MasterCard
Worldwide

MiGS
Virtual Payment Client
Integration Reference

October 2010
Software version: MR 25

Copyright

MasterCard and its vendors own the intellectual property in this Manual exclusively. You acknowledge that you must not perform any act which infringes the copyright or any other intellectual property rights of MasterCard or its vendors and cannot make any copies of this Manual unless in accordance with these terms and conditions.

Without our express written consent you must not:

- Distribute any information contained in this Manual to the public media or quote or use such information in the public media; or
- Allow access to the information in this Manual to any company, firm, partnership, association, individual, group of individuals or other legal entity other than your officers, directors and employees who require the information for purposes directly related to your business.

License Agreement

The software described in this Manual is supplied under a license agreement and may only be used in accordance with the terms of that agreement.

Trademarks

Trademark notices and symbols used in this manual reflect the registration status of MasterCard trademarks in the United States. Please consult with the Customer Operations Services team or the MasterCard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

MasterCard Asia-Pacific (Australia)

Level 8, 100 Arthur Street

North Sydney, NSW 2060

Australia

www.mastercard.com

Contents

1 About Virtual Payment Client

MasterCard Virtual Payment Client enables merchants to use payment enabled websites, e-commerce or other applications by providing a low effort integration solution. It is suitable for most website hosting environments as merchants can integrate payment capabilities into their application without installing or configuring any payments software.

This guide describes how to payment enable your e-commerce application or online store by using the functionality of the Virtual Payment Client.

It details the basic and supplementary fields for the different types of transactions, and includes additional material such as valid codes, error codes and security guidelines.

Where to Get Help

If you need assistance with Virtual Payment Client integration, please contact your support organisation’s help desk, the details of which you will be given once you sign up to the MiGS service via your bank.

Other documents

The following documents and resources provide information related to the subjects discussed in this manual.

- MiGS Merchant Product Guide
- MiGS Payment Client Integration Guide
- MiGS Virtual Payment Integration Client Guide.

2 Basic Transaction Fields

This section describes the commands, field types and valid values for basic transactions in Virtual Payment Client.

Field Types

Virtual Payment Client uses three different types of fields: **Alpha**, **Alphanumeric** and **Numeric** as described in the table below.

Table 1 Fields used in Virtual Payment Client

Field Types	Description
Alpha	Alphabetical characters only, in the range **A** to **Z** and **a** to **z** of the base US ASCII characters. The US ASCII ranges for these characters are hexadecimal 65 to 90 inclusive, and hexadecimal 97 to 122 inclusive.
Alphanumeric	Any of the base US ASCII characters in the range hexadecimal 20 to 126, except the | character, hexadecimal 124.
Numeric	Numeric characters only in the range **0** to **9** in the base US ASCII characters. The US ASCII ranges for these characters are hexadecimal 30 to 39 inclusive.

Input Requirements

The Virtual Payment Client requires a number of inputs to perform a basic transaction. The values of these inputs are passed from the merchant software into the Payment Server via the Virtual Payment Client interface.

Depending on the model, 2-Party or 3-Party, the appropriate suffix must be appended to the Virtual Payment Client URL, https://migs.mastercard.com.au/

2-Party Payment Model

The 2-Party Payment Model can be used for any payment application, except where Verified by Visa™, MasterCard® SecureCode™ or JCB J/Secure™ authentication is required.

- Data is sent via a form POST to https://migs.masrercard.com.au/vpcdps
- Does not support GET data transfer. The request will be rejected.

3-Party Payment Model

The 3-Party Payment Model can be only used for payments where a web browser is involved.

- Data is sent via HTTP GET or POST to https://migs.mastercard.com.au/vpcpay
- Supports either HTTP GET or POST requests. POST must be used when sensitive data is present in the request. This includes one or more of the following fields:
- vpc_CardNum
- vpc_CardSecurityCode
- vpc_CardTrack1
- vpc_CardTrack2
- vpc_User
- vpc_Password.

Note: Sensitive data must never form part of the URL for HTTP GET or POST requests. It must always be sent via POST parameters. A failure to conform to this rule will result in a HTTP Response code of 400 (Bad Request), and the transaction will fail to proceed.

Input Fields for Basic 2-Party Transactions

Data is sent from the merchant application to the Payment Server via the Virtual Payment Client. A basic transaction requires a number of data fields as per the table below.

A fully qualified URL (https://migs.mastercard.com.au/vpcdps) must be included in the merchant's application code to send transaction information to the Virtual Payment Client.

Table 2 Fields required for basic 2-party transaction

<table>
<tr><td colspan="4"><b>Basic 2-Party Input Fields</b></td></tr>
<tr><td colspan="4">The following data fields must be included in a Transaction Request when using a 2-Party transaction.</td></tr>
<tr><td colspan="4"><b>Field Name</b></td></tr>
<tr><td colspan="4"><b>Field Description</b></td></tr>
<tr><td>Required/ Optional</td><td>Field Type</td><td>Min, Max or Set Field Length</td><td>Sample Data</td></tr>
</table>

vpc_Version			
The version of the Virtual Payment Client API being used. The current version is 1.			
Required	Alphanumeric	1,8	1
vpc_Command			
Indicates the transaction type. This must be equal to '**pay**' for a 2-Party or 3-Party payment.			
Required	Alphanumeric	1,16	pay
vpc_AccessCode			
Authenticates the merchant on the Payment Server. This means that a merchant cannot access another merchant's Merchant Id. The access code is provided when the merchant profile is registered with a Payment Provider.			
Required	Alphanumeric	8	6AQ89F3
vpc_MerchTxnRef			
A unique value created by the merchant. **Usage Notes:** The Merchant Transaction Reference is used as a reference key to the Payment Server database to obtain a copy of lost/missing receipts using the QueryDR function. It can also be used to identify a duplicate transaction if it is always kept unique for each transaction attempt. It can contain similar information to the vpc_OrderInfo field, but it must be unique for each transaction attempt if it is to be used properly. Typically, the vpc_MerchTxnRef is based on an order number, invoice number, timestamp, etc., but it should also reflect the transaction attempt. For example, if a cardholder has insufficient funds on their card and they are allowed to repeat the transaction with another credit card, the value may be INV1234/1 on the first attempt, INV1234/2 on the second attempt, and INV1234/3 on the third attempt. This identifier will be displayed in the Transaction Search results and also in the Download file (from Financial Transactions Search or Download Search Results link in Financial Transaction List) in the Merchant Administration portal on the Payment Server. **Note:** If "Enforce Unique Merchant Transaction Reference" privilege is enabled by your Payment Provider, this value must be unique across all the merchant's transactions.			
Required	Alphanumeric	1,40	ORDER958743-1
vpc_Merchant			
The unique Merchant Id assigned to a merchant by the Payment Provider. The Merchant ID identifies the merchant account against which settlements will be made.			
Required	Alphanumeric	1,16	TESTMERCHANT01
vpc_OrderInfo			
The merchant's identifier used to identify the order on the Payment Server. For example, a shopping cart number, an order number, or an invoice number. This identifier will be displayed in the Transaction Search results in the Merchant Administration portal on the Payment Server. **Note:** If 'Enforce Unique Order Reference" privilege is enabled by your Payment Provider, this value must be unique across all the merchant's orders.			
Optional	Alphanumeric	0,34	ORDER958743

<table>
<tr><td colspan="4"><b>vpc_Amount</b></td></tr>
<tr><td colspan="4">The amount of the transaction, expressed in the smallest currency unit. The amount must not contain any decimal points, thousands separators or currency symbols. For example, $12.50 is expressed as 1250.
This value cannot be negative or zero. The maximum amount is 2147483647.</td></tr>
<tr><td>Required</td><td>Numeric</td><td>1,10</td><td>1250</td></tr>
<tr><td colspan="4"><b>vpc_CardNum</b></td></tr>
<tr><td colspan="4">The number of the card used for the transaction. The format of the Card Number is based on the Electronic Commerce Modeling Language (ECML) and, in particular, must not contain white space or formatting characters.</td></tr>
<tr><td>Required</td><td>Numeric</td><td>15,19</td><td>5123456789012346</td></tr>
<tr><td colspan="4"><b>vpc_CardExp</b></td></tr>
<tr><td colspan="4">The expiry date of the card in the format YYMM. The value must be expressed as a 4-digit number (integer) with no white space or formatting characters. For example, an expiry date of May 2013 is represented as 1305.</td></tr>
<tr><td>Required</td><td>Numeric</td><td>4</td><td>1305</td></tr>
<tr><td colspan="4"><b>vpc_Currency</b></td></tr>
<tr><td colspan="4">The currency of the order expressed as an ISO 4217 alphanumeric code. This field is case-sensitive and must include uppercase characters only.
The merchant must be configured to accept the currency used in this field. To obtain a list of supported currencies and codes, please contact your Payment Provider.
<b>Note</b>: This field is required only if more than one currency is configured for the merchant.</td></tr>
<tr><td>Optional</td><td>Alpha</td><td>3</td><td>USD</td></tr>
<tr><td colspan="4"><b>vpc_SecureHash</b></td></tr>
<tr><td colspan="4">A secure hash which allows the Virtual Payment Client to authenticate the merchant and check the integrity of the Transaction Request. Secure hash provides better security to merchants than Access Code.
For more details see <i>Generating a Secure Hash</i> on page 76 and remember to <b><i>always store the Secure Hash secret securely</i></b> (see page 79).
<b>Note:</b> The secure secret is provided by the Payment Provider.</td></tr>
<tr><td>Required</td><td>Alphanumeric</td><td>64</td><td>9FF46885DCA8563ACFC62058E0FC447BD2C033D505BD8202F681DCAD7CED4DD2</td></tr>
<tr><td colspan="4"><b>vpc_SecureHashType</b></td></tr>
<tr><td colspan="4">The type of hash algorithm used to generate the secure hash of the Transaction Request and the Transaction Response.
It is strongly recommended that you generate your secure hash using SHA256 HMAC, in which case vpc_SecureHashType=SHA256
For more details see <i>Generating a Secure Hash</i> on page 76.</td></tr>
<tr><td>Optional</td><td>Alphanumeric</td><td>6</td><td>SHA256</td></tr>
</table>

vpc_ReturnAuthResponseData			
Specifies whether the authorisation response data must be included in the Transaction Response. Valid values for this field are: Y - indicates that the authorisation response data may be included in the Transaction Response, depending on the card type and acquirer used. N - indicates that the authorisation response data must not be included in the Transaction Response. This is the default value. For information on authorisation response data, see *Authorisation Response Data* on page 93.			
Optional	Alpha	1	Y

Input Fields for Basic 3-Party Transactions

Data is sent from the merchant application to the Payment Server via the Virtual Payment Client, a basic transaction requiring a number of data fields as per the table below.

A fully qualified URL (https://migs.mastercard.com.au/vpcpay) must be included in the merchant's application code to send transaction information to the Virtual Payment Client.

Table 3 Fields required for basic 3-party transaction

Basic 3-Party Input Fields			
The following data fields must be included in a Transaction Request when using a 3-Party transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_Version			
The version of the Virtual Payment Client API being used. The current version is 1.			
Required	Alphanumeric	1,8	1
vpc_Command			
Indicates the transaction type. This must be equal to '**pay**' for a 2 or 3-Party payment.			
Required	Alphanumeric	1,16	pay
vpc_AccessCode			
Authenticates the merchant on the Payment Server. This means that a merchant cannot access another merchant's Merchant Id. The access code is provided when the merchant profile is registered with a Payment Provider.			
Required	Alphanumeric	8	6AQ89F3

<table>
<tr><td colspan="4">**vpc_MerchTxnRef**</td></tr>
<tr><td colspan="4">A unique value created by the merchant.
Usage Notes: The Merchant Transaction Reference is used as a reference key to the Payment Server database to obtain a copy of lost/missing receipts using the QueryDR function. It can also be used to identify a duplicate transaction if it is always kept unique for each transaction attempt. It can contain similar information to the vpc_OrderInfo field, but it must be unique for each transaction attempt if it is to be used properly.
Typically, the vpc_MerchTxnRef is based on an order number, invoice number, timestamp, etc., but it should also reflect the transaction attempt. For example, if a cardholder has insufficient funds on their card and they are allowed to repeat the transaction with another credit card, the value may be INV1234/1 on the first attempt, INV1234/2 on the second attempt, and INV1234/3 on the third attempt.
This identifier will be displayed in the Transaction Search results and also in the Download file (from Financial Transactions Search or Download Search Results link in Financial Transaction List) in the Merchant Administration portal on the Payment Server.
Note: If "Enforce Unique Merchant Transaction Reference" privilege is enabled by your Payment Provider, this value must be unique across all the merchant's transactions.</td></tr>
<tr><td>Required</td><td>Alphanumeric</td><td>1,40</td><td>ORDER958743-1</td></tr>
<tr><td colspan="4">**vpc_Merchant**</td></tr>
<tr><td colspan="4">The unique Merchant Id assigned to a merchant by the Payment Provider. The Merchant ID identifies the merchant account against which settlements will be made.</td></tr>
<tr><td>Required</td><td>Alphanumeric</td><td>1,16</td><td>TESTMERCHANT01</td></tr>
<tr><td colspan="4">**vpc_ OrderInfo**</td></tr>
<tr><td colspan="4">The merchant's identifier used to identify the order on the Payment Server. For example, a shopping cart number, an order number, or an invoice number.
This identifier will be displayed in the Transaction Search results in the Merchant Administration portal on the Payment Server.
Note: if 'Enforce Unique Order Reference" privilege is enabled by your Payment Provider, this value must be unique across all the merchant's orders.</td></tr>
<tr><td>Required</td><td>Alphanumeric</td><td>1,100,34</td><td>ORDER958743</td></tr>
<tr><td colspan="4">**vpc_Amount**</td></tr>
<tr><td colspan="4">The amount of the transaction, expressed in the smallest currency unit. The amount must not contain any decimal points, thousands separators or currency symbols. For example, $12.50 is expressed as 1250.
This value cannot be negative or zero. The maximum valid value is 2147483647.</td></tr>
<tr><td>Required</td><td>Numeric</td><td>1,12</td><td>1250</td></tr>
<tr><td colspan="4">**vpc_Currency**</td></tr>
<tr><td colspan="4">The currency of the order expressed as an ISO 4217 alphanumeric code. This field is case-sensitive and must include uppercase characters only.
The merchant must be configured to accept the currency used in this field. To obtain a list of supported currencies and codes, please contact your Payment Provider.
Note: This field is required only if more than one currency is configured for the merchant.</td></tr>
<tr><td>Optional</td><td>Alpha</td><td>3</td><td>USD</td></tr>
</table>

vpc_Locale			
Specifies the language used on the Payment Server pages that are displayed to the cardholder, in 3-Party transactions. Please check with your Payment Provider for the correct value to use. In a 2-Party transaction the default value of 'en' is used.			
Required	Alphanumeric	2,5	en
vpc_ReturnURL			
URL supplied by the merchant in a 3-Party transaction. It is used by the Payment Server to redirect the cardholder's browser back to the merchant's website. The Payment Server sends the encrypted Digital Receipt with this URL for decryption. It must be a fully qualified URL starting with HTTP:// or HTTPS:// and if typed into a browser with Internet access, would take the browser to that web page. It is recommended that the browser is returned to an SSL secured page. This will prevent the browser pop-up indicating that the cardholder is being returned to an unsecure site. If the cardholder clicks 'No' to continue, then neither the merchant nor the cardholder will obtain any receipt details.			
Required	Alphanumeric	1,255	https://merchants_site/receipt.asp
vpc_SecureHash			
A secure hash which allows the Virtual Payment Client to authenticate the merchant and check the integrity of the Transaction Request. Secure hash provides better security to merchants than Access Code. For more details see *Generating a Secure Hash* on page 76 and remember to ***always store the Secure Hash secret securely*** (see page 79). **Note:** The secure secret is provided by the Payment Provider.			
Optional	Alphanumeric	64	9FF46885DCA8563ACFC62058E0FC447BD2C033D505BD8202F681DCAD7CED4DD2
vpc_SecureHashType			
The type of hash algorithm used to generate the secure hash of the Transaction Request and the Transaction Response. It is strongly recommended that you generate your secure hash using SHA256 HMAC, in which case vpc_SecureHashType=SHA256 For more details see *Generating a Secure Hash* on page 76.			
Optional	Alphanumeric	6	SHA256
vpc_ReturnAuthResponseData			
Specifies whether the authorisation response data must be included in the Transaction Response. Valid values for this field are: Y - indicates that the authorisation response data may be included in the Transaction Response, depending on the card type and acquirer used. N - indicates that the authorisation response data must not be included in the Transaction Response. This is the default value. For information on authorisation response data, see *Authorisation Response Data* on page 93.			
Optional	Alpha	1	Y

Basic Output Fields

Once a Transaction Response has been successfully received, the merchant application can retrieve the receipt details. These values are then passed back to the cardholder for their records.

Terminology: Returned Input fields are shown as "Input" in the table.

Basic Output Fields			
The following data fields are returned in a Transaction Response for standard 2-Party and 3-Party transactions.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_Command			
The value of the vpc_Command input field returned in the Transaction Response.			
Input	Alphanumeric	1,16	pay
vpc_MerchTxnRef			
The value of the vpc_MerchTxnRef input field returned in the Transaction Response. This field may not be returned in a transaction that fails due to an error condition.			
Input	Alphanumeric	0,40	ORDER958743-1
vpc_Merchant			
The value of the vpc_Merchant input field returned in the Transaction Response.			
Input	Alphanumeric	1,16	TESTMERCHANT01
vpc_OrderInfo			
The value of the vpc_OrderInfo input field returned in the Transaction Response.			
Input	Alphanumeric	1,34	ORDER958743
vpc_Amount			
The value of the vpc_Amount input field returned in the Transaction Response.			
Input	Numeric	1,10	1250
vpc_Currency			
The value of the vpc_Currency input field returned in the Transaction Response. This field is returned only if vpc_Currency was included in the Transaction Request.			
Input	Alpha	3	USD
vpc_Message			
This is a message to indicate what sort of errors the transaction encountered.			
Output	Alphanumeric	10,255	Merchant [TESTCORE23] does not exist.

<table>
<tr><td colspan="4"><b>vpc_TxnResponseCode</b></td></tr>
<tr><td colspan="4">A response code that is generated by the Payment Server to indicate the status of the transaction.
A vpc_TxnResponseCode of “0” (zero) indicates that the transaction was processed successfully and approved by the acquiring bank. Any other value indicates that the transaction was declined (it went through to the banking network) or the transaction failed (it never made it to the banking network).
For a list of values, see <i>Returned Response Codes</i> on page 80.</td></tr>
<tr><td>Output</td><td>Alphanumeric</td><td>1</td><td>0</td></tr>
<tr><td colspan="4"><b>vpc_ReceiptNo</b></td></tr>
<tr><td colspan="4">A unique identifier that is also known as the Reference Retrieval Number (RRN).
The vpc_ReceiptNo may be passed back to the cardholder for their records if the merchant application does not generate its own receipt number.
This field is not returned for transactions that result in an error condition.</td></tr>
<tr><td>Output</td><td>Alphanumeric</td><td>0,12</td><td>012413207163</td></tr>
<tr><td colspan="4"><b>vpc_AcqResponseCode</b></td></tr>
<tr><td colspan="4">Generated by the financial institution to indicate the status of the transaction. The results can vary between institutions so it is advisable to use the vpc_TxnResponseCode as it is consistent across all acquirers. It is only included for fault finding purposes.
Most Payment Providers return the vpc_AcqResponseCode as a 2-digit response; others return it as a 3-digit response.
This field is not returned for transactions that result in an error condition.</td></tr>
<tr><td>Output</td><td>Alphanumeric</td><td>2,3</td><td>00</td></tr>
<tr><td colspan="4"><b>vpc_TransactionNo</b></td></tr>
<tr><td colspan="4">Payment Server OrderID (or Shopping Transaction Number) is a unique number generated by the Payment Server for every transaction.
It is important to ensure that the TransactionNo is stored for later retrieval. It is used in Merchant Administration and Advanced Merchant Administration as a reference to perform refund, capture and void transactions.
This field is not returned for transactions that result in an error condition.</td></tr>
<tr><td>Output</td><td>Numeric</td><td>1,19</td><td>96841</td></tr>
<tr><td colspan="4"><b>vpc_BatchNo</b></td></tr>
<tr><td colspan="4">A value supplied by an acquirer which indicates the batch of transactions that the specific transaction has been grouped with for settlement. It is typically a date in the format YYYYMMDD.
This field will not be returned if the transaction fails due to an error condition.</td></tr>
<tr><td>Output</td><td>Numeric</td><td>0,8</td><td>20110105</td></tr>
<tr><td colspan="4"><b>vpc_AuthorizeId</b></td></tr>
<tr><td colspan="4">Authorisation Identification Code issued by the Acquirer to approve or deny a transaction.
This field is 6-digits maximum and is not returned for transactions that are declined or fail due to an error condition.</td></tr>
<tr><td>Output</td><td>Alphanumeric</td><td>0,6</td><td>654321</td></tr>
</table>

vpc_Card			
Identifies the card type used for the transaction. For a list of card types see *Card Type Code* on page 90. This field is not returned for transactions that result in an error condition.			
Output	Alpha	0,2	MC
vpc_SecureHash			
Allows the merchant application to check the integrity of the returning Transaction Response. ***Always store the Secure Hash secret securely*** (see *Generating a Secure Hash* on page 76).			
Output	Alphanumeric	64	9FF46885DCA8563ACFC62058E0FC447BD2C033D505BD8202F681DCAD7CED4DD2
vpc_SecureHashType			
The value of vpc_SecureHashType returned in the Transaction Response.			
Input	Alphanumeric	6	SHA256
vpc_CardNum			
The card number in 0.4 card masking format. This field is only returned if **System-Captured Masked Card in Digital Receipt** privilege is enabled for the merchant processing the transaction. See **Merchant Manager User Guide**			
Output	Alphanumeric Special	5	-1234
vpc_ReturnACI			
The ACI (Authorisation Characteristics Indicator) returned by the issuer. **Note**: This field is returned only if vpc_ReturnAuthResponseData was specified as "Y" in the Transaction Request.			
Output	Alphanumeric	1	N
vpc_TransactionIdentifier			
The unique identifier for the transaction returned by the issuer. **Note**: This field is returned only if vpc_ReturnAuthResponseData was specified as "Y" in the Transaction Request.			
Output	Alphanumeric	0, 19	ABC187659DEFGJ0
vpc_CommercialCardIndicator			
Indicates the type of commercial card as returned by the card issuer. For information, see *Authorisation Response Code* on page 93. **Note**: This field is returned only if vpc_ReturnAuthResponseData was specified as "Y" in the Transaction Request.			
Output	Alphanumeric	1	B

vpc_CommercialCard

Indicates if the card used is a commercial card. For more information, see *Authorisation Response Code* on page 93.

Note: This field is returned only if vpc_ReturnAuthResponseData was specified as "Y" in the Transaction Request.

Output	Alphanumeric	1	Y

vpc_CardLevelIndicator

Indicates the card level result returned by the issuer.

Note: This field is returned only if vpc_ReturnAuthResponseData was specified as "Y" in the Transaction Request.

Output	Alphanumeric	2	A [Character "A" followed by a space]

vpc_FinancialNetworkCode

Indicates the code of the financial network that was used to process the transaction with the issuer.

Note: This field is returned only if vpc_ReturnAuthResponseData was specified as "Y" in the Transaction Request.

Output	Alphanumeric	0,3	MCC

3 Supplementary Transaction Fields

The following sections detail the additional functionality available to merchants. The basic fields for either 2-Party or 3-Party transactions are used with the **extra** fields detailed in these sections.

Most functionality is available to both 2-Party and 3-Party transactions. Functionality limited to only 2-Party or 3-Party transactions is designated as such in the details.

Note: While these are supplementary fields, some of these fields may be mandatory for certain functions.

Address Verification Service (AVS) Fields

The Address Verification Service (AVS) is a security feature used for card not present transactions. It compares the card billing address data that the cardholder supplies with the records held in the card issuer's database. Once the transaction is successfully processed and authorised, the card issuer returns a result code (AVS result code) in its authorisation response message. The result code verifies the AVS level of accuracy used to match the AVS data.

In a standard 3-Party transaction, the merchant does not have to send the AVS data as the Payment Server prompts the cardholder for the information. However, in a 2-Party transaction or 3-Party with card details transaction, the AVS data must be sent by the merchant, if AVS is required.

Note: Applies to 2-Party transactions and 3-Party with card details transactions.

Transaction Request Input Fields

Table 4 Transaction Request Input Fields

Address Verification Service (AVS) Input Fields			
The data is sent by including the additional data with the required fields for a basic transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_AVS_Street01			
The street name and number, or the Post Office Box details, of the address used in the credit card billing Address Verification check by the card issuing bank.			
Required	Alphanumeric	1,128	1136 John Street
vpc_AVS_City			
The city/town/village of the address used in the credit card billing Address Verification check by the card issuing bank.			
Optional	Alphanumeric	1,128	Seattle
vpc_AVS_StateProv			
The State/Province code of the address used in the credit card billing Address Verification check by the card issuing bank.			
Optional	Alphanumeric	0,128	WA
vpc_AVS_PostCode			
The Postal/Zip code of the address used in the credit card billing Address Verification check by the card issuing bank.			
Required	Alphanumeric	4,9	98111
vpc_AVS_Country			
The 3 digit ISO standard alpha country code of the address used in the credit card billing Address Verification check by the card issuing bank.			
Optional	Alpha	3	USA

Transaction Response Output Fields

Table 5 Transaction Response Output Fields

Address Verification Service (AVS) Output Fields			
In addition to the standard output fields, the following fields are also returned in the Transaction Response for both 2-Party and 3-party transactions.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_AVS_Street01			
The value of the vpc_AVS_Street01 input field returned in the Transaction Response.			
Input	Alphanumeric	0,20	1136 John Street
vpc_AVS_City			
The value of the vpc_AVS_City input field returned in the Transaction Response.			
Input	Alphanumeric	0,20	Seattle
vpc_AVS_StateProv			
The value of the vpc_AVS_StateProv input field returned in the Transaction Response.			
Input	Alphanumeric	0,5	WA
vpc_AVS_PostCode			
The value of the vpc_AVS_PostCode input field returned in the Transaction Response.			
Input	Alphanumeric	0,9	98111
vpc_AVS_Country			
The value of the vpc_AVS_Country input field returned in the Transaction Response.			
Input	Alpha	0,3	USA
vpc_AVSResultCode			
The result code generated by the Payment Sever to indicate the AVS level that was used to match the data held by the cardholder's issuing bank. For more information see *Address Verification Service (AVS) Response Codes* page 86. **Note:** It can also be returned as '**Unsupported**' if the acquirer does not support this field.			
Output	Alpha	0,11	Y
vpc_AcqAVSRespCode			
Generated by the card issuing institution in relation to AVS. Provided for ancillary information only.			
Output	Alpha	0,1	

Card Present Fields

This feature allows merchants to add Card Present information and track data to a transaction. This feature applies where the merchant integration collects card track data from POS terminals. Card present functionality can only be performed as a 2-Party Authorisation/Purchase transaction.

For all card present transactions, the Merchant Transaction Source must be set to the value **'CARDPRESENT'**.

The card track data needs to contain the correct start and end sentinel characters and trailing longitudinal redundancy check (LRC) characters.

With card track data:

- If both are available, both **vpc_CardTrack1** and **vpc_CardTrack2** must be added to the Transaction Request

  or

- If only one is available, either **vpc_CardTrack1** or **vpc_CardTrack2** must be added to the Transaction Request.

If the magnetic stripe data is not available, for example, if the card is defective, or the POS terminal was malfunctioning at the time, it is sufficient to set the merchant transaction source to '**CARDPRESENT**' and change the '**PAN Entry Mode**' and '**PIN Entry Capability**' values in **vpc_POSEntryMode** field to indicate that the card was sighted, but manually entered.

Note: Card Track 3 data is not supported.

Transaction Request Input Fields

Table 6 Card Present Fields: Transaction Request Input Fields

<table>
<tr><td colspan="4"><b>Card Present Input Fields</b></td></tr>
<tr><td colspan="4">The data is sent by including the additional data with the required fields for a basic transaction.</td></tr>
<tr><td colspan="4"><b>Field Name</b></td></tr>
<tr><td colspan="4"><b>Field Description</b></td></tr>
<tr><td>Required/ Optional</td><td>Field Type</td><td>Min, Max or Set Field Length</td><td>Sample Data</td></tr>
</table>

<table>
<tr><td colspan="4"><b>vpc_CardTrack1</b></td></tr>
<tr><td colspan="4">7 bit ASCII text representing the card track 1 data.</td></tr>
<tr><td>Optional</td><td>Alphanumeric</td><td>79</td><td>%B5123456789012346^MR JOHN R SMITH ^13051019681143300001 840   ?;</td></tr>
</table>

vpc_CardTrack2			
7 bit ASCII text representing the card track 2 data. The PAN and expiry data component of vpc_CardTrack2 must match the PAN and expiry fields included in the Transaction Request.			
Optional	Alphanumeric	38,40	;5123456789012346=13051019681143384001?
vpc_POSEntryMode			
The first 2 characters define the actual PAN Entry Mode and the third character defines the PIN Entry Mode.			
Required	Alphanumeric	3	**PAN Entry Mode** 01 - Manual Entry 02 - Magnetic stripe read, but full unaltered contents not provided 04 - OCR/MICR coding read 90 - Magnetic stripe read and full, unaltered contents provided 05 - PAN auto entry via chip 79 - Chip card at chip-capable terminal was unable to process transaction using data on the chip or magnetic stripe on the card - therefore, PAN entry via manual entry 80 - Chip card at chip-capable terminal was unable to process transaction using data on the chip therefore the terminal defaulted to the magnetic stripe read for the PAN. This is referred to as fallback. 07 - Auto-entry via contactless magnetic chip 91 - Auto-entry via contactless magnetic strip **PIN Entry Mode** 0 – Unspecified or Unknown 1 - Terminal has PIN entry capability2 - Terminal does not have PIN entry capability (default) 8 - Terminal has PIN entry capability but PINpad is not currently operative. See *Card Present Data codes* on page 94 for more information.
vpc_CardSeqNum			
The card sequence number for transactions where the data is read through a chip on the EMV card. Valid values are 001 - 099.			
Optional	Numeric	3	001

<table>
<tr><td colspan="4"><b>vpc_EMVICCData</b></td></tr>
<tr><td colspan="4">Data read through a chip on the EMV card, base64 encoded.</td></tr>
<tr><td>Required</td><td>Alphanumeric</td><td>1, 340</td><td>XyoCA0SCAIgAhAegAAAABBAQlQUAAACAAJoDBx
EDnAEAnwIGAAAAEIFQnwMGAAAAAAAAAnwkCAA
KfEBIBEKAAACoAAC1jAAAAAAAAAP+fGgIDRJ8eCD
E1MDAzNjI3nyYIg4OCCwm2qYCfJwGAnzMD4CDInz
QDXgMAnzUBIp82AgAOnzcEDvo2AwExgZ9TAVIA</td></tr>
<tr><td colspan="4"><b>vpc_TxSource</b></td></tr>
<tr><td colspan="4">The source of the transaction.
This must be set to CARDPRESENT if the merchant's default transaction source has not been configured to CARDPRESENT.</td></tr>
<tr><td>Optional</td><td>Alphanumeric</td><td>11</td><td>CARDPRESENT</td></tr>
<tr><td colspan="4"><b>vpc_TerminalAttended</b></td></tr>
<tr><td colspan="4">Specifies whether the terminal is attended by the merchant.
Valid values are:
Y - indicates that the terminal is attended.
N - indicates that the terminal is unattended.
U - indicates that the status is unknown or unspecified.</td></tr>
<tr><td>Optional</td><td>Alphanumeric</td><td>1</td><td>Y</td></tr>
<tr><td colspan="4"><b>vpc_CardholderActivatedTerminal</b></td></tr>
<tr><td colspan="4">Specifies whether the terminal is activated by the cardholder.
Valid values are:
N - indicates that the terminal is not activated by the cardholder.
SS - indicates that the terminal is self serviced.</td></tr>
<tr><td>Optional</td><td>Numeric</td><td>1, 2</td><td>SS</td></tr>
<tr><td colspan="4"><b>vpc_TerminalInputCapability</b></td></tr>
<tr><td colspan="4">Indicates the input capability of the terminal.
Valid values are:
M Magnetic strip read (MSR) only (currently not supported)
KM MSR and key entry (currently not supported)
K Key entry only (currently not supported)
CM MSR and chip
CKM MSR, chip and key entry
C Chip read only
MX Contactless MSR
CX Contactless chip</td></tr>
<tr><td>Optional</td><td>Numeric</td><td>1, 5</td><td>MX</td></tr>
</table>

Transaction Response Output Fields

Table 7 Card Present Fields: Transaction Response Output Fields

Card Present Output Fields			
In addition to the standard output fields, the following optional fields are also returned in the Transaction Response for 2-Party transactions.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_EMVICCData			
The value of the EMV data returned in the Transaction Response.			
Output	Alphanumeric	1,340	XyoCA0SCAlgAhAegAAAABBAQlQUAAACAAJoDBxEDnAEAnwIGAAAAEIFQnwMGAAAAAAAAnwkCAAKfEBIBEKAAACoAAC1jAAAAAAAAAP+fGgIDRJ8eCDE1MDAzNjI3nyYIg4OCCwm2qYCfJwGAnzMD4CDInzQDXgMAnzUBIp82AgAOnzcEDvo2b59BAwExgZ9TAVIA

Card Security Code (CSC) Field

The Card Security Code (CSC) is a security feature for card not present transactions. It is also known as also known as CVV (Visa), CVC2 (MasterCard), CID/4DBC (Amex), or CVV2.

It compares the Card Security Code on the card with the records held in the card issuer's database. For example, on Visa and MasterCard credit cards, it is the three digit value printed on the signature panel on the back following the credit card account number. For American Express, the number is the 4 digit value printed on the front above the credit card account number.

Once the transaction is successfully processed and authorised, the card issuer returns a result code (CSC result code) in its authorisation response message. This verifies the CSC level of accuracy used to match the card security code.

In a standard 3-Party transaction, the merchant does not have to send the Card Security Code as the Payment Server prompts the cardholder for the information. However, in a 2-Party transaction or 3-Party with card details transaction, the merchant’s application must send the **vpc_CardSecurityCode** value, if CSC is required.

Note: Applies to 2-Party transactions and 3-Party with card details transactions.

Transaction Request Input Fields

Table 8 CSC Fields: Transaction Request Input Fields

Card Security Code (CSC) Input Field			
The data is sent by including the additional data with the required field for a basic transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_CardSecurityCode			
The Card Security Code (CSC), also known as CVV (Visa), CVC2 (MasterCard), CID/4DBC (Amex), or CVV2, which is printed, not embossed, on the card. It compares the code with the records held in the card issuing institution's database.			
Optional	Numeric	3,4	985

Transaction Response Output Fields

Table 9 CSC Fields: Transaction Response Output Fields

Output Fields			
In addition to the standard output fields, the following fields are also returned in the Transaction Response for both 2-Party and 3-Party transactions.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_CSCResultCode			
A single digit response from the Payment Server that is mapped from the AcqCSCRespCode showing the level of match that occurred with the CSC check. For more information, see CSC Level Codes. If the acquiring institution does not support CSC, the vpc_CSCResultCode will show '**Unsupported**'.			
Output	Alpha	1,11	M
vpc_AcqCSCRespCode			
The result code generated by the card issuing institution in relation to the Card Security Code. This is only provided for ancillary information.			
Output	Alpha	0,1	

External Payment Selection (EPS) Fields

External Payment Selection (EPS) is only used in a 3-Party transaction in order to bypass the Payment Server page that displays the logos of all the available cards that the payment processor accepts. This can be helpful if the merchant's application already allows the cardholder to select the card they want to pay with. This stops the cardholder having to do a double selection, once at the merchant's application and once on the Payment Server.

The first page displayed in the 3-Party Payment process is the card details page for the card type selected.

EPS data is also required to be passed in if the merchant wants to include card details in a 3-Party transaction. The Payment Provider must have set the correct privilege in the Payment Server for EPS to operate.

Note: Applies to 3-Party transactions.

Transaction Request Input Fields

Table 10 EPS Fields: Transaction Request Input Fields

External Payment Selection (EPS) Fields			
The data is sent by including the additional data with the required fields for a basic transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_card			
Used in External Payment Selection to determine what type of card is used. The field is case sensitive, and must comply with each of the card types valid in the Payment Server. This varies from Payment Server to Payment Server. The possible values are shown in *External Payment Selection (EPS)* on page 91***.*** To check the card types available for your Payment Provider, perform a 3-Party transaction and go to the Payment Server card selection page in a browser. Run the cursor over each card logo. The 'card' and 'gateway' values are displayed at the bottom of the browser window.			
Required	Alphanumeric	3,16	Visa
vpc_gateway			
Determines the type of payment gateway functionality. The field is case sensitive, and must comply with the gateways that are valid in the Payment Server. Valid values for this field are: • **ssl** - specifies the gateway for all standard 3-Party transactions • **threeDSecure** -specifies the gateway for a 3-D Secure Mode 3a-3-party Style Authentication Only transaction. **Note:** For most transactions the value of this field will be '**ssl**'.			
Required	Alphanumeric	3,15	ssl

Transaction Response Output Fields

There are no special output fields returned in the Transaction Response.

Merchant Transaction Source

This section describes how use the additional functionality of the Transaction Source field, which allows a merchant to indicate the source of a 2-Party transaction. Merchants and acquirers can optionally set the merchant transaction source so the payment provider can calculate correct fees and charges for each transaction.

Merchant transaction source is added to 2-Party transactions using the supplementary command at the appropriate point as indicated in their transaction flows.

If not specified, this transaction will be set to the merchant's default transaction source.

Note: Applies to 2-Party transactions.

Transaction Request Input Fields

Table 11 Merchant Transaction Source Transaction: Transaction Request Input Fields

Merchant Transaction Source Input Fields			
The data is sent by including the additional data with the required field for a basic transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_TxSource			
Allows the merchant to specify the source of the transaction. Valid values are: **INTERNET** - indicates an Internet transaction **MOTOCC** - indicates a call centre transaction **MOTO** - indicates a mail order or telephone order **MAILORDER** - indicates a mail order transaction **TELORDER** - indicates a telephone order transaction **CARDPRESENT** - indicates that the merchant has sighted the card. **VOICERESPONSE** - indicates that the merchant has captured the transaction from an IVR system. **Note:** This can only be used if the merchant has the *Allow the Merchant to Change the Transaction Source* privilege, otherwise the transaction will be set to the merchant's default transaction source as defined by your Payment Provider.			
Optional	Alphanumeric	6,16	INTERNET

Transaction Response Output Fields

There are no special output fields returned in the Transaction Response.

Merchant Transaction Source Frequency

This section describes how use the additional functionality of Transaction Frequency data, which allows a merchant to indicate the frequency of the transaction.

Note: Applies to 2-Party transactions.

Transaction Request Input Fields

Table 12 Merchant Transaction Source Frequency: Transaction Request Input Fields

<table>
<tr><td colspan="4"><b>Transaction Source Subtype Field</b></td></tr>
<tr><td colspan="4">The data is sent by including the additional data with the required fields for a basic transaction.</td></tr>
<tr><td colspan="4"><b>Field Name</b></td></tr>
<tr><td colspan="4">Field Description</td></tr>
<tr><td>Required/ Optional</td><td>Field Type</td><td>Min, Max or Set Field Length</td><td>Sample Data</td></tr>
</table>

<table>
<tr><td colspan="4"><b>vpc_TxSourceSubType</b></td></tr>
<tr><td colspan="4">Allows the merchant to flag the subtype of transaction for the cardholder's order.
vpc_TxSourceSubType must be one of the following values:
<b>SINGLE</b> - indicates a single transaction where a single payment is used to complete the cardholder's order.
<b>INSTALLMENT</b> - indicates an installment transaction where the cardholder authorises the merchant to deduct multiple payments over an agreed period of time for a single purchase
<b>RECURRING</b> - indicates a recurring transaction where the cardholder authorises the merchant to automatically debit their accounts for bill or invoice payments. This value only indicates to the acquirer that this is a recurring type payment; it does not mean that the merchant can use the Payment Server's Recurring Payment functionality.
<b>Note:</b> This can only be used if the merchant has their privilege set to use this command, otherwise the transaction will be set to the merchant's default transaction source as defined by your Payment Provider.</td></tr>
<tr><td>Optional</td><td>Alphanumeric</td><td>0,12</td><td>SINGLE</td></tr>
</table>

Transaction Response Output Fields

There are no special output fields returned in the Transaction Response.

Enhanced Industry Data Fields

Although Enhanced Industry Data functionality was originally designed for the travel industry, this functionality allows the merchant to enter any industry related data to be stored on the Payment Server for that transaction. It includes fields:

- Ticket Number — allows the merchant to submit airline ticket number in the Transaction Request, including Capture transactions. The previous ticket number is overwritten when a new ticket number is submitted. The Payment Server does not maintain an audit record of these changes. You can view the latest ticket number in the search results of a Transaction Search using the Merchant Administration portal on the Payment Server.

- Addendum Data — allows the merchant to include industry specific data in the Transaction Request. The data can include passenger names, ticket numbers, hotel bookings, etc. The addendum data is stored in the database, which may be used in creating reports external to the Payment Server.

Both Ticket Number and Addendum Data are passed with the Transaction Request and stored on the Payment Server. The ticket number is passed to the financial institution as part of certain transactions.

Note: Applies to 2-Party and 3-Party transactions.

Transaction Request Input Fields

Enhanced Industry Data Fields			
The data is sent by including the additional data with the required fields for a basic transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_TicketNo			
The airline ticket number that is passed with the Transaction Request and stored on the Payment Server.			
Optional	Alphanumeric	0,15	A234567F

<table>
<tr><th colspan="4">vpc_AddendumData</th></tr>
<tr><td colspan="4">Extra information about the industry, for example, passenger names, ticket numbers, hotel bookings, etc., that is passed with the Transaction Request and stored on the Payment Server.
<b>Prerequisite:</b> You must enable the privilege <b>May Include Addendum Data</b> to pass Addendum data in the Transaction Request.
<b>Note</b>: Though vpc_AddendumData supports 2048 characters, ensure that the Transaction Request does not exceed 2048 characters due to browser redirect limitations in 3-party transactions.</td></tr>
<tr><td>Optional</td><td>Alphanumeric Special</td><td>0, 2048</td><td>Scott Adam, VIP Client, Acme Hotel.</td></tr>
</table>

Transaction Response Output Fields

There are no special output fields returned in the Transaction Response.

Referral Message Fields

This response message occurs when the Acquirer needs to manually authorise the cardholder (by having the merchant contact them) as indicated by a **vpc_TxnResponseCode** '**E**'. See Transaction Response Codes.

The Authorisation code the merchant is given on contacting the Payment Provider is input using a '**Referral Transaction** (see "Referral Processing Transaction Fields" on page 32)'.

Note: Applies to 2-Party and 3-Party transactions.

Transaction Request Input Fields

There are no supplementary input fields in the Transaction Request.

Transaction Response Output Fields

Card Present Output Fields			
In addition to the standard output fields, the following optional field is also returned in the Transaction Response for both 2-Party and 3-Party transactions.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_AcquirerResponseAdvice			
Referral Message: This field is only present if vpc_TxnResponseCode is '**E**'. See ***Response Codes*** (see "Returned Response Codes" on page **Error! Bookmark not defined.**). This field is the referral message from the issuer. It may contain contact details to allow the merchant to contact the issuer directly to seek authorisation for the transaction. If Authorised the card company will provide a Manual Auth ID code that is input into the payment system using a '**Referral Transaction**'.			
Output	Alphanumeric	0,70	Please call John Doe at BankXYZ on 18004159896

Referral Processing Transaction Fields

Referral processing allows you to resubmit a referred initial transaction (Authorisation or Purchase transaction that received a "Refer to Issuer" acquirer response) as a new Authorisation or Purchase transaction with an authorisation code obtained from the issuer.

The cardholder may be required to provide additional information in order for the issuer to approve the transaction and provide an authorisation code/Manual Auth ID.

A fully qualified URL (https://migs.mastercard.com.au/vpcdps) must be included in the merchant's application code to send transaction information to the Virtual Payment Client.

Note: Applies to 2-party transactions.

Transaction Request Input Fields

Referral Processing Input Fields			
The following data fields must be included in a Transaction Request when performing a Referral transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_Version			
The version of the Virtual Payment Client API being used. The current version is 1.			
Required	Alphanumeric	1,8	1
vpc_Command			
Indicates the transaction type. This must be equal to '**doRequest**' for this type of transaction.			
Required	Alphanumeric	1,16	doRequest
vpc_RequestType			
This field is associated when the **vpc_Command** field equals '**doRequest**'. This must be equal to '**PAYMENT**' for this type of transaction.			
Required	Alphanumeric	1,20	PAYMENT
vpc_RequestCommand			
This field is associated when the **vpc_Command** field equals '**doRequest**'. Applicable values can be obtained from your Payment Services Provider. The value must be equal to '**doAuthorisedTransaction**' for this type of transaction.			
Required	Alphanumeric	1,25	doAuthorisedTransaction

vpc_AccessCode			
Authenticates the merchant on the Payment Server. This means that a merchant cannot access another merchant's Merchant Id. The access code is provided when the merchant profile is registered with a Payment Provider.			
Required	Alphanumeric	8	6AQ89F3
vpc_MerchTxnRef			
A unique value created by the merchant. **Usage Notes:** The Merchant Transaction Reference is used as a reference key to the Payment Server database to obtain a copy of lost/missing receipts using the QueryDR function. It can also be used to identify a duplicate transaction if it is always kept unique for each transaction attempt. It can contain similar information to the vpc_OrderInfo field, but it must be unique for each transaction attempt if it is to be used properly. Typically, the vpc_MerchTxnRef is based on an order number, invoice number, timestamp, etc., but it should also reflect the transaction attempt. For example, if a cardholder has insufficient funds on their card and they are allowed to repeat the transaction with another credit card, the value may be INV1234/1 on the first attempt, INV1234/2 on the second attempt, and INV1234/3 on the third attempt. This identifier will be displayed in the Transaction Search results and also in the Download file (from Financial Transactions Search or Download Search Results link in Financial Transaction List) in the Merchant Administration portal on the Payment Server.			
Required	Alphanumeric	1,40	ORDER958743-1
vpc_Merchant			
The unique Merchant Id assigned to a merchant by the Payment Provider. The Merchant ID identifies the merchant account against which settlements will be made.			
Required	Alphanumeric	1,16	TESTMERCHANT01
vpc_TransNo			
The unique Payment Server OrderID (Shopping Transaction) number of the existing order that has the referred transaction against it.			
Required	Numeric	1,19	10712
vpc_ManualAuthID			
An alphanumeric code of up to six characters used to specify the manual authorisation code supplied by the card issuer for the transaction.			
Optional	Alphanumeric	0,6	AB3456

Transaction Response Output Fields

There are no special output fields returned in the Transaction Response.

Risk Management Fields

Risk Management is a module used for Card-Not-Present (CNP) transactions, which enables MSOs and merchants to set a range of business risk screening rules. These risk rules are configured to screen transactions of perceived high/low risk thereby enabling merchants to accept, reject, or mark transactions for review based on their risk assessment. For more information on the MSO and merchant rules, see Virtual Payment Client Integration Guide.

This feature is available for both 2-party and 3-party transactions. Though risk rules can be configured only through the Merchant Administration or Merchant Manager portal, transactions processed through the Virtual Payment Client will be screened based upon the configured rules, and the overall result for each authorisation and purchase will be returned in the Transaction Response. However, merchants using the Virtual Payment Client will not be able to make a review decision on the order — orders can be reviewed for processing or cancellation only through the Merchant Administration portal. You can view the overall risk result details in the search results of an Order Search using the Merchant Administration or Merchant Manager portal on the Payment Server.

Note: Risk Management is applicable only to:

- Merchants who have **May Use Risk Management** privilege enabled.
- Transaction modes, **Auth Then Capture** and **Purchase.** Standalone Captures, Standalone Refunds, etc., will not be assessed for risk.

The Risk Management feature includes the following fields:

- Bypass Risk Management — allows the merchant to process orders without performing risk checks and assessment of orders. The Bypass Risk Management field is passed with the Transaction Request and stored by the Payment Server. This field is applicable only to merchants who have been assigned **May Bypass Risk Management** privilege.

Note: You cannot bypass MSO level risk rules.

- IP Address — allows the merchant to include the IP address of the source of the transaction in the Transaction Request — IP addresses are useful in identifying the location of the cardholder. The IP Address field is passed with the Transaction Request and stored by the Payment Server.
- Overall Risk Result — indicates the overall result of risk assessment for every authorisation or purchase, which is returned in the Transaction Response.
- Transaction Reversal Result — indicates the result of order reversal for each authorisation or purchase that occurred due to risk assessment.

Note: Applies to 2-Party and 3-Party transactions.

Transaction Request Input Fields

<table>
<tr><td colspan="4"><b>Risk Management Input Fields</b></td></tr>
<tr><td colspan="4">The data is sent by including the additional data with the required fields for a basic transaction.</td></tr>
<tr><td colspan="4"><b>Field Name</b></td></tr>
<tr><td colspan="4"><b>Field Description</b></td></tr>
<tr><td>Required/ Optional</td><td>Field Type</td><td>Min, Max or Set Field Length</td><td>Sample Data</td></tr>
</table>

<table>
<tr><td colspan="4"><b>vpc_RiskBypass</b></td></tr>
<tr><td colspan="4">Specifies whether the merchant wants to bypass risk checks and assessments for an order.
Valid values for this field are:
Y - indicates that the merchant wants to bypass risk checks.
N - indicates that the merchant wants to perform risk checks and assessment on orders. This is the default value.</td></tr>
<tr><td>Optional</td><td>Alphanumeric</td><td>1</td><td>Y</td></tr>
<tr><td colspan="4"><b>vpc_IPAddress</b></td></tr>
<tr><td colspan="4">The IP address of the source of the transaction.
<b>Note:</b> Applies only to 2-party transactions.</td></tr>
<tr><td>Optional</td><td>Alphanumeric Special</td><td>15</td><td>172.17.78.1</td></tr>
</table>

Transaction Response Output Fields

<table>
<tr><td colspan="4"><b>Risk Management Output Fields</b></td></tr>
<tr><td colspan="4">In addition to the standard output fields, the following fields are also returned in the Transaction Response for both 2-Party and 3-Party transactions.</td></tr>
<tr><td colspan="4"><b>Field Name</b></td></tr>
<tr><td colspan="4">Field Description</td></tr>
<tr><td>Returned Input or Output</td><td>Field Type</td><td>Min, Max or Set Field Length</td><td>Sample Data</td></tr>
</table>

vpc_RiskOverallResult			
The overall result of risk assessment for each authorisation or purchase. Valid values for this field are: ACC (Accept) — indicates that the order has been processed. REJ (Reject) — indicates that the order is rejected. REV (Review) — indicates that the order is marked for review. NCK (Not Checked) — indicates that the order is processed using the **Bypass Risk Management** option. It also implies a condition where neither MSO nor merchant risk rules are configured in the system. SRJ (System Reject) — indicates that the order is rejected at the system (MSO) level.			
Output	Alphanumeric	3	ACC
vpc_TxnReversalResult			
The result of order reversal for each authorisation or purchase that occurred due to risk assessment. Orders rejected after the financial transaction due to risk assessment are automatically reversed by the system. Valid values for this field are: OK — indicates that the order was reversed successfully. FAIL — indicates that the attempt to reverse the order failed. NA (Not Supported) — indicates that the acquirer does not support reversal of the required transaction so the reversal failed.			
Output	Alphanumeric	4	OK

Bank Account Type Field

The Bank Account Type card field is applicable to card types such as Maestro. The Bank Account Type functionality allows the merchant to enter the type of account, Savings or Cheque, to be stored on the Payment Server for that transaction. Bank Account Type is passed with the Transaction Request and stored on the Payment Server.

Note: Applies to 2-Party transactions and 3-Party with card details transactions.

Transaction Request Input Fields

Bank Account Type Field			
The data is sent by including the additional data with the required fields for a basic transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

<table>
<tr><td colspan="4"><b>vpc_BankAccountType</b></td></tr>
<tr><td colspan="4">The type of bank account the cardholder wants to use for the transaction. For example, Savings or Cheque.
Valid values for this field are:
CHQ - specifies that the cardholder wants to use the Cheque account linked to the card.
SAV - specifies that the cardholder wants to use the Savings account linked to the card.
<b>Usage Notes:</b> This identifier is mandatory if the card type is Maestro and will be displayed in the Order Search results in the Merchant Administration portal on the Payment Server.</td></tr>
<tr><td>Optional</td><td>Alphanumeric</td><td>3</td><td>SAV</td></tr>
</table>

Transaction Response Output Fields

There are no special output fields returned in the Transaction Response.

Cash Advance

Adding the CashAdvance field to a normal card present purchase mode transaction causes a cash advance transaction of the specified amount to be performed. It is only valid to submit the CashAdvance Transaction Request field when the Merchant Transaction Source field (vpc_TxSource) has a value of CARDPRESENT.

Transaction Request Input Fields

<table>
<tr><td colspan="4"><b>AMA Cash Advance Input Fields</b></td></tr>
<tr><td colspan="4">The data is sent by including the additional data with the required fields for a basic transaction.</td></tr>
<tr><td colspan="4"><b>Field Name</b></td></tr>
<tr><td colspan="4"><b>Field Description</b></td></tr>
<tr><td>Required/ Optional</td><td>Field Type</td><td>Min, Max or Set Field Length</td><td>Sample Data</td></tr>
</table>

<table>
<tr><td colspan="4"><b>vpc_CashAdvance</b></td></tr>
<tr><td colspan="4">Adding this field to a card present purchase mode transaction causes the transaction to be submitted as a cash advance transaction to the value specified in the Amount field.
Valid values are:
▪ <b>Y, Yes, True, 1</b> – all of the above indicate that a purchase mode transaction is to be put through as a cash advance.
▪ <b>Any other value</b> – Ignore this field. The purchase mode transaction is submitted as a normal purchase transaction.</td></tr>
<tr><td>Required</td><td>Alphanumeric</td><td>1,4</td><td>Yes</td></tr>
</table>

Transaction Response Output Fields

There are no special output fields returned in the Transaction Response.

Note: If using this field you must also use the Card Present Fields as well as the required DO Fields on page 7.

Payment Authentication

Payment Authentications are designed to reduce credit card fraud by authenticating cardholders when performing transactions over the Internet by using the 3-Domain Secure™ (3-D Secure or 3DS) protocol developed by Visa.

A 3-D Secure transaction is performed immediately before a merchant performs a payment transaction, that is, an Authorisation transaction in the Auth/Capture mode, or a Purchase transaction in the Purchase mode. Authentication ensures that the card is being used by its legitimate owner.

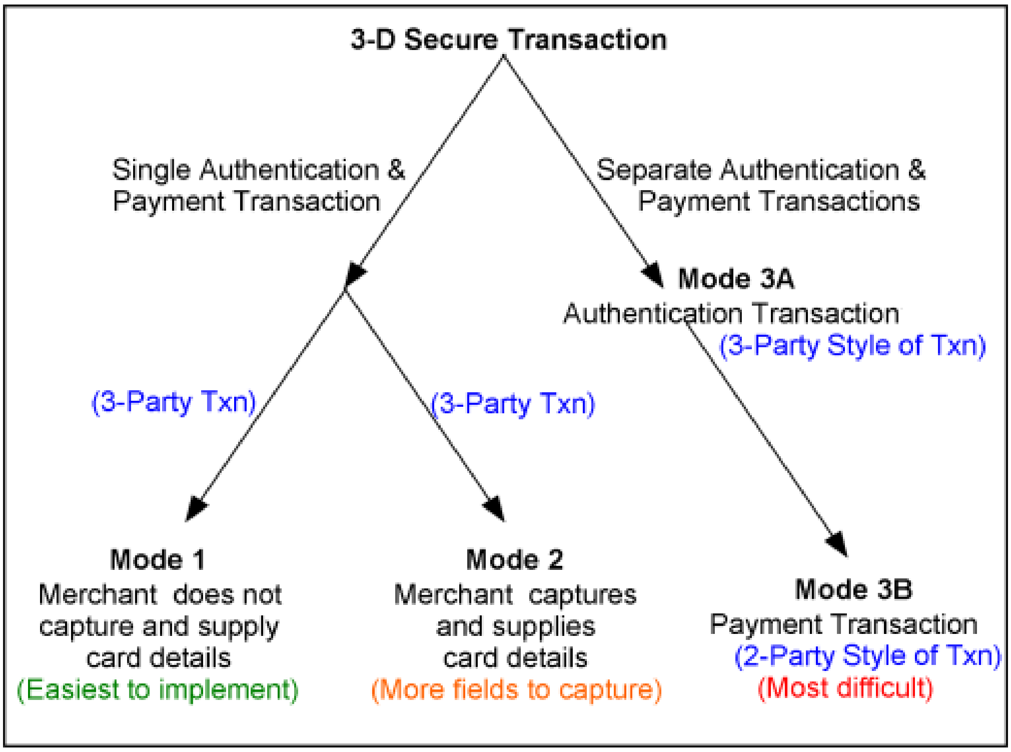
During a transaction, 3DS authentication allows the merchant to authenticate the cardholder by redirecting them to their card issuer where they enter a previously registered password.

Merchants using 3DS can be configured to block any transaction that fails 3DS authentication. A transaction is considered to fail 3DS authentication if it results in a Verification Security Level of '07'. A blocked transaction results in a Dialect Response Code of 'B', which is included in the DR and displayed in the Financial Transaction Details page.

Note: For 3DS Authentication to take place, the cardholder's browser has to be redirected to their card issuing bank where they enter their secret password. This is performed by the Payment Server if the cardholder is enrolled in the 3DS schemes of Verified by Visa™, MasterCard® SecureCode™ or JCB J/Secure™.

Payment Authentication 3-D Secure transaction modes

The following diagram shows an overview of the Payment Authentication 3-D Secure transaction modes.


3-D Secure Transaction
Single Authentication & Payment Transaction
Separate Authentication & Payment Transactions
Mode 3A
Authentication Transaction
(3-Party Style of Txn)
(3-Party Txn)
(3-Party Txn)
Mode 1
Merchant does not capture and supply card details
(Easiest to implement)
Mode 2
Merchant captures and supplies card details
(More fields to capture)
Mode 3B
Payment Transaction
(2-Party Style of Txn)
(Most difficult)

The available 3-D Secure transaction modes are:

1 **Mode 1 - Combined 3-Party Authentication and Payment transaction** - The merchant uses the Payment Server to perform the authentication and payment in the one transaction.

The **Payment Server collects the cardholder's card details** and not the merchant's application. The Payment Server redirects the cardholder to the card issuing institution to enter their 3-D Secure password. If the Authentication is performed correctly the Payment Server uses the Authentication information to perform the payment transaction.

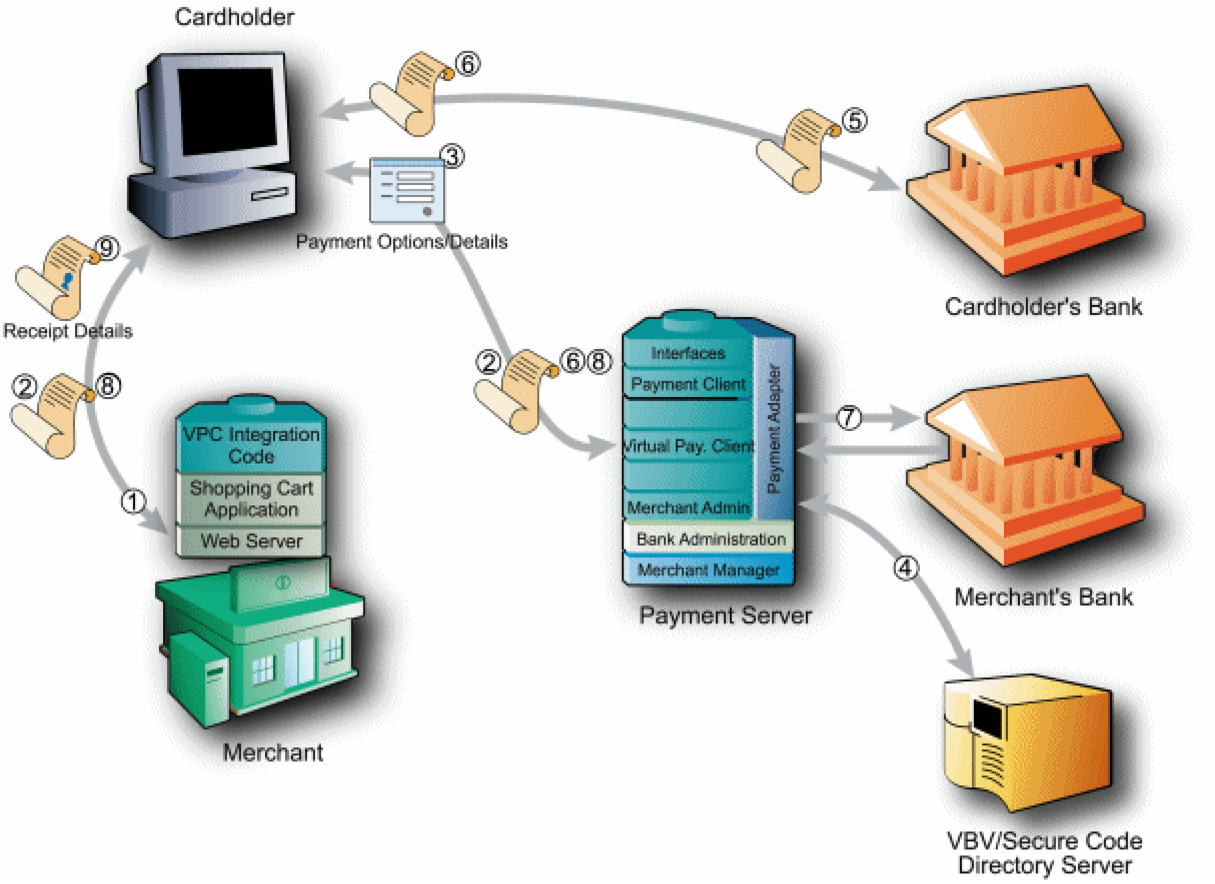
2 **Mode 2 - Combined 3-Party Authentication and Payment transaction, (merchant collects card details)** - The merchant uses the Payment Server to perform the authentication and payment in the one transaction.

The **merchant's application collects the cardholder's card details** and sends them to the Payment Server, which redirects the cardholder to the card issuing institution to enter their 3-D Secure password. If the Authentication is performed correctly the Payment Server uses the Authentication information to perform the payment transaction.

3 **Mode 3a - 3-Party - Authentication Only transaction** - The merchant uses the Payment Server to perform an authentication transaction and the payment transaction is processed as a separate transaction. This gives the merchant complete control as to when and if a payment transaction should proceed. The Authentication operation outputs become the inputs for a '3-Party with card details' transaction. The merchant needs to collect card details.

Mode 3b - 2-Party Style Pre-Authenticated Payment transaction - The merchant may use the 3-Party - Authentication only transaction through the Payment Server or an external authentication provider to perform the 3-D Secure Authentication, and use the outputs from this operation to perform a 2-Party payment transaction through the Payment Server. The merchant needs to collect card details.

Information Flow of a 3-D Secure Authentication/Payment transaction



If you have been enabled to use Verified by Visa, MasterCard SecureCode or JCB J/Secure, the information flow where the Payment Server collects the card details (Mode1) is as follows:

1 A cardholder browses the application, selects a product and enters their shipping details into the merchant's application at the checkout page.

2 The cardholder clicks a pay button and your application sends the payment Transaction Request to the Payment Server by redirecting the cardholder's Internet browser to the Payment Server.

3 The Payment Server prompts the cardholder for the card details.

4 If the card is a Visa, MasterCard or JCB card, the Payment Server then checks with the Directory Server to determine if the card is enrolled in either the Verified by Visa^{TM} (Visa 3-Domain Secure), MasterCard$^{®}$ SecureCode^{TM} (MasterCard 3-Domain Secure) or JCB J/Secure^{TM} (JCB 3-Domain Secure) scheme.

If the card is not enrolled in a payment authentication scheme then go to Step 7.

5 If the cardholder's card is registered in the payment authentication scheme, the Payment Server redirects the cardholder's browser to the card issuer's site for authentication. The card issuer's server displays the cardholder's secret message and the cardholder enters their secret password, which is checked against the Issuing bank's database.

6 At the completion of the authentication stage, the cardholder is redirected back to the Payment Server indicating whether or not the cardholder's password matched the password in the database.

If the cardholder was not authenticated correctly, then the payment does not take place and the cardholder is redirected back to the merchant's site with a Transaction Response containing details to indicate the authentication failed – see step 8.

7 If the cardholder was authenticated correctly, or Payment Authentication did not occur the Payment Server continues with processing the transaction with the results of the authentication attempt.

8 The Payment Server then redirects the cardholder back to merchant's site with the Transaction Response. The Transaction Response contains the result of the transaction.

9 The application processes the Transaction Response and displays the receipt.

Note: If the cardholder is enrolled in the 3-D Secure scheme but is not authenticated correctly, for example, because the cardholder may have entered their password incorrectly 3 times, then the merchant's application is sent a **vpc_TxnResponseCode** code of '**F**' to indicate the cardholder failed the authentication process and the transaction does not proceed.

Mode 2 and Mode 3a are slight variations on the above information flow. In mode 2 and mode 3a the merchant collects the card details and passes them through, which means step 3 is eliminated.

For Mode 3a step 7 is also eliminated, the payment being performed through a separate 2-Party transaction after the Authentication.

Advantages and Disadvantages of the 3-D Secure modes of transaction

Table 13 Advantages and Disadvantages of the 3-D Secure modes of transaction

Mode	Advantages	Disadvantages
Mode 1 3 Party Authentication and Payment transaction mode	• Simple to implement. • The Payment Provider collects the cardholder's card details and not the merchant, which provides highest level of security for the cardholder's card details.	• The merchant is not able to use their own branding throughout the whole transaction, as the Payment Provider displays their own branding while the card details are being captured. • If the cardholder is not enrolled in 3-D Secure, or the authentication could not be performed, the authentication will not take place and the transaction will automatically move into the payment stage.
Mode 2 3 Party Authentication and Payment transaction (merchant collects card details)	• Suits a merchant that normally collects all the card details. • Branding of the payment pages on the website remains consistent throughout the whole transaction, except the screen where the cardholder enters their password for 3-D Secure.	• If the cardholder is not enrolled in 3-D Secure the authentication will not take place and the transaction will automatically move into the payment stage.
Mode 3a 3 Party Authentication Only transaction mode	• Suits a merchant that normally collects all the card details. • Branding of the payment pages on the website remains consistent throughout the whole transaction, except the screen where the cardholder enters their password for 3-D Secure.	• It consists of two separate transactions, the Authentication and the Payment, which can be more difficult for a merchant to integrate.
Mode 3b 2 Party Pre-authenticated transaction mode	• Gives the merchant maximum control of the transaction. If the cardholder is not enrolled in 3-D Secure, then the merchant's application can stop the transaction from progressing to the Payment stage providing full control over the transaction risk. • Branding remains consistent throughout the whole transaction, except for the one screen where the cardholder enters their 3-D Secure password.	• Can only be performed if the merchant collects all the card details. • It consists of two separate transactions, the Authentication and the Payment, which can be more difficult for a merchant to integrate.

Mode 1 - 3-Party Authentication & Payment Transaction:
(Payment Server collects card details)

The 3-Party Authentication and Payment transaction mode uses the basic 3-Party style of transaction.

Mode 1 Transaction Request Input Fields

There are no additional input fields in the Transaction Request to add 3-D Secure authentication to a standard 3-Party transaction.

Mode 1 Transaction Response Outputs

The outputs from this transaction type are the same as ***Mode 2 type transactions*** (see next).

Mode 2 - 3-Party Authentication & Payment Txn:
(Merchant collects card details)

If you want to keep branding consistent throughout the transaction you can pass in extra fields to a 3-Party transaction, but you do need your Payment Provider to enable you to use card details in the Transaction Request. These fields are outlined below.

Mode 2 Transaction Request Input Fields

Table 14 Mode 2 Transaction Request Input Fields

Card Details in Transaction Request Fields			
The data is sent by including the additional data with the required fields for a basic transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_card			
Used in External Payment Selection to determine what type of card is used. The field is case sensitive, and must comply with each of the card types valid in the Payment Server. This varies from Payment Server to Payment Server. The possible values are shown in *External Payment Selection (EPS)* on page 91). To check the card types available for your Payment Provider, perform a 3-Party transaction and go to the Payment Server card selection page in a browser. Run the cursor over each card logo. The 'card' and 'gateway' values are displayed at the bottom of the browser window.			
Required	Alphanumeric	3,16	Visa

vpc_gateway			
Determines the type of payment gateway functionality. The field is case sensitive, and must comply with the gateways that are valid in the Payment Server. Valid values for this field are: • **ssl** - specifies the gateway for all standard 3-Party transactions • **threeDSecure** -specifies the gateway for a 3-D Secure Mode 3a-3-Party Style Authentication Only transaction. **Note:** For most transactions the value of this field will be '**ssl**'.			
Required	Alphanumeric	3,15	ssl
vpc_CardNum			
The number of the card used for the transaction. The format of the Card Number is based on the Electronic Commerce Modeling Language (ECML) and, in particular, must not contain white space or formatting characters.			
Required	Numeric	15,19	5123456789012346
vpc_CardExp			
The expiry date of the card in the format YYMM. The value must be expressed as a 4-digit number (integer) with no white space or formatting characters. For example, an expiry date of May 2013 is represented as 1305.			
Required	Numeric	4	1305
vpc_CardSecurityCode			
The Card Security Code (CSC), also known as CVV (Visa), CVC2 (MasterCard), CID/4DBC (Amex), or CVV2, which is printed, not embossed, on the card. It compares the code with the records held in the card issuing institution's database.			
Optional	Numeric	3,4	985
vpc_Desc			
An optional field that the merchant may supply in the Transaction Request as a description of the transaction. This description will be displayed on the Verified by Visa^{TM} page where the cardholder types in their secret password. **Note:** This is only used for Verified by Visa^{TM} transactions and cannot be used for MasterCard SecureCode^{TM} as this field is not displayed. **Note:** The field can only be used if the merchant collects the card details and passes them in. If the Payment Server is used to collect the card details, the merchant cannot use the Desc field.			
Optional	Alphanumeric	0,125	This is a description about the Verified by Visa^{TM} transaction.

Mode 2 Transaction Response Output Fields

These fields are only returned in the Transaction Response if the transaction is a Verified by Visa, MasterCard SecureCode or JCB J/Secure payment authentication. Other cards like Diners Club will not return these additional fields. You must also be enabled on the Payment Server by your Payment Provider to perform Verified by Visa, MasterCard SecureCode and JCB J/Secure payment authentications.

The **vpc_TxnResponseCode** can be used to determine if the authentication passed or failed. If the **vpc_TxnResponseCode** is equal to '**F**', the Authentication process failed and no payment took place. If the **vpc_TxnResponseCode** is not equal to '**F**', the payment authentication process was attempted and the payment process takes place.

If a payment authentication has been successful, extra fields are returned in the Transaction Response for a Verified by Visa, MasterCard SecureCode and JCB J/Secure payment authentication. These fields are not used by you but are returned to allow you to store them as a record of authentication for the transaction, which can be used to resolve disputes. They cannot be used again for any future transactions.

All payment authentication transactions use a **vpc_VerStatus** response code value to show whether the card authentication was successful or not. For details of this code, see ***3-D Secure Status Codes*** in *Verified by Visa™, MasterCard® SecureCode™ and JCB* J/Secure™ Status *Codes*, on page 92.

Table 15 Mode 2 Transaction Response Output Fields

Mode 2 Payment Authentication Output Fields			
In addition to the standard output fields, the following fields are also returned in the Transaction Response for this 3-Party transaction.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_3DSECI			
The 3-D Secure Electronic Commerce Indicator, which is set to '05' when the cardholder authenticates OK, and '06' when the cardholder is not enrolled. (These values may change depending on the locale or issuer).			
Output	Numeric	0,2	06
vpc_3DSXID			
It is a unique transaction identifier that is generated by the Payment Server on behalf of the merchant to identify the 3DS transaction. It is a 20-byte field that is Base64 encoded to produce a 28-character value.			
Output	Alphanumeric	0,28	uyPfGIgsoFQhklkIsto+IFWs92s=

vpc_3DSenrolled			
This field indicates if the card is within an enrolled range. This is the value of the VERes.enrolled field. It will take values (**Y** - Yes, **N** - No, **U** - Unavailable for Checking).			
Output	Alpha	1	N
vpc_3DSstatus			
This field is only included if payment authentication was attempted and a PARes was received by the MPI. It will take values (**Y** - Yes, **N** - No, **A** - Attempted Authentication, **U** - Unavailable for Checking).			
Output	Alpha	0,1	N
vpc_VerToken			
This value is generated by the card issuer as a token to prove that the cardholder authenticated OK. This is a base64 encoded value.			
Output	Alphanumeric	28	gIGCg4SFhoeIiYqLjI2Oj5CRkpM=
vpc_VerType			
This field will either be '**3DS**' 3-D Secure incorporating Verified by Visa, MasterCard SecureCode and JCB J/Secure, or '**SPA**' - Secure Payment Authentication from MasterCard (rarely used).			
Output	Alphanumeric	0,3	3DS
vpc_VerSecurityLevel			
The Verification Security Level is generated at the card issuer as a token to prove that the cardholder was enrolled and authenticated OK. It is shown for all transactions except those with authentication status "Failure". This field contains the security level to be used in the AUTH message. MasterCard '**0**' - Merchant not participating (a merchant will not see this if they are configured for MasterCard SecureCode). MasterCard '**1**' - Cardholder not participating MasterCard '**2**' - Cardholder authenticated. Visa '**05**' - Fully Authenticated. Visa '**06**' - Not authenticated, (cardholder not participating). Visa '**07**' - Not authenticated. Usually due to a system problem, for example the merchant password is invalid.			
Output	Numeric	0,2	06
vpc_VerStatus			
The status codes used by the Payment Server to show whether the payment authentication was successful or not (see *Verified by Visa™, MasterCard® SecureCode™ and JCB* J/Secure™ Status *Codes* on page 92).			
Output	Alphanumeric	1	N

Mode 3a - 3Party Style Authentication Only Transaction: (Merchant collects card details)

In certain cases a merchant may want to perform an Authentication of the cardholder separately to a payment transaction. This could because the merchant only wants to take a payment from cardholders that are both:

1. Enrolled in Verified by Visa, MasterCard SecureCode or JCB J/Secure

and

2. Correctly Authenticated

In a normal operation, if the cardholder is not enrolled in Verified by Visa, MasterCard SecureCode or JCB J/Secure, the payment still goes ahead. In Mode 3a if the cardholder is not enrolled they are returned to the merchant site before the payment goes ahead.

The following fields are added to a standard 3-Party transaction to perform an Authentication Only transaction. **No payment is carried out with this transaction.** The merchant must have the EPS privilege, and cardholders enrolled. The merchant must be set up to provide the card details on the Transaction Request.

To perform a payment, the outputs from this transaction are fed as additional inputs to a standard 2-Party transaction.

Mode 3a Payment Authentication Only Input Fields

Table 16 Mode 3a Payment Authentication Only Input Fields

Payment Authentication Only Fields			
The data is sent by including the additional data with the required fields for a basic transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_card			
Used in External Payment Selection to determine what type of card is used. The field is case sensitive, and must comply with each of the card types valid in the Payment Server. This varies from Payment Server to Payment Server. The possible values are shown in *External Payment Selection (EPS)* on page 91. To check the card types available for your Payment Provider, perform a 3-Party transaction and go to the Payment Server card selection page in a browser. Run the cursor over each card logo. The 'card' and 'gateway' values are displayed at the bottom of the browser window.			
Required	Alphanumeric	3,16	Visa
vpc_gateway			
Determines the type of payment gateway functionality. The field is case sensitive, and must comply with the gateways that are valid in the Payment Server. Valid values are shown in Appendix B. For an Authentication Only transaction the field value must be '**threeDSecure**'			
Required	Alphanumeric	3,15	threeDSecure

vpc_CardNum			
The number of the card used for the transaction. The format of the Card Number is based on the Electronic Commerce Modeling Language (ECML) and, in particular, must not contain white space or formatting characters.			
Required	Numeric	15,19	5123456789012346
vpc_CardExp			
The expiry date of the card in the format YYMM. The value must be expressed as a 4-digit number (integer) with no white space or formatting characters. For example, an expiry date of May 2013 is represented as 1305.			
Required	Numeric	4	1305
vpc_Desc			
An optional field that the merchant may supply in the Transaction Request as a description of the transaction. This description will be displayed on the Verified by Visa page where the cardholder types in their secret password.			
Note: This is only used for Verified by Visa transactions and cannot be used for MasterCard SecureCode as this field is not displayed.			
The field can only be used if the merchant collects the card details and passes them in. If the Payment Server is used to collect the card details, the merchant cannot use the vpc_Desc field.			
Optional	Alphanumeric	0,125	This is a description about the Verified by Visa transaction.

Mode 3a Payment Authentication Only Output Fields

These fields are only returned in the Transaction Response if the transaction is a Verified by Visa, MasterCard SecureCode or JCB J/Secure payment authentication. You must be enabled on the Payment Server by your Payment Provider to perform these 3DS payment authentications.

The **vpc_TxnResponseCode** is used to determine if the authentication passed or failed.

If the **vpc_TxnResponseCode** is not equal to '**F**', the payment authentication passed OK and the Authentication process has completed satisfactorily.

If the **vpc_TxnResponseCode** is equal to '**F**', the Authentication process failed and no payment will take place.

If a payment authentication has been successful, extra fields are returned in the Transaction Response for a Verified by Visa, MasterCard SecureCode or JCB J/Secure payment authentication. The fields are returned to be included in the mode 3b pre-authentication payment transaction. They cannot be used again for any future transactions.

All payment authentication transactions use a **vpc_VerStatus** response code value to show whether the card authentication was successful or not. For details of this code, please see ***3-D Secure Status Codes*** (see *Verified by Visa™, MasterCard® SecureCode™ and JCB J/Secure™ Status Codes* on page 92).

<table>
<tr><td colspan="4"><b>Payment Authentication Output Fields</b></td></tr>
<tr><td colspan="4">In addition to the standard output fields, the following fields are also returned in the Transaction Response for both 2-Party and 3-Party transactions.</td></tr>
<tr><td colspan="4"><b>Field Name</b></td></tr>
<tr><td colspan="4">Field Description</td></tr>
<tr><td>Returned Input or Output</td><td>Field Type</td><td>Min, Max or Set Field Length</td><td>Sample Data</td></tr>
</table>

<table>
<tr><td colspan="4"><b>vpc_3DSECI</b></td></tr>
<tr><td colspan="4">The 3-D Secure Electronic Commerce Indicator, which is set to '05' when the cardholder authenticates OK, and '06' when the cardholder is not enrolled. (These values may change depending on the locale or issuer).</td></tr>
<tr><td>Output</td><td>Numeric</td><td>0,2</td><td>06</td></tr>
<tr><td colspan="4"><b>vpc_3DSXID</b></td></tr>
<tr><td colspan="4">It is a unique transaction identifier that is generated by the Payment Server on behalf of the merchant to identify the 3DS transaction. It is a 20-byte field that is Base64 encoded to produce a 28-character value.</td></tr>
<tr><td>Output</td><td>Alphanumeric</td><td>0,28</td><td>uyPfGIgsoFQhklkIsto+IFWs92s=</td></tr>
<tr><td colspan="4"><b>vpc_3DSenrolled</b></td></tr>
<tr><td colspan="4">This field indicates if the card is within an enrolled range. This is the value of the VERes.enrolled field. It will take values (<b>Y</b> - Yes, <b>N</b> - No, <b>U</b> - Unavailable for Checking).</td></tr>
<tr><td>Conditional</td><td>Alpha</td><td>1</td><td>N</td></tr>
<tr><td colspan="4"><b>vpc_3DSstatus</b></td></tr>
<tr><td colspan="4">This field is only included if payment authentication was attempted and a PARes was received by the MPI. It will take values (<b>Y</b> - Yes, <b>N</b> - No, <b>A</b> - Attempted Authentication, <b>U</b> - Unavailable for Checking).</td></tr>
<tr><td>Conditional</td><td>Alpha</td><td>0,1</td><td>N</td></tr>
<tr><td colspan="4"><b>vpc_VerToken</b></td></tr>
<tr><td colspan="4">This value is generated by the card issuer as a token to prove that the cardholder authenticated OK. This is a base64 encoded value.</td></tr>
<tr><td>Output</td><td>Alphanumeric</td><td>28</td><td>gIGCg4SFhoeIiYqLjI2Oj5CRkpM=</td></tr>
<tr><td colspan="4"><b>vpc_VerType</b></td></tr>
<tr><td colspan="4">This field will either be ‘3DS’ 3-D Secure incorporating Verified by Visa, MasterCard SecureCode and JCB J/Secure, or '<b>SPA</b>' - Secure Payment Authentication from MasterCard (rarely used).</td></tr>
<tr><td>Output</td><td>Alphanumeric</td><td>0,3</td><td>3DS</td></tr>
<tr><td colspan="4"><b>vpc_VerStatus</b></td></tr>
<tr><td colspan="4">The status codes used by the Payment Server to show whether the payment authentication was successful or not (see <i>Verified by Visa™, MasterCard® SecureCode™ and JCB</i> J/Secure™ Status <i>Codes</i> on page 92).</td></tr>
<tr><td>Output</td><td>Alphanumeric</td><td>1</td><td>N</td></tr>
</table>

<table>
<tr><td colspan="4"><b>vpc_VerSecurityLevel</b></td></tr>
<tr><td colspan="4">The Verification Security Level is generated at the card issuer as a token to prove that the cardholder was enrolled and authenticated OK. It is shown for all transactions except those with authentication status “Failure”. This field contains the security level to be used in the AUTH message.
MasterCard '<b>0</b>' – Merchant not participating (a merchant will not see this if they are configured for MasterCard SecureCode).
MasterCard '<b>1</b>' – Cardholder not participating.
MasterCard '<b>2</b>' – Cardholder authenticated.
Visa '<b>05</b>' – Fully Authenticated.
Visa '<b>06</b>' – Not authenticated, (cardholder not participating).
Visa '<b>07</b>' – Not authenticated. Usually due to a system problem, for example the merchant password is invalid.</td></tr>
<tr><td>Output</td><td>Numeric</td><td>0,2</td><td>06</td></tr>
</table>

Mode 3b - 2-Party Style Pre-Authenticated Payment

The following additional inputs are added to a standard 2-Party Authorisation or Purchase transaction where the cardholder has already been pre-Authenticated in a Mode 3a operation.

Mode 3b Transaction Request Input Fields

Table 17 Mode 3b Transaction Request Input Fields

<table>
<tr><td colspan="4"><b>Pre Authentication Payment Fields</b></td></tr>
<tr><td colspan="4">The data is sent by including the additional data with the required fields for a basic transaction.</td></tr>
<tr><td colspan="4"><b>Field Name</b></td></tr>
<tr><td colspan="4">Field Description</td></tr>
<tr><td>Required/ Optional</td><td>Field Type</td><td>Min, Max or Set Field Length</td><td>Sample Data</td></tr>
</table>

<table>
<tr><td colspan="4"><b>vpc_VerType</b></td></tr>
<tr><td colspan="4">This field must be a value of '<b>3DS</b>' for the following fields to operate</td></tr>
<tr><td>Required</td><td>Alphanumeric</td><td>3</td><td>3DS</td></tr>
<tr><td colspan="4"><b>vpc_VerToken</b></td></tr>
<tr><td colspan="4">This value is generated by the Access Control Server at the card issuer as a token to prove that the cardholder authenticated OK. This is a base64 encoded value.</td></tr>
<tr><td>Required</td><td>Alphanumeric</td><td>28</td><td>gIGCg4SFhoeIiYqLjI2Oj5CRkpM=</td></tr>
<tr><td colspan="4"><b>vpc_3DSXID</b></td></tr>
<tr><td colspan="4">It is a unique transaction identifier that is generated by the Payment Server on behalf of the merchant to identify the 3DS transaction. It is a 20-byte field that is Base64 encoded to produce a 28-character value.</td></tr>
<tr><td>Required</td><td>Alphanumeric</td><td>28</td><td>HA1r1v2kDghhQw9DMQi/wQacCL8=</td></tr>
</table>

vpc_3DSECI			
It is the 3-D Secure Electronic Commerce Indicator, which is returned from the Issuers ACS. For Verified by Visa and JCB J/Secure, this is '05' where the Issuers ACS has validated the cardholder's password or '06' where an 'Attempts ACS' condition has occurred. For MasterCard SecureCode, if OK the value will be either '01' or '02', and '06' when the cardholder attempts to authenticate. (These values may change depending on the locale or issuer).			
Required	Alphanumeric	2	05
vpc_3DSenrolled			
This field is mandatory if the card is within an enrolled range. This is the value of the VERes.enrolled field. It will take values (**Y** - Yes, **N** - No, **U** - Unavailable for Checking).			
Optional	Alphanumeric	1	Y
vpc_3DSstatus			
This field is only included if 3-D Secure authentication was used and a PARes was received by the MPI. It will take values (**Y** - Yes, **A** - Attempted Authentication, **U** - Unavailable for Checking).			
Optional	Alphanumeric	1	Y

Mode 3b Transaction Response Output Fields

Table 18 Mode 3b Transaction Response Outputs

Payment Authentication Output Fields			
In addition to the standard output fields, the following fields are also returned in the Transaction Response for 2-Party Pre-authenticated transactions.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_3DSECI			
The 3-D Secure Electronic Commerce Indicator, which is set to '05' when the cardholder authenticates OK, and '06' when the cardholder is not enrolled. (These values may change depending on the locale or issuer).			
Output	Numeric	0,2	06
vpc_3DSXID			
It is a unique transaction identifier that is generated by the Payment Server on behalf of the merchant to identify the 3DS transaction. It is a 20-byte field that is Base64 encoded to produce a 28-character value.			
Output	Alphanumeric	0,28	uyPfGIgsoFQhklkIsto+IFWs92s=
vpc_3DSenrolled			
This field indicates if the card is within an enrolled range. This is the value of the VERes.enrolled field. It will take values (**Y** - Yes, **N** - No, **U** - Unavailable for Checking).			
Output	Alpha	1	N

vpc_3DSstatus			
This field is only included if payment authentication was attempted and a PARes was received by the MPI. It will take values (**Y** - Yes, **N** - No, **A** - Attempted Authentication, **U** - Unavailable for Checking).			
Output	Alpha	0,1	N
vpc_VerToken			
This value is generated by the card issuer as a token to prove that the cardholder authenticated OK. This is a base64 encoded value.			
Output	Alphanumeric	28	gIGCg4SFhoeIiYqLjI2Oj5CRkpM=
vpc_VerType			
This field will either be ‘3DS’ 3-D Secure incorporating Verified by Visa, MasterCard SecureCode and JCB J/Secure, or '**SPA**' - Secure Payment Authentication from MasterCard (rarely used).			
Output	Alphanumeric	0,3	3DS
vpc_VerStatus			
The status codes used by the Payment Server to show whether the payment authentication was successful or not (see *Verified by Visa™, MasterCard® SecureCode™ and JCB* J/Secure™ Status *Codes* on page 92).			
Output	Alphanumeric	1	N
vpc_VerSecurityLevel			
The Verification Security Level is generated at the card issuer as a token to prove that the cardholder was enrolled and authenticated OK. It is shown for all transactions except those with authentication status “Failure”. This field contains the security level to be used in the AUTH message. MasterCard '**0**' – Merchant not participating (a merchant will not see this if they are configured for MasterCard SecureCode). MasterCard '**1**' – Cardholder not participating. MasterCard '**2**' – Cardholder authenticated. Visa '**05**' – Fully Authenticated. Visa '**06**' – Not authenticated, (cardholder not participating). Visa '**07**' – Not authenticated. Usually due to a system problem, for example the merchant password is invalid.			
Output	Numeric	0,2	06

4 Advanced Merchant Administration (AMA) Transactions

Advanced Merchant Administration (AMA) is used when the volume of transactions is too great to be economically viable or too difficult to be carried out manually. AMA transactions allow the merchant to incorporate additional features such as refunds, into the merchant system. All of these transactions operate using the 2-Party model.

Capture, Refund, Void Capture, Void Refund and Void Purchase return standard output fields, plus a comma (',') delimited result string containing a host of other data.

Note: Some financial institutions do not support voids.

Merchants and users who need AMA transactions must have a username and password; in addition, they must be set up with the appropriate AMA privileges to perform a particular AMA transaction.

Note: Applies to 2-Party transactions. An AMA user cannot be used for Merchant Administration operations.

Basic Input Fields - AMA Transaction

Data is sent from the merchant application to the Payment Server via the Virtual Payment Client. A basic transaction requires a number of data fields as per the table below.

The fields are sent to a fully qualified URL (https://migs.mastercard.com.au/vpcdps) via a HTTP POST operation. This URL must be included in the merchant's application code to send transaction information to the Virtual Payment Client.

<table>
<tr><td colspan="4"><b>2-Party AMA Input Fields</b></td></tr>
<tr><td colspan="4">The following data fields must be included in a Transaction Request when using a 2-Party AMA transaction.</td></tr>
<tr><td colspan="4"><b>Field Name</b></td></tr>
<tr><td colspan="4"><b>Field Description</b></td></tr>
<tr><td>Required/ Optional</td><td>Field Type</td><td>Min, Max or Set Field Length</td><td>Sample Data</td></tr>
</table>

<table>
<tr><td colspan="4"><b>vpc_Version</b></td></tr>
<tr><td colspan="4">The version of the Virtual Payment Client API being used. The current version is 1.</td></tr>
<tr><td>Required</td><td>Alphanumeric</td><td>1,8</td><td>1</td></tr>
<tr><td colspan="4"><b>vpc_AccessCode</b></td></tr>
<tr><td colspan="4">Authenticates the merchant on the Payment Server. This means that a merchant cannot access another merchant's Merchant Id.
The access code is provided when the merchant profile is registered with a Payment Provider.</td></tr>
<tr><td>Required</td><td>Alphanumeric</td><td>8</td><td>6AQ89F3</td></tr>
<tr><td colspan="4"><b>vpc_MerchTxnRef</b></td></tr>
<tr><td colspan="4">A unique value created by the merchant.
<b>Usage Notes:</b> The Merchant Transaction Reference is used as a reference key to the Payment Server database to obtain a copy of lost/missing transaction receipts using the QueryDR function. It can also be used to identify a duplicate transaction if it is always kept unique for each transaction attempt. It can contain similar information to the vpc_OrderInfo field, but it must be unique for each transaction attempt if it is to be used properly.
Typically, the vpc_MerchTxnRef is based on an order number, invoice number, timestamp, etc., but it should also reflect the transaction attempt. For example, if a cardholder has insufficient funds on their card and they are allowed to repeat the transaction with another credit card, the value may be INV1234/1 on the first attempt, INV1234/2 on the second attempt, and INV1234/3 on the third attempt.
This identifier will be displayed in the Transaction Search results and also in the Download file (from Financial Transactions Search or Download Search Results link in Financial Transaction List) in the Merchant Administration portal on the Payment Server.
<b>Note</b>: If "Enforce Unique Merchant Transaction Reference" privilege is enabled by your Payment Provider, this value must be unique across all the merchant's transactions.</td></tr>
<tr><td>Required</td><td>Alphanumeric</td><td>1,40</td><td>ORDER958743-1</td></tr>
<tr><td colspan="4"><b>vpc_Merchant</b></td></tr>
<tr><td colspan="4">The unique Merchant Id assigned to a merchant by the Payment Provider. The Merchant ID identifies the merchant account against which settlements will be made.</td></tr>
<tr><td>Required</td><td>Alphanumeric</td><td>1,16</td><td>TESTMERCHANT01</td></tr>
<tr><td colspan="4"><b>vpc_TransNo</b></td></tr>
<tr><td colspan="4">This is the unique Payment Server OrderID (Shopping Transaction) number generated by the Payment Server for the initial transaction.</td></tr>
<tr><td>Required</td><td>Numeric</td><td>1,19</td><td>10712</td></tr>
<tr><td colspan="4"><b>vpc_Amount</b></td></tr>
<tr><td colspan="4">The amount of the transaction, expressed in the smallest currency unit. The amount must not contain any decimal points, thousands separators or currency symbols. For example, □12.50 is expressed as 1250.
This value cannot be negative or zero. The maximum valid value is 2147483647.</td></tr>
<tr><td>Required</td><td>Numeric</td><td>1,12</td><td>1250</td></tr>
</table>

vpc_User			
The user name of the user who is performing the AMA transaction. Each AMA User name may be assigned different privileges to perform particular functions. For example, an AMA User can be set to only perform refunds. **Note:** An AMA user cannot be used for Merchant Administration operations.			
Required	Alphanumeric	1,20	Maryellen
vpc_Password			
The password used by the merchant to authorise Advanced Merchant Administration transactions. It must be at least 8 characters long and contain at least one non-alphabetical character.			
Required	Alphanumeric	8,25	T1m34t*A

Basic Output Fields - AMA Transaction

Once a Transaction Response has been successfully received, the merchant application can retrieve the receipt details. These values are then passed back to the cardholder for their records.

Note: The Transaction Response provided by the Payment Server may contain other fields that are not documented in this guide. Such fields may be changed, added, or removed without notice, and must NOT be relied upon by merchant integrations.

Terminology: Returned Input fields are shown as "Input" in the table.

2-Party AMA Output Fields			
The following data fields are returned in a Transaction Response for a standard 2-Party transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_Version			
The version of the Virtual Payment Client API being used. The current version is 1.			
Input	Alphanumeric	1,8	1
vpc_Command			
The value of the vpc_Command input field returned in the Transaction Response.			
Input	Alphanumeric	1,16	pay
vpc_MerchTxnRef			
The value of the vpc_MerchTxnRef input field returned in the Transaction Response. This field may not be returned in a transaction that fails due to an error condition.			
Input	Alphanumeric	0,40	ORDER958743-1

vpc_Merchant			
The value of the vpc_Merchant input field returned in the Transaction Response.			
Input	Alphanumeric	1,16	TESTMERCHANT01
vpc_Message			
This is a message to indicate what sort of errors the transaction encountered. This field is not provided if vpc_TxnResponseCode has a value of zero.			
Output	Alphanumeric	1,255	Merchant [TESTCORE23] does not exist.
vpc_TxnResponseCode			
A response code that is generated by the Payment Server to indicate the status of the transaction. A vpc_TxnResponseCode of "0" (zero) indicates that the transaction was processed successfully and approved by the acquiring bank. Any other value indicates that the transaction was declined (it went through to the banking network) or the transaction failed (it never made it to the banking network). For a list of values, see *Returned Response Codes* on page 80.			
Output	Alphanumeric	1	0
vpc_AcqResponseCode			
Generated by the financial institution to indicate the status of the transaction. The results can vary between institutions so it is advisable to use the vpc_TxnResponseCode as it is consistent across all acquirers. It is only included for fault finding purposes. Most Payment Providers return the vpc_AcqResponseCode as a 2-digit response; others return it as a 3-digit response. This field is not returned for transactions that result in an error condition.			
Output	Alphanumeric	2,3	00
vpc_TransactionNo			
Financial Transaction Number is a unique number generated by the Payment Server for this transaction. This field will not be returned if the transaction failed due to an error condition.			
Output	Numeric	1,19	96841
vpc_BatchNo			
A value supplied by an acquirer which indicates the batch of transactions that the specific transaction has been grouped with. Batches of transactions are settled by the acquirer at intervals determined by them. This is an acquirer specific field, for example, it could be a date in the format YYYYMMDD. This field will not be returned if the transaction fails due to an error condition.			
Output	Numeric	0,8	20110105

<table>
<tr><td colspan="4"><b>vpc_AuthorizeId</b></td></tr>
<tr><td colspan="4">Authorisation Identification Code issued by the Acquirer to indicate the approval of a transaction.
This field is 6-digits maximum and is not returned for transactions that are declined or fail due to an error condition.
<b>Note</b>: This field may or may not be returned for some acquirers or combination of transactions even if the transaction is successful.</td></tr>
<tr><td>Output</td><td>Alphanumeric</td><td>0,6</td><td>654321</td></tr>
<tr><td colspan="4"><b>vpc_ReceiptNo</b></td></tr>
<tr><td colspan="4">A unique identifier that is also known as the Reference Retrieval Number (RRN).
The vpc_ReceiptNo may be passed back to the cardholder for their records if the merchant application does not generate its own receipt number.
This field is not returned for transactions that result in an error condition.</td></tr>
<tr><td>Output</td><td>Alphanumeric</td><td>0,12</td><td>RP12345</td></tr>
<tr><td colspan="4"><b>vpc_Amount</b></td></tr>
<tr><td colspan="4">The value of the vpc_Amount input field returned in the Transaction Response.</td></tr>
<tr><td>Input</td><td>Numeric</td><td>1,10</td><td>1250</td></tr>
<tr><td colspan="4"><b>vpc_Card</b></td></tr>
<tr><td colspan="4">Identifies the card type used for the transaction.
For a list of card types see <i>Card Type Codes</i> on page 90.
This field is not returned for transactions that result in an error condition.</td></tr>
<tr><td>Output</td><td>Alpha</td><td>0,2</td><td>MC</td></tr>
<tr><td colspan="4"><b>vpc_Currency</b></td></tr>
<tr><td colspan="4">The value of the vpc_Currency input field returned in the Transaction Response.
This field is returned only if vpc_Currency was included in the Transaction Request.</td></tr>
<tr><td>Input</td><td>Alpha</td><td>3</td><td>USD</td></tr>
<tr><td colspan="4"><b>vpc_ShopTransactionNo</b></td></tr>
<tr><td colspan="4">The Order ID (Shopping Transaction) corresponding to the initial transaction.</td></tr>
<tr><td>Input</td><td>Numeric</td><td>0,19</td><td>96841</td></tr>
<tr><td colspan="4"><b>vpc_TicketNumber</b></td></tr>
<tr><td colspan="4">The ticket number was originally aimed at the airline industry, however it can be used for any relevant information about this transaction you want stored. The ticket number is stored on the Payment Server database for that transaction and returned in the Transaction Response for capture transactions.</td></tr>
<tr><td>Output</td><td>Alphanumeric</td><td>0,15</td><td>VIP Client</td></tr>
<tr><td colspan="4"><b>vpc_AcqResponseText</b></td></tr>
<tr><td colspan="4">The response from the acquirer in the text form. This field is used instead of vpc_AcqResponseCode for acquirers that return text instead of a single code.</td></tr>
<tr><td>Optional</td><td>Alphanumeric</td><td>0,255</td><td>Success : Pending: Authorisation</td></tr>
</table>

AMA Capture Transaction

The AMA Capture command allows a merchant to capture the funds from a previous authorisation transaction.

Transaction Request Input Fields

Table 19 AMA Capture Transaction: Request Input Fields

2-Party Capture Input Fields			
The following additional data fields must be included in a Transaction Request when performing a Capture transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_Command			
Indicates the transaction type. This must be equal to '**capture**' for a capture transaction.			
Required	Alphanumeric	1,16	capture
vpc_TicketNumber			
The ticket number was originally aimed at the airline industry, however it can be used for any relevant information about this transaction you want stored. The ticket number is stored on the Payment Server database for that transaction and returned in the Transaction Response for capture transactions. If a ticket number is included in a Capture Transaction, it will overwrite any ticket number previously submitted for the order, whether in the original authorisation or a subsequent (partial) capture.			
Output	Alphanumeric	0,15	VIP Client

Transaction Response Output Fields

Once a Transaction Response has been successfully received, the merchant application can retrieve the receipt details. These values are then passed back to the cardholder for their records.

Table 20 AMA Capture Transaction Request: Output Results

AMA Output Fields			
The following additional data fields are returned in a Transaction Response for standard transactions.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_AuthorisedAmount			
This is the value of the Authorised transaction amount for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual Payment Client.			
Output	Numeric	0,10	10185
vpc_CapturedAmount			
This is the value of the total transaction amount captured for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual Payment Client.			
Output	Numeric	0,10	10100
vpc_RefundedAmount			
This is the total value of any Refunded transaction amounts for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual Payment Client.			
Output	Numeric	1,10	1295

AMA Refund Transaction

AMA Refund allows you to refund funds for a previous purchase or capture transaction from the merchant's account back to the cardholder's account.

Transaction Request Input Fields

Table 21 AMA Refund Transaction

2-Party Refund Input Fields			
The following additional fields must be included in a Transaction Request when performing a Refund transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_Command			
Indicates the transaction type. This must be equal to '**refund**' for a refund transaction.			
Required	Alphanumeric	1,16	refund

Transaction Response Output Fields

Table 22 AMA Refund Transaction: Output Results

AMA Output Fields			
The following additional data fields are returned in a Transaction Response for standard transactions.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_AuthorisedAmount			
This is the value of the Authorised transaction amount for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual Payment Client.			
Output	Numeric	0,10	10185
vpc_CapturedAmount			
This is the value of the total transaction amount captured for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual Payment Client.			
Output	Numeric	0,10	10100

<table>
<tr><th colspan="4">vpc_RefundedAmount</th></tr>
<tr><td colspan="4">This is the total value of any Refunded transaction amounts for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual Payment Client.</td></tr>
<tr><td>Output</td><td>Numeric</td><td>1,10</td><td>1295</td></tr>
</table>

AMA Void Capture Transaction

AMA Void Capture allows a merchant to void the funds from a previous capture transaction in Auth/Capture mode that has not been processed by the acquiring institution.

Transaction Request Input Fields

Table 23 AMA Void Capture Transaction: Data Fields

<table>
<tr><td colspan="4"><b>2-Party Void Capture Input Fields</b></td></tr>
<tr><td colspan="4">The following additional data fields must be included in a Transaction Request when using for a Void Capture transaction.</td></tr>
<tr><td colspan="4"><b>Field Name</b></td></tr>
<tr><td colspan="4">Field Description</td></tr>
<tr><td>Required/ Optional</td><td>Field Type</td><td>Min, Max or Set Field Length</td><td>Sample Data</td></tr>
</table>

<table>
<tr><td colspan="4"><b>vpc_Command</b></td></tr>
<tr><td colspan="4">Indicates the transaction type. This must be equal to '<b>voidCapture</b>' for a void capture transaction.</td></tr>
<tr><td>Required</td><td>Alphanumeric</td><td>1,16</td><td>voidCapture</td></tr>
</table>

Transaction Response Output Fields

Table 24 AMA Refund Transaction: Output Results

<table>
<tr><td colspan="4"><b>AMA Output Fields</b></td></tr>
<tr><td colspan="4">The following additional data fields are returned in a Transaction Response for Void Capture transactions.</td></tr>
<tr><td colspan="4"><b>Field Name</b></td></tr>
<tr><td colspan="4">Field Description</td></tr>
<tr><td>Returned Input or Output</td><td>Field Type</td><td>Min, Max or Set Field Length</td><td>Sample Data</td></tr>
</table>

<table>
<tr><td colspan="4"><b>vpc_AuthorisedAmount</b></td></tr>
<tr><td colspan="4">This is the value of the Authorised transaction amount for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual Payment Client.</td></tr>
<tr><td>Output</td><td>Numeric</td><td>0,10</td><td>10185</td></tr>
</table>

vpc_CapturedAmount			
This is the value of the total transaction amount captured for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual Payment Client.			
Output	Numeric	0,10	10100
vpc_RefundedAmount			
This is the total value of any Refunded transaction amounts for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual Payment Client.			
Output	Numeric	1,10	1295

AMA Void Refund Transaction

AMA Void Refund allows a merchant to void a previous refund transaction that has not been processed by the acquiring institution.

Transaction Request Input Fields

2-Party Void Refund Input Fields			
The following additional data fields must be included in a Transaction Request for a Void Refund transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_Command			
Indicates the transaction type. This must be equal to '**voidRefund**' for this transaction type.			
Required	Alphanumeric	1,16	voidRefund

Transaction Response Output Fields

2-Party Void Refund Output Fields			
The following additional data fields are returned in a Transaction Response for a Void Refund transaction.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_AuthorisedAmount			
This is the value of the Authorised transaction amount for the order and is returned in the Transaction Response of a Capture, Refund and Void transaction amount for Virtual Payment Client.			
Output	Numeric	0,10	10185
vpc_CapturedAmount			
This is the value of the total transaction amount captured for the order and is returned in the Transaction Response of a Capture, Refund and Void transaction amount for Virtual Payment Client.			
Output	Numeric	0,10	10100

vpc_RefundedAmount			
This is the total value of any Refunded transaction amounts for the order and is returned in the Transaction Response of a Capture, Refund and Void transaction amount for Virtual Payment Client.			
Output	Numeric	1,10	1295

AMA Void Purchase Transaction

AMA Void Purchase allows a purchase merchant to void a purchase transaction that has not been processed by the acquiring institution. It is not available for Auth/Capture mode merchants.

Transaction Request Input Fields

Table 25 AMA Void Purchase Transaction: Output Results

<table>
<tr><td colspan="4"><b>2-Party Void Purchase Input Fields</b></td></tr>
<tr><td colspan="4">The following additional data fields must be included in a Transaction Request when using for a Void Purchase transaction.</td></tr>
<tr><td colspan="4"><b>Field Name</b></td></tr>
<tr><td colspan="4">Field Description</td></tr>
<tr><td>Required/ Optional</td><td>Field Type</td><td>Min, Max or Set Field Length</td><td>Sample Data</td></tr>
</table>

<table>
<tr><td colspan="4"><b>vpc_Command</b></td></tr>
<tr><td colspan="4">Indicates the transaction type. This must be equal to '<b>voidPurchase</b>' for this transaction type.</td></tr>
<tr><td>Required</td><td>Alphanumeric</td><td>1,16</td><td>voidPurchase</td></tr>
</table>

Transaction Response Output Fields

Table 26 AMA Void Purchase Transaction: Output Results

<table>
<tr><td colspan="4"><b>AMA Output Fields</b></td></tr>
<tr><td colspan="4">The following additional data fields are returned in a Transaction Response for Void Purchase transactions.</td></tr>
<tr><td colspan="4"><b>Field Name</b></td></tr>
<tr><td colspan="4">Field Description</td></tr>
<tr><td>Returned Input or Output</td><td>Field Type</td><td>Min, Max or Set Field Length</td><td>Sample Data</td></tr>
</table>

<table>
<tr><td colspan="4"><b>vpc_AuthorisedAmount</b></td></tr>
<tr><td colspan="4">This is the value of the Authorised transaction amount for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual Payment Client.</td></tr>
<tr><td>Output</td><td>Numeric</td><td>0,10</td><td>10185</td></tr>
</table>

vpc_CapturedAmount			
This is the value of the total transaction amount captured for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual Payment Client.			
Output	Numeric	0,10	10100
vpc_RefundedAmount			
This is the total value of any Refunded transaction amounts for the order and is returned in the Transaction Response of a Capture, Refund or Void transaction amount for Virtual Payment Client.			
Output	Numeric	1,10	1295

AMA Standalone Capture Transaction

Standalone Capture allows you to capture funds against an order when the corresponding authorisation was obtained either manually, or in an external system.

Use the Standalone Capture command via the Virtual Payment Client to directly perform captures from your application. Your Payment Provider must enable this function on your Merchant Profile for you to use this functionality.

Transaction Request Input Fields

Standalone Capture Input Fields			
The following additional data fields must be included in a Transaction Request for a Standalone Capture transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_Command			
Indicates the transaction type. This must be equal to '**doRequest**' for this type of transaction.			
Required	Alphanumeric	1,16	doRequest
vpc_RequestType			
This field is associated when the **vpc_Command** field equals '**doRequest**'. This must be equal to **'CAPTURE'** for this type of transaction.			
Required	Alphanumeric	1,20	CAPTURE
vpc_RequestCommand			
This field is associated when the **vpc_Command** field equals '**doRequest**'. Applicable values can be obtained from your Payment Provider. The value must be equal to '**doStandaloneCapture**' for this type of transaction.			
Required	Alphanumeric	1,20	doStandaloneCapture
vpc_OrderInfo			
The merchant's identifier used to identify the order on the Payment Server. For example, a shopping cart number, an order number, or an invoice number. This identifier will be displayed in the Transaction Search results in the Merchant Administration portal on the Payment Server.			
Note: If 'Enforce Unique Order Reference" privilege is enabled by your Payment Provider, this value must be unique across all the merchant's orders.			
Optional	Alphanumeric	0,34	ORDER958743
vpc_ManualAuthID			
An alphanumeric code of up to six characters used to specify the manual authorisation code supplied by the card issuer for the transaction.			
Optional	Alphanumeric	0,6	ABC678

vpc_CardNum			
The number of the card used for the transaction. The format of the Card Number is based on the Electronic Commerce Modeling Language (ECML) and, in particular, must not contain white space or formatting characters.			
Required	Numeric	15,19	5123456789012346
vpc_CardExp			
The expiry date of the card in the format YYMM. The value must be expressed as a 4-digit number (integer) with no white space or formatting characters. For example, an expiry date of May 2013 is represented as 1305.			
Required	Numeric	4	1305
vpc_Currency			
The currency of the order expressed as an ISO 4217 alphanumeric code. This field is case-sensitive and must include uppercase characters only. The merchant must be configured to accept the currency used in this field. To obtain a list of supported currencies and codes, please contact your Payment Provider. **Note**: This field is required only if more than one currency is configured for the merchant.			
Optional	Alpha	3	USD

Transaction Response Output Fields

There are no special output fields returned in the Transaction Response.

AMA Standalone Refund Transaction

Standalone Refund allows you to refund funds from your account back to the cardholder without a previous purchase.

Use the Standalone Refund command via the Virtual Payment Client to directly perform refunds from your application. Your Payment Provider must enable this function on your Merchant Profile for you to use this functionality.

Transaction Request Input Fields

Standalone Refund Input Fields			
The following additional data fields must be included in a Transaction Request for a Standalone Refund transaction.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_Command			
Indicates the transaction type. This must be equal to '**doRequest**' for this type of transaction.			
Required	Alphanumeric	1,16	doRequest
vpc_RequestType			
This field is associated when the **vpc_Command** field equals '**doRequest**'. The value must be equal to '**credit**' for this type of transaction.			
Required	Alphanumeric	1,20	credit
vpc_RequestCommand			
This field is associated when the **vpc_Command** field equals '**doRequest**'. Applicable values can be obtained from your Payment Services Provider. The value must be equal to '**doStandaloneRefund**' for this type of transaction.			
Required	Alphanumeric	1,20	doStandaloneRefund
vpc_OrderInfo			
The merchant's identifier used to identify the order on the Payment Server. For example, a shopping cart number, an order number, or an invoice number. This identifier will be displayed in the Transaction Search results in the Merchant Administration portal on the Payment Server. **Note**: If 'Enforce Unique Order Reference" privilege is enabled by your Payment Provider, this value must be unique across all the merchant's orders.			
Optional	Alphanumeric	0,34	ORDER958743
vpc_CardNum			
The number of the card used for the transaction. The format of the Card Number is based on the Electronic Commerce Modeling Language (ECML) and, in particular, must not contain white space or formatting characters.			
Required	Numeric	15,19	5123456789012346
vpc_CardExp			
The expiry date of the card in the format YYMM. The value must be expressed as a 4-digit number (integer) with no white space or formatting characters. For example, an expiry date of May 2013 is represented as 1305.			
Required	Numeric	4	1305
vpc_CardSecurityCode			
The Card Security Code (CSC), also known as CVV (Visa), CVC2 (MasterCard), CID/4DBC (Amex), or CVV2 which is printed not embossed on the card. It compares the code with the records held in the card issuing institution's database.			
Optional	Numeric	3,4	985
vpc_Currency			
The currency of the order expressed as an ISO 4217 alphanumeric code. This field is case-sensitive and must include uppercase characters only. The merchant must be configured to accept the currency used in this field. To obtain a list of supported currencies and codes, please contact your Payment Provider. **Note**: This field is required only if more than one currency is configured for the merchant.			
Optional	Alpha	3	USD

Transaction Response Output Fields

There are no special output fields returned in the Transaction Response.

AMA QueryDR

The AMA QueryDR command allows a merchant to search for the current or the most recent transaction receipt. It also queries for unknown transactions (a transaction request for which a response was never received) and failed transactions.

The search is performed on the key - **vpc_MerchTxnRef**, so the **vpc_MerchTxnRef** field must be a unique value.

If more than one Transaction Response exists with the same **vpc_MerchTxnRef,** the most recent Transaction Response is returned. For QueryDR to return the current transaction, the transaction response code of the original Transaction Response must be "P-Pending" or "M-Submitted".

If you want to use QueryDR to return digital receipts, it must be done in under three days or no results matching the criteria will be returned. This is because the database only contains data up to three days old.

Transaction Request Input Fields

Table 27 AMA Query DR

2-Party QueryDR Input Fields			
The following additional data fields must be included in a Transaction Request when using a QueryDR check.			
Field Name			
Field Description			
Required/ Optional	Field Type	Min, Max or Set Field Length	Sample Data

vpc_Command			
Indicates the transaction type. This must be equal to '**queryDR**' for a QueryDR function.			
Required	Alphanumeric	1,16	queryDR

Transaction Response Output Fields

A QueryDR can be performed on a base transaction, or on AMA transactions such as a Capture, Refund or Void. Both of these transaction types return different fields.

Table 28 AMA Query DR: Output Fields

QueryDR Output Fields			
The following additional data fields are returned in a Transaction Response for a QueryDR transaction.			
Field Name			
Field Description			
Returned Input or Output	Field Type	Min, Max or Set Field Length	Sample Data

vpc_DRExists			
This key is used to determine if the QueryDR command returned any search results. If the value is "**Y**", there is one transaction with a MerchTxnRef number that matched the search criteria. If the value is "**N**", then there is no matching MerchTxnRef number result for the search criteria.			
Output	Alpha	1	Y
vpc_FoundMultipleDRs			
This is used after the previous command to determine if there are multiple results. If the value is "**Y**", there are multiple transactions with the MerchTxnRef number that matches the search criteria. If the value is "**N**", there could be zero or at most, one transaction with the MerchTxnRef number that matches the search criteria.			
Output	Alpha	1	N

If an original receipt exists, the QueryDR will return all the *Basic Output Fields - AMA Transaction* on page 56 in addition to vpc_DRExists and vpc_FoundMultipleDRs. If the transaction to be queried is a subsequent or AMA transaction such as Capture, Refund, or Void then the following additional fields are returned.

vpc_AuthorisedAmount			
This is the value of the Authorised transaction amount for the order and is returned in the Transaction Response of a Capture, Refund and Void transaction amount for Virtual Payment Client.			
Output	Numeric	0,10	10185

vpc_CapturedAmount			
This is the value of the total transaction amount captured for the order and is returned in the Transaction Response of a Capture, Refund and Void transaction amount for Virtual Payment Client.			
Output	Numeric	0,10	10100
vpc_RefundedAmount			
This is the total value of any Refunded transaction amounts for the order and is returned in the Transaction Response of a Capture, Refund and Void transaction amount for Virtual Payment Client.			
Output	Numeric	1,10	1295

If an original receipt doesn't exist, the QueryDR will return the following fields in addition to vpc_DRExists and vpc_FoundMultipleDRs.

vpc_Version			
The version of the Virtual Payment Client API being used. The current version is 1.			
Input	Alphanumeric	1,8	1
vpc_Amount			
The value of the vpc_Amount input field returned in the Transaction Response.			
Input	Numeric	1,10	1250
vpc_BatchNo			
A value supplied by an acquirer which indicates the batch of transactions that the specific transaction has been grouped with. Batches of transactions are settled by the acquirer at intervals determined by them. This is an acquirer specific field, for example, it could be a date in the format YYYYMMDD. This field will not be returned if the transaction fails due to an error condition.			
Output	Numeric	0,8	20110105
vpc_Command			
The value of the vpc_Command input field returned in the Transaction Response.			
Input	Alphanumeric	1,16	pay
vpc_Locale			
The value of the vpc_Locale input field returned in the Transaction Response.			
Input	Alpha	2,5	en
vpc_Merchant			
The value of the vpc_Merchant input field returned in the Transaction Response.			
Input	Alphanumeric	1,16	TESTMERCHANT01
vpc_TransactionNo			
Financial Transaction Number is a unique number generated by the Payment Server for this transaction. This field will not be returned if the transaction failed due to an error condition.			
Output	Numeric	1,19	96841

5 Payment Client References – Virtual Payment Client

Generating a Secure Hash

Note: Although the vpc_SecureHashType field is denoted as 'optional', new merchant integrations are required to generate a secure hash using the SHA-256 HMAC algorithm.

Creating a SHA-256 HMAC Secure Hash

The merchant code creates the Secure Hash value on the Transaction Request data. The Payment Server creates another Secure Hash value and sends it back to the merchant in the Transaction Response.

The Secure Hash is a hexadecimal encoded SHA-256 HMAC of a concatenation of VPC and User Defined parameters. The concatenation of parameters takes the form of a set of name-value pairs, similar to the parameter string for an HTTP GET call.

Merchant Supplied Parameters

For information that you want to return to your integration in the Transaction Response, you may either:

- Include it in an appropriate VPC parameter such as vpc_MerchTxnRef field or vpc_ReturnURL in the Transaction Request, or
- Provide User Defined parameters in the Transaction Request. User Defined parameters are identified by having a parameter name starting with "user_", or
- Provide other Merchant Supplied parameters. Other Merchant Supplied parameters are not included in the SHA-256 HMAC calculation.

Note: All field names are restricted to the character set defined by the regular expression [A-Z, a-z, 0-9]. Currently, merchant-supplied parameters are supported by 3-Party integrations only.

SHA-256 HMAC Calculation

The SHA-256 HMAC is calculated as follows:

1. The SHA-256 HMAC calculation includes all VPC fields, that is, all fields beginning with "vpc_", except the vpc_SecureHash and vpc_SecureHashType parameters.

   The field names are sorted in ascending of parameter name. Specifically, the sort order is:

   - Ascending order of parameter name using the ASCII collating sequence, for example, "Card" comes before "card"

   - Where one string is an exact substring of another, the smaller string should be ordered before the longer, for example, "Card" should come before "CardNum".

2. Construct a string by concatenating the string form of the sorted field name-value pairs. The string form of a name-value pair is the name followed by the value.

   - The field name and the value in each field name-value pair are joined using "=" as the separator.

   - The resulting joined field name-value pairs are themselves joined using "&" as the separator.

3. Create a SHA-256 HMAC of the resultant string using the hex decoded value of your merchant secret as the key. The SHA-256 HMAC algorithm is defined in Federal Information Processing Standard 180-2. We strongly recommend that you use one of the numerous implementations available in most programming languages.

4. Encode the HMAC in hexadecimal, and include it in the request as the value for the vpc_SecureHash field.

   For example, if your merchant secret is:

   BB48A64077A1CBF08FF0D91C5A9FE42B

   and the Transaction Request includes only the following parameters:

Field Name	Example Value
vpc_Version	2
vpc_Command	pay
vpc_MerchTxnRef	txn 1
vpc_CardNum	345678901234564
vpc_CardExp	1305
vpc_Merchant	TESTMERCHANT
vpc_Amount	1000

The concatenated value is as follows:

```
vpc_Amount=1000&vpc_CardExp=1305&vpc_CardNum=345678901234564&vp
c_Command=pay&vpc_MerchTxnRef=txn
1&vpc_Merchant=TNSITESTMERCHANT&vpc_Version=1
```

Note: The last character of each field value (other than the last) is followed directly by "&". The concatenated value must be represented in the UTF-8 character encoding format.

Note: The values in all name value pairs should not be URL encoded for the purpose of hashing.

The Secure Hash value is:

```
A4E4ADBADEC557A3DC079F697E942B9123371E59D89C6D8494F3A078C098A9B5
```

and the resultant Request is (note the Secure Hash and Secure Hash Type fields):

```
vpc_Amount=1000&vpc_CardExp=1305&vpc_CardNum=345678901234564&vp
c_Command=pay&vpc_MerchTxnRef=txn 1
&vpc_Merchant=TNSITESTMERCHANT&vpc_Version=1&vpc_SecureHash=A4E
4ADBADEC557A3DC079F697E942B9123371E59D89C6D8494F3A078C098A9B5&v
pc_SecureHashType=SHA256
```

Note: There is a line break in the example that is NOT part of the resultant Request.

The Payment Server also includes the vpc_SecureHash in the Transaction Response so you can check the integrity of the receipt data. You do this by calculating the secure hash using the above method, then comparing your calculation with the value you received from the Payment Server. If the values match, then you can be assured that we received the data you sent, and you received the data we sent.

Secure Hash Matching Error

Our Secure Hash method provides very good detection of attempts at fraud. However it is your responsibility to keep the key secret and to check the response. If the calculated and received values of the secure hash do not match, then you are at serious risk of eShoplifting. That is, providing your goods or service without being paid.

This could be due to:

- Fraud by your customer
- Fraud by a man-in-the-middle attack (you are especially vulnerable to this if you do not use SSL between the customer's browser and your website)
- Malicious corruption of the customer's web browser or computer.

It is extremely unlikely that the reason was corruption by the network. There is only a very small chance that a network packet will be corrupted and not corrected by the IP or TCP protocols.

Therefore you should take secure hash errors seriously, and when detected, take action that you think is appropriate to protect your business.

To simplify the calculation, the fields in the returned data in the Transaction Response are sorted in the order required for the Secure Hash calculation.

Store Secure Hash Secret Securely

You must keep your Secure Hash Secret stored securely. Do not store your secret within the source code of an ASP, JSP, or other website page as it is common for web server vulnerabilities to be discovered where source code of such pages can be viewed.

You should store your Secure Hash Secret in a secured database, or in a file that is not directly accessible by your web server and has suitable system security permissions.

You should change your Secure Hash Secret regularly in accordance with your company's security policy, and at any time when you believe that its security may have been compromised.

You can change your Secure Hash Secret in Merchant Administration in the Setup menu option on the Configuration Details page. For more information, please refer to your Merchant Administration User Guide.

Returned Response Codes

The **vpc_TxnResponseCode** is a response code generated by the Payment Server that indicates the result of attempting to perform a transaction. This response code can also be used to detect an error.

Any response code other than '0' is a declined/failed transaction. If the transaction is an error condition it will be contained in the vpc_Message field.

The response codes generated by the Payment Server are:

Table 29 Returned Response Codes

Vpc_Txn Response Code	Description	S2I	S2A-ANZ	S2A-WBC	S2A-NAB	Description
?	Response Unknown	-	-	-	-	-
0	Transaction Successful	00	00	00	00	Approved or completed successfully
		08	08	08	08	Honor with identification
		16	-	16	-	Approved, update Track #3
1	Transaction could not be processed	-	06	-	06	Error
		09	-	09	-	Request in progress
		10	10	10	10	Approved for partial amount
		11	11	11	11	Approved VIP
		12	12	12	12	Invalid transaction
		13	13	13	13	Invalid amount
		-	14	-	14	Invalid card number
		17	17	17	17	Customer cancellation
		18	18	18	18	Customer dispute
		20	20	20	20	Invalid response
		21	-	21	-	No action taken
		22	22	22	22	Suspected malfunction
		23	23	23	23	Unacceptable transaction fee
		24	24	24	24	File update not supported by receiver
		-	25	-	25	Unable to locate record on file
		26	26	26	26	Duplicate file update record, old record replaced
		27	27	27	27	File update field edit error
		28	28	28	28	File update file locked out
		29	29	29	29	File update not successful, contact acquirer
		30	30	30	30	Format error

Vpc_Txn Response Code	Description	S2I	S2A-ANZ	S2A-WBC	S2A-NAB	Description
		32	32	32	32	Completed partially
		35	35	35	35	Card acceptor contact acquirer
		37	37	37	37	Card acceptor call acquirer security
		38	-	38	-	Allowable PIN tries exceeded
		40	40	40	40	Request function not supported
		42	-	42	-	No universal account
		44	44	44	44	No investment account
		45-50	45-50	45-50	45-50	Reserved for ISO use
		52	-	52	-	No cheque account
		53	-	53	-	No savings account
		55	-	55	-	Incorrect PIN
		56	-	56	-	No card record
		-	-	57	-	Transaction not permitted to cardholder
		58	58	58	58	Transaction not permitted to acquirer
		60	60	60	60	Card acceptor contact acquirer
		62	-	62	-	Restricted card
		63	-	63	-	Security violation
		64	64	64	64	Original amount incorrect
		66	66	66	66	Card acceptor call acquirer’s security department
		67	67	67	67	Hard capture (requires that the card be picked up at ATM)
		69-74	69-74	69-74	69-74	Reserved for ISO use
		75	-	75	-	Allowable number of PIN tries exceeded
		76-89	76-89	76-89	76-89	Reserved for private use
		-	90	-	-	Cut-off is in process (switch ending a day’s business and starting the next. Transaction can be sent again in a few minutes.)
		-	92	-	92	Financial institution or intermediate network facility cannot be found for routing
		93	93	93	93	Transaction cannot be completed, violation of law

Vpc_Txn Response Code	Description	S2I	S2A-ANZ	S2A-WBC	S2A-NAB	Description
		94	-	94	-	Duplicate transmission
		95	95	95	95	Reconcile error
		96	96	96	96	System malfunction
		97	-	97	97	Advises that reconciliation totals have been reset
2	Transaction Declined - Contact Issuing Bank	-	01	01	01	Refer to card issuer
		02	02	02	02	Refer to card issuer's special conditions
		03	03	03	03	Invalid merchant
		04	-	04	-	Pick up card
		05	05	05	05	Do not honor
		06	-	06	-	Error
		07	-	07	-	Pick up card, special condition
		14	-	14	-	Invalid card number
		15	15	15	15	No such Issuer
		-	16	-	16	Approved, update Track #3
		19	19	19	19	Re-enter transaction
		-	21	-	21	No action taken
		25	-	25	-	Unable to locate record on file
		31	31	31	31	Bank not supported by switch
		34	-	-	-	Suspected fraud
		36	-	36	-	Restricted card
		-	38	-	38	Allowable PIN tries exceeded
		39	39	39	39	No credit account
		41	41	41	-	Lost card
		-	42	-	42	No universal account
		43	43	43	-	Stolen card, pick up
		-	52	-	52	No cheque account
		-	53	-	53	No savings account
		-	55	-	55	Incorrect PIN
		-	56	-	56	No card record
		57	57	-	57	Transaction not permitted to card holder
		59	59	59	59	Suspected fraud
		61	61	61	61	Exceeds withdrawal amount limits
		62	62	-	62	Restricted card
		-	63	-	63	Security violation

Vpc_Txn Response Code	Description	S2I	S2A-ANZ	S2A-WBC	S2A-NAB	Description
		65	65	65	65	Exceeds withdrawal frequency limit
		-	75	-	75	Allowable number of PIN tries exceeded
		81	-	-	-	Reserved for private use.
		90	-	90	90	Cut-off is in process (switch ending a day's business and starting the next. Transaction can be sent again in a few minutes.)
		91	-	91	-	Issuer or switch inoperative
		92	-	92	-	Financial institution or intermediate network facility cannot be found for routing
		-	94	-	94	Duplicate transmission
		98	-	98	-	MAC error
		99	99	99	-	Reserved for National Use
3	Transaction Declined- No reply from Bank	-	09	-	09	Request in progress
		68	68	68	68	Response received too late
4	Transaction Declined - Expired Card	-	04	-	04	Pick-up card
		-	07		-	Pick up card, special condition
		33	33	33	33	Expired card
		-	34	-	34	Suspected fraud
		-	36	-	36	Restricted card
		-	-	-	41	Lost card
		-	-	-	43	Stolen card, pick up
		54	54	54	54	Expired card
5	Transaction Declined - Insufficient credit	51	51	51	51	Not sufficient funds
6	Transaction Declined - Bank system error	-	-	-	-	Response received too late
		-	91	-	-	Issuer or switch inoperative
		-	97	-	-	Advises that reconciliation totals have been reset
		-	98	-	-	MAC error

Vpc_Txn Response Code	Description	S2I	S2A-ANZ	S2A-WBC	S2A-NAB	Description
7	Payment Server Processing Error - Typically caused by invalid input data such as an invalid credit card number. Processing errors can also occur. (This is only relevant for Payment Servers that enforce the uniqueness of this field) Processing errors can also occur.	-	-	-	-	-
8	Transaction Declined - Transaction Type Not Supported	-	-	-	-	-
9	Bank Declined Transaction (Do not contact Bank)	-	-	-	-	-
A	Transaction Aborted	-	-	-	-	-
B	Transaction Blocked - Returned when: • The Verification Security Level has a value of '07'. • If the merchant has 3-D Secure Blocking enabled, the transaction will not proceed. • The overall risk assessment result returns a "Reject" or "System Reject".	-	-	-	-	-
C	Transaction Cancelled	-	-	-	-	-
D	Deferred Transaction	-	-	-	-	-
E	Transaction Declined - Refer to card issuer	01	-	-	-	Refer to card issuer

Vpc_Txn Response Code	Description	S2I	S2A-ANZ	S2A-WBC	S2A-NAB	Description
F	3D Secure Authentication Failed	-	-	-	-	-
I	Card Security Code Failed	-	-	-	-	-
L	Shopping Transaction Locked (This indicates that there is another transaction taking place using the same shopping transaction number)	-	-	-	-	-
N	Cardholder is not enrolled in 3D Secure (Authentication Only)	-	-	-	-	-
P	Transaction is Pending	-	-	-	-	-
R	Retry Limits Exceeded, Transaction Not Processed	-	-	-	-	-
T	Address Verification Failed	-	-	-	-	-
U	Card Security Code Failed	-	-	-	-	-
V	Address Verification and Card Security Code Failed	-	-	-	-	-

Address Verification Service (AVS) Response Codes

A security feature used for card not present transactions that compares the address entered by the cardholder with the records held in the card issuer's database. Once the transaction is successfully processed and authorised, the card issuer returns an address verification result code (AVS result code) in its authorisation response message verifying the level of accuracy that matched the card billing address. These result codes are mapped to the AVS result codes returned by the Payment Server.

The AVS result codes returned by the Payment Server are:

Table 30 Returned Response Codes Address Verification Service (AVS) Response Codes.

Acquirer		Payment Server	
Result Code	Description	Result Code	Description
A	Address matches, postal code does not.	A	Address match only.
B	Visa only: Street address match. Postal code not verified because of incompatible formats. (Acquirer sent both street address and postal code).	B	Address match, zip not verified.
C	Visa only: Street address and postal code not verified because of incompatible formats. (Acquirer sent both street address and postal code).	C	Address and zip not verified.
D	Visa: Street address and postal code match	D	Address and zip match.
	Amex: Card Member Name incorrect, Billing Postal Code match.	Z	5-digit zip match only.
E	Amex: Card Member Name incorrect, Billing Address and Postal Code match.	D	Address and zip match.
F	Visa: Street address and Postal Code match. Applies to U.K. only.	F	Address and zip match UK only).
	Amex: Card Member Name incorrect, Billing Address matches.	A	Address match only.
G	Visa only. Non-AVS participant outside the U.S.; address not verified for international transaction.	G	International transaction, address information unavailable.
I	Visa only. Address information not verified for international transaction.	I	Address not verified for international transaction.
K	Amex: Card Member Name matches.	K	Cardholder name match only.
L	Amex: Card Member Name and Billing Postal Code match.	L	Cardholder name and zip match.
M	Visa: Street addresses and Postal Codes match. Amex: Card Member Name, Billing Address and Postal Code match.	M	Address and zip match.
N	Neither address nor postal code matches.	N	No address or zip match.
O	Amex: Card Member Name and Billing Address match.	O	Cardholder name and address match.

Acquirer		Payment Server	
Result Code	Description	Result Code	Description
P	Visa only. Postal Codes match. Street address not verified because of incompatible formats. (Acquirer sent both street address and postal code).	P	Zip match, address not verified.
R	Retry, system is unable to process.	R	Issuer system unavailable.
S	AVS currently not supported. Amex: SE not allowed AAV function.	S	Service not supported.
U	No data from Issuer/authorisation system.	U	Address unavailable.
W	For U.S. addresses, 9-digit postal code matches, address does not; for address outside the U.S., postal code matches, address does not.	W	9-digit zip match only.
	Amex: No, CM Name, Billing Address and Postal Code are all incorrect.	N	No address or zip match.
X	For U.S. addresses, 9-digit Postal Code and Address match; for address outside the U.S., Postal Code and Address match.	X	Exact match, 9-digit zip.
Y	For U.S. addresses, 5-digit Postal Code and Address match.	Y	Exact match, 5-digit zip.
Z	For U.S. addresses, 5-digit Postal Code matches, Address does not.	Z	5-digit zip match only.

Card Security Code Response Code

The Card Security Code (CSC) is a 3 or 4 digit numeric identifier printed on either the signature panel on the back of the card or on the front of the card. For example, MasterCard and Visa use a 3 digit CSC on the signature panel on the back of the card and American Express has a 4 digit CSC on the front of the card.

It is a security feature used for card not present transactions that compares the Card Security Code entered by the cardholder with the records held in the card issuer's database. Once the transaction is successfully processed and authorised, the card issuer returns a result code (CSC result code) in its authorisation response message verifying the level of accuracy of the card security code provided.

By default the Payment Server only accepts a transaction when the CSC result code returned from the issuer is in the range of M to S. Depending on the Payment Provider, the merchant can nominate a new CSC card acceptance level range. For example if they decide they can accept an order with a CSC card result code of U, the Payment Server accepts transactions in a new range from M to U, instead of S.

The CSC result codes are:

Table 31 Card Security Code Response Code

Code	Description
M	Valid or matched CSC
S	Merchant indicates CSC not present on card
P	CSC Not Processed
U	Card issuer is not registered and/or certified
N	Code invalid or not matched

Card Type Code

The Card Type Code is a two-character field that identifies the card type that was used for the transaction.

Not all of these cards are available for all Payment Providers. Check with your Payment Provider as to which cards you can use.

The Card Type Field values are shown in the following table.

Table 32 Card Type Code

Code	Description
AE	American Express
DC	Diners Club
JC	JCB Card
MS	Maestro Card
MC	MasterCard
PL	Private Label Card
VC	Visa Card

External Payment Selection (EPS)

vpc_gateway Field and Values

The vpc_gateway field is used in External Payment Selection and determines what type of transaction is being performed. The field is case sensitive, and must comply with the valid gateways in the Payment Server as shown in the following table.

Table 33 External Payment Selection (EPS)

Code	Description
ssl	Specifies the gateway for all standard 3-Party transactions.
threeDSecure	Specifies the gateway for a 3-D Secure Mode 3a - 3-Party Style Authentication Only transaction.

Input 'vpc_card' Field and Values

The vpc_card field is used in External Payment Selection to select the card type that is to be used for the transaction.

The field is case sensitive, and must comply with each of the card types valid in the Payment Server. Please check with your Payment Provider as to which cards you can use.

The card field values are shown in the following table.

Table 34 Input 'vpc_card' Field and Values

Code	Description
Amex	American Express Credit Card
Dinersclub	Diners Club Credit Card
JCB	JCB Credit Card
Maestro	Maestro Debit Card
Mastercard	MasterCard Credit Card
PrivateLabelCard	Private Label Card
Visa	Visa Credit Card

To check these values, open the 3-Party card selection page in a browser, and move the cursor over each card logo. The vpc_gateway and vpc_card values are displayed in the status bar at the bottom of the browser.

Verified by Visa™, MasterCard® SecureCode™ and JCB J/Secure™ Status Codes

All authentication transactions use a vpc_VerStatus response code value to show whether the card authentication was successful or not. The vpc_VerStatus response code values are shown in the following table:

Table 35 vpc_VerStatus response code values

Code	Description
Y	Success - The cardholder was successfully authenticated.
M	Success - The cardholder is not enrolled, but their card issuer attempted processing.
E	Not Enrolled - The cardholder is not enrolled.
F	Failed - An error exists in the request format from the Merchant.
N	Failed - Verification Failed.
S	Failed - The signature on the response received from the Issuer could not be validated. This should be considered a failure.
P	Failed - Error receiving input from Issuer.
I	Failed - Internal Error.
U	Undetermined - The verification was unable to be completed. This can be caused by network or system failures.
T	Undetermined - The cardholder session timed out and the cardholder's browser never returned from the Issuer site.
A	Undetermined - Authentication of Merchant ID and Password to the Directory Failed.
D	Undetermined - Error communicating with the Directory Server.
C	Undetermined - Card brand not supported.

Authorisation Response Data

Authorisation response data is additional data returned by the issuer during the authorisation process of a transaction. This data should be included in capture requests processed through an external system where applicable. When captures are processed through the Payment Server, this data is automatically included with the capture request as needed.

You can control the receipt of authorisation response data in the Transaction Response using the field vpc_ReturnAuthResponseData in the Transaction Request for both authorisation and purchase transactions. The received response data varies based on the card schemes, as shown in the following table:

Note: A tick (✓) indicates the field is returned for that card scheme.

Code	Visa	MasterCard	American Express
vpc_ReturnACI	✓	×	×
vpc_TransactionIdentifier	✓	✓	✓
vpc_CommercialCardIndicator	✓	✓	×
vpc_CardLevelIndicator	✓	×	×
vpc_FinancialNetworkCode	×	✓	×

The Commercial Card field, vpc_CommercialCard, generated by the Payment Server, indicates if the card was identified by the issuer as a commercial card, based on the response returned from the issuer in the Commercial Card Indicator field, vpc_CommercialCardIndicator, as shown in the following table:

vpc_CommercialCardIndicator		vpc_CommercialCard	
Code	Description	Code	Description
0 (zero)	Decline or not a Commercial Card	N	Not a Commercial Card
B	Business Card	Y	Commercial Card
R	Corporate Card	Y	Commercial Card
S	Purchasing Card	Y	Commercial Card
1	Consumer Card	N	Not a Commercial Card
2	Commercial Card	Y	Commercial Card
3	Both	U	Undetermined
Other	Undefined	U	Undetermined

Note: Codes 1-3 are returned only for MasterCard cards. Codes 0-S are returned for Visa cards.

Card Present Data

The Payment Server supports both EMV and Contactless Card Present transactions.

EMV stands for Europay MasterCard Visa, a smart card standard for financial chip cards. EMV cards are a type of smart card which offers a more secure payment through an embedded microchip. The card details can be obtained using a chip reader, magnetic stripe reader or manually entering the card details into the system. The first two methods of obtaining card details are a benefit to the merchant as it helps to minimise fraud through the presence of the card. EMV card transactions contain extra data fields such as Point of Sale (POS) Entry Type, Card Sequence Number and Integrated Circuit Card (ICC) Data, sent through in the message to the acquirer.

With contactless transactions, a chip in the card communicates with the card reader through RFID. Only close proximity to the card reader is required without having to swipe/insert the card, or enter a PIN, or sign a credit card slip. Contactless payments are used to process transactions quickly or hands-free and are generally used for low value transactions.

Note: Contactless Card Present payments do not apply to Standalone Capture or Standalone Refund transactions. They are only supported with MasterCard card types.

Card Present Data Codes

Card Present Transaction Type	Supported values for vpc_POSEntryMode	vpc_TerminalInput Capability	Mandatory Fields
EMV	052	CM, CKM, C	vpc_EMCVICCData, vpc_CardSeqNum, vpc_POSEntryMode, vpc_CardTrack2
	792	CM, CKM, C	-
	802	CM, CKM, C	vpc_POSEntryMode, vpc_CardTrack2
Contactless	072	CX (if supplied)	vpc_EMCVICCData, vpc_CardSeqNum, vpc_POSEntryMode, vpc_CardTrack2
	912	MX (if supplied)	vpc_POSEntryMode, vpc_CardTrack2

Note: The contents of vpc_CardTrack2 must match the PAN and expiry fields included in the Transaction Request. For EMV transactions, the data included on the chip is referred to as Card Track 2 data even though it's not read from a track on a magnetic stripe.

Error Codes

In an unsuccessful transaction with a vpc_TxnResponseCode of "7", an error description may be contained in the field **vpc_Message** to describe the reason for the error.

The format of the error message is:

E**<error number>-<Date/Time Stamp MMDDHHMM>**: **<error description>**

For example: Where the error code is "5431" and the error description is "Invalid Field : CardNum", the full error message returned is;

"**E5431-08131458: Invalid Field : CardNum**"

The common errors that a merchant may encounter are listed in the table below followed by a complete list of error codes that may be returned.

Error Codes and Their Descriptions for the Most Commonly Encountered Errors

Error Number	Description
5001	Invalid Digital Order
5004	Invalid Digital Order: invalid session ID
5005	Invalid Digital Order: invalid Merchant Id
5006	Invalid Digital Order: invalid purchase amount
5007	Invalid Digital Order: invalid locale
5050	Invalid Permission
5061	Unsupported payment method
5065	Runtime exception
5121	Try to access an invalid key file
5134	RSA Decrypt Failed
5135	RSA Encrypt Failed
5231	Retrieved Digital Receipt Error
5423	Bad User Name or Password
5425	Invalid Recurring Transaction Number
5426	Invalid Permission
5433	Invalid Permission
5435	Max No of Deferred Payment reached
5436	Invalid recurring transaction number

The complete list of Error Codes and their descriptions are:

Error Number	Description
5000	Undefined error
5001	Invalid Digital Order
5002	Invalid Digital Order: not enough fields
5003	Invalid Digital Order: too many fields
5004	Invalid Digital Order: invalid session ID
5005	Invalid Digital Order: invalid Merchant Id
5006	Invalid Digital Order: invalid purchase amount
5007	Invalid Digital Order: invalid locale
5008	Invalid Digital Order: outdated version
5009	Invalid Digital Order: bad or too many Transaction Request parameters. It could be one of the following: ▪ Invalid Digital Order: Invalid PAN Entry Mode ▪ Invalid Digital Order: Invalid PIN Entry Capability ▪ Bad Credit Payment Type ▪ Bad Account Balance Type ▪ Unsupported Transaction Type ▪ Invalid Digital Order: Invalid Payment Method ▪ Invalid Digital Order: Invalid PIN field ▪ Invalid Digital Order: Invalid KSN field ▪ Invalid Digital Order: Invalid STAN field ▪ Invalid Digital Order: Invalid PhysicalTerminalId field ▪ Invalid Digital Order: Invalid POSEntryMode field ▪ PIN Entry Capability Terminal Cannot Accept PIN ▪ PIN Entry Capability Terminal PIN pad down ▪ Authorisation Code must be provided ▪ Authorisation Code must be numeric and 1 to 6 characters in length
5010	Bad DCC Base Amount
5011	Bad DCC Base Currency
5012	Bad DCC Exchange Rate
5013	Bad DCC Offer State
5014	DCC Offer State Unsupported
5015	Missing or Invalid Currency
5016	Missing or Invalid Merchant Transaction Reference
5020	Invalid Digital Receipt
5021	Invalid Digital Receipt: not enough fields
5022	Invalid Digital Receipt: too many fields

Error Number	Description
5023	Invalid Digital Receipt: invalid session ID
5024	Invalid Digital Receipt: invalid Merchant Id
5025	Invalid Digital Receipt: invalid purchase amount
5026	Invalid Digital Receipt: invalid locale
5027	Error in generating Digital Receipt ID
5028	Invalid Digital Receipt Delivery URL
5029	Invalid Digital Receipt Delivery IO
5030	Invalid Transaction log string
5031	Invalid Transaction log string: not enough fields
5032	Invalid Transaction log string: too many fields
5033	Invalid Transaction log string: invalid purchase amount
5034	Invalid Transaction log string: invalid locale
5035	Transaction Log File error
5040	Invalid QsiFinTrans message
5041	Unsupported acquirer
5042	Unsupported transport
5043	Unsupported message format
5044	Invalid Merchant transaction mode
5045	Unsupported transaction counter
5046	SecureCGIParam verification of digital signature failed
5047	Failed to read a QsiSigner object back from a serialized file!
5048	Failed to create a DCOM object
5049	Receipt is invalid.
5050	Invalid Permission
5051	Unsatisfied DLL link error
5052	Invalid Merchant Id
5053	Transmission error from QSIFinTrans
5054	Parser error
5055	Acquirer Response Error
5056	Trace file I/O error
5057	Invalid cookie
5058	RMI exception
5059	Invalid session
5060	Invalid locale
5061	Unsupported payment method
5065	Runtime exception

Error Number	Description
5066	Bad parameter name or value
5070	File backup error
5071	File save error
5072	File IO error
5073	File not found error
5074	File not found
5080	SQL Error
5081	SQL Error : Cannot locate the database
5082	SQL Error : Cannot connect to the database
5083	SQL Error : Incorrect row count
5084	SQL Error : Invalid value format
5085	SQL Error : Bad line count
5086	Duplicate primary agent
5087	Unknown database type
5090	Illegal user name
5091	Illegal password error
5101	Could not create and load the specified KeyStore object. If you are using a QSIDB KeyStore the database connection may have failed
5103	Could not create the specified javax.crypto.Cipher object. You may not have a provider installed to create this type of Cipher object or the Cipher object that is specified in your config file is incorrect
5104	Error in call to javax.crypto.Cipher.doFinal. Either the input was too large or the padding was bad
5106	The Message type specified is not supported. Check the com.qsipayments.technology.security.MessageCrypto.properties file to ensure that the MsgType is valid
5108	The message received has a bad format
5109	Error verifying signature
5110	Error creating a signature
5161	Customer Reference too long
5175	Card track data exceeded the allowed lengths
5120	Unable to generate new keys
5121	Try to access an invalid key file
5122	Not able to store the security keys
5122	Not able to store the security keys
5123	Not able to retrieve the security keys
5124	Encryption format invalid for Digital Order
5125	Encryption signature invalid for Digital Order

Error Number	Description
5126	Invalid transaction mode
5127	Unable to find user keys
5128	Bad key Id
5129	Credit Card No Decryption failed
5130	Credit Card Encryption failed
5131	Problem with Crypto Algorithm
5132	Key used is invalid
5133	Signature Key used is invalid
5134	RSA Decrypt Failed
5135	RSA Encrypt Failed
5136	The keys stored in the keyfile given to SecureCGIParam was corrupt or one of the keys is invalid
5137	The private key stored in the keyfile given to SecureCGIParam was corrupt or one of the keys is invalid
5138	The public key stored in the keyfile given to SecureCGIParam was corrupt or one of the keys is invalid
5140	Invalid Acquirer
5141	Generic error for a financial transaction
5142	Generic reconciliation error for a transaction
5143	Transaction counter exceeds predefined value
5144	Generic terminal pooling error
5145	Generic terminal error
5146	Terminal near full
5147	Terminal Full
5148	Attempted to call a method that required a reconciliation to be in progress but this was not the case
5150	Invalid credit card: incorrect issue number length
5151	Invalid Credit Card Specifications
5152	Invalid Credit Card information contained in the database
5153	Invalid Card Number Length
5154	Invalid Card Number
5155	Invalid Card Number Prefix
5156	Invalid Card Number Check Digit
5157	Invalid Card Expiry Date
5158	Invalid Card Expiry Date Length
5162	Invalid Card Initialisation file
5166	Invalid Credit Card: incorrect secure code number length

Error Number	Description
5170	Unable to delete terminal
5171	Unable to create terminal
5161	Customer Reference too long
5175	Card track data exceeded the allowed lengths
5176	Bad Card Track, invalid card track sentinels
5185	Invalid Acknowledgement
5200	Payment Client Creation Failed
5201	Creating Digital Order Failed
5202	Creating Digital Receipt Failed
5204	Executing Administration Capture Failed
5205	Executing Administration Refund Failed
5206	Executing Administration Void Capture Failed
5207	Executing Administration Void Refund Failed
5208	Executing Administration Financial Transaction History Failed
5209	Executing Administration Shopping Transaction History Failed
5210	PaymentClient Access to QueryDR Denied
5220	Executing Administration Reconciliation Failed
5221	Executing Administration Reconciliation Item Detail Failed
5222	Executing Administration Reconciliation History Failed
5230	Retrieving Digital Receipt Failed
5231	Retrieved Digital Receipt Error
5232	Digital Order Command Error
5233	Digital Order Internal Error
5234	MOTO Internal Error
5235	Digital Receipt Internal Error
5336	Administration Internal Error
5400	Digital Order is null
5401	Null Parameter
5402	Command Missing
5403	Digital Order is null
5410	Unknown Field
5411	Unknown Administration Method
5412	Invalid Field
5413	Missing Field
5414	Capture Error
5415	Refund Error

Error Number	Description
5416	VoidCapture Error
5417	VoidRefund Error
5418	Financial Transaction History Error
5419	Shopping Transaction History Error
5420	Reconciliation Error
5421	Reconciliation Detail Error
5422	Reconciliation History Error
5423	Bad User Name or Password
5424	Administration Internal Error
5425	Invalid Recurring Transaction Number
5426	Invalid Permission
5427	Purchase Error
5428	VoidPurchase Error
5429	QueryDR Error
5430	Missing Field
5431	Invalid Field Digital.TRANS_NO must be provided to indicate which existing order this transaction is to be performed against
5432	Internal Error
5433	Invalid Permission
5434	Deferred Payment service currently unavailable
5435	Max No of Deferred Payment reached
5436	Invalid recurring transaction number
5450	DirectPaymentSend: Null digital order
5451	DirectPaymentSend: Internal error
5500	Error in card detail
5501	Errors exists in card details
5600	Transaction retry count exceeded
5601	Instantiation of AcquirerController for this transaction failed.
5602	An I/O error occurred
5603	Could not get a valid terminal
5604	Unable to create the ProtocolReconciliationController for the protocol
5661	Illegal Acquirer Object Exception
5670	Message Exception
5671	Malformed Message Exception
5672	Illegal Message Object Exception

Error Number	Description
5680	Transport Exception
5681	Transport type not found
5682	Transport connection error
5683	Transport IO error
5684	Illegal Transport Object Exception
5690	Permanent Socket Transport connected
5691	Permanent Socket Transport JII class exception
5692	Permanent Socket Transport mismatched message received
5693	Permanent Socket Transport malformed message received
5694	Permanent Socket Transport unavailable
5695	Permanent Socket Transport disconnected
5696	The connection has been closed prematurely
5730	Host Socket unavailable
5750	Message header not identified
5751	Message length field was invalid
5752	Start of text marker (STX) not found where expected
5753	End of text marker (ETX) not found where expected
5754	Message checksum (LRC) did not match
5800	Init service started
5801	Init service stopped
5802	Invalid entry
5803	Duplicate entry
5804	Parse error
5805	Executing task
5806	Cannot execute task
5807	Terminating task
5808	Task killed
5809	Respawning task
5810	Cron service started
5811	Cron service stopped
5812	Parse error
5813	Invalid entry
5910	Null pointer caught
5911	URL Decode Exception occurred
5930	Invalid card type for excessive refunds
5931	Agent not authorized to perform excessive refunds for this amount

Error Number	Description
5932	Too many excessive refunds apply to this shopping transaction already
5933	Merchant agent is not authorized to perform excessive refunds
5934	Merchant is not authorized to perform excessive refunds
5935	Merchant cannot perform excessive refunds due to its transaction type
6010	Bad format in Rulefile
6100	Invalid host name
7000	XML parser [Fatal Error]
7001	XML parser [Error]
7002	XML parser [Warning]
7003	XML Parameter is invalid
7004	XML Parameter had an invalid index. Check input .html file
7005	XML [Bad Provider Class]
7050	SleepTimer: Time value is not in a valid format (ignored this time value)
7100	No valid times and/or interval specified in StatementProcessing.properties file. Execution terminated
7101	Status file for this data file was never created – deleting
7102	Error loading Statement.properties file
7104	Can’t find file
7106	IOException thrown attempting to create or write to file
7107	Overwriting file
7108	SecurityException thrown when attempting to create output file
7109	Invalid Merchant Id. This Advice element will not be processed
7110	Can’t create file name from the given date string
7111	Duplicate Advice element found in input document and skipped. Check input document
7112	Invalid payment type specified. This file will be skipped
7113	Null directory: can’t create output file
7114	Validation of input file provided by host failed
7120	IOException thrown attempting to create or write to file
7121	IOException thrown while attempting to create a ZIP archive
7122	An inaccessible output directory was specified in the configuration file
7200	PRE Issue Id Error
7201	No Login User Object stored in session.
7202	Error Occurred while creating the merchant on the Payment Server.

Error Number	Description
7203	Logging out
7204	Error occurred while instantiating Payment.
7205	Error occurred while instantiating SSL Payment
7207	Error occurred while sending email
7208	Invalid Access. User is trying to access a page illegally.
7209	Invalid User Input.
7300	Error parsing meta data file
7301	Invalid field
7302	Field validator not present
7303	Validation of field failed
7304	Field not present in arbitrary data
7305	Mandatory field missing
7306	Date mask is invalid
7307	Error creating field validator
7308	Failed to update arbitrary data
7400	Invalid transaction type
7500	Record has changed since last read
8000	Invalid Local Tax Flag
8001	Local Tax Amount Equal to or Greater then Initial Transaction Amount
8002	Purchaser Postcode Too Long
8003	Invalid Local Tax Flag and Local Tax Flag Amount Combination
8004	Invalid Local Tax Amount
8015	Payment method must be EBT for a balance inquiry
8015	Invalid Digital Order: Invalid PaymentMethod
8016	Invalid Digital Order: Invalid PIN field
8017	Invalid Digital Order: Invalid KSN field
8019	Invalid Digital Order: Invalid PhysicalTerminalID field
8020	Invalid Digital Order: Invalid POSEntryMode field
8021	Invalid Digital Order: Invalid AdditionalAmount field
9000	Acquirer did not respond
9150	Missing or Invalid Secure Hash
9151	Invalid Secure Hash Type, or Secure Hash Type not allowed for this merchant
9152	Missing or Invalid Access Code
9153	Request contains more than one instance of the same field [FieldName]

Error Number	Description
9154	General merchant configuration error preventing request from being processed
9200	Missing or Invalid Template Number

6 Glossary

Term	Description
Access Code	An identifier that is used to authenticate you as the merchant while you are using the Virtual Payment Client. The access code is generated and allocated to you by Merchant Administrator.
Acquirer Bank	Where your business account is maintained and settlement payments are deposited. This is normally the same bank with which you maintain your merchant facility for your online credit card payments.
Bank	The bank with which you have a merchant facility that allows you to accept online credit card payments.
Capture	A transaction that uses the information from an authorisation transaction to initiate a transfer of funds from the cardholder's account to the merchant's account.
Card Token	The identifier for the stored card details that may be used later to refer to the card details to perform a payment.
Financial Institution (FI)	See Bank.
Issuing Bank	The bank or financial institution that issues credit cards to customers.
Merchant Administration	Allows you to monitor and manage your electronic transactions through a series of easy to use, secure web pages.
Payment Provider	Acts as a gateway between your application or website and the financial institution. It uses the Payment Server to take payment details (Transaction Request) from your cardholder and checks the details with the cardholder's bank. It then sends the Transaction Response back to your application. Approval or rejection of the transaction is completed within seconds, so your application can determine whether or not to proceed with the cardholder's order. Your Payment Provider may be your acquirer bank or a third party technology services provider.
Payment Server	Facilitates the processing of secure payments in real-time over the Internet between your application/website and the Payment Provider. All communications between the cardholder, your application, the Payment Server and the Payment Provider is encrypted, making the whole procedure not only simple and quick, but also secure.
Purchase	A single transaction that immediately debits the funds from a cardholder's credit card account.
RRN	The Reference Retrieval Number is a unique number generated by the Payment Provider for a specific merchant ID. It is used to retrieve original transaction data and it is useful when your application does not provide a receipt number.

Term	Description
Transaction Request	Also called the Digital Order (DO) and is a request from the Virtual Payment Client to the Payment Server to provide transaction information.
Transaction Response	Also called the Digital Receipt (DR) and is a response from the Payment Server to the Virtual Payment Client to indicate the outcome of the transaction.
Virtual Payment Client	The interface that provides a secure method of communication between your application and the Payment Server, which facilitates the processing of payments with your financial institution. It allows a merchant application to directly connect using HTTPS protocol in the merchant's choice of programming language.
Transaction	A combination of a Transaction Request and a Transaction Response. For each customer purchase or order, merchants may issue several transactions.