M03: Secure Acceptance Hosted Checkout integration

Version	2.1
Date	March 2023

1 Version control

Revision	Date	Description
1.0	July 2020	Initial release
1.1	Oct 2020	Added footer/disclaimer. Updated EBC URLS and screenshots.
2.1	Jan 2023	Merged in latest specification changes

2 Audience

This guide is written for merchants who want to accept payments using Secure Acceptance Hosted Checkout Integration and who do not want to handle or store sensitive payment information on their own servers.

Using Secure Acceptance Hosted Checkout requires minimal development to start accepting payments. You develop only the code to initialize and invoke a payment form but do not need to code the form or workflow required to capture a card and process the transaction. You will also use the Enterprise Business Centre (EBC) to review and manage orders.

Smartpay Fuse offers several different ways for you to integrate and to take payments online. These options come with differing integration overheads and levels of functionality. It is important for you to spend a little time selecting the right approach for your needs before jumping in directly to integration.

- eCommerce Plugins: Easy integration to eCommerce platforms with our range of eCommerce platform plugins and partner integrations.
- Hosted Payment Pages: Secure Acceptance Hosted Checkout is the Smartpay Fuse solution for hosted payment pages. Payment capture forms are hosted by Smartpay Fuse and you either full page redirect from your site to these pages or host within an iFrame on your site. PCI overheads and integration effort is minimized with this approach. Some degree of branding and payment flow customisation is possible.
- Hosted Fields: Card fields are hosted independently, allowing you greater control over styling while retaining reduced PCI overheads.

- Direct Integration (REST API): Capture card details on your own website and control payment processing directly with our APIs. You can also use this API to query the status of a transaction or perform maintenance operations such as refunds.

If you do not wish to create an integration to our service using any of the options above, then it is possible to take Payments in a Mail Order Telephone Order (MOTO) environment using a Virtual Terminal in our Enterprise Business Centre. Find out more about the "Virtual Terminal" and how to get started here.

3 Smartpay Fuse in partnership with VISA Cybersource

ⓘ Smartpay Fuse has been created in partnership with VISA Cybersource. You may notice that some content in this guide refers or links out to content that references the Cybersource brand or Cybersource platform. While Cybersource provides the Smartpay Fuse technology platform it is important to note that not all features provided by Cybersource are available on the Smartpay Fuse gateway. Before integrating, please confirm that the features of Smartpay Fuse meet your needs. If you have any questions

4 Website requirements

Your website must meet these requirements to integrate with the Smartpay Fuse gateway:

- It must have a shopping-cart, customer order creation software, or an application for initiating the process of taking a payment.
- It must be capable of initiating HTTP POST requests to communicate with the Smartpay Fuse service.
- Your IT infrastructure must be Public Key Infrastructure (PKI) enabled and support TLS based form POST submissions.
- Your IT infrastructure must be capable of creating message signatures prior to submission of Secure Acceptance requests.
- If you are using an eCommerce platform plugin, then please follow guidance on system requirements using the collateral supplied with your chosen plugin.

If you have any questions about scheme, acquirer, GDPR or PCI compliance then please refer to our Merchant Procedure Guide. If the information you require is not available in the merchant procedure guide, please Get in contact.

5. Table of Contents

M03: Secure Acceptance Hosted Checkout integration 1

1 Version Control 2

2 Audience 2

3 Smartpay Fuse in partnership with VISA Cybersource 3

4 Website Requirements 3

5 Table of Contents 5

6 Glossary of terms 9

7 Introduction 10

7.1 Secure Acceptance Hosted Checkout workflow 14

7.2 Key Concepts 16

7.2.1 Payment tokens 16

7.2.2 One-Click Checkout 16

7.2.3 Level II and III Data 17

8 Creating and Configuring Secure Acceptance Profiles 17

8.1 Introduction to Secure Acceptance Hosted Checkout Profiles 17

8.1.1 Preliminary checks of the Transacting MID 18

8.1.2 Structure and Sections of a Secure Acceptance Profile 21

8.2 Creating a Secure Acceptance Profile 25

8.2.1 Profile Details 25

8.3 Payment Method Configuration 26

8.3.1 Adding Card Types and Currencies 27

8.3.2 Payer Authentication Configuration 28

8.3.3 Enabling Automatic Authorization Reversals 28

8.3.4 Visa Click to Pay Configuration 30

8.3.5 Enabling PayPal Express Checkout 30

8.4 Security Keys 32

8.4.1 Creating Security Keys 32
8.5 Checkout Configuration 33
8.5.1 Configuring the Payment Form 33
8.5.2 Configuring Billing Information Fields 34
8.5.3 Configuring Shipping Information Fields 35
8.5.4 Configuring Order Review Details 36
8.6 Merchant Notifications 36
8.6.1 Configuring Merchant Notifications 37
8.7 Customer Receipts 38
8.7.1 Configuring Customer Notifications 38
8.8 Customer Response Page 39
8.9 Configuring a Cybersource Hosted Response Page 39
8.10 Configuring a Custom Hosted Response Page 40
8.11 Configuring a Custom Cybersource Hosted Response Page 40
8.12 Configuring a Custom Cancel Response Page 41
8.13 Custom Checkout Appearance 41
8.13.1 Changing the Header Content 41
8.13.2 Changing the Body Color and Font Settings 42
8.13.3 Changing the Total Amount Background and Text Color 42
8.13.4 Changing the Progress Bar Color 43
8.13.5 Changing the Color and Text on the Pay or Finish Button 43
8.13.6 Changing the Footer Color and Uploading a Small Logo or Image 44
8.14 Checkout Language Localization 45
8.14.1 Locale Codes 45
8.14.2 Locale Codes (continued) 46
8.15 Activating a Profile 47
9 Processing Secure Acceptance transactions 48

9.1 Mandatory request fields 51
9.2 Important request fields 51
9.3 Important response message fields 54
9.4 Request fields example 55
9.5 Reply fields example 55
9.6 Secure Acceptance source code examples 58
9.7 Request Field 59
9.8 Example transaction use cases 61
9.8.1 Creating a Payment Card Token 61
9.8.2 Payment Token Transactions 62
9.8.3 Recurring Payments 64
9.8.4 Instalment Payments 66
9.8.5 Payment Token Updates 68
10 Testing transactions 70
11 Viewing Hosted Checkout transaction search in EBC 71
11.1 Secure Acceptance search 71
11.2 General Transaction search 74
12 Secure Acceptance merchant notifications 76
13 Secure Acceptance testing 77
13.1 Testing in test environment 77
13.2 Testing in live environment 78
14 Hosted Checkout Integration API Fields 79
14.1 Data Type Definitions 79
15 Request Fields 80
15.1 Request Field Description 80
16 Response Fields 128
16.1 Response Field Descriptions 129

17 Reason codes 166
18 Types of Notification 170
19 Response codes 171
19.1 International AVS Codes 171
19.2 CVN Codes 172
19.3 American Express SafeKey Response Codes 172
19.4 Visa Secure Response Codes 173
20 iFrame Implementation 174
20.1 Clickjacking Prevention 174
20.2 Iframe Transaction Endpoints 175
21 Get In contact 176
22 References 176
23 Disclaimer 178

6 Glossary of terms

Term	Description
Authorisation	Transaction authorisation is a standard part of the payment processing flow. This step isn't a guarantee of payment, but it does confirm that the cardholder has sufficient funds for the transaction to proceed and checks that the card hasn't been reported as lost or stolen.
Capture	Capturing an authorised transaction initiates the transfer of part/all of the funds reserved during authorisation. The combination of an authorisation and a capture is typically referred to as a 'sale'.
Enterprise Business Centre (EBC)	An online portal used by clients for payments, administration, maintenance and reporting.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS). A set of guidelines to make sure payment information is stored securely by your company and anyone else who stores, transmits or processes the cardholder's payment information on your behalf. It consists of a number of controls and the level of compliance is dictated by the type of integration you select. When using Secure Acceptance Hosted Checkout to collect and process payment cards the solution attracts a low PCI overhead (SAQ A). Please refer to our PCI FAQ for further information.
Reversal	Authorization reversals attempt to notify the issuer that all, or part, of a authorization has been cancelled and requests for the hold/ reservation of funds to be released (where possible).
Secure Acceptance Hosted Checkout	A hosted customer checkout page consisting of securely managed payment forms or a single page payment form for capturing payment card data.
Secure Acceptance profile	A Secure Acceptance profile consists of settings that you configure to create a secure and custom checkout experience.

SAQ	The PCI DSS Self-Assessment Questionnaires (SAQs) are validation tools for merchants and service providers that are eligible to evaluate and report their PCI DSS compliance via self-assessment.
Void	The cancellation of a settlement request prior to the batch cut-off time.

7 Introduction

This document describes the frontend Secure Acceptance Hosted Checkout integration method, which allows merchants to collect cardholder information in a secure and convenient way.

ⓘ **Smartpay Fuse has been created in partnership with VISA Cybersource. You may notice that some content in this guide refers or links out to content that references the Cybersource brand or Cybersource platform. While Cybersource provides the Smartpay Fuse technology platform it is important to note that not all features provided by Cybersource are available on the Smartpay Fuse gateway. Before integrating, please confirm that the features of Smartpay Fuse meet your needs. If you have any questions about the platform capability of integration options, then please Get in Contact.**

Secure Acceptance Hosted Checkout has the following functionality:

- Smartpay Fuse hosted payment page with customer redirect or iFrame, which supports Payer Authentication (3D Secure) and allows merchants to apply for SAQ-A PCI DSS scope.
- Available payment services:
    - Authorization
    - Sale (Authorization + Capture)
    - Token Create (can be combined with Authorization or Sale)
    - Token Update (can be combined with Authorization or Sale)
    - Token Usage (e.g., Customer-initiated Transactions; can be combined with Authorization or Sale)

- Other payment services like Capture, Authorization Reversal, Void and Credit can be implemented using a backend API integration such as our REST API or the Enterprise Business Centre.
- Use the Enterprise Business Centre for back-office administration, account maintenance and reporting.
- Payment Page set-up, look, feel and flow can be self-served through the Enterprise Business Centre.

Using Secure Acceptance Hosted Checkout you are able to accept the following payment methods:

- Visa
- Mastercard
- Maestro

The following payment methods can be accepted with further configuration:

- Amex
- Discover
- Diners

Note: a separate agreement is required to process Amex transactions. To arrange for Amex, Discover or Diners, please Get in contact. Get in

Smartpay Fuse is able to support a wide range of currencies. Depending on your configuration, you may have the ability to accept payments in only GBP. If you have any questions about multi-currency options, the please Get in Contact.

To accept payments through Secure Acceptance Hosted Checkout you will need to a create and configure a profile using the Enterprise Business Centre. The Enterprise Business Centre has the following access URLs:

1. Test Enterprise Business Centre: https://admin.smartpayfuse-test.barclaycard/ebc2
2. Live Enterprise Business Centre: https://admin.smartpayfuse.barclaycard/ebc2

To log-in you will need to know your Organisation ID and password. These credentials will be created as part of the Smartpay Fuse merchant on-boarding process. If you are not the primary admin user and do not have log-in credentials, then please contact the primary admin user to request access to the Enterprise Business Centre.

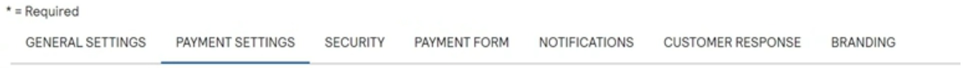
Secure Acceptance profiles are managed through the Payment Configuration > Secure Acceptance Settings side-bar menu in the Enterprise Business Centre:

- **Create a Secure Acceptance profile**: You can create a new profile here (+New Profile button on the top right of this page) or search through existing Active or Inactive profiles.

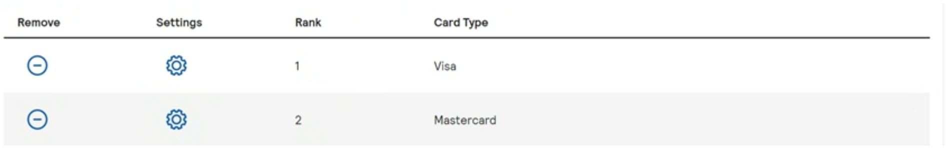
  ⓘ **We recommend that you copy and modify the default template (if one exists) which can be viewed by selecting the "Inactive" label in the "Profile Status" dropdown selection box.**

- **Configure the Secure Acceptance profile**: Customise and configure the Secure Acceptance profile to meet your functional and branding needs. Finalise the Secure Acceptance profile settings, adding security keys, URLs for transactional notifications and test.

If you wish to use the Secure Acceptance hosted checkout to process MOTO only transactions, you will need to create a dedicated profile, configured without 3D Secure. To do this, after creating a Secure Acceptance Hosted Checkout new profile, you will need to disable 3D Secure on each accepted payment card type. This can be done by visiting the Secure Acceptance Profile and selecting the "PAYMENT SETTINGS" tab, as below:

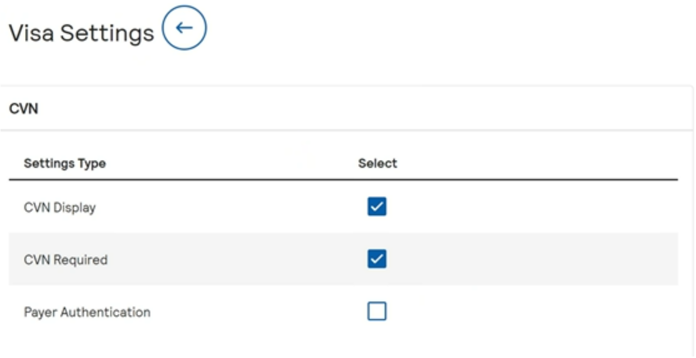


Select the "settings" cog for each payment type:



Remove	Settings	Rank	Card Type
⊖	⚙	1	Visa
⊖	⚙	2	Mastercard

Deselect the “Payer Authentication” checkbox, example below:



Visa Settings

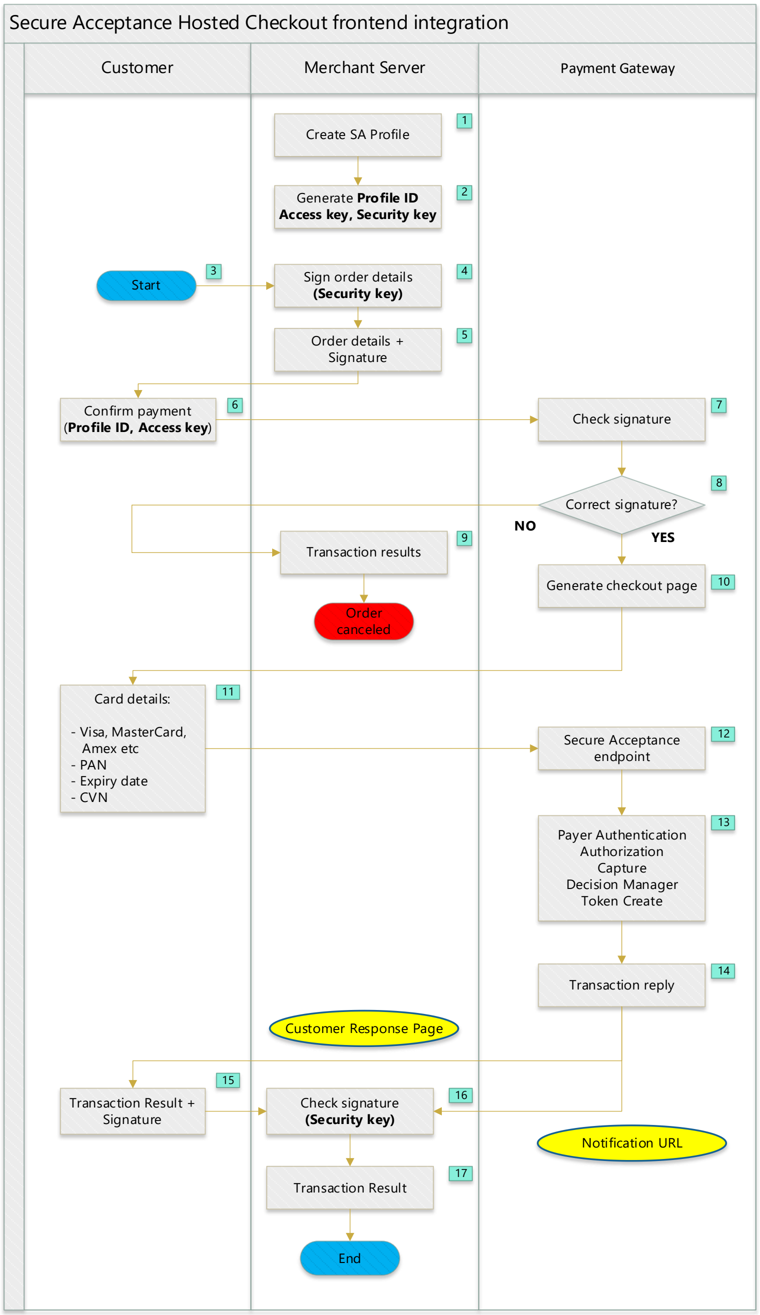
CVN

Settings Type	Select
CVN Display	☑
CVN Required	☑
Payer Authentication	□

You will need to ensure that when initiating a Secure Acceptance Hosted Checkout hosted payment page request via the Secure Acceptance API that you include the value `”MOTO”` in the field `e_commerce_indicator` within your request (please see page 95).

7.1 Secure Acceptance Hosted Checkout workflow

Secure Acceptance Hosted Checkout is a front-end integration method that provides a fully hosted payment page to the merchant and allows card data to be sent directly from customer browser to the payment gateway. The integration flow for this type of integration is illustrated below:



ID	Description
1	A Secure Acceptance profile is created using the Enterprise Business Centre. It is possible to create a new profile afresh or copy any that are pre-configured on your account (select “Inactive” from the “Profile Status” dropdown on the Secure Acceptance Settings page).
2	As a part of Secure Acceptance profile configuration, a merchant generates three credentials: • Profile ID • Access key • Security key
3	Customer clicks on the Pay button on the merchant website, starting the checkout process
4	Merchant server creates a SA request message and signs key fields; order fields, billing address fields, shipping address fields, transaction type etc. (but not card details), using Security Key.
5	Order details with a signature are sent to the customer browser together with a confirmation page.
6	Customer proceeds to payment and HTTPS POST message with signed order details is sent to Smartpay Fuse URL, depending on the transaction type. **Profile ID** and **Access key** are used for defining Secure Acceptance profile and authentication.
7	Smartpay Fuse creates a signature for the received order fields and compares it with the signature sent by the merchant.
8	If the signature is not correct, go to the step 9. If the signature is correct, go to the step 10.
9	Reply message is sent to the customer browser that transaction was declined. This message must be forwarded to the merchant server. The flow ends.
10	Smartpay Fuse generates the checkout page(s), based on Secure Acceptance profile settings.
11	The payment page is presented to the customer to enter card details.

12	Card details are sent directly from customer browser to the Smartpay Fuse service. **IMPORTANT**: this flow from customer browser directly to Smartpay Fuse must be followed to retain a PCI SAQ A level of compliance. If you pass card details through your own servers at any point then you will be in scope of much more stringent PCI requirements.
13	Depending on the payment workflow, different Smartpay Fuse services are run. Please note, that different services require different Smartpay Fuse endpoints.
14	SA creates reply message which is sent to the merchant via: • Customer Response Page and/or • Notification URL
15	In case of a Customer Response Page notification, transaction results, with a signature created by Smartpay Fuse, are sent to the URL, specified in the Secure Acceptance profile.
16	Merchant generates a signature of the received fields and compares it with the signature received from Smartpay Fuse.
17	If the signature check is successful, the merchant saves the transaction results.

7.2 Key concepts

7.2.1 Payment Tokens

Payment tokens are unique identifiers that replace sensitive payment information and that cannot be mathematically reversed. Smartpay Fuse securely stores relevant card information in accordance with scheme rules, replacing it with the payment token. The token is also known as a subscription ID, which you store on your server.

The payment token replaces the card number, and optionally the associated billing, shipping, and card information. No sensitive card information is stored on your servers, thereby reducing your PCI DSS obligations.

7.2.2 One-Click Checkout

With one-click checkout, customers can buy products with a single click. Secure Acceptance supports payment card tokenization, saving returning customers from re-entering all of their payment details on subsequent transactions. Before a customer can use one-click checkout, they must create a payment token during the first transaction on the merchant website. See Payment Token Transactions (page 62). The payment token is a non card representation of the payment details that can be stored by Smartpay Fuse in accordance with scheme rules. When the payment token is included in a payment request, Smartpay Fuse retrieves the card, billing, and shipping information related to the original payment request and uses those secured details to process a transaction.

7.2.3 Level II and III Data

Secure Acceptance does not support Level II and III data. Please refer to the REST API integration method in order to utilise this functionality.

8 Creating and configuring Secure Acceptance Profiles

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 websites. You can display a multi-step checkout process or a single page checkout to the customer as well as configure the appearance and branding, payment options, languages, and customer notifications.

8.1 Introduction to Secure Acceptance Hosted Checkout Profiles

Before accepting payments using Secure Acceptance Hosted Checkout, two steps are required:

1. Make sure that a Secure Acceptance profile has been created for the transacting MID
2. Complete the Secure Acceptance profile configuration on the transacting MID, by creating security keys, setting up the notification URLs and adding customization (if required). Merchant can do this while logged in to the account MID or from transacting MID. In the latter case transacting MID must have a user account created.

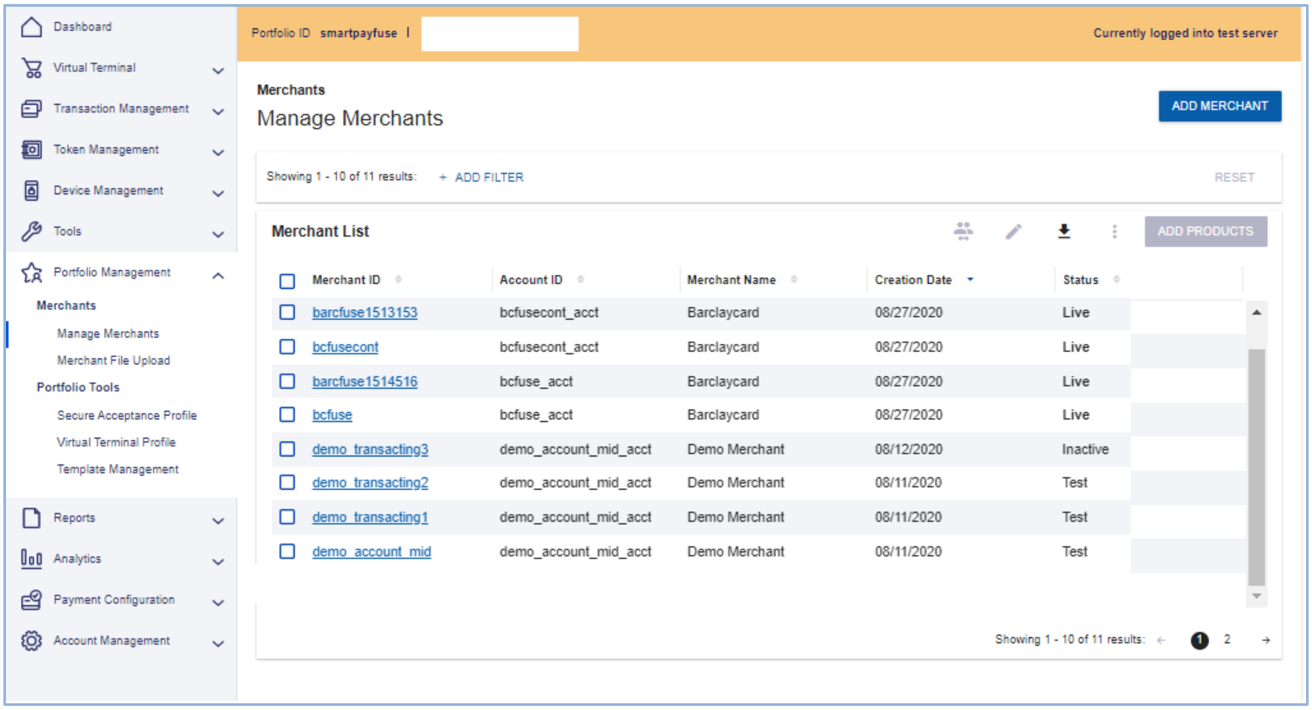
An ‘Active’ profile is required on the chosen transacting MID before you will be able to use Secure Acceptance Hosted Checkout to start processing transactions; this is true in both test and live environments.

8.1.1 Preliminary checks of the Transacting MID

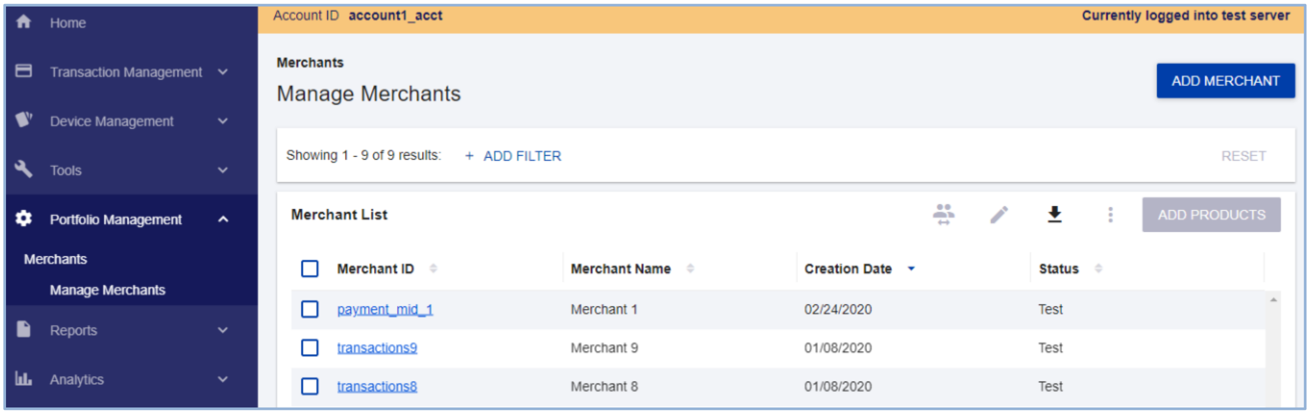
Depending on how your service has been set-up, you may have multiple or only one transacting MID.

> **If your service was configured with only one transacting MID you will not have the Portfolio Management option available in the Enterprise Business Centre sidebar menu and can skip this section.**

To select a transacting MID, log in into account MID and proceed to **Portfolio Management -> Manage Merchants** menu:



□	Merchant ID	Account ID	Merchant Name	Creation Date	Status
□	barcfuse1513153	bcfusecont_acct	Barclaycard	08/27/2020	Live
□	bcfusecont	bcfusecont_acct	Barclaycard	08/27/2020	Live
□	barcfuse1514516	bcfuse_acct	Barclaycard	08/27/2020	Live
□	bcfuse	bcfuse_acct	Barclaycard	08/27/2020	Live
□	demo_transacting3	demo_account_mid_acct	Demo Merchant	08/12/2020	Inactive
□	demo_transacting2	demo_account_mid_acct	Demo Merchant	08/11/2020	Test
□	demo_transacting1	demo_account_mid_acct	Demo Merchant	08/11/2020	Test
□	demo_account_mid	demo_account_mid_acct	Demo Merchant	08/11/2020	Test



Account ID account1_acct

Currently logged into test server

Merchants

Manage Merchants

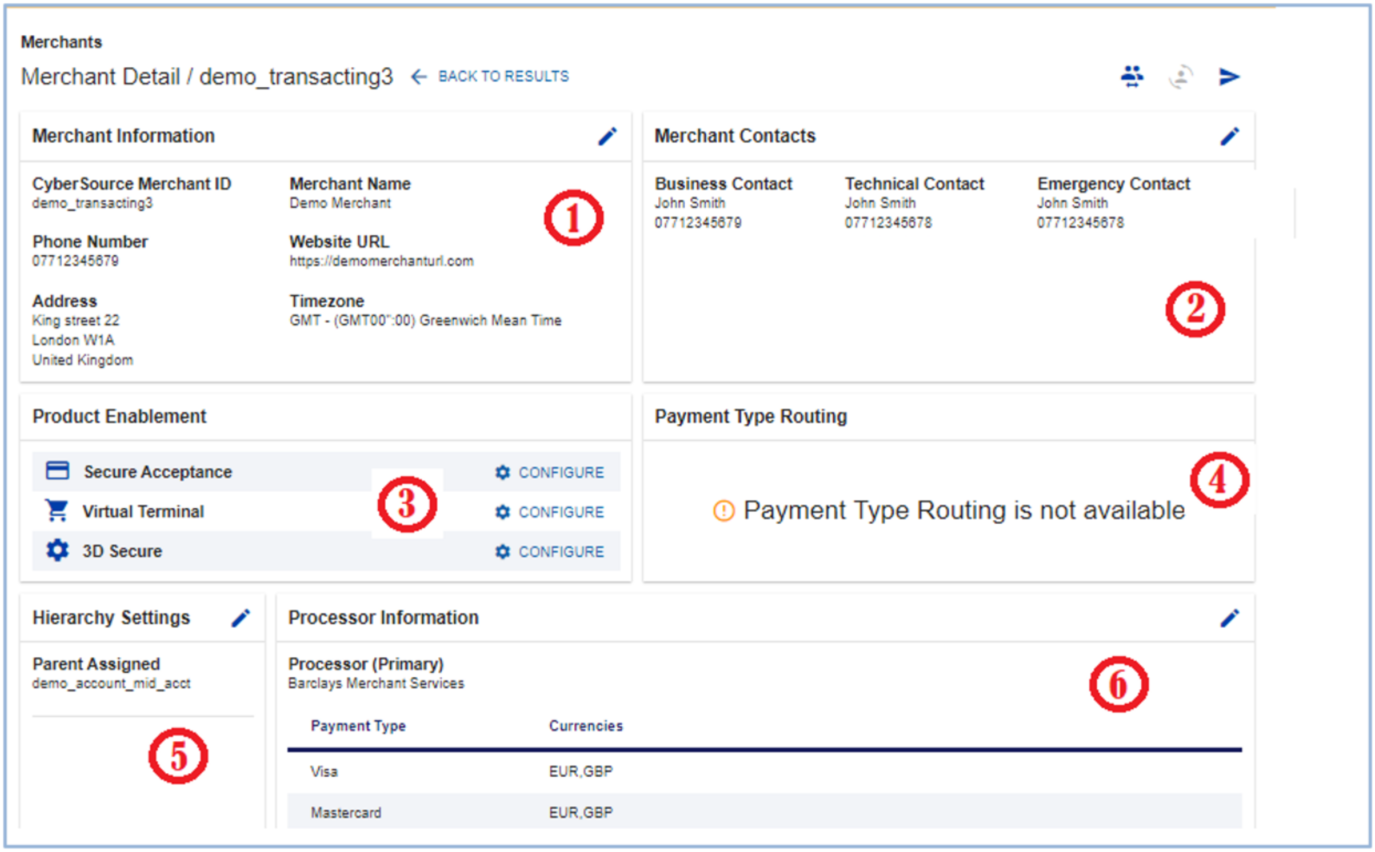
Showing 1 - 9 of 9 results:

Merchant List

□	Merchant ID	Merchant Name	Creation Date	Status
□	payment_mid_1	Merchant 1	02/24/2020	Test
□	transactions9	Merchant 9	01/08/2020	Test
□	transactions8	Merchant 8	01/08/2020	Test

Click the MID name of the merchant for whom you are wanting to configure a Secure Acceptance profile (in the example transacting MID has a name **demo_transacting3**).

Merchant will see the **Merchant Detail** window, which displays all merchant details that were previously configured by Barclays:



Merchants

Merchant Detail / demo_transacting3

Merchant Information

CyberSource Merchant ID
demo_transacting3

Merchant Name
Demo Merchant

Phone Number
07712345679

Website URL
https://demomerchanturl.com

Address
King street 22
London W1A
United Kingdom

Timezone
GMT - (GMT00":00) Greenwich Mean Time

Merchant Contacts

Business Contact
John Smith
07712345679

Technical Contact
John Smith
07712345678

Emergency Contact
John Smith
07712345678

Product Enablement

Secure Acceptance

Virtual Terminal

3D Secure

Payment Type Routing

Payment Type Routing is not available

Hierarchy Settings

Parent Assigned
demo_account_mid_acct

Processor Information

Processor (Primary)
Barclays Merchant Services

Payment Type	Currencies
Visa	EUR,GBP
Mastercard	EUR,GBP

Below is a description of different sections of **Merchant Detail** window:

Section number	Section Name	Description
1	Merchant Information	General merchant information
2	Merchant Contacts	Merchant business, technical and emergency contacts. Please make sure this information is correct.
3	Product enablement	Allows merchant to enable different payment services on the transacting MID.
4	Payment Type Routing	Not used at the moment
5	Hierarchy Settings	Shows the parent MID for the transacting MID
6	Processor Information	Processors, card types and currencies enabled for this transacting MID

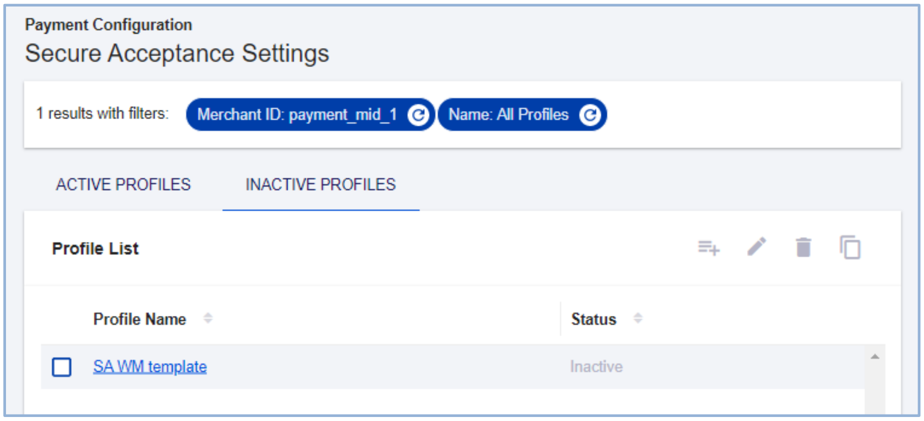
ⓘ **A merchant may change details in the Merchant Information and the Merchant Contacts configuration sections. In the Processor Information section, the merchant can only add processors and card types supported by Barclays. If the merchant needs another processor or card type, they should speak to Barclays.**

ⓘ **Merchants need to call Barclaycard to advise of any changes to the main business contact credentials to ensure those changes are reflected correctly across Barclaycard systems.**

To change the information, click on the "**Pen**" icon in the right-hand top corner of the section.

8.1.2 Structure and sections of a Secure Acceptance Profile

To configure a Secure Acceptance profile, log in to the account MID or transacting MID and select **Payment Configuration -> Secure Acceptance.** If logging in at the account MID level, you will need to specify the transacting MID name. Then switch to the **INACTIVE PROFILES** tab.



Payment Configuration

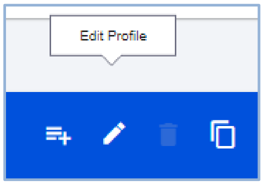
Secure Acceptance Settings

1 results with filters: Merchant ID: payment_mid_1 Name: All Profiles

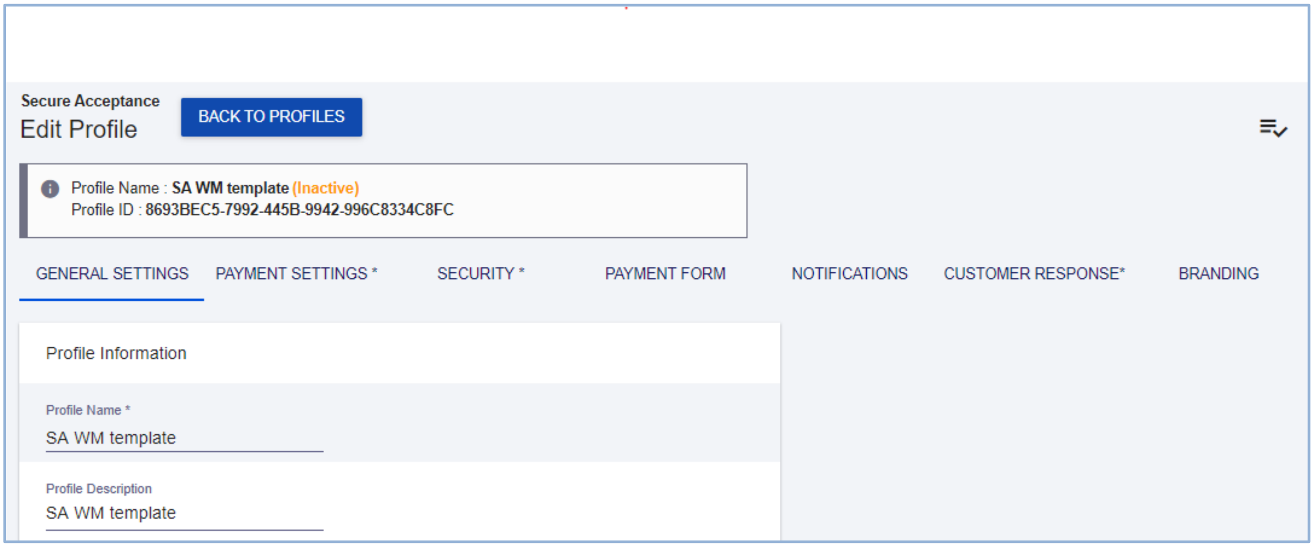
	Profile Name	Status
□	SA WM template	Inactive

There should be one or more profile templates already assigned. If there are no Secure Acceptance profiles in the **INACTIVE PROFILES** section, contact support to assign the profile templates to the transacting MID.

Select the profile merchant want to configure and click on the **Edit Profile** icon.



The Edit Profile window will be opened with several tabs to configure the profile:



Profile Name : **SA WM template** (Inactive)
Profile ID : 8693BEC5-7992-445B-9942-996C8334C8FC

Profile Name *
SA WM template

Profile Description
SA WM template

Below is a summary table of what merchants need to review/update to finalize Secure Acceptance profile settings:

Tab name	**Settings**
General Settings	Contact Information - Name - Email Address - Phone Number Added Value Services: - Payment Tokenization - Don't enable BIN Lookup
Payment settings	Add Card Types (to change accepted card types) Card Type - CVN Display - CVN Required - Payer Authentication (must be enabled) - Currencies
Security	Merchant must generate a security key. The **Access Key**, **Secret Key** and the **Profile ID** are required for SA integration
Payment Form	This is where Merchant setup the cardholder checkout experience.

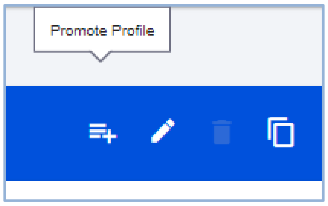
	Please note, that billing address fields are mandatory, so merchant needs to send billing address fields in the request message to SA or collect billing address during checkout.
Notifications	Merchant Notifications - Merchant POST URL - Merchant POST Email Customer Notifications - Email Receipt to Customer Please note, that Merchant POST URL notifications require sending acknowledgment messages back to Smartpay Fuse. If merchant fail to do this, notifications can be delayed and eventually cancelled.
Customer Response	Transaction Response Page - If **Hosted By You** is selected, merchant can specify a merchant response page URL. The cardholder will be re-directed to this page after the authorization is complete, so merchant can display the result to the cardholder. The page will receive the transaction results in its payload. This is the same information that is posted to the Merchant POST URL on the Notifications tab. Merchant can update merchants order system based on the Transaction response page or the Merchant POST URL or a combination of both. - If **Hosted by Cybersource** is selected the customer will be shown the result of the payment and then redirected to the **Custom Redirect After Checkout** page. However, there will NOT be a payload with this page, so it is important to enable Merchant notifications to actually receive the result of the payment. Custom Cancel Response Page Custom Redirect After Checkout - This will only be shown if merchant have both of the above options set to **Hosted by Cybersource**
Branding	This tab allows merchant to customize the checkout pages to match merchant’s branding.

After making changes to the tab, merchant needs to click SAVE button before moving to the next tab.

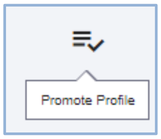
When merchant has made all necessary changes to the Secure Acceptance profile, merchant needs to make it active - or promote it. Until the profile is promoted, it is inactive and cannot be used for transaction processing and all transaction will be declined.

Note: it is possible to edit an active profile without affecting transactions. This will create a new profile in EDIT state within the Inactive Profile list. This new profile in EDIT state will require configuration and promotion before any changes will take effect. Please ensure that all settings are correct before promoting a profile in EDIT state to live.

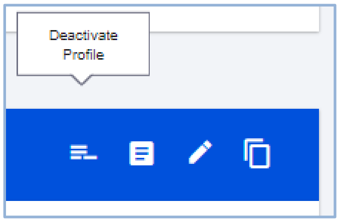
To promote a profile from the **Secure Acceptance Settings** menu in the **INACTIVE PROFILES** tab, select the profile and click the **Promote Profile** button.



Or use the **Promote Profile** button, in the **Edit Profile** menu.



If merchant need to make changes to the profile with an Active status, deactivate it first in the **Secure Acceptance Settings** menu in the **ACTIVE PROFILES** tab using the **Deactivate Profile** button.



Copy of the active profile will be created in the **INACTIVE PROFILES** tab, with initial active profile still in ACTIVE PROFILE tab and ready to accept payments.

After you make all the changes to the inactive profile, activate it, so it replaces active profile currently in use.

8.2 Creating a Secure Acceptance Profile

If you have created a sandbox account through our developer center then Secure Acceptance will already be active and available for you to evaluate in test. If you are working with our corporate client professional services team, then they may have already provided you a test service if required.

To create a Secure Acceptance Hosted Checkout profile:

1. Log in to the Business Centre:

   Test: https://admin.smartpayfuse-test.barclaycard/ebc2/

   Production: https://admin.smartpayfuse.barclaycard/ebc2/

2. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
3. Click **New Profile**. The Create Profile page appears.
4. Enter or verify these profile details.
5. Click **Submit**.

8.2.1 Profile details

Profile detail	Description
Profile Name	The Secure Acceptance profile name is required and cannot exceed 40 alphanumeric characters.

Profile Description	The profile description cannot exceed 255 characters.
Integration Method	Check Hosted Checkout Integration.
Company Name	The company name is required and cannot exceed 40 alphanumeric characters.
Company Contact Name	Enter company contact information: name, email, and phone number.
Company Contact Email	
Company Phone Number	
Payment Tokenization	Check **Payment Tokenization**. For more information, see Processing Secure Acceptance transactions (on page 48)
Decision Manager	Check **Decision Manager**. For more information, see **Error! Reference source not found.** (on page 52).
Verbose Data	Check **Verbose Data**. For more information, see **Error! Reference source not found.** (on page 52).
Generate Device Fingerprint	Check **Generate Device Fingerprint**. For more information, see **Error! Reference source not found.** (on page 52).

8.3 Payment method configuration

You must configure at least one payment method before you can activate a profile.

A payment method selection page is displayed as part of the checkout process for any of these scenarios:

- Multiple payment methods are enabled for the profile and no payment_method field is included in the request.
- payment_method=`visacheckout` is included in the request.
- Visa Click to Pay is the only enabled payment method for the profile.

You can skip displaying the payment method selection page by specifying card as the only available payment method. Customers can change the payment method during the checkout process.

ⓘ **Smartpay Fuse offers many ways to pay. Some of these options require furtherset-up, including Visa Click to Pay. If you would like to use Click to Pay then please Get in contact to enable the feature.**

8.3.1 Adding card types and currencies

For each card type you choose, you can also manage currencies and payer authentication options. Smartpay Fuse offers only GBP as standard at present, so confirm that this is selected in your configuration.

ⓘ **The Smartpay Fuse platform can offer additional currencies, but these require further set-up and configuration. If you would like to use additional currencies, then please Get in contact to discuss further.**

The card verification number (CVN) is a three- or four-digit number that helps ensure that the customer possess the card at the time of the transaction.

- In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
- Choose a profile. The General Settings page appears.
- Click **Payment Settings**. The Payment Settings page appears.
- Click **Add Card Types**. The list of card types appears.
- Check each card type that you want to offer to the customer as a payment method. Your payment processor must support the card types.
- Click the settings icon for each card type. The card settings and currencies lists appear.
- Check **CVN Display** to display the CVN field on Secure Acceptance. The customer decides whether to enter the CVN. Barclaycard recommends that you display the CVN to reduce fraud.
- Check **CVN Required**. The CVN Display option must also be checked. If this option is checked, the customer is required to enter the CVN. Barclaycard recommends that you require the CVN to reduce fraud.
- Check Payer Authentication.
- Check the currencies for each card.
- By default, the currencies will be configured correctly for Smartpay Fuse; at present this is GPB only.
- Click **Submit**. The card types are added as an accepted payment type.
- Click **Save**.

8.3.2 Payer Authentication configuration

Payer Authentication will be set-up for you by Barclaycard during account creation. Please note that Payer Authentication can take up to 36 hours to be live once configured due to downstream system dependencies. Normally this is process takes up to 24 hours but can take up to 3 days over weekends and public holidays. For more information about Payer Authentication please see [**4**] in References.

Payer authentication is the implementation of 3D Secure. It prevents unauthorized card use and provides added protection from fraudulent chargeback activity. Secure Acceptance supports 3D Secure version 2.2.

For Secure Acceptance, Smartpay Fuse supports these types of payer authentication:

- American Express SafeKey
- Diners ProtectBuy
- Mastercard Identity Check
- Visa Secure

For each transaction, you receive detailed information in the replies and in the transaction details page of the Business Centre. You can store this information for 12 months. Barclaycard recommends that you store the payer authentication data because you can be required to display this information as enrolment verification for any payer authentication transaction that you re-present because of a chargeback.

The Chargebacks team may request you to provide all data in human-readable format as defined in our Merchant Procedure Guide.

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 Secure Acceptance testing (on page 77).

8.3.3 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 reversal. An automatic reversal releases the reserved funds held against a customer's card.

1. In the left navigation panel, choose Payment Configuration > Secure Acceptance Settings. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click Payment Settings. The Payment Settings page appears.
4. Check Fails AVS check. Authorization is automatically reversed on a transaction that fails an AVS check.
5. Check Fails CVN check. Authorization is automatically reversed on a transaction that fails a CVN check.
6. Click Save.

ⓘ **When the AVS and CVN options are disabled and the transaction fails an AVS or CVN check, the customer is notified that the transaction was accepted. You are notified to review the transaction details if your account is set up for these AVS and CVN rules. This can be performed within the Transaction Search view of EBC. See Types of notification (on page 170).**

ⓘ **For Mastercard this functionality is only compliant when using pre-authorisation instead of final authorisation (the default). Please contact support if you wish to configure your account for pre-authorisation.**

8.3.4 Visa Click to Pay configuration

Visa Click to Pay requires the customer to enter only a username and password to pay for goods. It eliminates the need to enter account, shipping, and billing information. The customer logs in to their Visa Click to Pay account and chooses the card with which they would like to pay.

ⓘ **Smartpay Fuse offers many ways to pay. Some of these options require further set-up, including Visa Click to Pay. If you would like to use, Click to Pay then please Get in contact to enable the feature.**

The payment methods selection page is displayed as part of the checkout process for these scenarios:

- Multiple payment methods are enabled for the profile and no payment_method field is included in the request.
- Visa Click to Pay is the only enabled payment method for the profile.
- payment_method=visacheckout is included in the request.

If the Secure Acceptance profile is enabled to request the payer authentication service for a specific card type, the customer is redirected to the relevant payer authentication screen before Secure Acceptance processes the transaction and redirects the customer to your website.

8.3.5 Enabling PayPal Express checkout

ⓘ **PayPal Express checkout requires additional configuration by our service and support teams before use. If you would like to use this feature, please Get in contact to have your account configured for this feature.**

PayPal Express Checkout is not supported on a Secure Acceptance iframe integration.

Add the PayPal Express Checkout payment method to the Hosted Checkout Integration payment methods selection page. Redirect the customer to their PayPal account login. When logged in to their PayPal account they can review orders and edit shipping or payment details before completing transactions.

The payment methods selection page is displayed as part of the checkout process when multiple payment methods are enabled for the profile and no **payment_method** field is included in the request. If you include **payment_method=**`paypal` in the request, the payment methods selection page is not displayed, and the customer is redirected to PayPal.

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Payment Settings**. The Payment Settings page appears.
4. Check Enable PayPal Express Checkout.
5. Check **Allow customers to select or edit their shipping address within PayPal** to allow customers to edit the shipping address details that they provided in the transaction request to Secure Acceptance. Customers select a new address or edit the address when they are logged in to their PayPal account.
6. When the transaction type is authorization, check one of these options:
   - Request a PayPal authorization and include the authorization response values in the response—check this option to create and authorize the PayPal order.

ⓘ **The customer funds are not captured using this option. You must request a PayPal capture; see the PayPal guide. If the transaction type is `sale`, Secure Acceptance authorizes and captures the customer funds.**

   - Request a PayPal order setup and include the order setup response values in the response—check this option to create the PayPal order.

ⓘ **The customer funds are not authorized or captured using this option. You must request a PayPal authorization followed by a PayPal capture request; see the PayPal guide. If the transaction type is `sale`, Secure Acceptance authorizes and captures the customer funds.**

7. Click **Save**.

8.4 Security Keys

You must create a security key before you can activate a Secure Acceptance Hosted Checkout profile.

You cannot use the same security key for both test and production transactions. You must download a security key for each version of Secure Acceptance for test and production.

21 Test: https://admin.smartpayfuse-test.barclaycard/ebc2/

22 Production: https://admin.smartpayfuse.barclaycard/ebc2/

On the Profile Settings page, click **Security**. The Security Keys page appears. 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. A security key expires in two years and protects each transaction from data tampering.

8.4.1 Creating Security Keys

1. Log in to the Business Center.
2. In the left navigation panel, choose Payment Configuration > Secure Acceptance Settings. The Secure Acceptance Settings page appears.
3. Choose a profile. The General Settings page appears
4. Click **Security**. The security keys page appears.
5. Click the Create Key plus sign (+).
6. Enter a key name (required)
7. Choose signature version 1 (default).
8. Choose signature method **HMAC-SHA256** (default).
9. Click **Create**
10. Click **Confirm**. The Create New Key window expands and displays the new access key and secret key. This panel closes after 30 seconds.
11. Copy and save or download 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 Secure Acceptance source code examples (on page 58).

- Secret key: signs the transaction data and is required for each transaction. Copy and paste this secret key into your security script. See Secure Acceptance source code examples (on page 58).

ⓘ **Remember to delete the copied keys from your clipboard or cached memory.**

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.

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.

8.5 Checkout configuration

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

8.5.1 Configuring the Payment Form

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Payment Form**. The Payment Form page appears.
4. Choose the payment form flow:
    - **Multi-step payment form**—the checkout process consists of a sequence of pages on which the customer enters or reviews information before submitting a transaction. The default sequence is payment selection (if multiple payment methods are enabled), billing, shipping, payment, review, and receipt.
    - **Single page form**—the checkout process consists of one page on which the customer enters or reviews information before submitting a transaction.

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

5. Check Display the total tax amount in each step of the checkout process.

The total tax amount must be included in each transaction. Calculate and include the total tax amount in the **tax_amount** field.

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

6. Click **Save**.

8.5.2 Configuring Billing Information fields

ⓘ **These can be collected on your pages and supplied via the Secure Acceptance API or via the payment form presented for you by Secure Acceptance hosted checkout. If you chose to use our payment form to collect these fields then the precise fields can be defined in the Billing Information field configuration.**

Select the customer billing information fields that you want displayed on Secure Acceptance. If these fields are captured at an earlier stage of the order process (for example on your website), they can be passed into Secure Acceptance as hidden form fields. See Request Fields (on page 91). You can shorten the checkout process by not selecting billing information.

1. In the left navigation panel, choose Payment Configuration > Secure Acceptance Settings.

The Secure Acceptance Settings page appears.

2. Choose a profile. The General Settings page appears.
3. Click **Payment Form**. The Payment Form page appears.
4. Check **Billing Information**. The billing information fields appear.
5. Check the billing information fields that your merchant provider requires. The options for each field are:
    - Display: the customer can view the information displayed in this field. Choose this option if you want to pre-populate the billing information fields when the

Secure Acceptance Hosted Checkout is rendered—these fields must be passed into Secure Acceptance as hidden form fields.

- Edit: the customer can view and edit the billing information on the Secure Acceptance Hosted Checkout. When you select this option, the display option is automatically selected.
- Require: the customer is required to enter the billing information on the Secure Acceptance Hosted Checkout before they submit the transaction. When you select this option, all other options are automatically selected.

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

6. Indicate whether to mask sensitive fields.
7. Click **Save**.

8.5.3 Configuring Shipping Information fields

Select the shipping information fields that your merchant provider requires.

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. If these fields are captured at an earlier stage of the order process (for example, on your website), they can be passed into Secure Acceptance as hidden form fields. See Request fields (on page 80). You can shorten the checkout process by not selecting shipping information.

1. In the left navigation panel, choose Payment Configuration > Secure Acceptance Settings. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click Payment Form. The Payment Form page appears.
4. Check Shipping Information.
5. Check the shipping information fields that your merchant provider requires. The options for each field are:

- Display: the customer can view the information displayed in this field. Choose this option if you want to pre-populate the shipping information fields when the Secure Acceptance Hosted Checkout is rendered—these fields must be passed into Secure Acceptance as hidden form fields.

- Edit: the customer can view and edit the shipping information on the Secure Acceptance Hosted Checkout. When you select this option, the display option is automatically selected.
- Require: the customer is required to enter the shipping information on the Secure Acceptance Hosted Checkout before they submit the transaction. When you select this option, all other options are automatically selected.

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

1. Indicate whether to mask sensitive fields.
2. Click **Save**.

8.5.4 Configuring Order Review details

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

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Payment Form**. The Payment Form page appears.
4. Check the fields that you want displayed on the Order Review page of Secure Acceptance Hosted Checkout. 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.
5. Click **Save**.

8.6 Merchant notifications

Secure Acceptance sends merchant and customer notifications in response to transactions. You can receive a merchant notification by email or as an HTTPS POST to a URL for each transaction processed. Both notifications contain the same transaction result data.

Ensure that your system acknowledges POST notifications (even when under load) as quickly as possible. Delays of more than 10 seconds might result in delays to future POST notifications.

ⓘ **Barclaycard recommends that you implement the merchant POST URL to receive notification of each transaction. Parse the transaction response sent to the merchant POST URL and store the data within your order management system. This ensures the accuracy of the transactions and informs you of the transaction state and state changes.**

8.6.1 Configuring merchant notifications

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Notifications**. The Notifications page appears.
4. Choose a merchant notification in one of two ways:
   - Check **Merchant POST URL**. Enter the HTTPS URL.
     Smartpay Fuse sends transaction information to this URL. For more information, see Response Fields (on page 170). Only an HTTPS URL supporting TLS 1.2 or higher should be used for the merchant POST URL. If you encounter any problems, contact Barclaycard Customer Support.
   - Check **Merchant POST Email**. Enter your email address.
     Smartpay Fuse sends transaction response information to this email address including payment information, return codes, and all relevant order information. See Response Fields (on page 170).
5. Choose the card number digits that you want displayed in the merchant or customer receipt:
   - Return payment card BIN: displays the card's Bank Identification Number (BIN), which is the first eight digits of the card number. All other digits are masked: 12345678xxxxxxxx
   - Return last four digits of payment card number: displays the last four digits of the card number. All other digits are masked: xxxxxxxxxxxx1234

- Return BIN and last four digits of payment card number: displays the BIN and the last four digits of the card number. All other digits are masked: 12345678xxxx1234

6. Click **Save**.

8.7 Customer receipts

You can send a purchase receipt email to your customer and a copy to your own email address. Both are optional. Customers can 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).

8.7.1 Configuring customer notifications

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Notifications**. The Notifications page appears.
4. Check Email Receipt to Customer.
5. Enter the sender email address to be displayed on the customer receipt. The customer will reply to this email with any queries.
6. Enter the sender name of your business. It is displayed on the customer receipt.
7. Check **Send a copy to**. This setting is optional.
8. Enter your email address to receive a copy of the customer's receipt. Your copy of the customer receipt will contain additional transaction response information.
9. Check Display Notification Logo.
10. Click **Upload Company Logo**. Find and upload the image that you want to display on the customer receipt and email. The image file must not exceed 840 (w) x 60 (h) pixels and must be GIF, JPEG, or PNG. The logo filename must not contain any special characters, such as a hyphen (-).
11. Check Custom Email Receipt. Barclaycard recommends that you implement a DNS configuration to enable Smartpay Fuse to send email receipts on your behalf.
12. Check the type of email receipt you want to send to a customer:
    - Standard email receipt: this email is automatically translated based on the locale used for the transaction.

- Custom email receipt: this email can be customized with text and data references. The email body section containing the transaction detail appears between the header and footer. Custom text is not translated when you use different locales.

13. Check **Custom Email Subject** and enter up to 998 characters. When the maximum number of characters is exceeded, the subject heading defaults to Order Confirmation. You can insert email smart tags in the email subject, header, and footer sections to include specific information. Select each smart tag from the drop-down list and click Insert.
14. Click **Save**.

8.8 Customer response page

You must configure the customer response page before you can activate a profile.

You can choose to have a transaction response page displayed to the customer at the end of the checkout process, and a cancel response page displayed during 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 might be able to correct problems related to address or card verification, or you might 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.

ⓘ **Smartpay Fuse has been created in partnership with VISA Cybersource. You may notice that some content in this guide refers, or links out to, content that references the Cybersource brand or Cybersource platform. While Cybersource provides the Smartpay Fuse technology platform it is important to note that not all features provided by Cybersource are available on the Smartpay Fuse gateway. Before integrating, please confirm that the features of Smartpay Fuse meet your needs by getting in touch here.**

8.9 Configuring a Cybersource hosted response page

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.

2. Choose a profile. The General Settings page appears.
3. Click **Customer Response**. The Customer Response page appears.
4. Under the Transaction Response Page heading, check **Hosted by Cybersource**.
5. Under the Transaction Response Message heading, choose a number from the **Retry Limit** drop-down list. The maximum number of times a customer can retry a declined transaction is five.
6. Under the Customer Redirect after Checkout heading, enter the redirect URL of the web page. This web page is displayed to the customer after the checkout process is completed.
7. Click **Save**. The Profile Settings page appears.

8.10 Configuring a custom hosted response page

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Customer Response**. The Customer Response page appears.
4. Under the Transaction Response Page heading, check **Hosted by You**.
5. Enter the URL for your customer response page. Use port 80, 443, or 8080 in your URL. Only port 443 should be used with a HTTPS URL. Parse the transaction results from the URL according to the reason code () and redirect your customer to the appropriate response page. See Reason Codes (on page 223).
6. Under the Transaction Response Message heading, choose a number from the **Retry Limit** drop-down list. The maximum number of times a customer can retry a declined transaction is 5.
7. Under the Customer Redirect after Checkout heading, enter the redirect URL of the web page. This web page is displayed to the customer after the checkout process is completed.
8. Click **Save**.

8.11 Configuring a custom Cybersource hosted response page

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Customer Response**. The Customer Response page appears.

4. Under the Custom Cancel Response Page heading, check **Hosted by Cybersource**.
5. Click **Save**.

8.12 Configuring a custom cancel response page

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Customer Response**. The Customer Response page appears.
4. Under the Custom Cancel Response Page heading, check **Hosted by You**.
5. Enter the URL for your customer response page. Use port 80, 443, or 8080 in your URL. Only port 443 should be used with a HTTPS URL. Parse the transaction results from the URL according to the reason code, and redirect your customer to the appropriate response page. See Reason Codes (on page 223).
6. Click **Save**.

8.13 Custom checkout appearance

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

Barclaycard recommends that you preview your changes in the Image Preview window.

To display an image as the header banner of the payment form, the image dimensions must not exceed 840 (w) x 60 (h) pixels and the image size must not exceed 100 kB. To display a small logo within the header banner, the logo height must not exceed 60 pixels. The image file must be GIF, JPEG, or PNG.

8.13.1 Changing the header content

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Branding**. The Branding page appears.
4. Check Display Header.
5. Click the header color icon.

6. 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 color icon to confirm your selection.
7. Click **Browse** to upload the image to display as the header banner or as a logo within the header banner.
8. Choose the alignment option for the image or logo: left-aligned, centered, or right-aligned.
9. Click **Save**.

8.13.2 Changing the body color and font settings

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Branding**. The Branding page appears.
4. Choose a background color for the main body in one of two ways:
    - Enter a hexadecimal value for the background color.
    - Click within the header color palette to choose a color. Click the color icon to confirm your selection.
5. Select a text font from the drop-down list.
6. Choose a text color in one of two ways:
    - Enter a hexadecimal value for the text color.
    - Click within the header color palette to choose a color. Click the color icon to confirm your selection.
7. Click **Save**.
8. Click **Set to Default** to restore all the default settings on this page.

8.13.3 Changing the total amount background and text color

> ⓘ **Important: If you are implementing the iFrame embedded version, the total amount figure is not displayed within the iFrame. Any settings you select below are ignored.**

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.

2. Choose a profile. The General Settings page appears.
3. Click **Branding**. The Branding page appears.
4. Choose a background color in one of two ways:
   - Enter a hexadecimal value for the background color.
   - Click within the header color palette to choose a color. Click the color icon to confirm your selection.
5. Choose a text color in one of two ways:
   - Enter a hexadecimal value for the text color of the total amount.
   - Click within the header color palette to choose a color. Click the color icon to confirm your selection.
6. Click **Save**.
7. Click **Set to Default** to restore all the default settings on this page.

8.13.4 Changing the progress bar color

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Branding**. The Branding page appears.
4. Choose a color in one of two ways:
   - Enter a hexadecimal value for the color of the progress bar.
   - Click within the header color palette to choose a color. Click the color icon to confirm your selection.
5. Click **Save**.
6. Click **Set to Default** to restore all the default settings on this page.

8.13.5 Changing the color and text on the Pay or Finish Button

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Branding**. The Branding page appears.
4. Choose a background color of the pay or the finish button in one of two ways:
   - Enter a hexadecimal value for the background color.

    - Click within the header color palette to choose a color. Click the color icon to confirm your selection.

5. Choose a color of the pay or the finish button text in one of two ways:
    - Enter a hexadecimal value for the text.
    - Click within the header color palette to choose a color. Click the icon at the bottom right to confirm your selection.
6. Check **Change Button text**. A text box appears for the pay button.
7. Enter the text you want displayed on the pay button. This button text is required.
8. Enter the text you want displayed on the finish button. This button text is required.
9. Click **Save**.
10. Click **Set to Default** to restore all the default settings on this page.

8.13.6 Changing the footer color and uploading as small logo or image

1. In the left navigation panel, choose **Payment Configuration > Secure Acceptance Settings**. The Secure Acceptance Settings page appears.
2. Choose a profile. The General Settings page appears.
3. Click **Branding**. The Branding page appears.
4. Check Display Footer.
5. Choose a color in one of two ways:
    - Enter a hexadecimal value for the footer color of the payment form.
    - Click within the header color palette to choose a color. Click the color icon to confirm your selection.
6. Click **Browse** to upload a footer logo. Upload the image that you want displayed within the footer of the payment form.

To display a small logo or image in the footer of the payment form, the file must not exceed 840 (w) x 60 (h) pixels. The image file must be GIF, JPEG, or PNG.

7. Choose the alignment option for the image: left-aligned, centered, or right-aligned.
8. Click **Save**.
9. Click **Set to Default** to restore all the default settings on this page.

8.14 Checkout language localization

Secure Acceptance supports multiple languages. This table lists all the supported languages and the locale code that you must include in your payment form.

From the list, include the locale code in the **locale** request field on your payment form. See Sample Transaction Process Using JSP (on page 44).

Example: American English

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

8.14.1 Locale codes

Language	Locale Code
Arabic	ar-xn
Catalan	ca-es
Chinese—Hong Kong	zh-hk
Chinese—Macau	zh-mo
Chinese—Mainland	zh-cn
Chinese—Singapore	zh-sg
Chinese—Taiwan	zh-tw
Croatian	hr-hr
Czech	cz-cz
Danish	da-dk
Dutch	nl-nl
English—United States of America	en-us
English—Australia	en-au
English—Great Britain	en-gb
English—Canada	en-ca
English—Ireland	en-ie

English—New Zealand	en-nz
Finnish	fi-fi
French	fr-fr
French—Canada	fr-ca
German	de-de
German—Austria	de-at
Greek	el-gr
Hebrew	he-il
Hungary	hu-hu
Indonesian	id-id
Italian	it-it
Japanese	ja-jp

8.14.2 Locale codes (continued)

Language	Locale Code
Korean	ko-kr
Lao People's Democratic Republic	lo-la
Malaysian Bahasa	ms-my
Norwegian (Bokmal)	nb-no
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—United States of America	es-us
Swedish	sv-se
Thai	th-th
Turkish	tr-tr
Vietnamese	vi-vn

8.15 Activating a profile

You must complete the required settings described in each of these sections before you can activate a profile:

- Payment Method Configuration (on page 21)
- Security Keys (on page 28)
- Customer Response Page (on page 36)

1. On the left navigation pane, click the **Payment Configuration > Secure Acceptance** Settings. The Secure Acceptance Settings page appears.
2. Perform one of these steps:
   - On the Active Profiles tab, select the profile that you want to activate, and click the **Promote Profile** icon.
   - On the Edit Profile page, click the **Promote Profile** icon.
3. Click **Confirm**.

9 Processing Secure Acceptance transactions

Below are tables of payment services merchant can use via SA and endpoints assigned to these services:

There are a number of transaction types that merchant can performed using Secure Acceptance Hosted Checkout. The most common are Authorizations on their own or Authorizations combined with Capture (known as a "Sale"). Merchant can also create and update TMS tokens and combine these with the Authorizations or Sales. Merchant must specify the transaction type in the POST payload, and the URL that merchant redirect cardholders to also depends on the transaction type. The following tables shows the transaction_type values and the corresponding URLs:

Endpoints for Full Page Redirect	
Service	**Endpoint**

`create_payment_token`	`Test Transactions`
	https://testsecureacceptance.cybersource.com/token/create
	`Live Transactions`
	https://secureacceptance.cybersource.com/token/create

`update_payment_token`	`Test Transactions`
	https://testsecureacceptance.cybersource.com/token/update
	`Live Transactions`
	https://secureacceptance.cybersource.com/token/update

`authorization`
`authorization,create_payment_token`
`authorization,update_payment_token`
`sale`
`sale,create_payment_token`
`sale,update_payment_token`
	`Test Transactions`
	https://testsecureacceptance.cybersource.com/pay
	`Live Transactions`
	https://secureacceptance.cybersource.com/pay

Endpoints for Payment page in an iFrame	
Service	**Endpoint**
create_payment_token	Test Transactions https://testsecureacceptance.cybersource.com/embedded/token/create Live Transactions https://secureacceptance.cybersource.com/embedded/token/create
update_payment_token	Test Transactions https://testsecureacceptance.cybersource.com/embedded/token/update Live Transactions https://secureacceptance.cybersource.com/embedded/token/update
authorization authorization,create_payment_token authorization,update_payment_token sale sale,create_payment_token sale,update_payment_token	Test Transactions https://testsecureacceptance.cybersource.com/embedded/pay Live Transactions https://secureacceptance.cybersource.com/embedded/pay

One-Click Endpoints	
Service	**Endpoint**
Test	https://testsecureacceptance.cybersource.com/oneclick/pay
Production	https://secureacceptance.cybersource.com/oneclick/pay
Supported transaction types	• authorization • authorization,update_payment_token • sale • sale,update_payment_token

Process Transaction Endpoints	
Service	**Endpoint**
Test	https://testsecureacceptance.cybersource.com/pay
Production	https://secureacceptance.cybersource.com/pay
Supported transaction types	• authorization • authorization,create_payment_token • authorization,update_payment_token • sale • sale,create_payment_token • sale,update_payment_token

9.1 Mandatory request fields

These signed fields are required in all Secure Acceptance requests:

- access_key
- amount
- currency
- locale
- profile_id
- reference_number
- signed_date_time
- signed_field_names
- transaction_type
- transaction_uuid

For descriptions of signed request fields, see Request fields (on page 80).

9.2 Important request fields

Field name	Field description	Recommended values
access_key	Required for authentication with Secure Acceptance. Generated in Enterprise Business Centre Secure Acceptance profile.	
auth_indicator	Flag that specifies the purpose of the authorization for MasterCard cards. Possible values: 0: Preauthorization 1: Final authorization	

billing information fields	Dummy address fields to be used with mandatory billing address fields if billing information is not collected	bill_to_forename - **NoReal** bill_to_surname - **Name** bill_to_email - **smartpayfusetest@barclaycard.co.uk**bill_to_address_line1 – **1 The Street** bill_to_address_city - **City** bill_to_address_state - **County** bill_to_address_country - **GB** bill_to_address_postal_code – **AB12CD**
ignore_avs	Ignore the results of AVS verification. Possible values: - true - false	true if dummy billing address fields are used, this field must be true to ignore results from the issuing bank **Please note:** real billing address is mandatory for UK, US and CA. Also, billing information is important for Decision Manager, so we recommend to request it for all countries.
ignore_cvn	Ignore the results of CVN verification. Possible values: - true - false	true/false if CVN (CVV) number is not collected, set **true** value, otherwise **false** (default value**)**
line_item_count	Total number of line items. Used when order has items and not just Grand Total Amount value.	
merchant_defined_ data#	MDD fields to provide additional information to Decision Manager	
override_backoffice_ post_url	Overrides the backoffice post URL profile setting with merchant URL. URL	

	must be HTTPS and support TLS 1.2 or later.	
override_custom_cancel_page	Overrides the custom cancel page profile setting with merchant URL. URL must be HTTPS and support TLS 1.2 or later.	
override_custom_receipt_page	Overrides the custom receipt profile setting with merchant URL. URL must be HTTPS and support TLS 1.2 or later.	
reference_number	Unique merchant generated order reference or tracking number for each transaction	
transaction_type	Define type of SA transaction	This field may have the following values: “authorization” “authorization,create_payment_token” “authorization,update_payment_token” “sale” “sale,create_payment_token” “sale,update_payment_token” “create_payment_token” “update_payment_token” Decision Manager and Payer Authentication services will be configured in Secure Acceptance profile.
transaction_uuid	Unique merchant-generated identifier. This	

	field is used to check for duplicate transaction attempts.	

9.3 Important response message fields

Field name	Field description
payer_authentication_cavv	Cardholder authentication verification value (CAVV).
payer_authentication_eci	Electronic commerce indicator (ECI). This field is used by payer authentication validation and enrollment services.
payment_token	Payment instrument token or Customer token from TMS system, depending on TMS settings.
payment_token_instrument_identifier_id	Instrument identifier token from the TMS system.
reason_code	Numeric value corresponding to the result of the credit card authorization request.
signature	The Base64 signature returned by the server.
transaction_id	The transaction identifier from the payment gateway.

For the full list of Response fields, please refer to the full integration guide

Further reading referenced from within this guide:

.

9.4 Request fields example

Field	/alue
access_key	455346d31e683e07b29893d2d7066d9e
amount	40.00
currency	GBP
locale	en
profile_id	A8B7D8BC-BF3D-4A8D-906F-BED595521A18
reference_number	MRN_1234567
signature	lD4ap59e2u/6aBl+XG4Ndtx1ftXyBBFqccFUqq382Q8=
signed_date_time	2020-04-08T19:46:25Z
signed_field_name	access_key,profile_id,transaction_uuid,signed_field_names, unsigned_field_names,signed_date_time,locale,transaction_type, reference_number,amount,currency
transaction_type	authorization,create_payment_token
transaction_uuid	5e8e2a1198c14
unsigned_field_na	

9.5 Reply fields example

Field	Value
auth_amount	40.00
auth_avs_code	U
auth_avs_code_raw	00
auth_code	40
auth_cv_result	2
auth_cv_result_raw	3
auth_response	0
auth_time	2020-04-08T195042Z
decision	ACCEPT
merchant_id	bc_test
Message	Request was processed successfully.
payer_authentication_cavv	MTIzNDU2Nzg5MDEyMzQ1Njc4OTA=
payer_authentication_eci	05
payer_authentication_enroll_veres_enrolled	Y

payer_authentication_pares_status	Y
payer_authentication_reason_code	100
payer_authentication_specification_version	2.1.0
payer_authentication_transaction_id	1J4nR6MgwuFKif93zWr0
payer_authentication_validate_e_commerce_indicator	vbv
payer_authentication_validate_result	0
payer_authentication_xid	MTIzNDU2Nzg5MDEyMzQ1Njc4OTA=
payment_token	A2CDA448A2761E12E05341588E0AE961
payment_token_instrument_identifier_id	9699364CEF5B2E23E05341588E0A7C3D
payment_token_instrument_identifier_new	N
payment_token_instrument_identifier_status	ACTIVE
reason_code	100
req_access_key	455346d31e683e07b29893d2d7066d9e
req_amount	40.00
req_bill_to_address_city	Reading
req_bill_to_address_country	GB
req_bill_to_address_line1	Queens road 41
req_bill_to_address_postal_code	RG1 4BQ
req_bill_to_email	test@smartpayfuse.barclaycard
req_bill_to_forename	John
req_bill_to_surname	Doe
req_card_expiry_date	04-2024
req_card_number	XXXXXXXXXXXX1091
req_card_type	001
req_card_type_selection_indicator	1
req_currency	GBP
req_locale	en
req_payment_method	card
req_profile_id	A8B7D8BC-BF3D-4A8D-906F-BED595521A18
req_reference_number	MRN_1234567
req_transaction_type	authorization,create_payment_token

req_transaction_uuid	5e8e2a1198c14
request_token	Axj77wSTPd/wiXUFhh4kAAJRHBd0YIACojgu6 MEDOhn0ADHDJpJl6MV1iSEB8me7/hEuoLDDxIAAnBBy
signature	oF2Ju5jBLUV67TqDbA8OnJiAUbFxtx5mF1FooUjFb74=
signed_date_time	2020-04-08T19:50:42Z
signed_field_names	transaction_id,decision,req_access_key,req_profile_id, req_transaction_uuid,req_transaction_type, req_reference_number,req_amount,req_currency, req_locale, req_payment_method,req_bill_to_forename, req_bill_to_surname, req_bill_to_email,req_bill_to_address_line1, req_bill_to_address_city,req_bill_to_address_country, req_bill_to_address_postal_code,req_card_number, req_card_type,req_card_type_selection_indicator, req_card_expiry_date, payer_authentication_reason_code, payer_authentication_specification_version, payer_authentication_transaction_id, payer_authentication_enroll_veres_enrolled, message,reason_code,auth_avs_code, auth_avs_code_raw,auth_response,auth_amount, auth_code,auth_cv_result,auth_cv_result_raw, auth_time,request_token, payment_token_instrument_identifier_id, payment_token_instrument_identifier_new,

	payment_token_instrument_identifier_status, payer_authentication_validate_result, payer_authentication_cavv, payer_authentication_validate_e_commerce_indicator, payer_authentication_eci,payer_authentication_pares_status, payer_authentication_xid, payment_token,signed_field_names, signed_date_time
transaction_id	5863754419966493204004

9.6 Secure Acceptance source code examples

Secure Acceptance source code examples can be obtained using the links in the **Secure Acceptance Hosted Checkout Integration Guide** pdf document in the **Samples in Scripting Languages** section:

Secure Appetence can support any dynamic scripting language that supports HMAC256 hashing algorithms. Select from the options below to download from a selection of sample applications in the following languages:

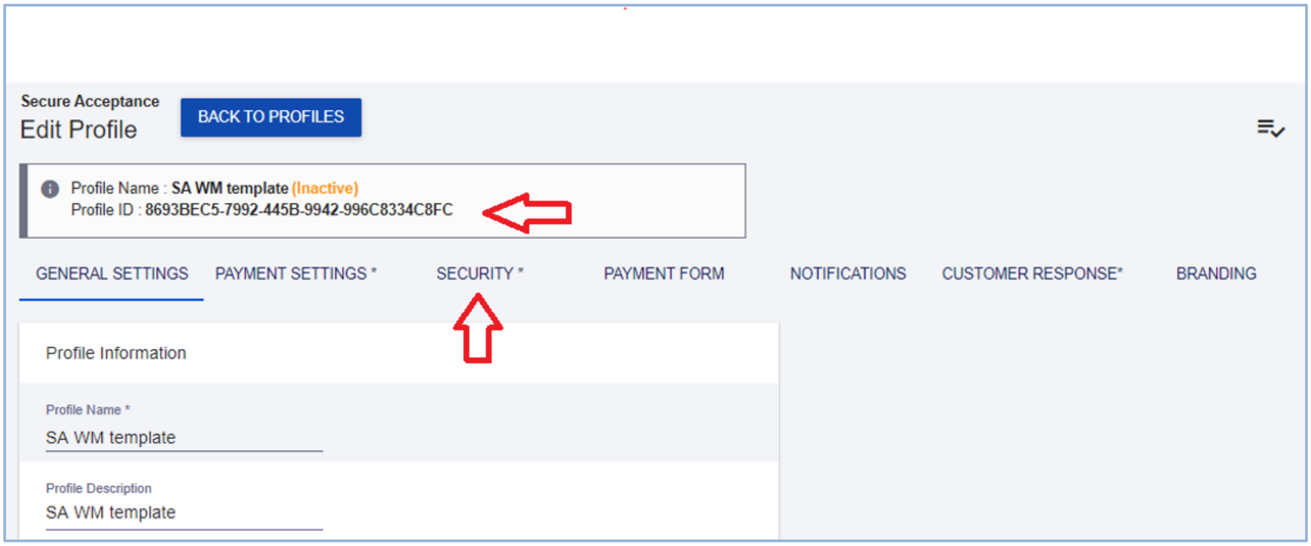
JSP C# Ruby Perl PHP VB

By default, the example code gives merchant SA authorization request, but merchant can modify this to perform any available SA transaction type. To run the example code for the test MID, merchant need to add the three credentials, from merchant Secure Acceptance profile:

- Profile ID (used in the browser)
- Access Key (used in the browser)
- Secret Key (used on the merchant server only)

Profile ID can be found in SA **Edit Profile** menu.

Access Key and Secret Key are generated in the **SECURITY** tab of Secure Acceptance profile.



Profile Name : **SA WM template** (Inactive)
Profile ID : 8693BEC5-7992-445B-9942-996C8334C8FC

Profile Information

Profile Name *
SA WM template

Profile Description
SA WM template

9.7 Request Field

Below is a summary table of most frequently used SA request fields. Please note, that some fields are mandatory and transactions without these fields will be declined. Please note:

- M = Mandatory
- R = Recommended
- O = Optional
- C = Conditional

Field Name	Field requirement
access_key	M
amount	M
auth_indicator	C
bill_to_address_city	M
bill_to_address_country	M
bill_to_address_line1	M
bill_to_address_line2	O
bill_to_address_postal_code	M
bill_to_address_state	C
bill_to_email	M
bill_to_forename	M
bill_to_phone	O

bill_to_surname	M
card_cvn	M
card_expiry_date	M
card_number	M
card_type	M
currency	M
customer_ip_address	O
ignore_avs	C
ignore_cvn	C
item_#_name	R
item_#_quantity	R
item_#_sku	R
item_#_unit_price	R
line_item_count	C
locale	M
merchant_defined_data#	C
profile_id	M
reference_number	M
ship_to_address_city	R
ship_to_address_country	R
ship_to_address_line1	R
ship_to_address_line2	C
ship_to_address_postal_code	R
ship_to_address_state	R
ship_to_company_name	R
ship_to_forename	R
ship_to_phone	R
ship_to_surname	R
shipping_method	R
signature	M
signed_date_time	M
signed_field_names	M
transaction_type	M
transaction_uuid	M
unsigned_field_names	M

9.8 Example transaction use cases

9.8.1 Creating a Payment Card Token

Important: Include the appropriate endpoint that supports the `create_payment_token` transaction type. See Processing Secure Acceptance transactions (on page 48). For descriptions of all request and response fields. See Hosted Checkout Integration API Fields (on page 80 and 128).

Include all request fields in the **signed_field_names** field with the exception of the **card_number** field. The **signed_field_names** field is used to generate a signature that is used to verify the content of the transaction in order to prevent data tampering.

Create a Standalone Payment Card Token request

```
reference_number=123456789
transaction_type=create_payment_token
currency=usd
amount=100.00
locale=en
access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2020-07-11T15:16:54Z
signed_field_names=comma separated list of signed fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
payment_method=card
card_type=001
card_number=4111111111111111
card_expiry_date=12-2022
card_cvn=005
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=Mountain View
bill_to_address_postal_code=94043
bill_to_address_state=CA
bill_to_address_country=US
```

Create a standalone Payment Card Token Response

```
req_reference_number=123456789
req_transaction_type=create_payment_token
req_locale=en
req_amount=100.00
req_payment_method=card
req_card_type=001
req_card_number=xxxxxxxxxxxx1111
req_card_expiry_date=12-2022
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=joesmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_city=Mountain View
req_bill_to_address_postal_code=94043
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_access_key=e2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p3
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=02815b4f08e56882751a043839b7b481
signed_date_time=2020-07-11T15:16:54Z
signed_field_names=comma separated list of signed fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
decision=ACCEPT
reason_code=100
transaction_id=3735553783662130706689
req_payment_token=CF2194C8A0F545CDE053AF598E0A20DA
```

9.8.2 Payment Token Transactions

One-Click

The customer is directed to the Order Review page. Depending on the settings you configured for Secure Acceptance Hosted Checkout Integration, the customer can view or update billing, shipping, and payment details before confirming to pay. See Checkout Configuration (on page 29).

ⓘ **Include the appropriate endpoint that supports the authorization or sale transaction types. See Endpoints and Transaction Types (on page 48). For descriptions of all request and response fields, see Hosted Checkout Integration API Fields (on pages 79 and 128).**

The **payment_token** field identifies the card and retrieves the associated billing, shipping, and payment information.

One-Click Transaction Request

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
reference_number=1350029885978
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
consumer_id=1239874561
transaction_type=authorization
amount=100.00
currency=USD
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2020-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

One-Click Transaction Response

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization
req_reference_number=1350029885978
req_amount=100.00
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=jsmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
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
req_payment_token=CF2194C8A0F545CDE053AF598E0A20DA
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
req_amount=100.00
req_tax_amount=15.00
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=jsmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
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=CF2194C8A0F545CDE053AF598E0A20DA
payment_token_latest_card_suffix=3283
payment_token_latest_card_expiry_date=07-2024
payment_solution=015
signed_field_names=comma separated list of signed fields
signed_date_time=2012-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

9.8.3 Recurring payments

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

> ⓘ **Include the appropriate endpoint that supports the authorization, create_payment_token or sale,create_payment_token transaction types. See endpoints and Transaction Types (on page 48). For descriptions of all request and response fields, see Integration API Fields (on pages 79 and 128).**

Create a Recurring Billing payment token request

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_type=authorization,create_payment_token
locale=en
amount=5.00
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2020-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
consumer_id=1239874561
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_state=CA
bill_to_address_country=US
card_type=001
card_number=4111111111111111
card_expiry_date=12-2022
card_cvn=005
recurring_frequency=monthly
recurring_amount=25.00
recurring_start_date=20200125
payment_method=card
```

Create a Recurring Billing payment token response

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,create_payment_token
req_reference_number=1350029885978
req_amount=5.00
req_tax_amount=2.50
req_currency=USD
req_locale=en
```

```
req_payment_method=card
req_consumer_id=1239874561
req_recurring_frequency=monthly
req_recurring_amount=25.00
req_recurring_start_date=20200125
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=joesmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx1111
req_card_type=001
req_card_expiry_date=12-2022
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time=2022-08-14T134608Z
req_payment_token=CF2194C8A0F545CDE053AF598E0A20DA
signed_field_names=comma separated list of signed fields
signed_date_time=2022-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

9.8.4 Instalment Payments

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

> ⓘ **Include the appropriate endpoint that supports the authorization, create_payment_token or sale,create_payment_token transaction types. See endpoints and Transaction Types (on page 48). For descriptions of all request and response fields, see Integration API Fields (on pages 79 and 128).**

Create an Instalments payment token request

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
transaction_type=authorization,create_payment_token
```

```
amount=5.00
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2020-01-17T10:46:39Z
signed_field_names=comma separated list of signed fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
consumer_id=1239874561
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_state=CA
bill_to_address_country=US
card_type=001
card_number=4111111111111111
card_expiry_date=12-2022
card_cvn=005
recurring_frequency=monthly
recurring_number_of_installments=6
recurring_amount=25.00
recurring_start_date=20200125
payment_method=card
```

Create an Instalments payment token response

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,create_payment_token
req_reference_number=1350029885978
req_amount=5.00
req_currency=USD
req_locale=en
req_payment_method=card
req_consumer_id=1239874561
req_recurring_frequency=monthly
req_recurring_number_of_installments=6
req_recurring_amount=25.00
req_recurring_start_date=20200125
req_bill_to_forename=Joe
req_bill_to_surname=Smith
```

```
req_bill_to_email=joesmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx1111
req_card_type=001
req_card_expiry_date=12-2022
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time==2022-08-14T134608Z
req_payment_token=CF2194C8A0F545CDE053AF598E0A20DA
signed_field_names=comma separated list of signed fields
signed_date_time=2022-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

9.8.5 Payment Token updates

The **payment_token** field identifies the card and retrieves the associated billing, shipping, and payment information. The customer is directed to the Order Review page and clicks **Edit Address** or **Edit Details** to return to the relevant checkout page. The customer clicks **Pay** to confirm the transaction.

You must configure the billing, shipping, and payment details so that a customer can edit their details on the Order Review page. See Configuring Order Review details (on page 36).

> ⓘ **Include the endpoint that supports update_payment_token or the endpoint that supports authorization,update_payment_token (updates the token and authorizes the transaction) or sale,update_payment_token (updates the token and processes the transaction). See Sample Transaction Process Using JSP (on page 41). You must include the field allow_payment_token _update and set it to true.**

Update a Payment Card token request

```
access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
transaction_type=update_payment_token
profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
```

```
reference_number=1350029885978
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
amount=100.00
currency=USD
payment_method=card
card_type=001
card_number=4111111111111111
card_expiry_date=12-2022
card_cvn=005
bill_to_forename=Joe
bill_to_surname=Smith
bill_to_email=joesmith@example.com
bill_to_address_line1=1 My Apartment
bill_to_address_state=CA
bill_to_address_country=US
locale=en
transaction_uuid=fcfc212e92d23be881d1299ef3c3b314
signed_date_time=2020-01-17T10:46:39Z
consumer_id=1239874561
signed_field_names=comma separated list of signed fields
signature=WrXOhTzhBjYMZROwiCug2My3jiZHOqATimcz5EBA07M=
```

Update a Payment Card token response

```
transaction_id=3500311655560181552946
decision=ACCEPT
message=Request was processed successfully.
req_access_key=a2b0c0d0e0f0g0h0i0j0k0l0m0n0o0p2
req_profile_id=0FFEAFFB-8171-4F34-A22D-1CD38A28A384
req_transaction_uuid=55d895790bc4c8a0f4464f9426ba3b79
req_transaction_type=authorization,update_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_consumer_id=1239874561
req_bill_to_forename=Joe
req_bill_to_surname=Smith
req_bill_to_email=jsmith@example.com
req_bill_to_address_line1=1 My Apartment
req_bill_to_address_state=CA
req_bill_to_address_country=US
req_card_number=xxxxxxxxxxxx1111
req_card_type=001
```

```
req_card_expiry_date=12-2022
reason_code=100
auth_avs_code=U
auth_avs_code_raw=00
auth_response=0
auth_amount=100.00
auth_time=2022-08-14T134608Z
payment_token=CF2194C8A0F545CDE053AF598E0A20DA
signed_field_names=comma separated list of signed fields
signed_date_time=2022-10-12T08:39:25Z
signature=jMeHnWRKwU3xtT02j2ufRibfFpbdjUSiuWGT9hnNm00=
```

10 Testing transactions

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 but must recreate the profile.

To run transaction tests, you will need to:

1. Log in to the EBC test environment: https://admin.smartpayfuse-test.barclaycard/ebc2/
2. Create a Secure Acceptance profile. See Creating a Secure Acceptance Profile (on page 17).
3. Integrate with Secure Acceptance. See Samples in Scripting Languages (on page 58).

Important: Include the test transactions endpoint in your HTML form. See Sample Transaction Process Using JSP (on page 58).

You can use these test payment card numbers for transactions. Remove spaces when sending the request to Smartpay Fuse.

Payment Card Type	Test Account Number
Visa	4111 1111 1111 1111
Mastercard	5555 5555 5555 4444
American Express (see note below)	3782 8224 6310 005
Discover (see note below)	6011 1111 1111 1117

Diners Club (see note below)	3800 0000 0000 0006
Maestro International (16 digits)	6000 3400 0000 9859
Maestro Domestic (16 digits)	6759 1800 0000 5546

ⓘ **Please Get in contact to discuss additional configuration requirements to enable American Express, Discover and Maestro Domestic acceptance.**

You can also refer to our developer hub for additional card numbers:

- Basic testing
- 3DSv2 test cards

11 Viewing Hosted Checkout transaction search in EBC

SA transaction search option is available in Enterprise Business Centre for users with Transaction Search permissions (configured by MID administrator).

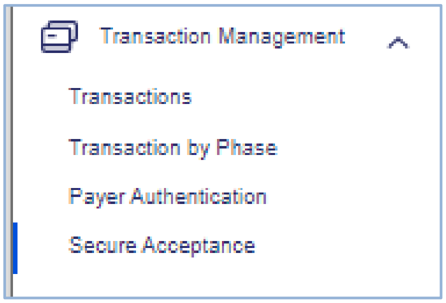
There are two options to find SA transactions details in Enterprise Business Centre:

- Using general transaction search
- Using Secure Acceptance search

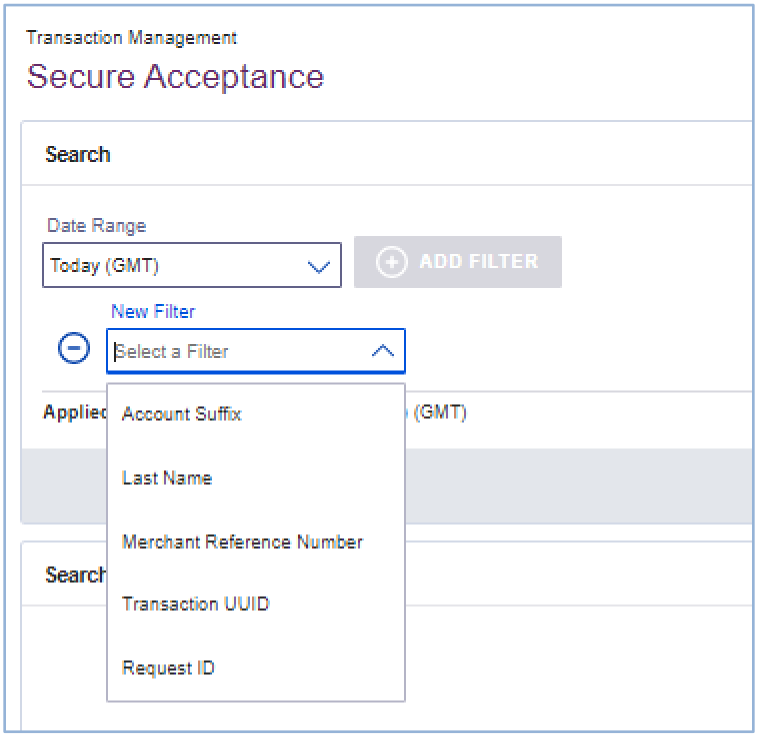
To highlight the difference between these two options, the following screen shots show an Authorization transaction with Token creation for a 3DS2-enrolled card.

11.1 Secure Acceptance search

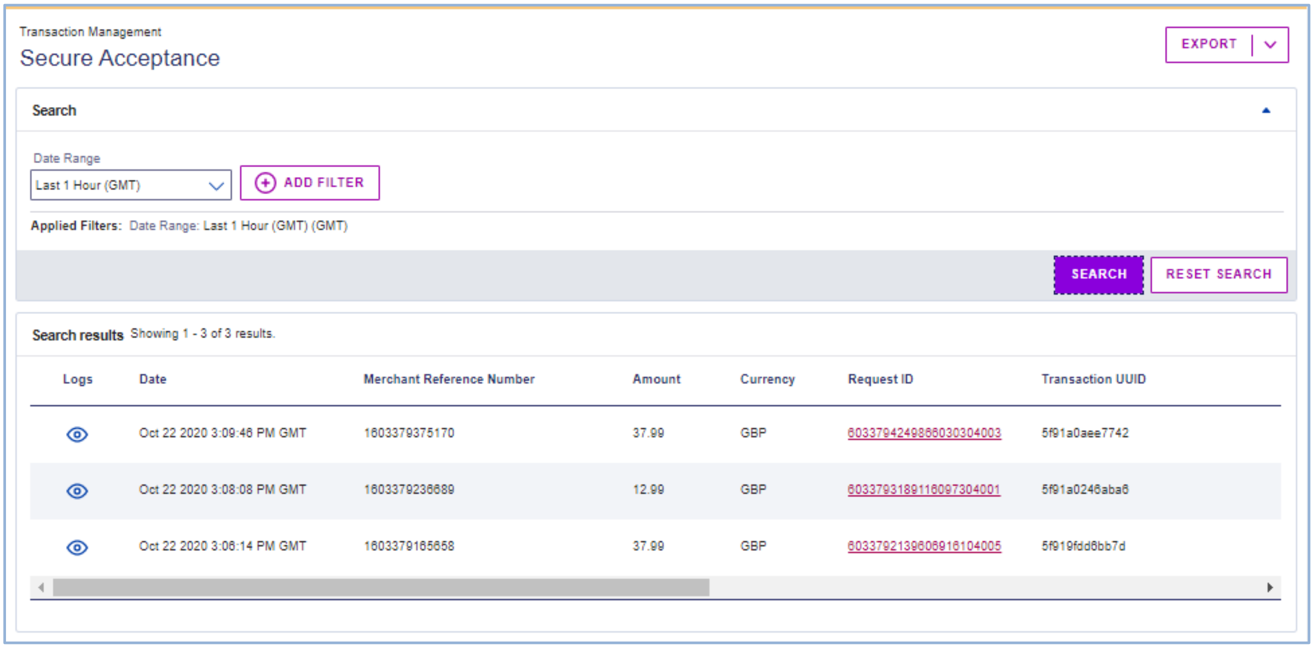
Log in the ENTERPRISE BUSINESS CENTRE and select the **Transaction Management** menu:



For the Secure Acceptance search, select **Secure Acceptance** menu and set search filters to find transactions.



An example of search result is shown below (split into two parts – left-hand side of the table and right-hand side of the table):



Transaction Management

Secure Acceptance

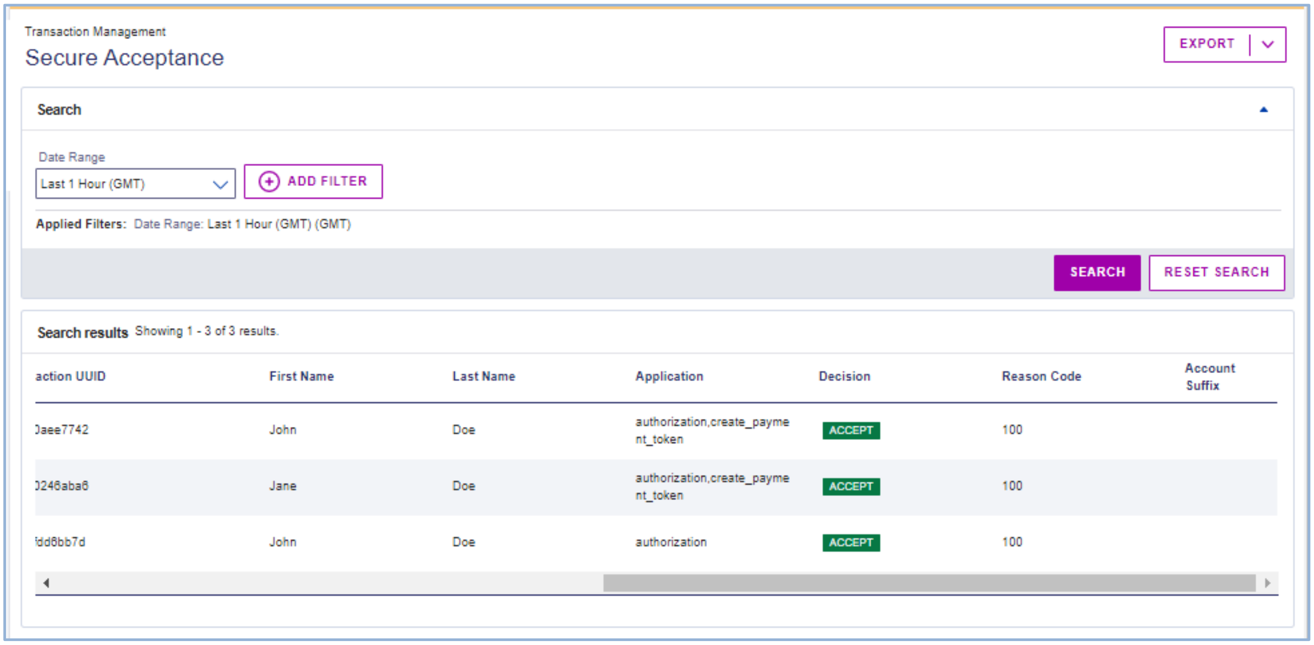
Search

Date Range: Last 1 Hour (GMT)

Applied Filters: Date Range: Last 1 Hour (GMT) (GMT)

Search results Showing 1 - 3 of 3 results.

Logs	Date	Merchant Reference Number	Amount	Currency	Request ID	Transaction UUID
👁	Oct 22 2020 3:09:46 PM GMT	1603379375170	37.99	GBP	6033794249866030304003	5f91a0aee7742
👁	Oct 22 2020 3:08:08 PM GMT	1603379236689	12.99	GBP	6033793189116097304001	5f91a0246aba6
👁	Oct 22 2020 3:06:14 PM GMT	1603379165658	37.99	GBP	6033792139606916104005	5f919fdd6bb7d



Transaction Management

Secure Acceptance

Search

Date Range: Last 1 Hour (GMT)

Applied Filters: Date Range: Last 1 Hour (GMT) (GMT)

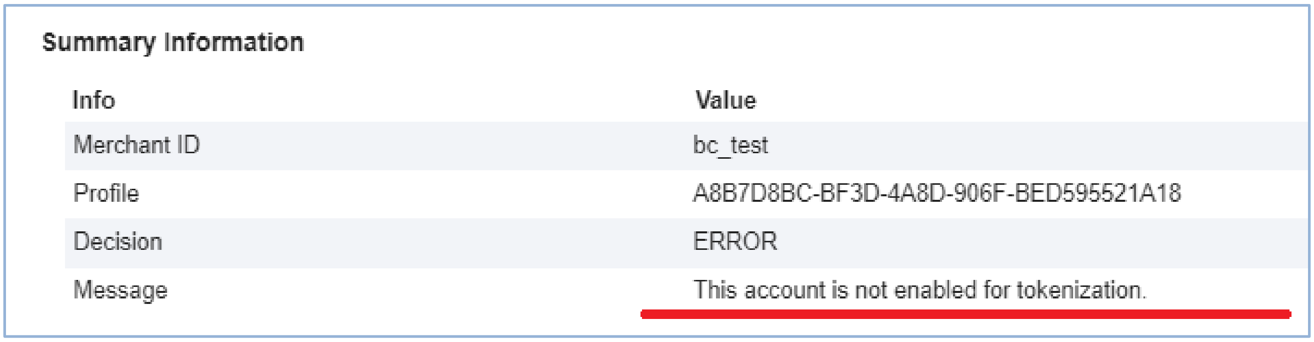
Search results Showing 1 - 3 of 3 results.

action UUID	First Name	Last Name	Application	Decision	Reason Code	Account Suffix
)aee7742	John	Doe	authorization,create_payment_token	ACCEPT	100	
)246aba6	Jane	Doe	authorization,create_payment_token	ACCEPT	100	
'dd6bb7d	John	Doe	authorization	ACCEPT	100	

Description of transaction results table is below.

Column name	Description
Date	Transaction data and time
Merchant Reference Number	Transaction identifier assigned by merchant (e.g. order ID)
Amount	Transaction amount
Currency	Transaction currency

Request ID	Unique transaction identifier assigned by Smartpay Fuse In this table Request ID field is used as a link to the full transaction description.
Logs	Link to the transaction log
Transaction UUID	Unique transaction identifier assigned by merchant
First Name	Cardholder first name (field is empty if data was entered on Secure Acceptance Hosted Checkout payment page)
Last Name	Cardholder last name (field is empty if data was entered on Secure Acceptance Hosted Checkout payment page)
Application	Payment services run in this transaction
Decision	Word description of the transaction result
Reason Code	Reason code of the transaction result
Account Suffix	Last four digits of PAN (field is empty if data was entered on Secure Acceptance Hosted Checkout payment page)

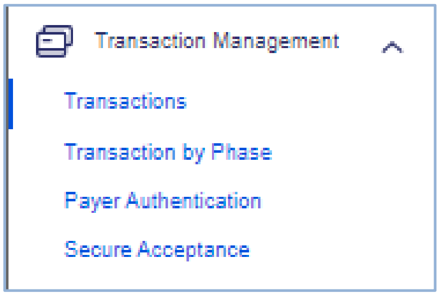


Summary Information

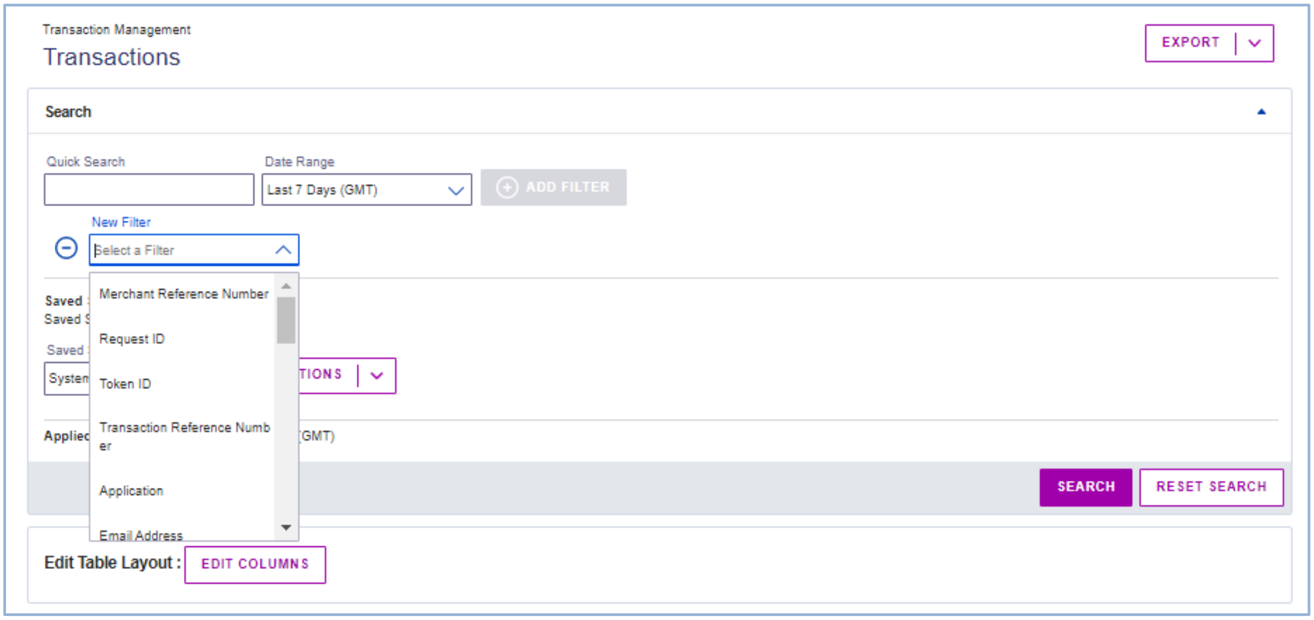
Info	Value
Merchant ID	bc_test
Profile	A8B7D8BC-BF3D-4A8D-906F-BED595521A18
Decision	ERROR
Message	This account is not enabled for tokenization.

11.2 General transaction search

Log in to EBC and select the **Transaction Management** menu:



For the general transaction search, select **Transactions** menu and set search filters to find transactions.



Transaction Management

Transactions

Search

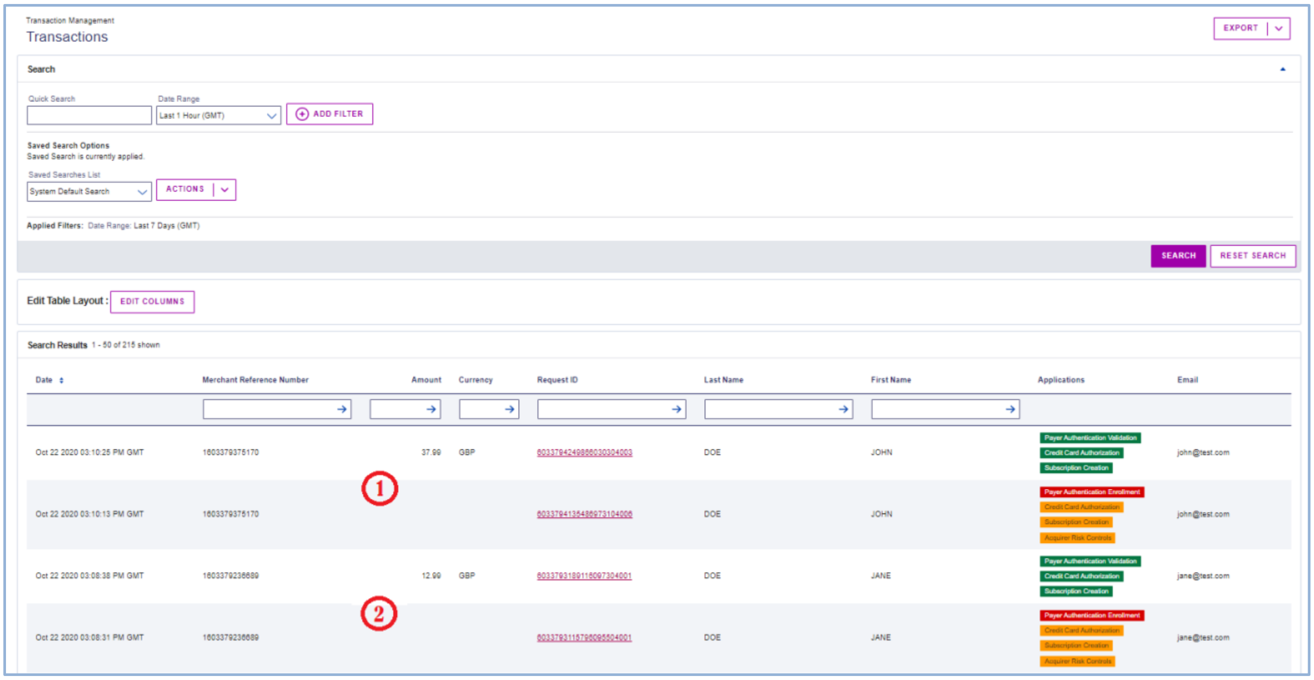
Quick Search:

Date Range: Last 7 Days (GMT)

New Filter: Select a Filter

Applied … (GMT)

Below is Transaction search result window, which presents the same transactions as in the previous chapter **9.1 Secure Acceptance search**.



Transaction Management

Transactions

Search

Quick Search:

Date Range: Last 1 Hour (GMT)

Saved Search Options

Saved Search is currently applied.

Saved Searches List: System Default Search

Applied Filters: Date Range: Last 7 Days (GMT)

Search Results 1 - 50 of 215 shown

Date	Merchant Reference Number	Amount	Currency	Request ID	Last Name	First Name	Applications	Email
Oct 22 2020 03:10:25 PM GMT	1603379375170	37.99	GBP	6033794249866030304003	DOE	JOHN	Payer Authentication Validation Credit Card Authorization Subscription Creation	john@test.com
Oct 22 2020 03:10:13 PM GMT	1603379375170			6033794135486973104006	DOE	JOHN	Payer Authentication Enrollment Credit Card Authorization Subscription Creation Acquirer Risk Controls	john@test.com
Oct 22 2020 03:08:38 PM GMT	1603379236689	12.99	GBP	6033793189116097304001	DOE	JANE	Payer Authentication Validation Credit Card Authorization Subscription Creation	jane@test.com
Oct 22 2020 03:08:31 PM GMT	1603379236689			6033793115796095504001	DOE	JANE	Payer Authentication Enrollment Credit Card Authorization Subscription Creation Acquirer Risk Controls	jane@test.com

The **Transactions** result table has the same set of columns as Secure Acceptance search plus several additional columns, which can be added to the result table using **EDIT LAYOUT** button top right-and corner on the screenshot above.

Please note, there is an important difference between how 3DS2 transactions are presented in the SA search and in the Transaction search:

- In the **Transaction** search window 3DS transactions for enrolled card are shown as two lines (1 and 2 on the screenshot above)
  - Combined call of Enrollment, Authorization and Subscription Creation
  - Combined call of Validation, Authorization and Subscription Creation
- In the **Secure Acceptance** search window, the transaction description is just one line, which is Validation, Authorization and Subscription Creation.

Therefore, the best approach to get SA transaction details is to use both options, depending on what exactly merchant is looking for.

12 Secure Acceptance merchant notifications

There are two main options for the merchant to receive Secure Acceptance transaction results:

1) Push notifications - configured in the **Notifications** tab of Secure Acceptance profile (Merchant notifications, page 36). Merchant can receive notifications to a **Merchant POST URL** or to a **Merchant POST Email** address.

ⓘ **URL notifications are POST messages to this URL and Smartpay Fuse expects merchants to send an acknowledgement file according to POST data exchange protocol. If your service fails to acknowledge via HTTP 200 response, future notifications may be delayed or halted.**

2) Pull notification - configured in the **Customer Response** tab of Secure Acceptance profile as a **Transaction Response Page URL.** Merchants specify the URL to which the customer is redirected after the payment page and this page will receive the transactions results. Merchant needs to retrieve the transaction results and save in the merchant backend system.

The Information provided to the merchant via **Merchant POST URL**, **Merchant POST Email** and **Transaction Response Page** is identical.

In case there is no reply from Smartpay Fuse (e.g. because of the connectivity issues) and the merchant has not received any notification from Smartpay Fuse, the merchant will not know, if the initial request to Smartpay Fuse was lost or the reply message was lost (possibly having been approved).

To get the transaction status, there is a **Transaction Search** service, which uses the REST API Reporting mechanism to retrieve the transaction details. This service identifies transactions based on the Merchant Reference Number– the transaction identifier assigned by the merchant.

If Transaction Search service returns the transaction details, it means that initial request to the gateway was successful and the notification has not been delivered for some reason. However, if Transaction Search service returns an empty report, it means the initial request to the gateway failed and merchant needs to resend it.

For additional information about the **Transaction Search** service, please refer to the Smartpay Fuse Developer Portal.

https://developer.smartpayfuse.barclaycard/api-reference-assets/index.html#transaction-search

The best option of implementing SA notifications is to use both notification options, one as a primary channel and another as a backup, and to implement the Transaction Search service for those rare cases where there is no reply from the gateway.

13 Secure Acceptance testing

13.1 Testing in test environment

To test Secure Acceptance integration please refer to the following documents [**1**, **2**, **3**]

There are two main groups of test scenarios described in [**1**]:

1) Payment testing – receiving error reason codes for payments, CVN and AVS tests. These tests are based on test amounts or AVS/CVN fields.
2) Payer Authentication testing – different Payer Authentication results (card enrolled/not enrolled, step up authentication, 3DS1 and 3DS2 etc.) depending on the test PANs used for payments.

These test cases are not mandatory, but we recommend running as many tests as possible to make sure merchant are able to handle any reply messages.

13.2 Testing in live environment

There are no test amounts or test PANs for the live testing. Once live you must closely monitor your settings, configuration and any transactions processed to ensure that your service is operating as intended.

Monitoring should cover all the payment services, Payer Authentication, Authorization, Capture, Credit etc. At the end of the day a batch file with capture and credit transactions sent to Barclays, which will be available to report on within the Enterprise Business Centre. You will need to run a reconciliation process to make sure that all payment amounts successfully reached merchant account in Barclays.

14 Hosted Checkout Integration API fields

14.1 Data type definitions

Unless otherwise noted, all fields are order and case sensitive. It is recommended that you not include URL-encoded characters in any request field prior to generating a signature.

Data Type	Permitted Characters and Formats
Alpha	Any letter from any language
AlphaNumeric	Alpha with any numeric character in any script
AlphaNumericPunctuation	Alphanumeric including ! "#$%&'()*+,-./:;=?@^_~
Amount	0123456789 including a decimal point (.)
ASCIIAlphaNumericPunctuation	Any ASCII alphanumeric character including !&'()+,-./:@
Date (a)	MM-yyyy
Date (b)	yyyyMMDD
Date (c)	yyyy-MM-dd HH:mm z yyyy-MM-dd hh:mm a z yyyy-MM-dd hh:mma z
Email	Valid email address.
Enumerated String	Comma-separated alphanumeric string
IP	Valid IP address
ISO 8601 Date	yyyy-MM-DDThh:mm:ssZ
Locale	[a-z] including a hyphen (-)
Numeric	0123456789
Phone	( ),+-.*#xX1234567890

URL	Valid URL (http or https)

15 Request fields

ⓘ To prevent data tampering please ensure that all fields are signed

ⓘ When generating the security signature, create a comma-separated name=value string of the POST fields that are included in the signed_field_names field. The ordering of the fields in the string is critical to the signature generation process. For example:

- **bill_to_forename=john**
- **bill_to_surname=doe**
- **bill_to_email=jdoe@example.com**
- **signed_field_names=bill_to_forename,bill_to_email,bill_to_surname**

The string to sign is bill_to_forename=john,bill_to_email=jdoe@example.com,bill_to_surname=doe

For information on the signature generation process, see the security script of the sample code for the scripting language you are using. See Samples in Scripting Languages (on page 58).

15.1 Request field description

Note: only the fields with override in the field name can be used to override back-end configuration.

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length

access_key	Required for authentication with Secure Acceptance. See Security Keys (on page 32). ⓘ **To prevent data tampering, sign this field.**	Required by the Secure Acceptance application.	Alphanumeric String (32)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
allow_payment_token_update	Indicates whether the customer can update the billing, shipping, and payment information on the order review page. Possible values: - `true`: Customer can update details. - `false`: Customer cannot update details.	update_payment_token (R)	Enumerated String (5)
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.	- create_payment_token (R) - authorization or sale (R) - authorization,create_payment_token (R) - sale,create_payment_token (R) - update_payment_token (O)	Amount String (15)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
auth_indicator	Flag that specifies the purpose of the authorization. Possible values: 0: Preauthorization 1: Final authorization Mastercard requires European merchants to indicate whether the authorization is a final authorization or a preauthorization. To set the default for this field, contact customer support.	authorization (See description)	String (1)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
auth_type	Authorization type. Possible values: AUTOCAPTURE: Automatic capture. STANDARDCAPTURE: Standard capture. verbal: Forced capture.	authorization (See description.) capture (Required for a verbal authorization; otherwise, not used.)	String (11)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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.	Optional	Enumerated String (5)
bill_to_address_city	City in the billing address. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Billing Information fields (page 34).	create_payment_token (R) authorization or sale (R) authorization,create_payment_token (R) sale,create_payment_token (R) update_payment_token (O)	AlphaNumericPunctuation String (50)
bill_to_address_country	Country code for the billing address. Use the two-character ISO country codes. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance.	create_payment_token (R) authorization or sale (R) authorization,create_payment_token (R)	Alpha String (2)

	See Configuring Billing Information fields (page 34).	sale,create_payment_token (R) update_payment_token (O)	
bill_to_address_line1	First line of the billing address. On JCN Gateway, this field is required when the authorization or sale request includes create_payment_token or Decision Manager. This field is optional when requesting an authorization or a sale without create_payment_token or Decision Manager. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Billing Information fields (page 34).	create_payment_token (R) authorization or sale (R) authorization, create_payment_token (R) sale,create_payment_token (R) update_payment_token (O)	AlphaNumericPunctuation String (60)
bill_to_address_line2	Second line of the billing address. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Billing Information fields (page 34).	Optional	AlphaNumericPunctuation String (60)

bill_to_address_ postal_code	Postal code for the billing address. When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits] Example: 12345-6789 When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric] Example: A1B2C3 For the rest of the world countries, the maximum length is 10. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Billing Information fields (page 34).	Mandatory See description.	AlphaNumericPunctuation See description.
bill_to_address_ state	State or province in the billing address. For the U.S. and Canada, use the standard state, province, and territory codes. This field is required if bill_to_address_country is U.S. or Canada. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Billing Information fields (page 34).	See description.	AlphaNumericPunctuation String (2)

	This field only to be provided for billing addresses in the U.S. or Canada.		
bill_to_company_name	Name of the customer's company. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Billing Information fields (page 34).	Optional	AlphaNumericPunctuation String (40)
bill_to_email	Customer email address, including the full domain name. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Billing Information fields (page 34).	create_payment_token (R) authorization or sale (R) authorization,create_payment_token (R) sale,create_payment_token (R) update_payment_token (O)	Email String (255)
bill_to_forename	Customer first name. This name must be the same as the name on the card. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Billing Information fields (page 34).	create_payment_token (R) authorization or sale (R) authorization,create_payment_token (R) sale,create_payment_token (R) update_payment_token (O)	AlphaNumericPunctuation String (60)

bill_to_phone	Customer phone number. Barclaycard recommends that you include the country code. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Billing Information fields (page 34). This field is optional for card payments.	See description.	Phone String (6 to 15)
bill_to_surname	Customer last name. This name must be the same as the name on the card. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Billing Information fields (page 34).	create_payment_token (R) authorization or sale (R) authorization,create_payment_token (R) sale,create_payment_token (R) update_payment_token (O)	AlphaNumericPunctuation String (60)

Field	**Description**	**Used By: Required (R) or Optional (O)**	**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. In your request, send either the complete route or the individual legs (journey_leg#_orig and journey_leg#_dest). If you	Optional See Decision Manager (on page 53).	AlphaNumericPunctuation String (255)

	send all the fields, the value of complete_route takes precedence over that of the journey_leg# fields.		
conditions_accepted	Indicates whether the customer accepted the service fee amount. Possible values: false: Customer did not accept. true: Customer did accept.	Required when service fee is enabled for the profile. See Service Fees (on page 53).	Enumerated String (5)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
consumer_id	Identifier for the customer's account. This field is defined when you create a subscription.	create_payment_token (O) authorization,create_payment_token (O) sale,create_payment_token (O) update_payment_token (O)	AlphaNumericPunctuation String (100)
credential_stored_on_file	Indicates whether to associate the new network transaction ID with the payment token for future merchant-initiated transactions (MITs). Set this field to true when you use a payment token for a cardholder-initiated transaction (CIT) and you	Optional	String (5)

	plan to set up a new schedule of MITs using an existing payment token. This will ensure that the new network transaction ID is associated with the token. Possible values: true false		
	Important: In Europe, enable Payer Authentication on Secure Acceptance and set the payer_authentication_challenge_code field to 04 on the initial cardholder-initiated transaction (CIT) to ensure compliance with Strong Customer Authentication (SCA) rules.		

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
currency	Currency used for the order; supported currencies will be agreed with Barclaycard during onboarding. For the possible values, see the ISO currency codes. ⓘ **To prevent data tampering, sign this field.**	• create_payment_token (R) • authorization or sale (R) • authorization,create_payment_token (R) • sale,create_payment_token (R) • update_payment_token (O)	Alpha String (3)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
customer_ browser_color_ depth	Indicates the bit depth of the color palette for displaying images, in bits per pixel. Secure Acceptance automatically populates this field, but you can override it. For more information, see https://en.wikipedia.org/wiki/Color_depth.	Optional	String (2)
customer_ browser_java_ enabled	Indicates the ability of the cardholder browser to execute Java. The value is returned from the navigator.javaEnabled property. Secure Acceptance automatically populates this field, but you can override it. Possible values: true false	Optional	String (5)
customer_ browser_ javascript_ enabled	Indicates the ability of the cardholder browser to execute JavaScript. This value is available from the fingerprint details of the cardholder's browser. Secure Acceptance automatically populates this field, but you can override it. Possible values: true false	Optional	String (5)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
customer_ browser_ language	Indicates the browser language as defined in IETF BCP47. Secure Acceptance automatically populates this field, but you can override it. For more information, see https://en.wikipedia.org/wiki/IETF_language_tag.	Optional	String (8)
customer_ browser_screen_ height	Total height of the customer's screen in pixels. Secure Acceptance automatically populates this field, but you can override it. Example: 864	Optional	String (6)
customer_ browser_screen_ width	Total width of the customer's screen in pixels. Secure Acceptance automatically populates this field, but you can override it.	Optional	String (6)
customer_ browser_time_ difference	Difference between UTC time and the cardholder browser local time, in minutes. Secure Acceptance automatically populates this field, but you can override it.	Optional	String (5)
customer_ cookies_accepted	Indicates whether the customer's browser accepts cookies. Possible values: true: Customer browser accepts cookies. false: Customer browser does not accept cookies.	Optional See Decision Manager (on page 53).	Enumerated String (5)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
customer_gift_ wrap	Indicates whether the customer requested gift wrapping for this purchase. Possible values: true: Customer requested gift wrapping. false: Customer did not request gift wrapping.	Optional See Decision Manager (on page 53).	Enumerated String (5)
customer_ip_ address	Customer's IP address reported by your web server using socket information.	Optional See Decision Manager (on page 53).	IP IPv4: String (15) IPv6: String (39)
date_of_birth	Date of birth of the customer. Use the format: yyyyMMDD. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance.	This is an optional field.	Date (b) String (8)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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.	Optional	Enumerated String (5)

departure_time	Departure date and time of the first leg of the trip. Use one of these 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. Examples 2023-01-20 23:30 GMT 2023-01-20 11:30 PM GMT 2023-01-20 11:30pm GMT	Optional See Decision Manager (on page 53).	Date (c) DateTime (29)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
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. ⓘ **The Smartpay Fuse-generated device fingerprint ID overrides the merchant-generated device fingerprint ID**	Optional See Decision Manager (on page 53).	AlphaNumericPunctuation String (88)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
driver_license_number	Driver's license number of the customer. Contact your TeleCheck representative to find out whether this field is required or optional. If you include this field in your request then you must also include the driver_license_state field. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance.	sale (See description) create_payment_token (See description) sale,create_payment_token (See description) update_payment_token (See description)	AlphaNumeric String (30)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
driver_license_state	State or province where the customer's driver's license was issued. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance.	sale (See description) create_payment_token (See description) sale,create_payment_token (See description) update_payment_token (See description)	Alpha String (2)
e_commerce_indicator	If call centre staff enter the payment details, e.g., payment card number, expiration, CVV, the default ECI value of internet (eCommerce) is not	(R) for MOTO transactions	Alpha String (4)

	valid. In that scenario, e_commerce_indicator=moto is the correct value to submit.		

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
health_care_#_amount	Amount of the healthcare payment. # can range from 0 to 4. Send this field with a corresponding health_care_#_amount_type field.	authorization (O)	String (13)
health_care_#_amount_type	Type of healthcare payment. # can range from 0 to 4. Mastercard possible values: eligible-total: total amount of healthcare. prescription Visa possible values: clinic dental healthcare: total amount of healthcare. healthcare-transit prescription vision Send this field with a corresponding health_care_#_amount field.	authorization (O)	String (35)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ignore_avs	Ignore the results of AVS verification. Possible values: true false ⓘ **To prevent data tampering, sign this field.**	Optional	Enumerated String (5)
ignore_cvn	Ignore the results of CVN verification. Possible values: true false ⓘ **To prevent data tampering, sign this field.**	Optional	Enumerated String (5)
industry_datatype	Indicates whether the transaction includes industry data. For certain industries, you must set this field to an industry data value to be sent to the processor. When this field is not set to an industry value or is not included in the request, industry data does not go to the processor. Possible values: healthcare_medical healthcare_transit	authorization (O)	String (20)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
item_#_code	Type of product. # can range from 0 to 199.	Optional If you include this field, you must also include the line_item_count field.	AlphaNumericPunctuation String (255)
item_#_name	Name of the item. # can range from 0 to 199. This field is required when the item_#_code value is not default nor related to shipping or handling.	See description. If you include this field, you must also include the line_item_count field.	AlphaNumericPunctuation String (255)
item_#_passenger_email	Passenger's email address.	Optional See Decision Manager (on page 53).	String (255)
item_#_passenger_forename	Passenger's first name.	Optional See Decision Manager (on page 53).	String (60)
item_#_passenger_id	ID of the passenger to whom the ticket was issued. For example, you can use this field for the frequent flyer number.	Optional See Decision Manager (on page 53).	String (32)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
item_#_passenger_phone	Passenger's phone number. If the order is from outside the U.S., include the country code.	Optional See Decision Manager (on page 53).	String (15)
item_#_passenger_status	Your company's passenger classification, such as with a frequent flyer number. In this case, you might use values such as standard, gold, or platinum.	Optional See Decision Manager (on page 52).	String (32)
item_#_passenger_surname	Passenger's last name.	Optional See Decision Manager (on page 52).	String (60)
item_#_passenger_type	Passenger classification associated with the price of the ticket. Possible values: ADT: Adult CNN: Child INF: Infant YTH: Youth STU: Student SCR: Senior Citizen MIL: Military	Optional See Decision Manager (on page 52).	String (32)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
item_#_quantity	Quantity of line items. The default value is 1. Required field when one of these product codes is used: adult_content coupon electronic_good electronic_software gift_certificate service subscription # can range from 1 to 199. This field is required when the item_#_code value is not default nor related to shipping or handling.	See description. If you include this field, you must also include the line_item_count field.	Numeric String (10)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
item_#_sku	Identification code for the product. Required field when one of these product codes is used: adult_content coupon electronic_good electronic_software gift_certificate service subscription # can range from 0 to 199.	See description. If you include this field, you must also include the line_item_count field.	AlphaNumericPunctuation String (255)
item_#_tax_amount	Tax amount to apply to the line item. # can range from 0 to 199. This value cannot be negative. The tax amount and the offer amount must be in the same currency.	Optional If you include this field, you must also include the line_item_count field.	Amount String (15)
item_#_unit_price	Price of the line item. # can range from 0 to 199. This value cannot be negative. ⓘ **You must include either this field or the amount field in the request**	See description. If you include this field, you must also include the line_item_count field.	Amount String (15)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
journey_leg#_dest	Airport code for the destination 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.	Optional See Decision Manager (on page 53).	Alpha String (3)
journey_leg#_orig	Airport code for the origin 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.	Optional See Decision Manager (on page 53).	Alpha String (3)

	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.		

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
journey_type	Type of travel, such as one way or round trip.	Optional See Decision Manager (on page 53).	AlphaNumericPunctuation String (32)
line_item_count	Total number of line items. Maximum number is 200.	This field is required when you include any item fields in the request.	Numeric String (2)
locale	Indicates the language to use for customer-facing content. Possible value: en-us. See "Activating a Profile" (on page 47). ⓘ **To prevent data tampering, sign this field.**	Required by the Secure Acceptance application.	Locale String (5)

merchant_defined_data#	Optional fields that you can use to store information (see Configuring Customer Notifications (on page 35)). # can range from 1 to 100. Merchant-defined data fields 1 to 4 are associated with the payment token and are used for subsequent token-based transactions. Merchant defined data fields 5 to 100 are passed through to Decision Manager as part of the initial payment request and are not associated with the payment token. 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 and any Secure Acceptance field that is not specifically designed to capture personally identifying information. Personally Identifying Information (PII) includes, but is not limited to, card number, bank account number, social security number, driver's license number, state issued identification number, passport number, card verification numbers (CVV, CVC2, CVV2, CID, CVN). If it is discovered that a merchant is capturing and/or transmitting personally identifying information via the merchant defined data fields, whether or not intentionally, the merchant's account WILL immediately be suspended, which will result in a rejection of any and all transaction requests submitted by the merchant after the point of suspension.	Optional See Decision Manager (on page 53).	AlphaNumericPunctuation String (100)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
merchant_descriptor	Your business name. American Express displays this value on the cardholder's statement. When you include more than one consecutive space, extra spaces are removed. When you do not include this value in your request, the value in your account is sent to the processor. To add this value to your account, contact customer support.	Capture (R when the merchant descriptor contact is included in the request. You can provide the merchant descriptor in your account instead of in the request.)	String (21)
merchant_descriptor_ alternate	Alternate contact information for your business, such as an email address or URL. This value might appear on the cardholder's statement. For information about what happens when you do not include this value in your request, see Merchant Descriptor Logic(on page 30). For authorizations, this value is not sent to the processor. Instead, this	Auth (O) Capture (O)	String (13)

	value is stored and sent to the processor for captures and follow-on credits.		
merchant_descriptor_city	City or phone number for your business. American Express might display this value on the cardholder's statement. For card-present transactions, American Express recommends that this field contain the city in which your business is located. For card-not-present transactions, American Express recommends that this field contain the phone number for your business. It should be a toll free number or a local number. When you do not include this value in your request, the value in your account is sent to the processor. To add this value to your account, contact customer support	Capture (O)	String (21)
merchant_ descriptor_contact	Contact information for your business. American Express might display this value on the cardholder's statement. This value could be used to resolve billing inquiries and disputes.	Capture (O)	String (40)

	When you include more than one consecutive space, extra spaces are removed. For card-present transactions, American Express recommends that this field contain your phone number. For card-not-present transactions, American Express recommends that this field contain the URL for your web site. When you do not include this value in your request, the URL or phone number in your account is sent to the processor. To add this value to your account, contact customer support.		
merchant_ descriptor_country	Country code for your business location. American Express might display this value on the cardholder's statement. Use the standard ISO Standard Country Codes. When you do not include this value in your request, the value in your account is sent to the processor. To add this value to your account, c	Capture (O)	String (2)
merchant_descriptor_postal_ code	Postal code for your business location. American Express might	Capture (O)	String (15)

	display this value on the cardholder's statement. When you do not include this value in your request, the value in your account is sent to the processor. To add this value to your account, contact customer support. Before sending the postal code to the processor, all non-alphanumeric characters are removed and, if the remaining value is longer than nine characters, the value is trunca		
merchant_ descriptor_state	State code or region code for your business location. American Express might display this value on the cardholder's statement. For the U.S. and Canada, use the standard State, Province, and Territory Codes for the United States and Canada.	Capture (O)	String (3)
merchant_descriptor_street	Street address for your business location. American Express might display this value on the cardholder's statement. If the street address is more than 38 characters, use meaningful	Capture (O)	String (38)

	abbreviations. When you do not include this value in your request, the value in your account is sent to the processor. To add this value to your account, contact customer support.		

Field	**Description**	**Used By: Required (R) or Optional (O)**	**Data Type & Length**
merchant_secure_data4	Optional field that you can use to store information. The data is encrypted before it is stored in the payment repository.	Optional	AlphaNumericPunctuation String (2000)
merchant_secure_data1 merchant_secure_data2 merchant_secure_data3	Optional fields that you can use to store information. The data is encrypted before it is stored in the payment repository.	Optional	AlphaNumericPunctuation String (100)
override_backoffice_post_url	Overrides the backoffice post URL profile setting with your URL. URL must be HTTPS and support TLS 1.2 or later.	Optional	URL String (255)
override_custom_cancel_page	Overrides the custom cancel page profile setting with your URL. URL must be HTTPS and support TLS 1.2 or later.	Optional	URL String (255)

override_custom_receipt_page	Overrides the custom receipt profile setting with your URL. URL must be HTTPS and support TLS 1.2 or later. ⓘ **To prevent data tampering, sign this field.**	Optional	URL String (255)
override_customer_utc_offset	Overrides the transaction date and time with the number of minutes the customer is ahead of or behind UTC. Use this field to override the local browser time detected by Secure Acceptance. This time determines the date on receipt pages and emails. For example, if the customer is 2 hours ahead, the value is 120; if 2 hours behind, then -120; if UTC, the value is 0.	Optional	Integer (5)
override_paypal_order_setup	Overrides the PayPal order setup profile setting. Possible values: include_authorization: The PayPal order is created and authorized. exclude_authorization: The PayPal order is created but not authorized.	Optional See Enabling PayPal Express Checkout (on page 30).	String (21)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
payer_ authentication_ acquirer_country	Send this to tell issuers that the acquirer's country differs from the merchant country, and the acquirer is in the European Economic Area (EEA) and UK and Gibraltar.	Optional	String (2)
payer_ authentication_ acs_window_size	Sets the challenge window size that displays to the cardholder. The Access Control Server (ACS) replies with content that is formatted appropriately for this window size. The sizes are width x height in pixels. Secure Acceptance calculates this value based on the size of the window in which Secure Acceptance is displayed, but you can override it. Possible values: 01: 250 x 400 02: 390 x 400 03: 500 x 600 04: 600 x 400 05: Full page	Optional	Integer (2)
payer_ authentication_ challenge_code	Possible values: 01: No preference 02: No challenge request 03: Challenge requested (3D Secure requestor preference) 04: Challenge requested (mandate) 06: No challenge requested (data share only) 07: No challenge requested (strong consumer	Optional	Integer (2)

	authentication is already performed) This field will default to 01 on merchant configuration and can be overridden by the merchant. EMV 3D Secure 2.1.0 supports values 01-04. Version 2.2.0 supports values 01-09.		
payer_authentication_customer_annual_transaction_count	Number of transactions (successful and abandoned) for this cardholder account within the past year.	Optional	Integer (3)
payer_authentication_customer_daily_transaction_count	Number of transaction (successful or abandoned) for this cardholder account within the past 24 hours.	Optional	Integer (3)
payer_authentication_indicator	Indicates the type of authentication request. Secure Acceptance automatically populates this field, but you can override it. Possible values: 01: Payment transaction 02: Recurring transaction 03: Installment transaction 04: Add card 05: Maintain card 06: Cardholder verification as part of EMV token identity and verification (ID&V)	Optional	Integer (2)
payer_authentication_marketing_source	Indicates origin of the marketing offer.	Optional	String (40)

payer_authentication_merchant_fraud_rate	Calculated by merchants according to Payment Service Directive 2 (PSD2) and Regulatory Technical Standards (RTS). European Economic Area (EEA) and UK and Gibraltar card fraud divided by all EEA and UK and Gibraltar card volumes. Possible values: 1: Represents fraud rate ≤1 2: Represents fraud rate >1 and ≤6 3: Represents fraud rate >6 and ≤13 4: Represents fraud rate >13 and ≤25 5: Represents fraud rate >25	Optional	Integer (2)
payer_authentication_merchant_name	Your company's name as you want it to appear to the customer in the issuing bank's authentication form. This value overrides the value specified by your merchant bank.	Optional	String (25)
payer_authentication_merchant_score	Risk score provided by merchants. Used for Cartes Bancaires transactions.	Optional	String (20)
payer_authentication_mobile_phone	Cardholder's mobile phone number. Important: Required for Visa Secure transactions in Brazil. Do not use this request field for any other types of transactions.	Optional	Integer (25)

payer_ authentication_ new_customer	Indicates whether the customer is a new or existing customer with the merchant. Possible values: true false	Optional	String (5)
payer_ authentication_ pre_order	Indicates whether cardholder is placing an order with a future availability or release date. Possible values: 01: Merchandise available 02: Future availability	Optional	Integer (2)
payer_ authentication_ pre_order_date	Expected date that a pre-ordered purchase will be available. Format: yyyyMMDD	Optional	Integer (8)
payer_ authentication_ prior_ authentication_ data	Data that the ACS can use to verify the authentication process.	Optional	String (2048)
payer_ authentication_ prior_ authentication_ method	Method that the cardholder used previously to authenticate to the 3D Secure requester. Possible values: 01: Frictionless authentication through the ACS 02: Cardholder challenge through the ACS 03: AVS verified 04: Other issuer methods 05-79: Reserved for EMVCo future use (values invalid until defined by EMVCo) 80-99: Reserved for directory server use	Optional	Integer (2)

payer_ authentication_ prior_ authentication_ reference_id	This field contains the ACS transaction ID for an authenticated transaction. For example, the first recurring transaction that was authenticated with the cardholder.	Optional	String (36)
payer_ authentication_ prior_ authentication_ time	Date and time in UTC of the previous cardholder authentication. Format: yyyyMMDDHHMM	Optional	Integer (12)
payer_ authentication_ recurring_end_ date	The date after which no further recurring authorizations should be performed. Format: yyyyMMDD. This field is required for recurring transactions. If recurring_frequency and recurring_number_of_installments are included in the request, Secure Acceptance will automatically populate this field. Specify a value to override this logic.	Optional	Integer (8)
payer_ authentication_ recurring_ frequency	Integer value indicating the minimum number of days between recurring authorizations. A frequency of monthly is indicated by the value 28. Multiple of 28 days will be used to indicate months. Example: 6 months= 168 This field is required for recurring transactions. If recurring_frequency is	Optional	Integer (3)

	included in the request, Secure Acceptance will automatically populate this field. Specify a value to override this logic.		
payer_ authentication_ reorder	Indicates whether the cardholder is reordering previously purchased merchandise. Possible values: 01: First time ordered 02: Reordered	Optional	Integer (2)
payer_ authentication_ secure_corporate_ payment	Indicates that dedicated payment processes and procedures were used. Potential secure corporate payment exemption applies. Possible values: 0 1	Optional	String (1)
payer_ authentication_ ship_to_address_ first_used	Date on which this shipping address was first used. Possible values: -1: Guest account 0: First used during this transaction If neither value applies, enter the date in yyyyMMDD format.	Optional	Integer (8)
payer_ authentication_ transaction_ mode	Transaction mode identifier. Identifies the channel from which the transaction originates. Possible values: M: MOTO (Mail Order Telephone Order) R: Retail S: E-commerce	Required by the Secure Acceptance application.	String (1)

	P: Mobile Device T: Tablet		
payer_ authentication_ whitelisted	Enables the communication of trusted beneficiary and whitelist status among the ACS, the directory server, and the 3D Secure requester. Possible values: true: 3D Secure requester is whitelisted by cardholder false: 3D Secure requester is not whitelisted by cardholder	Optional	String (5)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
payment_method	Method of payment. Possible values: card paypal visacheckout	Optional	Enumerated String (30)
payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the payment repository. When this field is included in the request, the card data and billing and shipping information are optional. You must be using Token Management Services. Populate this field with the customer token.	authorization or sale (R) authorization,update_payment_token (R) sale,update_payment_token (R) update_payment_token (R)	Numeric String (32)

	This field is required for token-based transactions.		
payment_token_comments	Optional comments you can add for the customer token.	Optional	AlphaNumericPunctuation String (255)
payment_token_title	Name or title for the customer token.	Optional	AlphaNumericPunctuation String (60)
profile_id	Identifies the profile to use with each transaction.	Assigned by the Secure Acceptance application.	ASCIIAlphaNumericPunctuation String (36)
promotion_code	Promotion code for a transaction.	Optional	String (100)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
recipient_account_id	Required for Financial Institutions (with Merchant Category Code of 6012) Identifier for the recipient's account. Use the first six digits and last four digits of the recipient's account number.	authorization (R for recipient transactions, otherwise not used)	Numeric String (10)
recipient_date_of_birth	Required for Financial Institutions (with Merchant Category Code of 6012) Recipient's date of birth. Format: yyyyMMDD.	authorization (R for recipient transactions, otherwise not used)	Date (b) String (8)

recipient_ postal_code	Required for Financial Institutions (with Merchant Category Code of 6012) Partial postal code for the recipient's address. For example, if the postal code is NN5 7SG, the value for this field should be the first part of the postal code: NN5.	authorization (R for recipient transactions, otherwise not used)	Alphanumeric String (6)
recipient_ surname	Required for Financial Institutions (with Merchant Category Code of 6012) Recipient's last name.	authorization (R for recipient transactions, otherwise not used)	Alpha String (6)

Field	**Description**	**Used By: Required (R) or Optional (O)**	**Data Type & Length**
reference_ number	Unique merchant-generated order reference or tracking number for each transaction. **Important:** To prevent data tampering, sign this field.	Required by the Secure Acceptance application.	AlphaNumericPunctuation String (50)
returns_accepted	Indicates whether product returns are accepted. This field can contain one of these values: • true • false	Optional See Decision Manager (on page 52).	Enumerated String (5)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
ship_to_address_city	City of shipping address. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Shipping Information Fields (on page 35).	Optional	AlphaNumericPunctuation String (50)
ship_to_address_country	Country code for the shipping address. Use the two-character ISO country codes. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Shipping Information Fields (on page 35).	Optional	Alpha String (2)
ship_to_address_line1	First line of shipping address. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Shipping Information Fields (on page 35).	Optional	AlphaNumericPunctuation String (60)
ship_to_address_line2	Second line of shipping address. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Shipping Information Fields (on page 35).	Optional	AlphaNumericPunctuation String (60)

ship_to_address_ postal_code	Postal code for the shipping address. This field is required if bill_to_address_country is U.S. or Canada. When the billing country is the U.S., the 9-digit postal code must follow this format: [5 digits][dash][4 digits] Example: 12345-6789 When the billing country is Canada, the 6-digit postal code must follow this format: [alpha][numeric][alpha][space] [numeric][alpha][numeric] Example: A1B 2C3 For the rest of the world countries, the maximum length is 10. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Shipping Information Fields (on page 35).	Optional	AlphaNumericPunctuation See description.
ship_to_forename	First name of the person receiving the product. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Shipping Information Fields (on page 35).	Optional	AlphaNumericPunctuation String (60)

ship_to_phone	Phone number of the shipping address. This value can be entered by your customer during the checkout process, or you can include this field in your request to Secure Acceptance. See Configuring Shipping Information Fields (on page 35).	Optional	Phone String (6 to 15)
ship_to_surname	Last name of the person receiving the product. This can be entered by your customer during the checkout process, or you can include this in your request to Secure Acceptance. See Configuring Shipping Information Fields (on page 35).	Optional	AlphaNumericPunctuation String (60)
ship_to_type	Shipping destination. Example: Commercial, residential, store	Optional	String (25)
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 pickup other: Other shipping method none: No shipping method	Optional	Enumerated String String (10)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
signature	Merchant-generated Base64 signature. This is generated using the signing method for the access_key field supplied.	Required by the Secure Acceptance application.	AlphaNumericPunctuation
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. Format: yyyy-MM-DDThh:mm:ssZ Example: 2020-08-11T22:47:57Z equals August 11, 2020, at 22:47:57 (10:47:57 p.m.). The T separates the date and the time. The Z indicates UTC. Your system time must be accurate to avoid payment processing errors related to the signed_date_time field. Important: To prevent data tampering, sign this field.	Required by the Secure Acceptance application.	ISO 8601 Date String (20)

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.	Required by the Secure Acceptance application.	AlphaNumericPunctuation Variable

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
skip_auto_auth	Indicates whether to skip or perform the preauthorization check when creating this token. Possible values: true (skip the preauthorization check) false (perform the preauthorization check)	Optional	Enumerated String (5)
skip_decision_ manager	Indicates whether to skip Decision Manager. This field can contain one of these values: true: Decision Manager is not enabled for this transaction, and the device fingerprint ID will not be displayed. false	Optional See Decision Manager (on page 52).	Enumerated String (5)

submerchant_city	Sub-merchant's city. FDC Compass This value must consist of uppercase characters.	authorization American Express Direct: R for all aggregator transactions.	American Express Direct: String (15)
submerchant_country	Sub-merchant's country. Use the two-character ISO country code. FDC Compass This value must consist of uppercase characters.	authorization American Express Direct: R for all aggregator transactions.	String (3)
submerchant_email	Sub-merchant's email address.	authorization American Express Direct: R for all aggregator transactions.	American Express Direct: String (40)
submerchant_id	The ID you assigned to your sub-merchant. FDC Compass This value must consist of uppercase characters.	authorization American Express Direct: R for all aggregator transactions.	American Express Direct: String (20)
submerchant_name	Sub-merchant's business name. FDC Compass This value must consist of uppercase characters.	authorization American Express Direct: R for all aggregator transactions.	American Express Direct: String (37)

submerchant_phone	Sub-merchant's telephone number. Visa Platform Connect	authorization American Express Direct: R for all aggregator transactions.	American Express Direct: String (20)
submerchant_postal_code	Partial postal code for the sub-merchant's address. FDC Compass This value must consist of uppercase characters.	authorization American Express Direct: R for all aggregator transactions.	American Express Direct: String (9)
submerchant_state	Sub-merchant's state or province. For the U.S. and Canada, use the standard state, province, and territory codes. FDC Compass This value must consist of uppercase characters.	authorization American Express Direct: R for all aggregator transactions.	String (2)
submerchant_street	First line of the sub-merchant's street address. FDC Compass This value must consist of uppercase characters.	authorization American Express Direct: R for all aggregator transactions.	American Express Direct: String (30)

Field	Description	Used By: Required (R) or Optional (O)	Data Type & Length
tax_amount	Total tax amount to apply to the order. This value cannot be negative. Important: To prevent data tampering, sign this field.	Optional	Amount String (15)
transaction_type	The type of transaction. Possible values: • authorization •authorization,create_payment_token •authorization,update_payment_token •sale •sale,create_payment_token •sale,update_payment_token •create_payment_token •update_payment_token Only authorization and sale are supported for Visa Click to Pay transactions. Important: To prevent data tampering, sign this field.	Required by the Secure Acceptance application.	Enumerated 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. ⓘ **To prevent data tampering, sign this field.**	Required by the Secure Acceptance application	ASCIIAlphaNumericPun String (50)

16 Response fields

Response fields are sent using these notification methods:

- Merchant POST URL. See "Merchant Notifications" (on page 36).
- Merchant POST Email. See "Merchant Notifications" (on page 36).
- POST to the URL specified in the Transaction or Custom Cancel Response page. See "Customer Response Page" (on page 39).

Notification methods are enabled on the Notifications and Customer Response pages of your Secure Acceptance profile.

To ensure the integrity of the response fields, a signature is included in the response. This signature is generated using the same **secret_key** value that was used to generate the request signature.

To verify that the response fields have not been tampered with, create a signature using the fields listed in the **signed_field_names** response field. This signature must be the same value that is included in the signature response field. Refer to the receipt page that is included in the sample scripts. See "Samples in Scripting Languages" (on page 58).

- POST to the URL specified in the Transaction or Custom Cancel Response page. See "Customer Response Page" (on page 39).

Notification methods are enabled on the Notifications and Customer Response pages of your Secure Acceptance profile.

To ensure the integrity of the response fields, a signature is included in the response. This signature is generated using the same **secret_key** value that was used to generate the request signature.

To verify that the response fields have not been tampered with, create a signature using the fields listed in the **signed_field_names** response field. This signature must be the same value that is included in the signature response field. Refer to the receipt page that is included in the sample scripts. See "Samples in Scripting Languages" (on page 58).

ⓘ **Because response fields and reason codes can be added at any time, proceed as follows:**

- **Parse the response data according to the names of the fields instead of their order in the response. For more information on parsing response fields, see the documentation for your scripting language.**
- **The signature that you generate must be the same value that is included in the signature response field.**

If configured, these response fields are sent back to your Merchant POST URL or email. See “Merchant Notifications" (on page 36). Your error handler should use the **decision** field to obtain the transaction result if it receives a reason code that it does not recognize.

16.1 Response Field descriptions

Field	Description	Data Type & Length
auth_amount	Amount that was authorized.	String (15)
auth_avs_code	AVS result code. See "AVS Codes" (on page 171).	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)

Field	Description	Data Type & Length
auth_cavv_result	Mapped response code for the Visa Secure and American Express SafeKey: See "Visa Secure Response Codes," on page 173 See "American Express SafeKey Response Codes," on page 172.	String (3)

auth_cavv_result_raw	Raw response code sent directly from the processor for Visa Secure and American Express SafeKey.	String (3)
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" (on page 172).	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_reconciliation_reference_number	Unique number that Smartpay Fuse generates to identify the transaction.	String (20)

Field	Description	Data Type & Length
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)

Field	Description	Data Type & Length
auth_trans_ref_no	Reference number that you use to reconcile your transaction reports with your processor reports. For authorization requests, the transaction reference number is returned only for these processors: American Express Direct	AlphaNumeric (60)

bill_trans_ref_no	Reference number that you use to reconcile your transaction reports with your processor reports. This field is not supported on Visa Platform Connect.	AlphaNumeric (60)

Field	**Description**	**Data Type & Length**
card_type_name	Name of the card type. For security reasons, this field is returned only in the merchant POST URL and email notifications (not in the receipt POST through the browser).	String (50)
decision	The result of your request. Possible values: ACCEPT DECLINE REVIEW ERROR CANCEL See "Types of Notifications" (on page 170).	String (7)
echeck_debit_ref_no	Reference number for the transaction.	AlphaNumeric (60)
echeck_debit_submit_time	Time when the debit was requested in UTC.	Date and Time (20)
exchange_rate	Exchange rate if a currency conversion occurred. The 17 characters include the decimal point.	Decimal (17)
invalid_fields	Indicates which request fields were invalid.	Variable
message	Response message from the payment gateway.	String (255)

payer_authentication_acs_transaction_id	Unique transaction identifier assigned by the ACS to identify a single transaction.	String (36)
payer_authentication_cavv	Cardholder authentication verification value (CAVV). Transaction identifier generated by the issuing bank or Visa Click to Pay. This field is used by the payer authentication validation service.	String (50)

Field	**Description**	**Data Type & Length**
payer_authentication_eci	Electronic commerce indicator (ECI). This field is used by payer authentication validation and enrolment services. Possible values for Visa and American Express: 05: Successful authentication. 06: Authentication attempted. 07: Failed authentication. Possible values for Mastercard: 01: Merchant is liable. 02: Card issuer is liable.	String (3)

Field	Description	Data Type & Length
payer_authentication_enroll_e_commerce_indicator	Commerce indicator for cards not enrolled. Possible values: internet: Card not enrolled or card type not supported by payer authentication. No liability shift. js_attempted: JCB card not enrolled, but attempt to authenticate is recorded. Liability shift. js_failure: J/Secure directory service is not available. No liability shift. spa: Mastercard card not enrolled in the Identity Check program. No liability shift. vbv_attempted: Visa card not enrolled, but attempt to authenticate is recorded. Liability shift. vbv_failure: For payment processor Barclays, Streamline, AIBMS, or FDC Germany, you receive this result if Visa's directory service is not available. No liability shift.	String (255)

Field	Description	Data Type & Length
payer_authentication_enroll_veres_enrolled	Result of the enrollment check. Possible values: Y: Card enrolled or can be enrolled; you must authenticate. Liability shift. N: Card not enrolled; proceed with authorization. Liability shift. U: Unable to authenticate regardless of the reason. No liability shift. This field applies only to the Asia, Middle East, and Africa Gateway. If you are configured for this processor, you must send the value of this field in your authorization request. This value can be returned if you are using rules-based payer authentication: B: Indicates that authentication was bypassed.	String (255)

Field	Description	Data Type & Length
payer_authentication_pares_status	Raw result of the authentication check. Possible values: A: Proof of authentication attempt was generated. N: Customer failed or cancelled authentication. Transaction denied. U: Authentication not completed regardless of the reason. Y: Customer was successfully authenticated.	String (255)
payer_authentication_pares_status_reason	Provides additional information about the PARes status value.	Integer (2)

payer_authentication_pares_timestamp	Decrypted time stamp for the payer authentication result. Format: Unix time, which is also called *epoch time*.	String

Field	Description	Data Type & Length
payer_authentication_reason_code	Numeric value corresponding to the result of the payer authentication request. See "Reason Codes" (on page 166).	String (5)
payer_authentication_specification_version	This field contains the 3D Secure version that was used to process the transaction. For example, 1.0.2 or 2.0.0.	String (20)
payer_authentication_transaction_id	Payer authentication transaction identifier used by Secure Acceptance to link the enrollment check and validate authentication messages.	String (20)

Field	Description	Data Type & Length
payer_authentication_type	Indicates the type of authentication that is used to challenge the card holder. Possible values: `01`: Static `02`: Dynamic `03`: OOB (Out of Band)	Integer (2)
payer_authentication_uad	Mastercard Identity Check UCAF authentication data. Returned only for Mastercard Identity Check transactions.	String (32)

payer_authentication_uci	Mastercard Identity Check UCAF collection indicator. This field indicates whether authentication data is collected at your website. 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)

Field	**Description**	**Data Type & Length**
payer_authentication_validate_e_commerce_indicator	Indicator that distinguishes Internet transactions from other types. The authentication failed if this field is not returned. For Visa, if your payment processor is Streamline, Barclays, AIBMS, or FDC Germany, you receive the value `vbv_failure` instead of internet when payer_authentication_eci is not present. The value of this field is passed automatically to the authorization service if you request the services together. Possible values: `aesk`: American Express SafeKey authentication verified successfully. `aesk_attempted`: Card not enrolled in American Express SafeKey, but the attempt to authenticate was recorded. `internet`: Authentication was not verified successfully.	String (255)

	`js`: J/Secure authentication verified successfully. `js_attempted`: JCB card not enrolled in J/Secure, but the attempt to authenticate was recorded. `spa`: Mastercard Identity Check authentication verified successfully. `spa_failure`: Mastercard Identity Check failed authentication. `vbv`: Visa Secure authentication verified successfully. `vbv_attempted`: Card not enrolled in Visa Secure, but the attempt to authenticate was recorded. `vbv_failure`: Visa Secure authentication unavailable.	

Field	**Description**	**Data Type & Length**
payer_authentication_validate_result	Raw authentication data that comes from the card-issuing bank that indicates whether authentication was successful and whether liability shift occurred. Possible values: `-1`: Invalid PARes. `0`: Successful validation. `1`: Cardholder is not participating, but the attempt to authenticate was recorded. `6`: Issuer unable to perform authentication. `9`: Cardholder did not complete authentication.	String (255)
payer_authentication_veres_timestamp	Decrypted time stamp for the verification response. Visa Click to Pay generates this value. Format: Unix time, which is also called epoch time.	String

Field	Description	Data Type & Length
payer_authentication_white_list_status	Enables the communication of trusted beneficiary and whitelist status among the ACS, the directory server, and the 3D Secure requester. Possible Values: `Y`: 3D Secure requester is whitelisted by cardholder `N`: 3D Secure requester is not whitelisted by cardholder	String (1)
payer_authentication_white_list_status_source	This field is populated by the system setting whitelist status. Possible Values: `01`: 3D Secure Server `02`: Directory server `03`: ACS	Integer (2)
payer_authentication_xid	Transaction identifier generated by payer authentication. Used to match an outgoing payer authentication request with an incoming payer authentication response.	String (28)
payment_account_reference	Reference number serves as a link to the cardholder account and to all transactions for that account. The same value is returned whether the account is represented by a PAN or a network token.	String (32)

Field	Description	Data Type & Length
payment_solution	Type of credential-on-file (COF) payment network token. Returned in authorizations that use a payment network token associated with a TMS token. Possible values: • `014`: Mastercard • `015`: Visa • `016`: American Express	String (3)

Field	Description	Data Type & Length
payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the payment repository. This payment token supersedes the previous payment token and is returned if: The merchant is configured for a 16-digit payment token that displays the last four digits of the primary account number (PAN) and passes Luhn mod-10 check. See "Payment Tokens" (on page 16). The customer has updated the card number on their payment token. This payment token supersedes the previous payment token and should be used for subsequent transactions.	String (32)

	You must be using Token Management Services.	
payment_token_latest_card_expiry_date	Card expiration date of the latest card issued to the cardholder. Returned when Network Tokenization is enabled, and a payment_token with an associated Network Token is used in a transaction. Network Tokens can continue to be used even if the original card has expired. Format: MM-yyyy	Date (a) (7)

Field	**Description**	**Data Type & Length**
payment_token_latest_card_suffix	Last four digits of the latest card issued to the cardholder. Returned when Network Tokenization is enabled, and a payment_token with an associated Network Token is used in a transaction. Network Tokens can continue to be used even if the original card number has changed due to a new card being issued. Use the last four digits in payment confirmation messages to cardholders, for example: "Thank you for your payment using your Visa card ending [payment_token_latest_card_suffix]".	String (4)
paypal_address_status	Status of the street address on file with PayPal. Possible values: None Confirmed Unconfirmed	String (12)
paypal_authorization_correlation_id	PayPal identifier that is used to investigate any issues.	String (20)

paypal_authorization_ transaction_id	Unique identifier for the transaction.	String (17)
paypal_customer_email	Email address of the customer as entered during checkout. PayPal uses this value to pre-fill the PayPal membership sign-up portion of the PayPal login page.	String (127)
paypal_do_capture_ correlation_id	PayPal identifier that is used to investigate any issues.	String (20)
paypal_do_capture_ transaction_id	Unique identifier for the transaction.	String (17)
paypal_ec_get_details_ correlation_id	PayPal identifier that is used to investigate any issues.	String (20)

Field	**Description**	**Data Type & Length**
paypal_ec_get_details_ request_id	Value of the request ID returned from a PayPal get details service request.	String (26)
paypal_ec_get_details_ transaction_id	Unique identifier for the transaction.	String (17)
paypal_ec_order_setup_ correlation_id	PayPal identifier that is used to investigate any issues.	String (20)
paypal_ec_order_setup_ transaction_id	Unique identifier for the transaction.	String (17)
paypal_ec_set_request_id	Value of the request ID returned from a PayPal set service request.	String (26)
paypal_fee_amount	PayPal fee charged for the transaction. This value does not exceed the equivalent of 10,000 USD in any currency and does not include a currency symbol. The decimal separator is a period (.), and the optional thousands separator is a comma (,).	String (9)

paypal_order_request_id	Value of the request ID returned from a PayPal order setup service request.	String (26)
paypal_payer_id	Customer's PayPal account identification number.	Alphanumeric String (13)
paypal_payer_status	Customer's status. Possible values: verified unverified	String (10)
paypal_pending_reason	Indicates the reason that payment is pending. Possible values: • address: Your customer did not include a confirmed shipping address, and your Payment Receiving preferences are set to manually accept or deny such payments. To change your preferences, go to the Preferences section of your PayPal profile.	String (14)

Field	Description	Data Type & Length
	authorization: The payment has been authorized but not settled. Capture the authorized amount. echeck: Payment was made by an echeck that has not yet cleared. intl: You have a non-U.S. account and do not have a withdrawal mechanism. You must manually accept or deny this payment in your PayPal Account Overview. multi-currency: You do not have a balance in the currency sent, and your Payment Receiving preferences are not set to automatically convert and accept this payment. You must manually accept or deny this payment in your PayPal Account Overview. none: No pending reason. order: The payment is part of an order that has been authorized but not settled. paymentreview: The payment is being reviewed by PayPal for possible fraud. unilateral: The payment was made to an email address that is not registered or confirmed. verify: Your account is not yet verified. You must verify your account before you can accept this payment.	
paypal_pending_status	Status of the transaction. Possible values: • Canceled-Reversal: PayPal canceled the reversal, which happens when you win a dispute, and the funds for the reversal are returned to you.	String (20)

Field	Description	Data Type & Length
paypal_protection_eligibility	Seller protection in force for the transaction. Possible values: Eligible: You are protected by the PayPal Seller Protection Policy for unauthorized payment and item not received. PartiallyEligible: You are protected by the PayPal Seller Protection Policy for item not received. Ineligible: You are not protected under the PayPal Seller Protection Policy.	String (17)

Field	Description	Data Type & Length
paypal_protection_eligibility_type	Seller protection in force for the transaction. Possible values: Eligible: You are protected by the PayPal Seller Protection Policy for unauthorized payment and item not received. ItemNotReceivedEligible: You are protected by the PayPal Seller Protection Policy for item not received. UnauthorizedPaymentEligible: You are protected by the PayPal Seller Protection Policy for unauthorized payment. Ineligible: You are not protected under the PayPal Seller Protection Policy. To enable the paypal_protection_eligibility_type field, contact customer support to have your account configured for this feature.	String (32)

paypal_request_id	Identifier for the request generated by the client.	String (26)

Field	Description	Data Type & Length
paypal_token	Timestamped PayPal token that identifies that PayPal Express Checkout is processing the transaction. Save this value to send in future request messages.	String (20)
paypal_transaction_type	Indicates the PayPal transaction type. Possible value: expresscheckout	String (16)
reason_code	Numeric value corresponding to the result of the payment card transaction request. See "Reason Codes" (on page 166).	String (5)
req_access_key	Authenticates the merchant with the application.	String (32)

Field	Description	Data Type & Length
req_allow_payment_token_update	Indicates whether the customer can update the billing, shipping, and payment information on the order review page. Possible 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_auth_indicator	Flag that specifies the purpose of the authorization. Possible values: 0: Preauthorization 1: Final authorization Mastercard requires European merchants to indicate whether the authorization is a final authorization or a preauthorization. To set the	String (1)

	default for this field, contact customer support.	
req_auth_type	Authorization type. Possible values: AUTOCAPTURE: Automatic capture. STANDARDCAPTURE: Standard capture. verbal: Forced capture. Set this field to AUTOCAPTURE and include it in a bundled request to indicate that you are requesting an automatic capture. If your account is configured to enable automatic captures, set this field to STANDARDCAPTURE and include it in a standard authorization or bundled request to indicate that you are overriding an automatic capture. Forced Capture Set this field to verbal and include it in the authorization request to indicate that you are performing a forced capture; therefore, you receive the authorization code outside the transaction processing system. Verbal Authorization Set this field to verbal and include it in the capture request to indicate that the request is for a verbal authorization.	String (max 15)

Field	Description	Data Type & Length
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	String (1)

	Visa cards to pay their bills. Possible values: true: Bill payment or loan payment. false (default): Not a bill payment or loan payment.	
req_bill_to_address_city	City in the billing address.	String (50)
req_bill_to_address_country	ISO country code for the billing address.	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. This field is returned if bill_to_address_country is U.S. or Canada.	String (10)
req_bill_to_address_state	State or province in the billing address. The two-character ISO state and province code. This field is returned for U.S and Canada.	String (2)
Field	Description	Data Type & Length
req_bill_to_company_name	Name of the customer's company.	String (40)
req_bill_to_email	Customer email address.	String (255)
req_bill_to_forename	Customer first name.	String (60)
req_bill_to_phone	Customer phone number.	String (15)

req_bill_to_surname	Customer last name.	String (60)

Field	Description	Data Type & Length
req_card_expiry_date	Card expiration date.	String (7)
req_card_number	Card number.	String (20)

Field	Description	Data Type & Length
req_card_type	Type of card.	String (3)
req_company_tax_id	Company's tax identifier. The the last four digits are not masked.	String (9)
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. 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_consumer_id	Identifier for the customer account. This value is defined when creating a customer token.	String (100)
req_currency	Currency used for the order. See ISO currency codes.	String (3)

req_customer_cookies_accepted	Indicates whether the customer's browser accepts cookies. Possible values: true: Customer browser accepts cookies. false: Customer browser does not accept cookies.	String (5)

Field	Description	Data Type & Length
req_customer_gift_wrap	Indicates whether the customer requested gift wrapping for this purchase. Possible values: true: Customer requested gift wrapping. false: Customer did not request gift wrapping.	String (5)
req_customer_ip_address	Customer IP address reported by your web server using socket information.	
req_date_of_birth	Date of birth of the customer. 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)

Field	Description	Data Type & Length
req_departure_time	Departure date and time of the first leg of the trip. Use one of these 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.	String (29)
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 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.	String (2)

Field	Description	Data Type & Length
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_issuer_additional_data	Data defined by the issuer.	Alphanumeric String (256)
req_item_#_code	Type of product. # can range from 0 to 199.	String (255)

Field	Description	Data Type & Length
req_item_#_description	Description of the item. # can range from 0 to 199.	String (255)
req_item_#_name	Name of the item. # can range from 0 to 199.	String (255)
req_item_#_passenger_email	Passenger's email address.	String (255)
req_item_#_passenger_forename	Passenger's first name.	String (60)
req_item_#_passenger_id	ID of the passenger to whom the ticket was issued. For example, you can use this field for the frequent flyer number.	String (32)
req_item_#_passenger_phone	Passenger's phone number. If the order is from outside the U.S., it is recommended that you include the country code.	String (15)

req_item_#_passenger_ status	Your company's passenger classification, such as with a frequent flyer classification. In this case, you might use values such as standard, gold, or platinum.	String (32)
req_item_#_passenger_ surname	Passenger's last name.	String (60)
req_item_#_passenger_type	Passenger classification associated with the price of the ticket. Possible values: `ADT`: Adult `CNN`: Child `INF`: Infant `YTH`: Youth `STU`: Student `SCR`: Senior Citizen `MIL`: Military	String (32)
req_item_#_quantity	Quantity of line items. # can range from `0` to `199`.	String (10)

Field	Description	Data Type & Length
req_item_#_sku	Identification code for the product. # can range from `0` to `199`.	String (255)
req_item_#_tax_amount	Tax amount to apply to the line item. # can range from `0` to `199`. 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 `199`. This value cannot be negative.	String (15)
req_journey_leg#_dest	Airport code for the origin of the leg of the trip, designated by the pound (#) symbol in the field name. For a complete list of airport codes, see IATA's City Code Directory.	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. This code is usually three digits long; for example: SFO = San Francisco. For a complete list of airport codes, see IATA's City Code Directory.	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 200.	String (2)
req_locale	Indicates the language to use for customer content. See "Activating a Profile" (on page 47).	String (5)

Field	Description	Data Type & Length
req_merchant_defined_data#	Optional fields that you can use to store information. # can range from `1` to `100`. Merchant-defined data fields `1` to `4` are associated with the payment token and are used for subsequent token-based transactions. Merchant-defined data fields `5` to `100` are passed through to Decision Manager as part of the initial payment request and are not associated with the payment token. Warning: 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 and any Secure Acceptance field that is not specifically designed to capture personally identifying information. 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, card verification numbers (CVV, CVC2, CVV2, CID, CVN). If it is discovered that a merchant is capturing and/or	String (100)

	transmitting personally identifying information via the merchant-defined data fields, whether or not intentionally, the merchant's account WILL immediately be suspended, which will result in a rejection of any and all transaction requests submitted by the merchant after the point of suspension.	

Field	Description	Data Type & Length
req_merchant_descriptor	Your business name. American Express displays this value on the cardholder's statement. When you include more than one consecutive space, extra spaces are removed. When you do not include this value in your request, the value in your account is sent to the processor. To add this value to your account, contact customer support.	String (21)
req_merchant_descriptor_alternate	Alternate contact information for your business, such as an email address or URL. This value might appear on the cardholder's statement. For information about what happens when you do not include this value in your request, see Merchant Descriptor Logic(on page 30). For authorizations, this value is not sent to the processor. Instead, this value is stored and	String (13)

	sent to the processor for captures and follow-on credits.	
req_merchant_descriptor_city	City or phone number for your business. American Express might display this value on the cardholder's statement. For card-present transactions, American Express recommends that this field contain the city in which your business is located. For card-not-present transactions, American Express recommends that this field contain the phone number for your business. It should be a toll free number or a local number. When you do not include this value in your request, the value in your account is sent to the processor. To add this value to your account, contact customer support	String (21)
req_merchant_descriptor_contact	Contact information for your business. American Express might display this value on the cardholder's statement. This value could be used to resolve billing inquiries and disputes. When you include more than one consecutive space, extra spaces are removed. For card-present transactions, American Express recommends that this field contain your phone number. For card-not-present transactions, American Express recommends that this field	String (40)

	contain the URL for your web site. When you do not include this value in your request, the URL or phone number in your account is sent to the processor. To add this value to your account, contact customer support.	
req_merchant_descriptor_country	Country code for your business location. American Express might display this value on the cardholder's statement. Use the standard ISO Standard Country Codes. When you do not include this value in your request, the value in your account is sent to the processor. To add this value to your account, c	String (2)
req_merchant_descriptor_ postal_code	Postal code for your business location. American Express might display this value on the cardholder's statement. When you do not include this value in your request, the value in your account is sent to the processor. To add this value to your account, contact customer support. Before sending the postal code to the processor, all non-alphanumeric characters are removed and, if the remaining value is longer than nine characters, the value is trunca	String (15)
req_merchant_descriptor_state	State code or region code for your business location. American Express might display this value on the cardholder’s statement. For the U.S. and	String (3)

	Canada, use the standard State, Province, and Territory Codes for the United States and Canada.	
req_merchant_descriptor_street	Street address for your business location. American Express might display this value on the cardholder’s statement. If the street address is more than 38 characters, use meaningful abbreviations. When you do not include this value in your request, the value in your account is sent to the processor. To add this value to your account, contact customer support.	String (38)
req_merchant_secure_data1 req_merchant_secure_data2 req_merchant_secure_data3	Optional fields that you can use to store information. The data is encrypted before it is stored in the payment repository.	String (100)
req_merchant_secure_data4	Optional field that you can use to store information. The data is encrypted before it is stored in the payment repository.	String (2000)
req_override_backoffice_ post_url	Overrides the backoffice post URL profile setting with your own URL.	URL (255)

Field	Description	Data Type & Length
req_override_custom_cancel_page	Overrides the custom cancel page profile setting with your own URL.	URL (255)
req_override_custom_receipt_page	Overrides the custom receipt profile setting with your own URL.	URL (255)

req_payment_method	Method of payment. Possible values: card paypal visacheckout	String (30)
req_payment_token	Identifier for the payment details. The payment token retrieves the card data, billing information, and shipping information from the payment repository. When this field is included in the request, the card data and billing and shipping information are optional. You must be currently using Token Management Services.	String (32)
req_payment_token_ comments	Optional comments about the customer token.	String (255)
req_payment_token_title	Name of the customer token.	String (60)
req_profile_id	Identifies the profile to use with each transaction.	String (36)
req_promotion_code	Promotion code included in the transaction.	String (100)
req_recipient_account_id	Identifier for the recipient's account. Use the first six digits and last four digits of the recipient's account number.	Numeric String (10)
req_recipient_date_of_birth	Recipient's date of birth. Format: yyyyMMDD.	Date (b) String (8)
req_recipient_postal_code	Partial postal code for the recipient's address.	Alphanumeric String (6)

Field	Description	Data Type & Length
req_recipient_surname	Recipient's last name.	Alpha String (6)
req_recurring_amount	Payment amount for each installment or recurring subscription payment.	String (15)
req_recurring_automatic_renew	Indicates whether to automatically renew the payment schedule for an installment subscription. Possible values: `true` (default): Automatically renew. `false`: Do not automatically renew.	Enumerated String String (5)
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.	String (3)
req_recurring_start_date	First payment date for an installment or recurring subscription payment.	String (8)
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. Possible values: true false	String (5)

Field	Description	Data Type & Length
req_sales_organization_id	Company ID assigned to an independent sales organization. Obtain this value from Mastercard.	Nonnegative integer (11)
req_ship_to_address_city	City of shipping address.	String (50) Visa Click to Pay: String (100)
req_ship_to_address_country	The two-character ISO country code.	String (2)
req_ship_to_address_line1	First line of shipping address.	String (60) Visa Click to Pay: String (100)
req_ship_to_address_line2	Second line of shipping address.	String (60) Visa Click to Pay: String (100)

Field	Description	Data Type & Length
req_ship_to_address_postal_code	Postal code for the shipping address.	String (10) Visa Click to Pay: String (100)
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) Visa Click to Pay: String (256)
req_ship_to_phone	Phone number for the shipping address.	String (15) Visa Click to Pay: String (30)
req_ship_to_surname	Last name of person receiving the product.	String (60) Visa Click to Pay: String (256)

Field	**Description**	**Data Type & Length**
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)
req_skip_decision_manager	Indicates whether to skip Decision Manager. See Decision Manager (on page 53). Possible values: true false	String (5)

req_submerchant_city	Sub-merchant's city.	American Express Direct: String (15)
req_submerchant_country	Sub-merchant's country.	String (3)

Field	Description	Data Type & Length
req_submerchant_email	Sub-merchant's email address.	American Express Direct: String (40)
req_submerchant_id	The ID you assigned to your sub-merchant.	American Express Direct: String (20)

Field	Description	Data Type & Length
req_submerchant_name	Sub-merchant's business name.	American Express Direct: String (37)
req_submerchant_phone	Sub-merchant's telephone number. Visa Platform Connect With American Express, the value for this field corresponds to this data in the TC 33 capture file: Record: CP01 TCRB Position: 5-24 Field: American Express Seller Telephone Number	American Express Direct: String (20)
Field	Description	Data Type & Length
req_submerchant_postal_code	Partial postal code for the sub-merchant's address.	American Express Direct:
req_submerchant_state	Sub-merchant's state or province.	String (2)
req_submerchant_street	First line of the sub-merchant's street address.	American Express Direct: String (30)
req_tax_amount	Total tax to apply to the product.	String (15)

Field	Description	Data Type & Length
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) Visa Click to Pay: String (100)
request_token	Request token data created for each response. This field is an encoded string that contains no confidential information. Atos You must store the request token value so that you can retrieve and send it in follow-on requests.	String (256)
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. Format: yyyy-MM-DDThh:mm:ssZ Example 2020-08-11T22:47:57Z equals August 11, 2020, at 22:47:57 (10:47:57 p.m.). The T separates the date and the time. The Z indicates UTC.	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)
utf8	Indicates whether the unicode characters are encoded. Possible value: #	String (3)
vc_avs_code_raw	Decrypted raw (unmapped) AVS code provided by Visa Click to Pay.	String (10)

17 Reason codes

The following table describes the Reason Codes returned for the Smartpay Fuse gateway.

Please note that this is not a definitive list of all Smartpay Fuse Reason Codes, but it does detail the Reason Codes that should be expected to be returned. It is strongly recommended that merchants regularly refer to the Smartpay Fuse documentation for all known Reason Codes.

New reason codes can be added at any time. Therefore, we recommend that merchant exception handling process is able to process any reason code, rather than being hardcoded to the current values. We recommend that any unrecognized Reason Codes are handled as per reason code 150, and that the error is logged for investigation with Gateway Support

Reason Codes

Reason Code	Description
0	Issuer system error.
100	Successful transaction.
101	The request is missing one or more required fields. Possible action: see the reply fields missingField_0...N for which fields are missing. Resend the request with the complete information.

102	One or more fields in the request contain invalid data.
104	The access_key and transaction_uuid fields for this authorization request match the access_key and transaction_uuid fields of another authorization request that you sent within the past 15 minutes. Possible action: resend the request with unique access_key and transaction_uuid fields. A duplicate transaction was detected. The transaction might have already been processed. Possible action: before resubmitting the transaction, use the single transaction query or search for the transaction using the Business Center to confirm that the transaction has not yet been processed.
110	Only a partial amount was approved.
150	General system failure.
151	The request was received but there was a server timeout. This error does not include timeouts between the client and the server. To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status in the Business Center or using Transaction Search REST API request. See the documentation for your Smartpay Fuse client for information about handling retries in the case of system errors.
152	The request was received, but a service did not finish running in time. To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status in the Business Center or using Transaction Search REST API request. See the documentation for your Smartpay Fuse client for information about handling retries in the case of system errors
200	The authorization request was approved by the issuing bank but declined by Smartpay Fuse because it did not pass the Address Verification System (AVS) check. You can capture the authorization, but consider reviewing the order for possible fraud.
201	The issuing bank has questions about the request. You do not receive an authorization code programmatically, but you might receive one verbally by calling the processor.

202	Expired card. You might also receive this value if the expiration date you provided does not match the date the issuing bank has on file. Possible action: request a different card or other form of payment.
203	General decline of the card. No other information was provided by the issuing bank. Request a different card or other form of payment.
204	Insufficient funds in the account. Possible action: request a different card or other form of payment.
205	Stolen or lost card. Possible action: review this transaction manually to ensure that you submitted the correct information
207	Issuing bank unavailable. Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status either directly in the Business Center or programmatically through the single transaction query
208	Inactive card or card not authorized for card-not-present transactions. Possible action: request a different card or other form of payment
210	The card has reached the credit limit. Possible action: request a different card or other form of payment.
211	Invalid CVN. Possible action: request a different card or other form of payment.
222	Account frozen
230	The authorization request was approved by the issuing bank but declined because it did not pass the CVN check. Possible action: you can capture the authorization, but consider reviewing the order for the possibility of fraud.
231	Invalid account number. Possible action: request a different card or other form of payment.
232	The card type is not accepted by the payment processor.

	Possible action: contact your merchant bank to confirm that your account is set up to receive the card in question
233	General decline by the processor. Possible action: request a different card or other form of payment
234	There is a problem with the information in your account. Possible action: do not resend the request. Contact customer support to correct the information in your account.
236	Processor failure. Possible action: To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status either directly in the Business Center or programmatically through the single transaction query.
240	The card type sent is invalid or does not correlate with the payment card number. Possible action: confirm that the card type correlates with the payment card number specified in the request; then resend the request.
250	The request was received, but there was a timeout at the payment processor. To avoid duplicating the transaction, do not resend the request until you have reviewed the transaction status in the Business Center or using Transaction Search REST API request.
475	The customer is enrolled in Payer Authentication. Authenticate the cardholder before continuing with the transaction.
476	The customer cannot be authenticated.
478	Strong customer authentication (SCA) is required for this transaction
480	The order is marked for review by Decision Manager.
481	The order is rejected by Decision Manager.
520	The authorization request was approved by the issuing bank but declined based on your Decision Manager settings. Possible action: review the authorization request.

18 Types of notification

Decision	Description	Type of Notification	Hosted Page
ACCEPT	Successful transaction. Reason codes 100 and 110.	• Custom receipt page • Customer receipt email • Merchant POST URL • Merchant receipt email	Accept
REVIEW	Authorization was declined; however, a capture might still be possible. Review payment details. See reason codes 200, 201, 230, and 520.	• Custom receipt page • Customer receipt email • Merchant POST URL • Merchant receipt email	Accept

Decision	Description	Type of Notification	Hosted Page
DECLINE	Transaction was declined. See reason codes 102, 200, 202, 203, 204, 205, 207, 208, 210, 211, 221, 222, 230, 231, 232, 233, 234, 236, 240, 475, 476, 478, and 481. If the retry limit is set to `0`, the customer receives the decline message, *Your order was declined.* *Please verify your information.* before the merchant receives it. The decline message relates to	• Custom receipt page • Merchant POST URL • Merchant receipt email	Decline

	either the processor declining the transaction or a payment processing error, or the customer entered their 3D Secure credentials incorrectly.		
ERROR	Access denied, page not found, or internal server error. See reason codes 102, 104, 150, 151 and 152.	• Custom receipt page • Merchant POST URL	Error
CANCEL	The customer did not accept the service fee conditions. The customer cancelled the transaction.	• Custom receipt page • Merchant POST URL	Cancel

19 Response codes

19.1 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.

19.2 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.

19.3 American Express SafeKey response codes

The American Express SafeKey response code is returned in the **auth_cavv_result** field in the response message for an authorization request.

Response Code	Description
1	CAVV failed validation and authentication.
2	CAVV passed validation and authentication.

3	CAVV passed the validation attempt.
4	CAVV failed the validation attempt.
7	CAVV failed the validation attempt and the issuer is available.
8	CAVV passed the validation attempt and the issuer is available.
9	CAVV failed the validation attempt and the issuer is not available.
A	CAVV passed the validation attempt and the issuer is not available.
U	Issuer does not participate or 3D Secure data was not used.
99	An unknown value was returned from the processor.

19.4 Visa Secure response codes

The Visa Secure response code is returned in the **auth_cavv_result** field in the response message for an authorization request

Response Code	Description
0	CAVV not validated because erroneous data was submitted.
1	CAVV failed validation and authentication.
2	CAVV passed validation and authentication.
3	CAVV passed the validation attempt.
4	CAVV failed the validation attempt.
6	CAVV not validated because the issuer does not participate.
7	CAVV failed the validation attempt and the issuer is available.
8	CAVV passed the validation attempt and the issuer is available.
9	CAVV failed the validation attempt and the issuer is not available.
A	CAVV passed the validation attempt and the issuer is not available.
B	CAVV passed the validation with information only; no liability shift.
C	CAVV attempted but not validated; issuer did not return CAVV code.

D	CAVV not validated or authenticated; issuer did not return CAVV code.
I	Invalid security data.
U	Issuer does not participate or 3D Secure data was not used.
99	An unknown value was returned from the processor.

20 iFrame implementation

> **Important: If you plan to embed Secure Acceptance in an iframe ensure that you follow the steps in this appendix. PayPal Express Checkout is not supported on a Secure Acceptance iframe integration.**
>
> **Important: For the payer authentication 3D Secure 2.x process ensure that the iframe is large enough to display the issuer's access control server (ACS) challenge content (at least 390 x 400 pixels). For more information about ACS see the Payer Authentication guide.**

You must select the single page checkout option for the hosted checkout iFrame implementation. See Checkout Configuration (on page 33).

The total amount value and the transaction cancel button are not displayed within the iFrame. Any settings that you configured for the total amount figure are ignored. See Custom Checkout Appearance (on page 41).

Barclaycard recommends that you manage the total amount value on your website containing the inline frame. You must also provide customers a cancel order functionality on your website containing the inline frame.

20.1 Clickjacking prevention

Clickjacking (also known as *user-interface redress attack* and *iframe overlay*) is used by attackers to trick users into clicking on a transparent layer (with malicious code) above legitimate buttons or clickable content for a site. To prevent clickjacking, you must prevent third-party sites from including your website within an iframe.

While no security remediation can prevent every clickjacking, these are the minimum measures you must use for modern web browsers:

- Set HTTP response header X-FRAME_OPTIONS to either “DENY” or “SAMEORIGIN”.

- Provide frame-busting scripts to ensure that your page is always the top level window or disabling code for older browsers that do not support X-FRAME_OPTIONS.

Do not use double framing on the same page where the hosted checkout iframe implementation is used.

You are required to implement the recommended prevention techniques in your website. See the OWASP Clickjacking Defense page and the Cross Site Scripting page for up-to-date information.

Web application protections for Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF), etc. must also be incorporated.

- For XSS protection, you must implement comprehensive input validation and the OWASPrecommended security encoding library to do output encoding on your website.
- For CSRF protection, you are strongly encouraged to use a synchronized token pattern. This measure requires generating a randomized token associated with the user session. The token will be inserted whenever an HTTP request is sent to the server. Your server application will verify that the token from the request is the same as the one associated with the user session.

20.2 Iframe transaction endpoints

For iframe transaction endpoints and supported transaction types for each endpoint, see Endpoints and Transaction Types (on page 48).

21 Get in contact

If you have questions or queries about the content in this document, please do not hesitate to get in contact with our teams. Please use the following contact points:

- If you are not yet a Smartpay Fuse customer contact our sales team using this form:
- https://www.barclaycard.co.uk/business/forms/bps-sme?Area=BOC

- If you are a current Smartpay Fuse customer – contact our support team*:
- Via Email: supportsmartpayfuse@barclays.com
  - Via Phone: +44 (0)1604 269 518

*Note: the support team is available Mon-Fri 9am-5pm excluding public holidays.

22 References

Smartpay Fuse has been created in partnership with VISA Cybersource. The following links refer to integration documents provided for the VISA Cybersource platform, which contains features that are not available on Smartpay Fuse. You can find out more about the Smartpay Fuse features set by visiting our developer portal "About Fuse" pages here:

https://developer.smartpayfuse.barclaycard/barclays/introducing-smartpayfuse.html

Further reading referenced from within this guide:

[1] Secure Acceptance Hosted Checkout – Barclaycard Test Cases*1
https://www.barclaycard.co.uk/content/dam/barclaycard/documents/business/accepting-payments/M05-Test-Cases.pdf

[2] Secure Acceptance Hosted Checkout – Testing Information*1
https://developer.smartpayfuse.barclaycard/docs/barclays/en-us/payer-authentication/developer/all/so/payer-auth/pa-testing-intro/pa-testing-3ds-2x-intro.html

[3] Secure Acceptance Hosted Checkout – Test Service 3DSv2 test cards and use cases[*1]
https://developer.smartpayfuse.barclaycard/docs/barclays/en-us/payer-authentication/developer/all/so/payer-auth/pa-testing-intro/pa-testing-3ds-2x-intro.html

[4] 3DSv2 Integration Guide
https://www.barclaycard.co.uk/content/dam/barclaycard/documents/business/accepting-payments/M13-Implementing-Payer-Authentication-Direct-REST-API.pdf

*1 - If you open any integration guides created by VISA Cybersource you may see some features that are not part of the Smartpay Fuse gateway. If you have any questions about this plugin or its feature set, then please don't hesitate to Get in Contact.

23 Disclaimer

Barclays and Barclaycard offers corporate banking products and services to its clients through Barclays Bank PLC. This presentation has been prepared by Barclays Bank PLC ("Barclays"). This presentation is for discussion purposes only, and shall not constitute any offer to sell or the solicitation of any offer to buy any security, provide any underwriting commitment, or make any offer of financing on the part of Barclays, nor is it intended to give rise to any legal relationship between Barclays and you or any other person, nor is it a recommendation to buy any securities or enter into any transaction or financing. Customers must consult their own regulatory, legal, tax, accounting and other advisers prior to making a determination as to whether to purchase any product, enter into any transaction of financing or invest in any securities to which this presentation relates. Any pricing in this presentation is indicative. Although the statements of fact in this presentation have been obtained from and are based upon sources that Barclays believes to be reliable, Barclays does not guarantee their accuracy or completeness. All opinions and estimates included in this presentation constitute Barclays' judgement as of the date of this presentation and are subject to change without notice. Any modelling or back testing data contained in this presentation is not intended to be a statement as to future performance. Past performance is no guarantee of future returns. No representation is made by Barclays as to the reasonableness of the assumptions made within or the accuracy or completeness of any models contained herein.

Neither Barclays, nor any officer or employee thereof, accepts any liability whatsoever for any direct or consequential losses arising from any use of this presentation or the information contained herein, or out of the use of or reliance on any information or data set out herein.

Barclays and its respective officers, directors, partners and employees, including persons involved in the preparation or issuance of this presentation, may from time to time act as manager, co-manager or underwriter of a public offering or otherwise deal in, hold or act as market-makers or advisers, brokers or commercial and/or investment bankers in relation to any securities or related derivatives which are identical or similar to any securities or derivatives referred to in this presentation.

Barclays Bank PLC is a member of the London Stock Exchange.

Barclays is a trading name of Barclays Bank PLC and its subsidiaries. Barclays Bank PLC is registered in England and authorised and regulated by the Financial Services Authority (FSA No. 122702). Registered Number is 1026167 and its registered office 1 Churchill Place, London E14 5HP.

Barclaycard is a trading name of Barclays Bank PLC and Barclaycard International Payments Limited. Barclays Bank PLC is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Financial Services Register number: 122702). Registered in England No. 1026167. Registered Office: 1 Churchill Place, London E14 5HP. Barclaycard International Payments Limited, trading as Barclaycard, is regulated by the Central Bank of Ireland. Registered Number: 316541. Registered Office: One Molesworth Street, Dublin 2, Ireland, D02 RF29. Directors: James Kelly, Mary Lambkin Coyle, Steven Lappin (British), Peter Morris and David Rowe. Calls may be recorded for security and other purposes.