MasterCard Worldwide

Virtual Payment Client Integration Planner

July 2008
Software version: 3.1.18.0

Copyright

License Agreement

Trademarks

MasterCard Asia-Pacific (Australia)

Level 8, 100 Arthur Street

North Sydney, NSW 2060

Australia

www.mastercard.com

Contents

1 About Merchant 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 on-line store by using the functionality of the Virtual Payment Client.

It details the base 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 organization's help desk, the details of which are provided after 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.

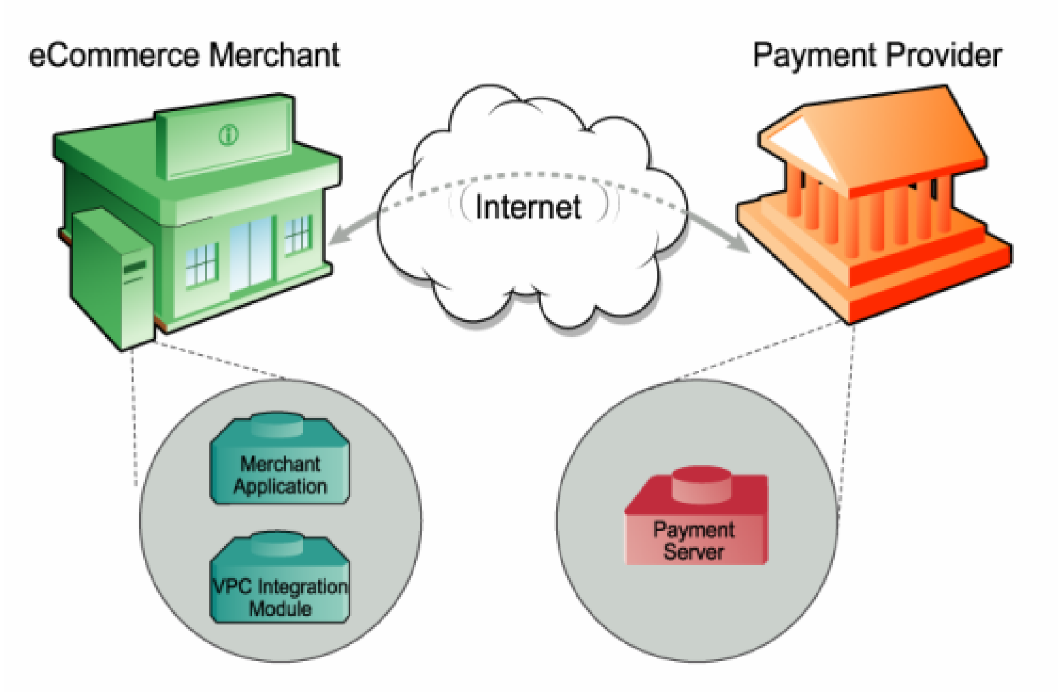
- MiGS Merchant Product Guide.
- MiGS Payment Client Integration Guide.
- MiGS Virtual Payment Client Guide.

2 Understanding e-Payments

What are e-Payments?

e-Payments are secure real time payments that transfer funds (using the Internet) between a cardholder and the merchant's financial institutions. e-Payments require secure communication between all components of the e-Payment process.

e-Payments are represented in the following diagram:



The Components of an e-Payment Solution

An end-to-end e-Payment solution is made up of the following components:

- **The Merchant application**—a business application or website on the merchant's system that uses Virtual Payment Client to process payments.
- **The Integration module**—a communication bridge between the merchant application and Virtual Payment Client.
- **Virtual Payment Client—**provides secure communication between the merchant application and the Payment Server. Virtual Payment Client can be integrated with a number of systems including merchant

applications, Interactive Voice Response (IVR) systems, and integrated ERPs.

- **Payment Server**—processes merchant Transaction Requests.
- **The Payment Provider**—enables the merchant to accept payments online.

How e-Payments Transfer Funds

e-Payments transfer funds using the following steps:

1. The cardholder purchases goods or services from the merchant (for example, in person, using the Internet, or over the phone).
2. The merchant application sends a Virtual Payment Client Transaction Request (via the Payment Server) to the merchant's Payment Provider.
3. The merchant's Payment Provider directs the request to the cardholder's bank.
4. The cardholder's bank debits the cardholder's account and transfers the funds to the merchant's account at the merchant's Payment Provider.

About e-Payment Information Flows

This section describes how information is transferred between the merchant application and the Payment Server.

The Merchant Application

To process a payment, the merchant application must send the required information to the Payment Server. The merchant application must create a message in a specified format to send this information using the Virtual Payment Client, which is part of the Payment Server using two messages:

- **Transaction Request** is sent to the Virtual Payment Client in the Payment Server to provide transaction information.
- **Transaction Response** is returned from the Payment Server using the Virtual Payment Client to indicate the outcome of the transaction (that is, successful or otherwise).
- A **Transaction** is the combination of a Transaction Request and a Transaction Response. For each customer order, merchants may issue several transactions.

The Virtual Payment Client

- Receives the Transaction Request from the merchant application; and
- Sends the information to the Payment Server

- The Virtual Payment Client receives the result from the Payment Server, creates a response in the appropriate format and forwards it to the Merchant Application.

Payment Models

Virtual Payment Client supports the most commonly used payment models in the e-Payments process. These are include the Authorisation/Capture model..

Payment Integration models are described in *Preparing for Integration* on page 10.

Purchase Model

Purchase is the most common type of payment model used by merchants to accept payments. A single transaction is used to authorise the payment and initiate the debiting of funds from a cardholder's credit card account.

This is typically used when the goods are delivered immediately after a successful transaction.

Authorisation/Capture Model

The authorisation/capture payment type is a two step process. The merchant uses an Authorisation transaction to reserve the funds.

Authorisation in the Auth/Capture Model

The Authorisation (Auth) transaction verifies that the card details are correct and may or may not also reserve the funds, depending on the merchant's Payment Provider. To find out what models are available to you, contact your Payment Provider.

The authorisation is used to ensure that the cardholder has sufficient funds available against their line of credit. The full amount of the order is sent to the card Issuing Bank to verify the details against the cardholder's card account. The authorisation does not debit funds from the cardholders account, but reserves the total amount, ready for the capture transaction to debit the card and transfer the funds to your account.

The cardholder's credit limit is reduced by the authorised amount. If they make another transaction, this current authorisation transaction is taken into account and comes off the cardholder's available funds as though the transaction had already taken place. This authorisation reserves the funds for a predetermined period of time, (such as 5–8 days), as determined by the card scheme and the cardholder's card issuing rules.

The API does not have a method to void an Authorisation transaction so it must fade out at the end of the appropriate period. Authorisation transactions do not appear in the cardholder's account records, only the capture transactions appear.

The Authorisation transaction uses the same API as the standard payment transaction used in the Purchase model where a Capture transaction is not required. The only difference is how the merchant profile is configured with the Payment Provider.

Pre-Authorisation/Purchase Mode

This is a variation of the Authorisation/Capture process where your Payment Provider verifies the card details with the card issuing institution, and if the transaction were carried out at this exact point in time whether the transaction would be successful. No funds are reserved on the cardholder's account.

If the cardholder performed another transaction between the pre-authorisation transaction and the purchase transaction that used up all the available funds on the card, then the later purchase transaction may fail due to lack of funds (if applicable). The merchant must include the full amount in their Pre-authorisation transaction as the Payment Server uses it to ensure that later Purchase transactions do not exceed the total amount specified in the Pre-authorisation transaction.

The Pre-Authorisation and Purchase transactions in this mode use exactly the same API as the Authorisation/Capture transactions outlined earlier. The only difference is how the merchant's Payment Provider actions the two transactions.

Nominal Auth/Purchase Mode

This is a variation of the Pre-authorisation/Purchase model where the Payment Server strips the value in the Authorisation transaction and substitutes a nominal transaction value. The acquiring bank checks the card details with the issuing card institution to ensure they are correct. No funds at all are reserved on the card. The merchant must include the full amount in their Nominal Authorisation transaction as the Payment Server uses it to ensure that later Purchase transactions do not exceed the total amount specified in the Nominal Authorisation transaction.

The Nominal Auth/Purchase transactions in this mode use exactly the same API as the Authorisation/Capture transactions outlined earlier. The only difference is how the merchant's Payment Provider actions the two transactions.

Capture in the Auth/Capture Model

The capture transaction refers back to the initial authorisation transaction, and transfers the funds from a cardholder's card into the merchant's account.

The merchant can perform any number of capture transactions on the original authorisation transaction, however the total of all the amounts from all the captures cannot exceed the original authorised amount. For example, the merchant may not have the full ordered amount of goods in stock. Hence they ship what they do have and capture the funds from the cardholder accordingly. Later when the remaining goods are shipped the merchant performs another capture transaction that refers back to the same initial authorisation transaction. This causes the remaining funds to be transferred from the cardholder's account to the merchant's account. The capture transactions will be successful, provided:

- The total amount for the all captures do not exceed the original Authorisation amount, and
- The card issuing institution has not expired the original Authorisation transaction.

3 Preparing for Integration

Before you start integrating, you must determine if your Payment Provider supports the functions that you require. This will determine the transaction types you can or cannot integrate.

Integration Models and Communication Methods

There are two ways that you can communicate with the Payment Server to process transactions, the Redirect method and the Direct method. The method you choose is directly related to the Integration Model, either or 2-Party, that you use. You may use both methods concurrently if necessary, for example, you may have a Web Store that uses , and at the same time a Call Centre taking phone orders using 2-Party. Both applications could be using the Payment Client at exactly the same time.

3-Party Payments Integration Model

3-Party Payments allow the Payment Server to manage the payment pages and collect the cardholder's card details on your behalf. The Payment Server's payment pages could be Bank or Payment Provider branded to help assure the cardholder of a secure transaction. The advantage of 3-Party payments is that the complexity of securely collecting and processing card details is handled by the Payment Server, allowing you to focus on your application's part of the payment process.

However, 3-Party Payments do also allow you to collect card details on your web site and pass them through with the other transactional details. If this is done the Payment Server does not display any 3rd party branded pages, keeping the branding consistent throughout the whole transaction, except the 3-D Secure pages if the merchant and the cardholder are both enrolled in this antifraud initiative. To do this you would have to comply with the same obligations associated with 2-Party payments.

The 3-Party Redirect method only works for web applications where a web browser is involved. This method is also required to implement 3-D Secure antifraud initiatives of Verifed by Visa™ and MasterCard SecureCode™. The redirect method works with most network configurations and you do not need to take into account proxy servers as the information is communicated to and from the Payment Server using the cardholder's Internet browser.

The cardholder's Internet browser is redirected to take the Transaction Request to the Payment Server to process the transaction. After processing the transaction, the cardholder's Internet browser is returned to a web page that you nominate in the transaction together with a Transaction Response. The Transaction Response processing of the receipt information finalises the transaction.

The 3 parties involved in a 3-Party transaction are the merchant, the payment provider and the cardholder. The cardholder's browser provides the redirect method to communicate the information between the merchant and the payment provider. This is an a-synchronous connection and the cardholder leaves your web site to go to the Payment Server, which means the transaction is broken or disrupted into 2 distinct sessions, the creation of the Transaction Request and the processing of the Transaction Response.

Because of this, you may be required to capture session variables and include them in the Transaction Request so they can be passed back appended to the Transaction Response for restoring the original web session.

2-Party Payments Integration Model

Merchants who want full control over the transaction and want to manage their own payment pages use the 2-Party integration model. Implementing 2-Party requires you to securely collect the cardholder's card details and then use the Virtual Payment Client to send the Transaction Requests directly to the Payment Server. This is also called the merchant-managed, or direct model. This model means that you are responsible for securing the cardholders card number and details.

The 2-Party does not allow you to implement the 3-D Secure anti-fraud initiatives of Verifed by Visa™ and MasterCard SecureCode™.

The 2 parties involved in a 2-Party transaction are the merchant and the payment provider. The merchant communicates directly through the Virtual Payment Client to the Payment Server and back again. This is a synchronous connection and the cardholder does not leave your site, which means the session is not broken or disrupted.

The Direct method is also used for advanced Payment Server operations such as captures, refunds, voids and queries. Your application communicates to the Payment Server via the Virtual Payment Client, so you need to take into account working with proxy servers.

The methods used to work with these proxy servers will vary slightly depending on the programming language used by your application.

Selection Guidelines for Integration Models

Use the following guidelines to select an integration model, depending on your application, preferred communication method, security needs, and future plans.

When to use 3-Party Payments

Consider using 3-Party Payments if:

- You are integrating a web browser-based application only. Call centres, IVRs and other applications cannot use this transaction mode.
- You want to, either now or in the future, increase security by using 3-D Secure authentication (for example, Verifed by Visa™ and MasterCard SecureCode™).
- It is acceptable to have the cardholder's browser redirected away from your web site to the Payment Server.
- You want the Payment Provider to collect and manage the cardholder's card details and to manage the associated security and privacy issues.
- It is acceptable to display Payment Provider-branded pages in the payment flow.

Note: If you require branding to be consistent throughout a transaction, you can collect card details and include them into the Transaction Request. However the higher risk and responsibility of collecting card details remains the same as in a 2-Party transaction.

When to use 2-Party Payments

Consider using 2-Party Payments if:

- You are willing to collect card details and manage the associated security and privacy issues. (VISA AIS, MasterCard SDP and so forth).
- You are integrating an application with the Virtual Payment Client (for example, web, call centre, billing application, Interactive Voice Response (IVR) system) that does not use 3-D Secure authentication (for example, Verifed by Visa™ and MasterCard SecureCode™). For more information see *Payment Authentication* in the VPC Integration Guide.
- You do not want the cardholder's browser to be redirected away from your web site to the Payment Server for payment processing.
- You do not want to display Payment Provider-branded pages in the payment flow.

When to combine 3-Party and 2-Party Payments

Consider using both 2-Party and 3-Party if any of the following are true:

- You want to use a combination of 3-Party for Web and 2-Party for call centre/IVR/other applications.
- You have a web application in which you want to perform some form of repeat payment, as in a subscription, where you want to take advantage of 3-D Secure authentication for the first payment and then use 2-Party payment transactions for each subsequent installment payment. (You must capture and store the card details to do this).

- You are willing to use 3-Party transactions for payments and are also using other transactions like refunds and queries, which are all 2-Party mode transactions.

Note: If you are collecting card details and want to implement 3-D Secure authentication, you only need to perform transactions for those transactions that require 3-D Secure authentication like MasterCard and Visa. Other transactions that don't use 3-D Secure authentication such as Bankcard and American Express can be performed using 2-Party transactions as they don't support Authentication.

Note: Advanced Merchant Administration functions such as captures, refunds, voids and queries all use the 2-Party style of transaction, so if you need to use any of these transaction types through the Virtual Payment Client, you will also need to install the Virtual Payment Client with the 2-Party options installed. These operations, captures, refunds, voids and queries carry no higher risk than as you do not need to pass in cardholder card information to carry out these transaction types.

4 Advanced Function Compatibility Matrix

The following table lists the common functions available on the Payment Server and the compatibility of functions the merchant can use. To determine the functionality that can be included in a Transaction Request choose a function in a column and follow it down to the appropriate row.

✓ Enabled for this transaction type or compatible with this feature.

× Not enabled for this transaction type or not compatible with this feature

Table 1 Advanced Function Compatibility Matrix

Supplementary Feature Compatibility	Address Verification	Card Security Code	Ticket Number	External Payment Selection	Card Details in 3-Party	3-D Secure Authentication & Payment	Card Present	CPC 2
2-Party Transaction	✓	✓	✓	×	×	×	✓	✓
3-Party Transaction	✓	✓	✓	✓	✓	✓	×	✓
Address Verification	🟦	✓	✓	✓	✓	✓	✓	✓
Card Security Code	✓	🟦	✓	✓	✓	✓	✓	✓
Ticket Number	✓	✓	🟦	✓	✓	✓	✓	✓
External Payment Selection	✓	✓	✓	🟦	✓	✓	×	✓
Card Details in 3-Party	✓	✓	✓	✓	🟦	✓	×	✓
3-D Secure Authentication & Payment	✓	✓	✓	✓	✓	🟦	×	✓
Card Present	✓	✓	✓	×	×	×	🟦	✓

Suggested Merchant Actions

Table 2 Suggested Merchant Actions

Acq Resp Code	Recur Resp Code	Merchant Advice Description	Examples of reason for decline	Suggested Merchant Action
DE39	DE48 SE84			
00 05 14 51 54	01	New account information available	• Expired card • Account upgrade • Portfolio sale • Conversion	Obtain new account information before next billing cycle.
51	02	Try again later	• Over credit limit • Insufficient funds	Recycle transaction 72 hours later.
05 14 51 54	03	Do not try again	• Account closed • Fraudulent	Obtain another type of payment from customer.

Optional DO Fields for 2-Party Payment Requests

The optional fields that can be included in a DO when using 2-Party Payments are shown in the following table.

Table 3 Optional DO Fields for 2-Party Payment Requests

Field Name	Required Optional Input	Field Type	Length	Example Value
Card Security Code (CSC) - Optional DO Fields				
The Card Security Code (CSC) is a security feature used for card not present transactions that compares the Card Security Code on the card with the records held in the card issuer's database.				
vpc_CardSecurityCode	The Card Security Code (CSC) is a security feature used for card not present transactions that 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 verifying the CSC level (vpc_CSCLevel) of accuracy used to match the card security code.			
	Optional	Numeric	1,4	123
Ticket Number - Optional DO Fields				
vpc_TicketNo	This allows the merchant to include a ticket number, such as an airline ticket number in the DO. The ticket number is stored on the Payment Server database for that transaction. The ticket number value is not returned in the DR.			

	Optional	Alphanumeric - Special characters	1,15	AB1234
Merchant Transaction Source				
Merchant transaction source functionality 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 **addDigitalOrderField** supplementary command at the appropriate point as indicated in their transaction flows. The fields that need to be added to the Digital Order for transaction source are:				
vpc_TxSource	Allows the merchant to specify the source of the transaction. This can only be used if the merchant has their privilege set to use this command, otherwise the transaction is set to the merchant's default transaction source as defined by your Merchant Manager.			
	Optional	Alphanumeric	1,16	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.

Merchant Transaction Source Subtype (Merchant Transaction Frequency)	
The Merchant Transaction Source Subtype data is added to the Digital Order using the supplementary command: addDigitalOrderField("FieldName", FieldValue)	
vpc_TxSourceSubType	Allows the merchant to flag the subtype of transaction for the cardholder's order.

	Required	Alphanumeric	12	Must be one of the following values: **SINGLE** - indicates a single transaction where a single payment is used to complete the cardholder's order **INSTALLMENT** - indicates an installment transaction where the cardholder authorises the merchant to deduct multiple payments over an agreed period of time for a single purchase **RECURRING** - 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.

Manual Auth ID				
This field is used when the transaction has been manually □uthorized. For example, this feature allows merchants to complete a transaction that was returned by the Payment Server with a referral response. Receipt of a referral response will require the merchant to contact the issuer. The card holder may be required to provide additional information in order for the issuer to approve the transaction. The issuer would then provide a Manual Auth ID to the merchant indicating success of a Manual Auth. The fields that must be added to the DO to send the Manual Auth ID are:				
vpc_ManualAuthID	Optional	Alphanumeric	6	ABC678

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.

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

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

Regarding 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: Track 3 data is not supported.

For EMV transactions, **'CARDPRESENT'** is used. The other mandatory fields are: vpc_*EMVICCData*, *vpc_CardSeqNum*, *vpc_POSEntryMode*, and *vpc_CardTrack2*. Card types must be MasterCard or Visa.

Transaction Request Input Fields

Table 4   Transaction Request Input Fields

<table>
<tr><th colspan="4">vpc_CardTrack1</th></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
^1305101968114330001 840   ?;</td></tr>
</table>

<table>
<tr><th colspan="4">vpc_CardTrack2</th></tr>
<tr><td colspan="4">7 bit ASCII text representing the card track 2 data.</td></tr>
<tr><td>Optional</td><td>Alphanumeric</td><td>38,40</td><td>;5123456789012346=13051019681143384001?</td></tr>
</table>

<table>
<tr><th colspan="4">vpc_PaymentMethod</th></tr>
<tr><td colspan="4">Payment method used. It has 3 values as shown below.
<b>Note:</b> Check with your Payment Provider for supported payment methods.</td></tr>
<tr><td>Required</td><td>Alpha</td><td>3,6</td><td>One of the following:
CREDIT - Credit (default)
DEBIT - DEBIT
EBT - Electronic Benefits Transfer</td></tr>
</table>

vpc_POSEntryMode			
The first 2 characters define the actual PAN Entry Mode and the third character defines the PIN Entry Capability.			
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 **PIN Entry Capability** 0 - Unknown 1 - Terminal is PIN capable 2 - Terminal is not PIN capable 8 - Terminal PIN pad is down **EMV Transactions** 052 - PAN auto entry via chip 792 - 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 802 - 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.

Vpc_CardSeqNum			
The card sequence number for transactions where the data is read through a chip on the EMV card.			
Optional	Numeric	3	133

vpc_EMVICCData			
Data read through a chip on the EMV card, base 64 encoded			
Required	Alphanumeric	1,340	XyoCA0SCAlgAhAegAAAABBAQlQUAAACAAJoDBxEDn AEAnwlGAAAAEIFQnwMGAAAAAAAAnwkCAAKfEBIBE KAAACoAAC1jAAAAAAAAAP+fGgIDRJ8eCDE1MDAzNjI 3nyYlg4OCCwm2qYCfJwGAnzMD4CDInzQDXgMAnzUBI p82AgAOnzcEDvo2b59BAwExgZ9TAVIA

vpc_TxSource			
The source of the transaction. This must be set to CARDPRESENT if the merchant's default transaction source has not been configured to CARDPRESENT.			
Optional	Alphanumeric	11	CARDPRESENT

Transaction Response Output Fields

In addition to the standard output fields, the following optional fields are also returned in the Transaction Response for 2-Party transactions.

Table 5 Card Present output fields for 2-Party Payment Response

vpc_EMVICCData			
The value of the vpc_EMVICCData input field returned in the Transaction Response.			
Output	Alphanumeric	1,340	kQpfNkntBaTpPAAS

Optional DR fields for 2-Party Payment Response

The optional fields that may be included in a DR when using 2-Party Payments are:

Table 6 Optional DR fields for 2-Party Payment Response

Field Name	**Required Optional**	**Field Type**	**Length**	**Example Value**
Recurring Transaction				
vpc_RecurringResponseCode	The response for a recurring transaction. This is one of the following values: 01 - New Account Information Available 02 - Try again later 03 - Do not try again later for recurring payment transactions			
	Output	Alphanumeric	2	01

Returned Response Codes

The **vpc_TxnResponseCode** is a response code generated by the Payment Server that shows whether the transaction was successful. 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 can be determined by executing the DigitalReceipt.ERROR command. If this returns a response it is an error condition, not only if the transaction data is incorrect but it could also trigger an error value if the Payment Client generates a Java exception.

The response codes generated by the Payment Server are shown in the following table.

Table 7 Response codes generated by the Payment Server

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

Code	Description	S2I	S2A-ANZ	S2A-WBC	S2A-NAB	Description
		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
		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	-	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

Code	Description	S2I	S2A-ANZ	S2A-WBC	S2A-NAB	Description
		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
		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

Code	Description	S2I	S2A-ANZ	S2A-WBC	S2A-NAB	Description
		-	55	-	55	Incorrect PIN
		-	56	-	56	No card record
		-	57	-	57	Transaction not permitted to card holder
		59	59	59	59	Suspected fraud
		61	61	61	61	Exceeds withdrawal amount limits
		-	62	-	62	Restricted card
		-	63	-	63	Security violation
		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

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.	-	-	-	-	-
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.	-	-	-	-	-
C	Transaction Cancelled	-	-	-	-	-
D	Deferred Transaction	-	-	-	-	-
E	Transaction Declined - Refer to card issuer	01	-	-	-	Refer to card issuer
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)	-	-	-	-	-

Code	Description	S2I	S2A-ANZ	S2A-WBC	S2A-NAB	Description
N	Cardholder is not enrolled in 3D Secure (Authentication Only)	-	-	-	-	-
P	Transaction is Pending	-	-	-	-	-
R	Retry Limits Exceeded, Transaction Not Processed	-	-	-	-	-
S	Duplicate OrderInfo used. (This is only relevant for Payment Servers that enforce the uniqueness of this field)	-	-	-	-	-
T	Address Verification Failed	-	-	-	-	-
U	Card Security Code Failed	-	-	-	-	-
V	Address Verification and Card Security Code Failed	-	-	-	-	-
