# HOSTED

## INTEGRATION GUIDE

Version: 9.13

# 1 Hosted Form Integration

## *1.1 About This Guide*

The Cardstream Hosted Form Integration method requires the merchant (or the merchant's web developer) to have knowledge of server side scripting languages (e.g. PHP, ASP etc.), although less so than the Direct method. Unlike the Direct method, the merchant's website does not need to have a SSL Certificate, and PCI compliance becomes more straightforward.

If you wish to process card details on your own website, or style the payment pages of your website, you either need to use the Direct integration method or request a Custom Hosted Form for your business.

## *1.2 Cardstream Integration Disclaimer*

Cardstream provides all integration documentation necessary for enabling merchant clients to process payments via our Payment Gateway. Whilst every effort has been made to ensure these guides are accurate and complete, we expect Merchants undertaking any integration to test all their technical work fully and satisfy their own standards. Cardstream is not responsible or liable for any Merchant or Third Party integration.

## *1.3 New Customers Testing*

New customers who have not yet received their live Merchant ID can still perform an integration for testing purposes. Simply enter one of the below Test Merchant IDs and the use the Cardstream test cards to run a test transaction.

Standard Visa and MasterCard Testing use **100001**
3D Secure Testing use **100856**

This guide provides the information required to integrate with Cardstream, and gives a very basic example of code for doing so (further examples can be found on our website at www.cardstream.com). It is expected that the Merchant, or the Merchant's developers, have some experience in server side scripting with languages such as PHP or ASP, or that an off-the-shelf software package is being used that has in-built Cardstream integration support.

If you do require programming assistance, please contact Cardstream on 0845 00 99 575 or via email to solutions@cardstream.com.

## *1.4 Pre-Requisites*

You will need the following information to integrate with Cardstream Hosted Forms.

| | |
|---|---|
| **Cardstream Merchant ID** | Your Merchant ID enables you to access and communicate with the payment gateway. Please note that these details will differ to the login details supplied to access the Merchant Management System. You should have received these details when your account was set up.<br><br>You may also use test account IDs (listed above) and swap these for your live account details when you receive them. |
| **Integration URL** | https://gateway.cardstream.com/hosted/ |

## 1.5 3D Secure

If your merchant account is enrolled with 3D Secure, the hosted form method will automatically attempt to perform 3D Secure transactions. If the customer's card is not participating in 3D Secure then the transaction will be processed as normal, otherwise it will take the customer through the 3D Secure authentication process.

You can choose how to deal with 3D Secure transactions that fail authentication – either declining the transaction or continuing without 3D Secure protection. These preferences are set in the Merchant Management System.

## 1.6 Test Cards

For the latest copy of the test cards, for both 3D Secure and non 3D Secure transactions, please see Appendix A-6 & A-7 below.

# 2 Gateway Request

Your website will need to send the request details to the integration URL via an HTTP POST request. The details should be URL encoded Name=Value fields separated by '&' characters (refer to RFC 1738 and the application/x-www-form-urlencoded media type).

For example, you might create an HTML form to collect the customer information (without card details), then use hidden fields to post the other options.

*Please note that the field names are cAsE sEnSiTiVe.*

## *2.1 General Fields*

| Field Name | Mandatory? | Description |
|---|---|---|
| **merchantID** | Yes | Your Cardstream Merchant user ID, or "100001" if you are just testing. |
| **merchantPwd** | No * | The password you have configured for the merchantID. This is set within the MMS<br><br>* Using this field may result in your password being visible in plain text within the source code. |
| **signature** | Yes | The hash used to sign the transaction request. |
| **amount** | Yes | The amount of the transaction in minor currency. For the UK, this is pence, so £10.99 should be sent as 1099.<br><br>**Numeric values only – no decimal points or currency symbols.** |
| **action** | Yes | The transaction action.<br><br>Possible values are:<br><br>**PREAUTH**<br><br>This will reserve an amount from the customer's card but not collect them. For a period of up to 5 days (depending on the card issuing bank) after the transaction is placed, you can place a subsequent transaction with an action of SALE |

| | | |
|---|---|---|
| | | and the xref value returned from the first transaction in order to collect the previously reserved funds – This subsequent transaction is usually preformed using a direct integration.<br><br>If the period of time between the first and second transactions is greater than the card issuing bank reserves the funds for, then new, unreserved funds will be taken from the cardholders account.<br><br>**SALE**<br><br>This will collect an amount from the customer's card. |
| **type** | Yes | The type of transaction.<br><br>Possible values are:<br>**1** - Cardholder Not Present: Ecommerce.<br>**2** - Cardholder Not Present: Mail Order.<br>**3** - Point of Sale: Card Keyed.<br>**4** - Point of Sale: Card Swiped.<br>**5** - Point of Sale: Card Chip & Pin. |
| **countryCode** | Yes | ISO standard country code for the merchant's location. |
| **currencyCode** | Yes | ISO standard currency code for this transaction. You may only use currencies that are enabled for your merchant account. |
| **transactionUnique** | No | A unique identifier for this transaction. This should be set by your website or shopping cart. This is an added security feature to combat transaction spoofing. |
| **orderRef** | No | This text field allows you to describe the order or provide an invoice number/reference number for the merchant's records. |

## 2.2 Redirection and Verification Fields

The Hosted Form, after completion, will redirect the customer to the **`redirectURL`**, which will be called with POST data attached. Since this POST could conceivably be forged by a malicious user, it is a good idea to also supply a **`callbackURL`**. If supplied, the Hosted Form will POST the same transaction result data to the Callback URL in the background. This background page should be used to update your database.

| Field Name | Mandatory? | Description |
|---|---|---|
| `redirectURL` | Yes | The URL to which the customer will be redirected and the transaction result will be POSTed. |
| `callbackURL` | No (Recommended) | A non-public URL which will receive a copy of the transaction result by POST. |

## 2.3 Customer Details Fields

Customer details are optional by default, however if the merchant has chosen to require AVS checking in their preferences, then **`customerAddress`** and **`customerPostCode`** become mandatory. All data is stored and accessible within the administration panel.

| Field Name | Mandatory? | Description |
|---|---|---|
| `customerName` | No | The customer or cardholder's name. |
| `customerAddress` | Yes, if AVS enabled | The customer or cardholder's address. For AVS checking this must be the registered billing address of the card. |
| `customerPostCode` | Yes, if AVS enabled | The customer or cardholder's post code. For AVS checking this must be the registered billing post code of the card. |
| `customerEmail` | No | The customer's email address. |
| `customerPhone` | No | The customer's telephone number. |

## 2.4 American Express and Diners Card Fields

American Express or Diners Card cards require additional information about the customer's purchase to be posted to the hosted form. Only one order line needs to be entered. For other card types all items are optional and will be stored for reference purpose only.

| Field Name | Mandatory? | Description |
|---|---|---|
| `item1Description` | Yes† | A short text description of the item. |
| `item1Quantity` | Yes† | The quantity of the item purchased. |
| `item1GrossValue` | Yes† | The gross, or tax inclusive, value of this order line. |
| `item2Description` | No | A short text description of the item. |
| `item2Quantity` | No | The quantity of the item purchased. |
| `item2GrossValue` | No | The gross, or tax inclusive, value of this order line. |
| `item3Description` | No | A short text description of the item. |
| `item3Quantity` | No | The quantity of the item purchased. |
| `item3GrossValue` | No | The gross, or tax inclusive, value of this order line. |
| `item4Description` | No | A short text description of the item. |
| `item4Quantity` | No | The quantity of the item purchased. |
| `item4GrossValue` | No | The gross, or tax inclusive, value of this order line. |
| `item5Description` | No | A short text description of the item. |
| `item5Quantity` | No | The quantity of the item purchased. |
| `item5GrossValue` | No | The gross, or tax inclusive, value of this order line. |

†These fields are only mandatory if an American Express or Diners Card is used for payment.

With American Express or Diners Cards you may also provide tax ***or*** discount information. Once again for other cards types any values provided will be stored for reference purposes only.

| Field Name | Mandatory? | Description |
|---|---|---|
| `taxValue` | No | The total amount of tax for this order. |
| `taxDiscountDescription` | No | A text field to describe the tax applied *(e.g. "VAT at 20%")* |

***OR***

| Field Name | Mandatory? | Description |
|---|---|---|
| `discountValue` | No | The total amount of discount applied to this order. |
| `taxDiscountDescription` | No | A text field to describe the discount applied. |

## 2.5 Merchant Data Field

The merchant may send arbitrary data with the request by appending extra fields which will be returned in the response unmodified. These extra fields are merely 'echoed' back and not stored by CardStream.

However the Merchant can put extra information that should be stored into a **`merchantData`** field. Associative data can be serialised using the notation **`merchantData[name]=value`**.

| Field Name | Mandatory? | Description |
|---|---|---|
| `merchantData` | No | Arbitrary data to be stored along with this transaction. |

# 3 Gateway Response

The Cardstream Hosted Form method returns data to the Redirect URL (and Callback URL, if supplied) via an HTTP POST request. The details are sent URL encoded Name=Value fields separated by '&' characters (refer to RFC 1738 and the application/x-www-form-urlencoded media type).

The fields initially sent to the integration URL are returned and in addition the following fields may be returned.

*Please note that the field names are cAsE sEnSiTiVe.*

## *3.1 Response Fields*

| Field Name | Returned? | Description |
|---|---|---|
| **responseCode** | Always | A numeric code providing the outcome of the transaction.<br><br>Possible values are:<br><br>**0** - Successful / authorised transaction.<br>**2** - Card referred.<br>**4** - Card declined – keep card<br>**5** - Card declined.<br><br>Check **responseMessage** for more detail or any error that occurred.<br><br>For a full list of error codes please refer to the table in Appendix A. |
| **responseMessage** | Always | The message received from the acquiring bank, or any error message. |
| **signature** | Always | The hash used to sign the transaction reply. |
| **xref** | Always | The merchant may store the cross reference for repeat transactions and refunds. |
| **transactionUnique** | If supplied | The value supplied in the initial request, if any. |
| **amountReceived** | On success | The amount of the transaction. This field used in conjunction with **transactionUnique** |

| | | |
|---|---|---|
| | | can help provide a measure of security. |
| **transactionID** | Always | The ID of the transaction on the Cardstream system – can be used to easily reconcile transactions in the administration panel. |
| **orderRef** | If supplied | The value supplied in the initial request, if any. |
| **avscv2ResponseCode** | Optional | The result of the AVS/CV2 check. Please see Appendix A-4 for a full list of possible responses. |
| **avscv2ResponseMessage** | Optional | The message received from the acquiring bank, or any error message with regards to the AVS/CV2 check. Please see Appendix A-4 for a full list of possible responses. |
| **cv2Check** | Optional | Textual description of the AVS/CV2 CV2 check as described in Appendix A-4.<br><br>Possible values are: **'not known', 'not checked', 'matched', 'not matched', 'partially matched'** |
| **addressCheck** | Optional | Textual description of the AVS/CV2 address check as described in Appendix A-4.<br><br>Possible values are: **'not known', 'not checked', 'matched', 'not matched', 'partially matched'** |
| **postcodeCheck** | Optional | Textual description of the AVS/CV2 postcode check as described in Appendix A-4.<br><br>Possible values are: **'not known', 'not checked', 'matched', 'not matched', 'partially matched'** |
| **avscv2AuthEntity** | Optional | Textual description of the AVS/CV2 authorizing entity.<br><br>Possible values are: **'not known', 'merchant host', 'acquirer host', 'card scheme', 'issuer'** |
| **cardNumberMask** | Always | Card number masked so only the last 4 digits are visible - for example:<br><br>**********1234 |
| **cardTypeCode** | Always | The code of card used. See appendix A-2 for |

| | | |
|---|---|---|
| | | a full list. |
| **cardType** | Always | The description of the card used. See Appendix A-2 for a full list. |

## *3.2 3D Secure Fields*

When a 3D Secure transaction is processed then the following additional fields may be returned.

| Field Name | Returned? | Description |
|---|---|---|
| **threeDSEnabled** | Yes | The 3D Secure status of the merchant account.<br><br>Possible values are:<br>**N** – the merchant is not 3DS enabled<br>**Y** – the merchant is 3DS enabled |
| **threeDSEnrolled** | Yes | The 3D Secure enrolment status for the credit card.<br><br>Possible values are:<br>**Y** - Enrolled.<br>**N** - Not Enrolled.<br>**U** - Unable To Verify<br>**E** - Error Verifying Enrolment.<br><br>Refer to Appendix 3.2A-4 for further information. |
| **threeDSAuthenticated** | No | The 3D Secure authentication status for the credit card.<br><br>Possible values are:<br>**Y** - Authentication Successful.<br>**N** - Not Authenticated.<br>**U** - Unable To Authenticate.<br>**A** - Attempted Authentication.<br>**E** - Error Checking Authentication.<br><br>Refer to Appendix 3.2A-4 for further information. |
| **threeDSPaReq** | No | Payer Authentication Request (PaReq) that is sent to the Access Control Server (ACS) in order to verify the 3D Secure status of the credit card. |

| | | |
|---|---|---|
| **threeDSPaRes** | No | Payer Authentication Response (PaRes) that is returned from the Access Control Server (ACS) determining the 3D Secure status of the credit card. |
| **threeDSACSURL** | No | The URL of the Access Control Server (ACS) to which the Payer Authentication Request (PaReq) should be sent. |
| **threeDSECI** | No | This contains a two digit Electronic Commerce Indicator (ECI) value, which is to be submitted in a credit card authorization message.<br><br>This value indicates to the processor that the customer data in the authorization message has been authenticated.<br><br>The data contained within this property is only valid if the **threeDSAuthenticated** value is **Y** or **A**. |
| **threeDSCAVV** | No | This contains a 28-byte Base-64 encoded Cardholder Authentication Verification Value (CAVV).<br><br>The data contained within this property is only valid if the **threeDSAuthenticated** value is **Y** or **A**. |
| **threeDSCAVVAlgorithm** | No | This contains the one digit value which indicates the algorithm used by the Access Control Server (ACS) to generate the CAVV.<br><br>Valid algorithms include (amongst others):<br>**0** - HMAC<br>**1** - CVV<br>**2** - CVV with ATN<br><br>The data contained within this property is only valid if the **threeDSAuthenticated** value is **Y** or **A**. |
| **threeDSXID** | No | A unique identifier for the transaction as used in the 3D Secure process. This is normally a 20 character string. |
| **threeDSErrorCode** | No | Any error response code returned by the 3D Secure Access Control Server (ACS) should there be an error in determining the cards 3D Secure status. |

| | | |
|---|---|---|
| **threeDSErrorDescription** | No | Any error response description returned by the 3D Secure Access Control Server (ACS) should there be an error in determining the cards 3D Secure status. |
| **threeDSMerchantPref** | No | Any merchant 3D Secure preference used to block or allow this transaction should the card not be authorized. These preferences can be set in the merchant control panel. |
| **threeDSVETimestamp** | No | The time the card was checked for 3D Secure enrolment. |
| **threeDSCATimestamp** | No | The time the card was checked for 3D Secure authentication. |

# A-1 Response Codes

The gateway will always issue a **`responseCode`** to report the status of the transaction. These codes should be used rather than the **`responseMessage`** field to determine the outcome of a transaction.

A zero response code always indicates a successful outcome.

Response codes are grouped as follows, the groupings are for informational purposes only and not all codes in a group are used;

| **Acquirer (FI) Error codes: 1-99** | |
|---|---|
| **Code** | **Description** |
| **0** | Successful / authorised transaction.<br><br>Any code other than **0** indicates an unsuccessful transaction |
| **2** | Card referred |
| **4** | Card declined – keep card |
| **5** | Card declined |
| **30** | An error occurred. Check **`responseMessage`** for more detail |

| **General Error Codes: 65536 - 65791** | |
|---|---|
| **Code** | **Description** |
| **65536** | Transaction in progress. Refer to CardStream if this error occurs |
| **64437** | Reserved for future use. Refer to CardStream if this error occurs |
| **64438** | Reserved for future use. Refer to CardStream if this error occurs |
| **64439** | Invalid Credentials: **`merchantID`** is unknown |
| **64440** | Permission denied: caused by sending a request from an unauthorized IP address |
| **64441** | Reserved for future use. Refer to CardStream if this error occurs |

| | |
|---|---|
| **64442** | Request Mismatch: fields sent while completing a request do not match initially requested values. Usually due to sending different card details when completing a 3D Secure transaction to those used to authorise the transaction |
| **64443** | Request Ambiguous: request could be misinterpreted due to inclusion of mutually exclusive fields |
| **64444** | Request Malformed: couldn't parse the request data |
| **64445** | Suspended Merchant account |
| **64446** | Currency not supported by Merchant |
| **65547** | Request Ambiguous, both **`taxValue`** and **`discountValue`** provided when should be one only |
| **65548** | Database error |
| **65549** | Payment processor communications error |
| **65550** | Payment processor error |
| **65551** | Internal communications error |
| **65552** | Internal error |

| **3D Secure Error Codes: 65792 - 66047** | |
|---|---|
| **Code** | **Description** |
| **65792** | 3D Secure transaction in progress. Refer to CardStream if this error occurs |
| **65793** | Unknown 3D Secure Error |
| **65794** | 3D Secure processing is unavailable. Merchant account doesn't support 3D Secure |
| **65795** | 3D Secure processing is not required for the given card |
| **65796** | 3D Secure processing is required for the given card |
| **65797** | Error occurred during 3D Secure enrolment check |
| **65798** | Reserved for future use. Refer to CardStream if this error occurs |
| **65799** | Reserved for future use. Refer to CardStream if this error occurs |
| **65800** | Error occurred during 3D Secure authentication check |

| | |
|---|---|
| **65801** | Reserved for future use. Refer to CardStream if this error occurs |
| **65802** | 3D Secure authentication is required for this card |
| **65803** | 3D Secure enrolment or authentication failure and Merchant 3DS preferences are to STOP processing |

| **Missing Request Field Error Codes: 66048 - 66303** | |
|---|---|
| **Code** | **Description** |
| **66048** | Missing request. No data posted to integration URL |
| **66049** | Missing **`merchantID`** field |
| **66050** | Reserved for future use. Refer to CardStream if this error occurs. |
| **66051** | Reserved for internal use. Refer to CardStream if this error occurs |
| **66052** | Reserved for internal use. Refer to CardStream if this error occurs |
| **66053** | Reserved for internal use. Refer to CardStream if this error occurs |
| **66054** | Reserved for internal use. Refer to CardStream if this error occurs |
| **66055** | Missing **`action`** field |
| **66056** | Missing **`amount`** field |
| **66057** | Missing **`currencyCode`** field |
| **66058** | Missing **`cardNumber`** field |
| **66059** | Missing **`cardExpiryMonth`** field |
| **66060** | Missing **`cardExpiryYear`** field |
| **66061** | Missing **`cardStartMonth`** field (reserved for future use) |
| **66062** | Missing **`cardStartYear`** field (reserved for future use) |
| **66063** | Missing **`cardIssueNumber`** field (reserved for future use) |
| **66064** | Missing **`cardCVV`** field |
| **66065** | Missing **`customerName`** field |

| | |
|---|---|
| **66066** | Missing **`customerAddress`** field |
| **66067** | Missing **`customerPostCode`** field |
| **66068** | Missing **`customerEmail`** field |
| **66069** | Missing **`customerPhone`** field (reserved for future use) |
| **66070** | Missing **`countyCode`** field |
| **66071** | Missing **`transactionUnique`** field (reserved for future use) |
| **66072** | Missing **`orderRef`** field (reserved for future use) |
| **66073** | Missing **`remoteAddress`** field (reserved for future use) |
| **66074** | Missing **`redirectURL`** field |
| **66075** | Missing **`callbackURL`** field (reserved for future use) |
| **66076** | Missing **`merchantData`** field (reserved for future use) |
| **66077** | Missing **`origin`** field (reserved for future use) |
| **66078** | Missing **`duplicateDelay`** field (reserved for future use) |
| **66079** | Missing **`itemQuantity`** field (reserved for future use) |
| **66080** | Missing **`itemDescription`** field (reserved for future use) |
| **66081** | Missing **`itemGrossValue`** field (reserved for future use) |
| **66082** | Missing **`taxValue`** field (reserved for future use) |
| **66083** | Missing **`discountValue`** field (reserved for future use) |
| **66084** | Missing **`taxDiscountDescription`** field (reserved for future use) |
| **66085** | Missing **`xref`** field (reserved for future use) |
| **66086** | Missing **`type`** field (reserved for future use) |
| **66087** | Reserved for future use |
| **66088** | Reserved for future use |

| | |
|---|---|
| **66089** | Missing **`transactionID`** field (reserved for future use) |
| **66090** | Missing **`threeDSRequired`** field (reserved for future use) |
| **66091** | Missing **`threeDSMD`** field (reserved for future use) |
| **66092** | Missing **`threeDSPaRes`** field |
| **66093** | Missing **`threeDSECI`** field |
| **66094** | Missing **`threeDSCAVV`** field |
| **66095** | Missing **`threeDSXID`** field |

| **Invalid Request Field Error Codes: 66304 - 66559** | |
|---|---|
| **Code** | **Description** |
| **66304** | Invalid request |
| **66305** | Invalid **`merchantID`** field |
| **66306** | Reserved for future use. Refer to CardStream if this error occurs |
| **66307** | Reserved for internal use. Refer to CardStream if this error occurs |
| **66308** | Reserved for internal use. Refer to CardStream if this error occurs |
| **66309** | Reserved for internal use. Refer to CardStream if this error occurs |
| **66310** | Reserved for internal use. Refer to CardStream if this error occurs |
| **66311** | Invalid **`action`** field |
| **66312** | Invalid **`amount`** field |
| **66313** | Invalid **`currencyCode`** field |
| **66314** | Invalid **`cardNumber`** field |
| **66315** | Invalid **`cardExpiryMonth`** field |
| **66316** | Invalid **`cardExpiryYear`** field |

| | |
|---|---|
| **66317** | Invalid **`cardStartMonth`** field |
| **66318** | Invalid **`cardStartYear`** field |
| **66319** | Invalid **`cardIssueNumber`** field |
| **66320** | Invalid **`cardCVV`** field |
| **66321** | Invalid **`customerName`** field |
| **66322** | Invalid **`customerAddress`** field |
| **66323** | Invalid **`customerPostCode`** field |
| **66324** | Invalid **`customerEmail`** field |
| **66325** | Invalid **`customerPhone`** field |
| **66326** | Invalid **`countyCode`** field |
| **66327** | Invalid **`transactionUnique`** field (reserved for future use) |
| **66328** | Invalid **`orderRef`** field (reserved for future use) |
| **66329** | Invalid **`remoteAddress`** field |
| **66330** | Invalid **`redirectURL`** field |
| **66331** | Invalid **`callbackURL`** field (reserved for future use) |
| **66332** | Invalid **`merchantData`** field (reserved for future use) |
| **66333** | Invalid **`origin`** field (reserved for future use) |
| **66334** | Invalid **`duplicateDelay`** field (reserved for future use) |
| **66335** | Invalid **`itemQuantity`** field |
| **66336** | Invalid **`itemDescription`** field |
| **66337** | Invalid **`itemGrossValue`** field |
| **66338** | Invalid **`taxValue`** field |
| **66339** | Invalid **`discountValue`** field |

| | |
|---|---|
| **66340** | Invalid **`taxDiscountDescription`** field (reserved for future use) |
| **66341** | Invalid **`xref`** field |
| **66342** | Invalid **`type`** field |
| **66343** | Reserved for future use |
| **66344** | Reserved for future use |
| **66345** | Invalid **`transactionID`** field |
| **66356** | Invalid **`threeDSRequired`** field |
| **66347** | Invalid **`threeDSMD`** field |
| **66348** | Invalid **`threeDSPaRes`** field |
| **66349** | Invalid **`threeDSECI`** field |
| **66350** | Invalid **`threeDSCAVV`** field |
| **66351** | Invalid **`threeDSXID`** field |
| **66416** | Invalid card expiry date. Must be a date sometime in the next 10 years |
| **66417** | Invalid card start date. Must be a date sometime in the last 10 years |
| **66418** | Invalid item count. Tried to supply more than 6 line item details |
| **66419** | Invalid item sequence. Out of sequence line item details |

## A-2 Types of card

The following is a list of card types which may be returned by the gateway.

| Card Code | Card Type |
|---|---|
| **AM** | American Express |
| **CF** | Clydesdale Financial Services |
| **DI** | Diners Club |
| **EL** | Electron |
| **JC** | JCB |
| **MA** | International Maestro |
| **MC** | Mastercard |
| **SO** | Solo |
| **ST** | Style |
| **SW** | Domestic Maestro (Formerly Switch) |
| **VC** | Visa Credit |
| **VD** | Visa Debt |
| **VP** | Visa Purchasing |

## A-3 AVS / CV2 Check Response

The AVS/CV2 Check Response Message field **`avscv2ResponseMessage`** is sent back in the raw form that is received from the acquiring bank and can contain the following values:

| Response | Description |
|---|---|
| **ALL MATCH** | AVS and CV2 match. |
| **SECURITY CODE MATCH ONLY** | CV2 match only. |
| **ADDRESS MATCH ONLY** | AVS match only. |
| **NO DATA MATCHES** | No matches for AVS and CV2. |
| **DATA NOT CHECKED** | Supplied data not checked. |
| **SECURITY CHECKS NOT SUPPORTED** | Card scheme does not support checks. |

The AVS/CV2 Response Code **`avscv2ResponseCode`** is made up of six characters and is sent back in the raw form that is received from the acquiring bank. The first 4 characters can be decoded as below, the remaining 2 characters are currently reserved for future use:

| Position 1 Value | Description |
|---|---|
| **0** | No additional information available. |
| **1** | CV2 not checked. |
| **2** | CV2 matched. |
| **4** | CV2 not matched. |
| **8** | Reserved. |

| Position 2 Value | Description |
|---|---|
| **0** | No additional information available. |
| **1** | Postcode not checked. |
| **2** | Postcode matched. |
| **4** | Postcode not matched. |
| **8** | Postcode partially matched. |

| Position 3 Value | Description |
|---|---|
| **0** | No additional Information. |
| **1** | Address numeric not checked. |
| **2** | Address numeric matched. |
| **4** | Address numeric not matched. |
| **8** | Address numeric partially matched. |

| Position 4 Value | Description |
|---|---|
| **0** | Authorising entity not known. |
| **1** | Authorising entity – merchant host. |
| **2** | Authorising entity – acquirer host. |
| **4** | Authorising entity – card scheme. |
| **8** | Authorising entity – issuer. |

# A-4 3D Secure Enrolment/Authentication Codes

The 3D Secure enrolment check field **`threeDSEnrolled`** can return the following values:

**Y - Enrolled**: The card is enrolled in the 3DSecure program and the payer is eligible for authentication processing.

**N - Not Enrolled**: The checked card is eligible for the 3DSecure (it is within the card association's range of accepted cards) but the card issuing bank does not participate in the 3D Secure program. If the cardholder later disputes the purchase, the issuer may not submit a chargeback to the merchant.

**U - Unable To Verify Enrolment**: The card associations were unable to verify if the cardholder is registered. As the card is ineligible for 3D Secure, merchants can choose to accept the card nonetheless and precede the purchase as non-authenticated and submits authorization with ECI 7. The Acquirer/Merchant retains liability if the cardholder later disputes making the purchase.

**E - Error Verify Enrolment**: The CardStream system encountered an error. This card is flagged as 3D Secure ineligible. The card can be accepted for payment, yet the merchant may not claim a liability shift on this transaction in case of a dispute with the cardholder.

The 3D Secure authentication check field **`threeDSAuthenticated`** can return the following values:

**Y - Authentication Successful:** The Issuer has authenticated the cardholder by verifying the identity information or password. A CAVV and an ECI of 5 is returned. The card is accepted for payment.

**N - Not Authenticated:** The cardholder did not complete authentication and the card should not be accepted for payment.

**U - Unable To Authenticate:** The authentication was not completed due to technical issues or another problem. A transmission error prevented authentication from completing. The card should be accepted for payment but no authentication data will be passed on to authorization processing and no liability shift will occur.

**A - Attempted Authentication:** A proof of authentication attempt was generated. The cardholder is not participating, but the attempt to authenticate was recorded. The card should be accepted for payment and authentication information passed to authorization processing.

**E - Error Checking Authentication:** The CardStream system encountered an error. The card should be accepted for payment but no authentication information will be passed to authorization processing and no liability shift will occur.

## A-5 Example Code

The following example shows how to send the initial request using a HTML form to POST the data to the CardStream integration URL:

/myshop/orderconfirmation.php:

```
<?php
// PreShared Key entered on MMS. The demo accounts is fixed, but merchant accounts can
be updated from the MMS.
$pre shared key = "Circle4Take40Idea";

$fields = array(
        "merchantID"          =>      "100856",
        "merchantPwd"         =>      "Carry21After46Pardon",
        "amount"              =>      "1050",
        "countryCode"         =>      "826",
        "currencyCode"        =>      "826",
        "transactionUnique"   =>      "AZ2045-PY",
        "orderRef"            =>      "Groceries",
        "redirectURL"         =>      "http://www.shop.com/ordercomplete.php"
);

// Sort the array
ksort($fields);

?>
<form action="https://gateway.cardstream.com/hosted/" method="post">
<input type="hidden" name="merchantID" value="100856" />
<input type="hidden" name="merchantPwd" value="Carry21After46Pardon" />
<input type="hidden" name="amount" value="1050" />
<input type="hidden" name="countryCode" value="826" />
<input type="hidden" name="currencyCode" value="826" />
<input type="hidden" name="transactionUnique" value="AZ2045-PY" />
<input type="hidden" name="orderRef" value="Groceries" />
<input type="hidden" name="redirectURL" value="http://www.shop.com/ordercomplete.php"
/>
<input type="hidden" name="signature" value="<?= hash("SHA512",
http build query($fields) . $pre shared key) ?>" />
<input type="submit" value="Pay Now" />
</form>
```

When the user submits the form their browser will be taken to the CardStream integration page at https://gateway.cardstream.com/hosted/ where the user will be given the option to enter their card details and billing address. If additional customer or transaction information is supplied in the HTTP POST request, then the values sent will be used to populate the initial values of the controls on the CardStream hosted form. When the customer submits this hosted form the transaction will be attempted and the results sent as a HTTP POST request to the specified **`redirectURL`** an example of which is given below:

/myshop/ordercomplete.php:

```
if( $_POST['responseCode'] === "0" ) {

  echo "<p>Thank you for your payment</p>";
```

```
}else{

  echo "<p>Failed to take payment: " . htmlentities($_POST['responseMessage']) .
"</p>";


}
```

# A-6 Test Cards

The expiry date used for each test card should be December of the current year; in two digit format – E.g. 12/15 for December 2015

## The authorisation response is dependent on the transaction amount:

| Amount range from | Amount range to | Expected response |
|---|---|---|
| **101 (£1.01)** | 4999 (£49.99) | AUTH CODE: XXXXXX |
| **5000 (£50.00)** | 9999 (£99.99) | CARD REFERRED |
| **10000 (£100.00)** | 14999 (£149.99) | CARD DECLINED |
| **15000+ (£150.00+)** | | CARD DECLINED – KEEP CARD* |

* If applicable to transaction / merchant / acquirer type

**Visa Credit**

| Card Number | CVV Number | Address |
|---|---|---|
| **4929421234600821** | 356 | Flat 6<br>Primrose Rise<br>347 Lavender Road<br>Northampton<br>NN17 8YG |
| **4543059999999982** | 110 | 76 Roseby Avenue<br>Manchester<br>M63X 7TH |
| **4543059999999990** | 689 | 23 Rogerham<br>Mansions<br>4578 Ermine Street<br>Borehamwood<br>WD54 8TH |

### Visa Debit

| Card Number | CVV Number | Address |
|---|---|---|
| **4539791001730106** | 289 | Unit 5<br>Pickwick Walk<br>120 Uxbridge Road<br>Hatch End<br>Middlesex<br>HA6 7HJ |
| **4462000000000003** | 672 | Mews 57<br>Ladybird Drive<br>Denmark 65890 |

### MasterCard Credit

| Card Number | CVV Number | Address |
|---|---|---|
| **5301250070000191** | 419 | 25 The Larches<br>Narborough<br>Leicester<br>LE10 2RT |
| **5413339000001000** | 304 | Pear Tree Cottage<br>The Green<br>Milton Keynes<br>MK11 7UY |
| **5434849999999951** | 470 | 34a Rubbery Close<br>Cloisters Run<br>Rugby<br>CV21 8JT |
| **5434849999999993** | 557 | 4-7 The Hay Market<br>Grantham<br>NG32 4HG |

### MasterCard Debit

| Card Number | CVV Number | Address |
|---|---|---|
| **5573 4712 3456 7898** | 159 | Merevale Avenue<br>Leicester<br>LE10 2BU |

### UK Maestro

| Card Number | CVV Number | Address |
|---|---|---|

| | | |
|---|---|---|
| **6759 0150 5012 3445 002** | 309 | The Parkway<br>5258 Larches Approach<br>Hull<br>North Humberside<br>HU10 5OP |
| **6759 0168 0000 0120 097** | 701 | The Manor<br>Wolvey Road<br>Middlesex<br>TW7 9FF |

**JCB**

| Card Number | CVV Number | Address |
|---|---|---|
| **3540599999991047** | 209 | 2 Middle Wallop<br>Merideth-in-the-Wolds<br>Lincolnshire<br>LN2 8HG |

**Electron**

| Card Number | CVV Number | Address |
|---|---|---|
| **4917480000000008** | 009 | 5-6 Ross Avenue<br>Birmingham<br>B67 8UJ |

**American Express**

| Card Number | CVV Number | Address |
|---|---|---|
| **374245455400001** | 4887 | The Hunts Way<br>Southampton<br>SO18 1GW |

**Diners Club**

| Card Number |
|---|
| **36432685260294** |

# A-7 3D Secure Test Cards

3D Secure test cards for MasterCard using SecureCode

The expiry date used for each test card should be December of the current year; in two digit format – E.g. 12/15 for December 2015

| Card Number | CVV Number | Address | Postcode | Amount | Test Scenario |
|---|---|---|---|---|---|
| **5033961989000000818** | 332 | 31 | 18 | £11.01 | Enrolled International Maestro account number – valid SecureCode (multiple cardholder). Select 'MEGAN SANDERS' with SecureCode password: secmegan1 |
| **5453010000070789** | 508 | 20 | 52 | £11.02 | Enrolled account number - valid SecureCode (single) SecureCode password: sechal1 |
| **5453010000070151** | 972 | 22 | 08 | £11.03 | Enrolled account number – mixed SecureCode (multi) SecureCode password: Hannah – sechannah1 (bad) Haley – sechaley1 (good) |
| **5453010000070284** | 305 | 35 | 232 | £11.04 | Enrolled account number – invalid SecureCode Invalid SecureCode password: invseccode |
| **5453010000084103** | 470 | 73 | 170 | £11.05 | Attempts processing |
| **5453010000070888** | 233 | 1 | 248 | £11.06 | Account number not enrolled |
| **5199992312641465** | 006 | 21 | 14 | £11.07 | Card range not participating |

3D Secure test cards for Visa using Verified by Visa

The expiry date used for each test card should be December of the current year; in two digit format – E.g. 12/15 for December 2015

| Card Number | CVV Number | Address | Postcode | Amount | Test Scenario |
|---|---|---|---|---|---|
| **4909630000000008** | | | | £12.01 | Card range not participating |
| **4012010000000000009** | | | | £12.02 | Card registered with VbV (automated ACS response – click on Submit button) |

| | | | | | |
|---|---|---|---|---|---|
| **4012001037141112** | 083 | 16 | 155 | £12.03 | Card registered with Visa (automated ACS response – click on Submit button) |
| **4012001037484447** | 450 | 200 | 19 | £12.04 | Failed authentication – issuer database unavailable |
| **4015501150000216** | | | | £12.05 | Attempts processing (automated ACS response – click on Submit button) |

## A-8 Signing Your Request

A message can be signed by hashing the whole URL encoded Name=Value request string with a secret passphrase appended. This security passphrase can be configured on a per merchant account basis in the Merchant Management System (MMS).

Care must be taken to normalise any embedded line ending to just use a single New Line character (ascii character 10).

Various hashing algorithms are supported allowing you to choose the one most suitable for your integration language. SHA512 is the default and preferred, if using an algorithm other than SHA512 then the algorithm name should be pre-pended to the hash enclosed in braces.

The following algorithms are supported (from most secure to least secure order): SHA512, SHA256, SHA1, MD5, CRC32.

The hash must be sent in the signature field. This field must not be included in the message that is used to generate the hash.

Note: when a secret is configured for the merchant account then every message must be signed – failure to sign a message will cause it to be rejected due to a missing signature. The gateway will also sign any response and any details POSTed to any Callback URL using the same signature allowing the merchant to verify that any response has not been tampered with.