ANZ EGATE™ VIRTUAL PAYMENT CLIENT

INTEGRATION NOTES

Contents

Purpose of notes

These notes are supplementary to the MIGS Payment Client Integration Guide (PCIG). The PCIG contains technical details of the Virtual Payment Client (VPC) interface which is a technical reference Guide to implementing VPC.

These notes are not written in lay terms and are aimed specifically at web developers, as a degree of technical knowledge is required to implement VPC.

If you are using a Shopping Cart with plug-in to ANZ eGate you do not need to refer to these integration notes, you simply need to ensure that the shopping cart includes the following:

- Merchant ID
- Access Code
- Secure Secret
  (this is only required if you are using Bank Hosted mode).

Please refer to the development documents of your Shopping Cart for instructions on how to do this, you probably will not require assistance from a web developer if your Shopping Cart has a plug-in to ANZ eGate.

For enquiries and support

You may find what you are looking for in the Frequently Asked Questions document included in the ANZ eGate kit.

If you require assistance at any stage, please contact ANZ on 1800 039 025 and have your Merchant ID or Job Number on hand. If you have a technical problem, you can email us at ANZeCommerceSupport@anz.com and include:

- A screenshot of the html page with all details loaded or a list of variable names and values you are attempting to send
- Details of any error message
- Your contact details
- The Job Number in the Welcome Email you received, or the Merchant Name.

Our team will review the error and contact you within 24 hours.

Contents of ANZ eGate kit

Along with these notes and the PCIG, the ANZ eGate kit also contains five different sets of Sample Codes. Which set of Sample Codes you need to use will depend on the scripting language you are using to develop the merchant's website.

Sample Codes

The Sample Codes have been zipped so you will need to open one of the following files to access the individual Sample Codes:

3 Party SHA256 JSP
3 Party SHA256 ASP.NET (#C)
3 Party SHA256 PHP
2 Party VPC_JSP
2 Party VCP_ASP
2 Party VPC_PERL
2 Party VPC_PHP
2 Party VPC_ASP.NET(#C)

Note that 3 Party is also referred to Bank/Server Hosted and 2 Party is referred to Merchant Hosted

Bank Hosted, Merchant Hosted and Merchant Hosted with Verified by Visa and MasterCard® SecureCode

Once you have selected the correct zip file according to your scripting language, you must then select the correct files depending on whether the Merchant has chosen to implement ANZ eGate in Bank Hosted mode, Merchant Hosted mode, or Merchant Hosted mode with Verified by Visa (VbV) and MasterCard SecureCode (MCSC).

Bank Hosted mode

Bank Hosted means that, after 'checking out' of the merchant's website, purchasers are re-directed to a secure page hosted by ANZ eGate to submit their card details. Then, following an 'approved' or 'declined' message the purchaser is returned to a results page on the Merchant's website. Bank Hosted mode is sometimes also referred to as Server Hosted mode.

The JSP and PHP codes will require for Bank Hosted mode are:

VPC 3 Party – this code sends the order details to the **VPC_3P_DO** page VPC_3_3Party_DO – this code initiates Secure Hashing and re-directs the purchaser to the secure page hosted by ANZ eGate to enter their card details. The DO page also serves to calculate a Secure Hash value based on the input details and an SHA256 routine. Please refer to the PCIG for details on this hashing routine.
VPC_3_3Party_DR – this code is for the page the purchaser will be returned to on the merchant's website after the transaction has been processed. This URL needs to be entered into the .html page.

The ASP.NET codes you will require for Bank Hosted mode are:

3 Party_Order.aspx - The HTML page for the Order Page
3 Party_Order.aspx.cs - The code behind the Digital Order page
3 Party_Order.aspx.designer.cs - Layout of the Order Page
3 Party_Receipt.aspx - The HTML page for the Receipt page

3 Party_Receipt.aspx.cs - The code behind the Digital Receipt page
3 Party_Receipt.aspx.designer.cs - Layout of the Receipt Page
PaymentCodesHelper.cs - Response code mapping table to assist digital receipt displays
VPCRequest.cs - .NET C# library which contains the communication with the Payment Gateway
Web.config - The configuration file which contains merchant's specific information.

Merchant Hosted mode

Merchant Hosted means that the merchant has a Secure Sockets Layer (SSL) page as part of their own website where the purchaser enters their card details. Card details are transmitted to the ANZ eGate server in the background via a secure, encrypted connection. If a merchant chooses to implement in this mode, they need to adopt appropriate card security measures including firewall and intruder detection software, regular scanning for viruses and worms, and they must ensure that their website does not store full card details.

Please note that if the merchant does not wish to use VbV and MCSC, please email the ANZ eGate team at ANZeCommerceSupport@anz.com and include your ANZ eGate Merchant ID and request to have Verified by Visa and/or MasterCard SecureCode turned off.

The codes you will require for Merchant Hosted mode are:

VPC_2P_CSC.html – this code sends the order details to the VPV_2P page.
VPV_2P_CSC – this code establishes the http secure connection, sends the card details and displays the results.

All modes:

In the 2 Party zipped files you will also find three codes that can be used for special features. Please discuss with the merchant before use as they may not require these features. The codes for the additional features are:

VPC_CAPT – this code is used to complete a Pre-Authorisation transaction
QueryDR – this code is used for automated queries of transaction outcomes, this is normally only used by high volume merchants
Refund – this code is used for system-generated refunds.

Approach to development and integration

ANZ Merchant Services recommend that the first step in integration is to load the ANZ eGate Sample Codes on to your Server, use these to get a successful transaction, then integrate these functions to the merchant's website.

As already indicated above, ANZ eGate cannot be implemented with simple html. Bank Hosted mode requires a higher scripting language to handle the sha256 hash routine required for authentication when purchasers are re-directed. Merchant Hosted mode should not be implemented in simple html because security details such as the Access Code should not be viewable in Source Code.

Obtaining the Merchant Access Code and Secure Secret

Before commencing any testing, you will need to obtain your Merchant Access Code. If you are implementing in Bank Hosted mode, you will also need to obtain your Secure Hash.

Please follow the steps below:

1 Contact ANZ Merchant Services on **1800 039 025** and quote the Job Number included in your Welcome Email to obtain your password.

2 You will then need to log onto the ANZ eGate Merchant Administration (MA) site https://migs.mastercard.com.au/ma/ANZAU. To log on you will need your Merchant ID from your Welcome Email and your password from step 1. The MA site will also require you to enter an Operator ID. To logon for the first time, please enter '**Administrator**' as your Operator ID.

3 When you are logged onto the MA site you will need to create a new Operator ID for future use. To do this, select the **Admin** tab from the top of the screen, then click Operators on the left. Select **Create Merchant Administration Operator**. You must ensure that you create this Operator ID with the privilege level **May Modify Merchant Configuration**. You will also need to set a new password which must be at least 8 characters in length and contain alpha and numeric characters.

4 Once you have created a Merchant Administration Operator ID, log out of the MA site and log back on using the new Operator ID. Click the **Configuration** tab on the left of the screen.

5 You can now view the Access Code and Secure Secret in the Configuration Screen. Make a note of the Access Code and Secure Secret for use in development and integration. The Secure Hash value needs to go into the constant SECURE_SECRET in both the DO and DR pages.

In the case of the ASP.NET 3 party example this would be configured in the web.config file.

As you proceed with integration, you should ensure that the Merchant Access Code and the Secure Secret are extracted from configuration files or a separate database for additional security.

Once the ANZ eGate facility goes live, the Merchant Access Code and Secure Secret will change and the above steps will need to be repeated.

Each time the password for the Administrator Operator ID is reset by ANZ, it is reset for both the test and live Merchant ID. With this exception, all other Operator IDs and passwords are separately reset for test and live mode.

Testing – integrating and testing Sample Codes

There are two basic Reference Fields that can be sent through with each transaction to allow merchants to identify and reconcile transactions and three optional reference fields.

Basic:

vpc_OrderInfo – This is a required field and may have a maximum of 34 alpha numeric characters. This will appear in the Shopping Transactions Report on the MA site and is a searchable field so should be used as the primary reference number for transactions, for example the order number, invoice number, or customer number. This field label is **Transaction OrderInfo** in the Sample Code.

vpc_MerchTxnRef – This is a required field and may have a maximum of 40 alpha numeric characters. This reference should be unique for each transaction attempt and is used for the Query DR function. This field label is **Merchant Transaction Reference** in the Sample Code.

Optional:

vpc_TicketNo – This is a further reference field that is stored in the transaction details and may have a maximum of 15 alpha numeric characters. This field label is **TicketNo** in the Sample Code.
vpc_anzExtendedOrderInfo – If you wish to use this field, you must first notify the ANZ eGate team at ANZ Merchant Services. This field is an additional reference field and may have a maximum of 108 alpha numeric characters. If this field is used, the first 36 characters appear in the Shopping Transaction Report and the full details are stored in the Transaction detail. This field label is **ExtendedOrderInfo** in the Sample Code.

If you only have one transaction reference we suggest you pass each value through both Reference Fields.

Bank Hosted

To process a transaction successfully, your Shopping Cart or billing application needs to create a secure POST string in the form

https://migs.mastercard.com.au/vpcdps?[FieldName1]=[FieldValue1]&[FieldName2] =[FieldValue2]&.....

It must also calculate and append the sha256 secure hash to the end of the post query string.

When preparing to process a transaction using the Sample Codes please refer to the following materials:

- The html sample input page for details on the correct field names
- Appendix 1 for explanation of the field values.

One possible approach for the JSP and PHP examples are to:

- Copy the Secure Secret into the constant SECURE_SECRET in the DO & DR pages
- Load the DO & DR pages on to your web server
- Change the POST action on the .html page to point to the DO page.
- Enter test transaction values into .html page and submit the transaction.

A possible approach for ASP.NET examples is to:

- Copy your Merchant ID, Access Code and Secure Secret into web.config file
- Copy the ASP.NET sample code to an app on IIS
- Load the 3Party_Order.aspx page from your IIS app in the browser
- Enter test transaction values into the displayed page and submit the transaction.

It is recommended that, after you successfully process a test transaction, you integrate the posting of the transaction data of the html form into an order confirmation page, and then integrate the DR page. The DR page is the page on your website that the purchaser will be returned by the ANZ eGate Payment Server once the transaction has been processed. Functions of the DR or Return URL should therefore include:

- Printable receipts for purchasers for an approved transaction
- An appropriate message for declines
- Functionality to save order details to a 'paid items' table
- And any other function the merchant's business may require, such as allowing download or access.

Merchant Hosted (with or without VbV and MCSC)

To process a transaction successfully, the merchant's Shopping Cart or billing application needs to create a secure POST string in the form

https://migs.mastercard.com.au/vpcdps?[FieldName1]=[FieldValue1]&[FieldName2] =[FieldValue2]&.....

When preparing to process a transaction using the Sample Codes please refer to the following materials:

- The .html sample input page for details on the correct field names
- Appendix 2 for an explanation of the field values

One possible approach is to:

- Load the main processing page to your server and change the post action of the .html input page to post to the main processing page
- Enter test transaction values into the html page and submit the transaction.

It is recommended that, after you have successfully processed a test transaction, that you integrate the posting of the transaction data of the html form into an order confirmation page. You can then integrate the response functions of the main processing page. Functions of the main processing page should include:

- Printable receipts for purchasers for an approved transaction
- An appropriate message for declines
- Functionality to save order details to a 'paid items' table
- And any other function the merchant's business may require, such as allowing download or access.

We suggest that you do a minimum of two tests for each of the amounts displayed in Figure 1 on page 8. You should then check the results of the pages as they are displayed, as well as checking results in the MA site and your system, if you are saving results. To find results in the MA site, log on then click on **'Merchant Admin Search'** then look under **'Order Search'**.

If a test transaction is successful, proceed to integrate the payment page functions into the look and feel of the merchant's website.

Testing – test transaction values and Response Codes

The ANZ eGate test system allows you to control the outcome of a test transaction by specifically selecting the last two digits of the transaction value. In a dollar value these digits correlate to the cents. Transactions can then be compared to our Response Codes to determine whether to return an approved, declined or error resulted.

Please note that only transactions in whole dollar amounts where the last two digits are both zeros will return an approved result. Most cent amounts will not correspond to a Response Code and will return a result of 'unspecified error' so please only use amounts from Figure 1 on page 7. You also need to use one of our test card numbers to get an approval.

The amount of a transaction must be converted into units of cents. For example, an amount of $1 must be entered as 100. If the amount was $100.50, this must be entered as 10050.

As a general rule, only transactions processed correctly within test parameters will return a result to the MA site. If an invalid field name or transaction value was used, the transaction will return a 'Payment Server 7' error and you will not see any transaction result in the Order Search screen.

Figure 1: Approved test amounts:

Response	Name	Amount
0	Transaction approved	$ XXX.00
1	Transaction could not be processed	$ XXX.10
2	Transaction declined - contact issuing bank	$ XXX.05
3	No reply from Processing Host	$ XXX.68*
4	Card has expired	$ XXX.33
5	Insufficient credit	$ XXX.51

* Because this test transaction value is designed to mimic a real system outage, you may not be able to process any test transactions for approximately 1-2 minutes after using a test value ending in .68.

Figure 2: Test card details to use are:

	Test Card Number	Expiry Date	Card Sec Code#
MasterCard	5123456789012346	05/21	123
MasterCard	5313581000123430	05/21	123
Visa	4005550000000001	05/21	123
Visa	4557012345678902	05/21	123
Amex	345678901234564	05/21	1234
Diners Club	30123456789019	05/21	123

#If the Card Security Code (standard set up) has been set as a mandatory field by the Bank, you may use any value such as 123 or 111, or 1234/1111 for AMEX cards.

Only use AMEX and Diners Club test cards if you have been approved by AMEX and/or Diners as a Merchant and the ANZ eGate support team have been advised of your AMEX/Diners Merchant Number. If the merchant profile has not been set up with these links the test transactions will fail.

Important Note: sufficient testing must be done with your test Merchant ID to ensure that your shopping application is handling approved, declined and error conditions appropriately.

ANZ eGate Response Codes

ANZ eGate returns two Response Codes for each transaction. These are the same for testing and when the ANZ eGate facility goes live.

Transaction Response Code

The Transaction Response Code (also known as the Grouped Code or QSI) shows the overall result of a transaction. The field name for the Transaction Response Code is vpc_TxnResponse.

QSI Resp	Description
0	Transaction approved
1	Transaction could not be processed
2	Transaction declined - contact issuing bank
3	No reply from Processing Host
4	Card has expired
5	Insufficient credit
6	Error Communicating with Bank
7	Message Detail Error
8	Transaction declined – transaction type not supported
9	Bank Declined Transaction – Do Not Contact Bank

Acquirer Response Code

This is the specific response from the card issuer.

Issuer Response	Description
0	Approved
1	Refer to Card Issuer
2	Refer to Card Issuer
3	Invalid Merchant
4	Pick Up Card
5	Do Not Honour
7	Pick Up Card
12	Invalid Transaction
14	Invalid Card Number (No such Number)
15	No Such Issuer
33	Expired Card
34	Suspected Fraud
36	Restricted Card
39	No Credit Account
41	Card Reported Lost
43	Stolen Card
51	Insufficient Funds
54	Expired Card
57	Transaction Not Permitted
59	Suspected Fraud
61	Daily limit with card
62	Restricted Card
65	Exceeds withdrawal frequency limit
91	Bank link error
92	Bank link error
96	Bank link error

Appendix 1 - Field values for Bank Hosted transactions

Virtual Payment Client URL

Always the same value for test and live transactions. This should be located in a configuration file or extracted from a database.

VPC Version

The value for this field is always 1 and is the same for test and live transactions.

Command Type

The value for this field is always 'pay' and is the same for test and live transactions. This should be located in a configuration file or extracted from a database.

Merchant Access Code

You need to log into the MA site to obtain this value. This value will be different for test and live transactions. This should be located in a configuration file or extracted from a database.

Merchant Transaction Reference

This is a unique reference number assigned by the merchant to the transaction for identification purposes.

Merchant ID

Your Merchant ID is supplied in your Welcome Email.

Purchase Amount

The amount of a transaction must be converted into units of cents. For example, an amount of $1 must be entered as 100. If the amount was $100.50, this must be entered as 10050.

Payment Server Display Language Locale

This value is always 'en_US' and is the same for test and live transactions.

Receipt ReturnURL

This is the URL that the purchaser will be returned to after a transaction has been completed. It should be located in a configuration file or extracted from a database.

Secure Hash Type

This is the function that is used to create the Secure Hash. This value needs to be set to SHA256.

Optional Ticket Number Field

This is an optional field that can store up to 15 alpha numeric characters.

Optional Transaction Source Subtype Field

Only use this field if you are implementing an application that mixes web shopping transactions and a phone order system. You must discuss the use of this field with the ANZ eGate team. If you are not using this field, please leave it as 'please select' or 'do not send this field'.

Appendix 2 - Field values for Merchant Hosted transactions

Virtual Payment Client URL

This is always the same value and is the same for test and live transactions. It is usually a hidden field.

VPC Version

This value is always '1' and is the same for test and live transactions.

Command Type

This value is always 'pay' and is the same for test and live transactions. It should be located in a configuration file or extracted from a database,

Merchant Access Code

You need to log into the MA site to obtain this value. This value will be different for test and live transactions. This should be located in a configuration file or extracted from a database.

Merchant Transaction Reference

This is a unique reference number assigned by the merchant to the Transaction for identification purposes.

Merchant ID

Your Merchant ID is supplied in your Welcome Email.

Purchase Amount

The amount of a transaction must be converted into units of cents. For example, an amount of $1 must be entered as 100. If the amount was $100.50, this must be entered as 10050.

Card Number

The card number must be without spaces or dashes. The field allows a maximum of 16 characters for Visa and MasterCard, 15 characters for AMEX and 14 characters for Diners. It is recommended that the input is limited to these lengths to prevent purchasers from using spaces or dashes when they enter card details.

Card Expiry Date

The expiry date must be in the YYMM format.

Card Security Code (CSC)

The Card Security Code is a number that is generally printed on the back of the card and should always be used for phone order or telephone sourced transactions. The CSC is 3 digits for all card types except American Express which are 4 digits. By default, we set this field as mandatory in the Merchant Profile. Please contact us to discuss if you believe this should not be mandatory.

Optional Ticket Number Field

This is an optional field that can store up to 15 characters. Most merchants do not use this field

Optional Transaction Source Subtype Field

Only use this field if you are implementing an application that mixes web shopping transactions and a phone order system. You must discuss the use of this field with the ANZ eGate team. If you are not using this field, please leave it as 'please select' or 'do not send this field'.

Appendix 3 - ANZ's requirements for displaying consumer information

In accordance with the Secure Internet Site Declaration agreed to by the merchant, ANZ will check for the following when testing a merchant's site prior to going live:

- Complete description of the goods or services offered
- Export or legal restriction(s), if applicable
- Delivery policy
- Consumer data/privacy policy
- Returned merchandise and refund policy
- Country of merchant's domicile is Australia
- Currency of transaction is Australian Dollars (AUD) only
- Disclosure of merchant's country of domicile at the time of presenting payment options to the cardholder
- Address of the merchant's permanent establishment must be the trading address
- Security capabilities and policy for transmission of payment card details where the merchant is collecting card information. If a merchant is using ANZ eGate in Bank Hosted mode, their website must state that card details are protected because customers are re-directed to a secure page hosted by ANZ eGate to enter their card details. If a merchant is using ANZ eGate in Merchant Hosted mode, details of the measures taken to protect card details during transmission and storage must be evident
- Customer Service contact is available. Must include an electronic mail address and telephone number
- Return page must clearly show a result and, if approved, a transaction or receipt number
- If Bank Hosted mode was used, the ANZ eGate payment page must not be embedded in the Merchant's website as this will generally have the effect of hiding the SSL padlock symbol.

We strongly recommend that part of the check out process/payment process is that Purchasers must tick a box to accept Terms and Conditions to proceed with payment. Where acceptance of the Terms and Conditions is a condition of purchase, the Terms and Conditions, including refund and delivery policies, must be available for viewing prior to acceptance of the Terms and Conditions. This provides supporting evidence that the cardholder has accepted terms and conditions in event of a dispute.

Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522. Australian Credit Licence Number 234527. Item No. 88477 06.2017 W577353

anz.com