill_to_address_state=CA
signed_field_names=comma separated list of signed fields
req_payment_method=echeck
req_transaction_type=create_payment_token
req_echeck_account_type=c
signature=NuxlJilx5YbvKoXlt0baB5hUj5gk4+OozqJnyVF390s=
req_locale=en
reason_code=100
req_bill_to_address_postal_code=94043
req_echeck_account_number=xxxxx4100
req_bill_to_address_line1=1 My Apartment
req_echeck_sec_code=WEB
req_bill_to_address_city=San Francisco
signed_date_time=2013-07-11T15:11:41Z
req_currency=USD
req_reference_number=17305600137355420242946 83
req_echeck_routing_number=xxxxx2882
transaction_id=3735553783662130706689
req_amount=100.00
req_profile_id=ECP0001
req_company_tax_id=123456789
req_transaction_uuid=38f2efe650ea699597d325ecd7432b1c
payment_token=352989331 4302130706689
req_bill_to_surname=Soap
req_bill_to_forename=Joe
req_bill_to_email=joesoap@yahoo.com
req_access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p1
```

With Recurring Payments

Endpoint:

- Test transactions: https://testsecureacceptance.cybersource.com/pay
- Live transactions: https://secureacceptance.cybersource.com/pay

Example Recurring Payment Create Payment Token Request

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=HPA0002
reference_number=1350029885978
transaction_type=authorization,create_payment_token
amount=100.00
tax_amount=15.00
currency=USD
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
merchant_secure_data1=my secure data one
merchant_secure_data2=my secure data two
merchant_secure_data3=my secure data three
merchant_secure_data4=my secure data four
payment_token_comments=These are my token comments
payment_token_title=This is my payment token title
consumer_id=1239874561
recurring_frequency=monthly
recurring_amount=25.00
recurring_start_date=20121112
```

Example Recurring Payment Create Payment Token Reply

```
transaction_id=350031165556018155294 6
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=HPA0002
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,create_payment_token
req_reference_number=1350029885978
req_amount=100.00
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_payment_token_comments=These are my token comments
req_payment_token_title=This is my payment token title
req_consumer_id=1239874561
req_merchant_secure_data1=my secure data one
req_merchant_secure_data2=my secure data two
req_merchant_secure_data3=my secure data three
req_merchant_secure_data4=my secure data four
req_recurring_frequency=monthly
req_recurring_amount=25.00
req_recurring_start_date=20130125
req_bill_to_forename=John
req_bill_to_surname=Doe
req_bill_to_email=null@example.com
req_bill_to_address_line1=19 Alburn Street
req_bill_to_address_city=San Francisco
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_bill_to_address_postal_code=94043
req_card_number=xxxxxxxxxxxx4242
req_card_type=001
req_card_expiry_date=11-2020
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
payment_token=342707583000018155255 6
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

With Installment Payments

Endpoint:

- Test transactions: https://testsecureacceptance.cybersource.com/pay
- Live transactions: https://secureacceptance.cybersource.com/pay

Example Installment Payment Create Payment Request

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=HPA0002
reference_number=1350029885978
transaction_type=authorization,create_payment_token
amount=100.00
tax_amount=15.00
currency=USD
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
merchant_secure_data1=my secure data one
merchant_secure_data2=my secure data two
merchant_secure_data3=my secure data three
merchant_secure_data4=my secure data four
payment_token_comments=These are my token comments
payment_token_title=This is my payment token title
consumer_id=1239874561
recurring_frequency=monthly
recurring_amount=25.00
recurring_start_date=20121112
recurring_number_of_installments=6
```

Example Installment Payment Create Payment Reply

```
transaction_id=350031165556018155294 6
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=HPA0002
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,create_payment_token
req_reference_number=1350029885978
req_amount=100.00
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_payment_token_comments=These are my token comments
req_payment_token_title=This is my payment token title
req_consumer_id=1239874561
req_merchant_secure_data1=my secure data one
req_merchant_secure_data2=my secure data two
req_merchant_secure_data3=my secure data three
req_merchant_secure_data4=my secure data four
req_recurring_frequency=monthly
req_recurring_amount=25.00
req_recurring_start_date=20130125
req_recurring_number_of_installments=6
req_bill_to_forename=John
req_bill_to_surname=Doe
req_bill_to_email=null@example.com
req_bill_to_address_line1=19 Alburn Street
req_bill_to_address_city=San Francisco
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_bill_to_address_postal_code=94043
req_card_number=xxxxxxxxxxxx4242
req_card_type=001
req_card_expiry_date=11-2020
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
payment_token=342707583000018155255 6
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

Using a Payment Token

one-click Checkout Transaction

Endpoint:

- Test transactions: https://testsecureacceptance.cybersource.com/oneclick/pay
- Live transactions: https://secureacceptance.cybersource.com/oneclick/pay

Example one-click Checkout Create Payment Token Request

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=HPA0002
reference_number=1350029885978
transaction_type=authorization,create_payment_token
amount=100.00
tax_amount=15.00
currency=USD
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2013-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
merchant_secure_data1=my secure data one
merchant_secure_data2=my secure data two
merchant_secure_data3=my secure data three
merchant_secure_data4=my secure data four
payment_token_comments=These are my token comments
payment_token_title=This is my payment token title
consumer_id=1239874561
```

Example one-click Checkout Create Payment Token Reply

```
transaction_id=350031165556018155294 6
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=HPA0002
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,create_payment_token
req_reference_number=1350029885978
req_amount=100.00
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_payment_token_comments=These are my token comments
req_payment_token_title=This is my payment token title
req_consumer_id=1239874561
req_merchant_secure_data1=my secure data one
req_merchant_secure_data2=my secure data two
req_merchant_secure_data3=my secure data three
req_merchant_secure_data4=my secure data four
req_bill_to_forename=John
req_bill_to_surname=Doe
req_bill_to_email=null@example.com
req_bill_to_address_line1=19 Alburn Street
req_bill_to_address_city=San Francisco
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_bill_to_address_postal_code=94043
req_card_number=xxxxxxxxxxxx4242
req_card_type=001
req_card_expiry_date=11-2020
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2012-08-14T134608Z
payment_token=342707583000018155255 6
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

Processing a one-click Checkout Transaction

Endpoint:

- Test transactions: https://testsecureacceptance.cybersource.com/oneclick/pay
- Live transactions: https://secureacceptance.cybersource.com/oneclick/pay

Example Transaction with Decision Manager Request

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=HPA0002
payment_token=342707583000018155255 6
reference_number=123456789
transaction_type=authorization
currency=USD
locale=en
customer_cookies_accepted=true
device_fingerprint_id=7685380BB8A476AB4C21FE705DC3AA66
consumer_id=123456
returns_accepted=true
customer_ip_address=192.168
customer_gift_wrap=true
date_of_birth=19830612
merchant_secure_data1=my secure data one
merchant_secure_data2=my secure data two
merchant_secure_data3=my secure data three
merchant_secure_data4=my secure data four
journey_type=Round Trip
complete_route=BFH-SFO:SFO-HON
departure_time=2012-12-11 5:30 am EST
journey_leg1_orig=BFH
journey_leg1_dest=SFH
journey_leg2_orig=SFH
journey_leg2_dest=HON
merchant_defined_data1=merchant defined data 1
merchant_defined_data2=merchant defined data 2
merchant_defined_data3=merchant defined data 3
merchant_defined_data4=merchant defined data 4
line_item_count=2
item_0_name=item 1
item_0_sku=sw1
item_0_code=coupon
item_0_unit_price=40.00
item_0_tax_amount=10.00
item_0_quantity=1
item_1_name=item 2
item_1_sku=sw1
item_1_code=coupon
item_1_unit_price=40.00
item_1_tax_amount=10.00
item_1_quantity=1
```

Example Transaction with Decision Manager Reply

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=HPA0002
payment_token=3427075830000181552556
req_reference_number=123456789
req_transaction_type=authorization
req_currency=USD
req_locale=en
req_customer_cookies_accepted=true
req_device_fingerprint_id=7685380BB8A476AB4C21FE705DC3AA66
req_consumer_id=123456
req_returns_accepted=true
req_customer_ip_address=192.168
req_customer_gift_wrap=true
req_date_of_birth=19830612
req_merchant_secure_data1=my secure data one
req_merchant_secure_data2=my secure data two
req_merchant_secure_data3=my secure data three
req_merchant_secure_data4=my secure data four
req_journey_type=Round Trip
req_complete_route=BFH-SFO:SFO-HON
req_departure_time=2012-12-11 5:30 am EST
req_journey_leg1_orig=BFH
req_journey_leg1_dest=SFH
req_journey_leg2_orig=SFH
req_journey_leg2_dest=HON
message=Decision is REVIEW.
decision=REVIEW
decision_reason_code=480
decision_case_priority=3
decision_early_reason_code=100
decision_early_rcode=1
decision_early_return_code=9999999 decision_rcode=0
decision_return_code=1322001
decision_rflag=REVIEW
decision_rmsg=Decision is REVIEW.
score_reason_code=100
score_address_info=MM-A^MM-C^MM-CO^MM-ST^MM-Z^UNV-ADDR
score_factors=N^Y
score_host_severity=1
score_identity_info=MORPH-C
score_internet_info=FREE-EM
score_model_used=default_ca
score_phone_info=UNV-PH
score_rcode=1
score_return_code=1070000
score_rflag=SOK
score_rmsg=score service was successful
score_score_result=50
score_suspicious_info=NON-LN^RISK-FN
score_time_local=09:10:46
score_velocity_info=VEL-ADDR^VEL-NAME
```

Processing an eCheck Transaction

Endpoint:

- Test transactions: https://testsecureacceptance.cybersource.com/pay
- Live transactions: https://secureacceptance.cybersource.com/pay

Example eCheck Transaction Request

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=HPA0002
currency=USD
transaction_type=sale
amount=100.00
locale=en
bill_to_forename=Joe
bill_to_surname=Soap
bill_to_email=jsmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_city=San Francisco
bill_to_address_state=CA
bill_to_address_postal_code=94043
bill_to_address_country=US
payment_method=echeck
echeck_account_number=222234100
echeck_routing_number=121042882
echeck_account_type=c
echeck_sec_code=WEB
company_tax_id=123456789
driver_license_number=10-12234-123
driver_license_state=NY
date_of_birth=19901001
reference_number=77353001371031080772693
```

Example eCheck Transaction Reply

```
req_bill_to_address_country=US
req_driver_license_state=NY
req_driver_license_number=xx-xxxxx-xxx
req_date_of_birth=19901001
decision=ACCEPT
req_bill_to_address_state=CA
signed_field_names==comma separated list of signed fields
req_payment_method=echeck
req_transaction_type=sale
req_echeck_account_type=c
signature=ZUk7d99c/yb+kidvVUbz10JtykmjOt8LMPgkllRaZR8=
req_locale=en
reason_code=100
req_bill_to_address_postal_code=94043
req_echeck_account_number=xxxxx4100
req_bill_to_address_line1=1 My Apartment
req_echeck_sec_code=WEB
req_bill_to_address_city=San Francisco
signed_date_time=2013-06-12T09:59:50Z
req_currency=USD
req_reference_number=77353001371031080772693
req_echeck_routing_number=xxxxx2882
transaction_id=3710311877042130706689
req_amount=100.00
message=Request was processed successfully.
echeck_debit_ref_no=1
echeck_debit_submit_time=2013-03-25T104341Z
req_profile_id=HPA0002
req_company_tax_id=123456789
req_transaction_uuid=bdc596506c2677b79133c9705e5cf77c
req_bill_to_surname=Smith
req_bill_to_forename=Joe
req_bill_to_email=jsmith@example.com
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
```