



MiGS Virtual Payment Client

Guide to Errors and Frequently Asked Questions

23 October 2013

Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

Proprietary Rights

The information contained in this document is proprietary and confidential to MasterCard International Incorporated, one or more of its affiliated entities (collectively “MasterCard”), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of MasterCard.

Trademarks

Trademark notices and symbols used in this document 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.

Disclaimer

MasterCard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, MasterCard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not MasterCard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, MasterCard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

Translation

A translation of any MasterCard manual, bulletin, release, or other MasterCard document into a language other than English is intended solely as a convenience to MasterCard customers. MasterCard provides any translated document to its customers “AS IS” and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall MasterCard be liable for any damages resulting from reliance on any translated document. The English version of any MasterCard document will take precedence over any translated version in any legal proceeding.

Information Available Online

MasterCard provides details about the standards used for this document—including times expressed, language use, and contact information—on the Publications Support page available on MasterCard Connect™. Go to Publications [Support](#) for centralized information.

Troubleshooting Integration Errors

This section provides a brief explanation of the MasterCard Internet Gateway Service (MiGS), information useful for troubleshooting common integration errors, and some frequently asked questions.

About Integrating with MiGS	1
Common Integration Errors	1
vpc_Message=E5000: Merchant xxxxx does not have the required privilege to use the VirtualPaymentClient API.....	1
vpc_Message=E5000: Cannot form a matching secure hash based on the merchant's request using either of the two merchant's secrets.....	2
vpc_Message=E5000: No bank links are configured for merchant xxxxx	3
vpc_Message=E5009: Invalid Digital Order	3
vpc_Message=Unspecified Failure	4
Acquirer Response Code: 30	4
vpc_Message=E5432: Internal Error: Failed to perform transaction via payment engine.....	5
vpc_Message=No Value Returned.....	5
vpc_Message=E5028: Invalid Digital Receipt Delivery URL.....	6
Merchant ID must be unique, a merchant ID cannot be re-used if it has been previously deleted.....	7
vpc_Message=I5433: Invalid Permission: CardNum	7
vpc_Message=I5433: Invalid Permission: MOTO	8
vpc_Message=E5416: VoidCaptureError: Field in error: 'initialTransaction.orderNumber', value 'xxxxxxx' reason: Not a capture transaction.....	8
vpc_Message=E5431: Invalid Field: Card Security Code	8
vpc_Message=E5431: Invalid Field: No CSC Value Was Provided.....	9
vpc_Message=E5411: Unknown Administration Method: Invalid command: null vpc_TxnResponseCode=7.....	9
vpc_Message=E5415: Refund Error: Field in error: 'transaction amount', value '3500'—reason: Excessive refund attempted	10
vpc_Message=E5408: Failed to process transaction.....	10
vpc_Message=Merchant [xxxxxxx] does not exist.....	11
vpc_Message=E5062: Merchant does not support this payment type.....	11
Authentication State: A—Authentication Failed; Error Description: Merchant Not Participating.....	12
Frequently Asked Questions (FAQs).....	13
Why does the browser display a blank page?	13
Why can't I see the void capture button on the Merchant Administration page? I'm sure that the void privilege is enabled.	13

Why can't I see the void authorization button on the Merchant Administration page? I'm sure that the void privilege is enabled.....	13
How do I release the amount reserved or on hold in the cardholder's account after a successful authorization, when the transaction needs to be cancelled but settlement has not yet occurred?	13
How can a single merchant support multiple currencies?	14
How do I obtain a member's Verified by Visa certificate on MiGS?.....	15
How can a merchant provide a refund to a cardholder for a transaction that occurred through MiGS more than one year ago?	15
Why are some user IDs created for a Merchant ID unable to login to the Merchant Administration portal?	16
How can a merchant use dynamic descriptors—for example, type of service provided or other details—for inclusion in the cardholder statement?	16
How can a merchant generate different responses in the test environment to test the system for all possible cases?	17

About Integrating with MiGS

The MasterCard Internet Gateway Service (MiGS) is an Internet gateway solution for processing merchants' e-commerce and card not present (CNP) payment transactions. Acquirers and their merchants that are integrating their systems with MiGS sometimes may experience integration errors or have questions about integrating with the service. This guide provides examples of and potential solutions to common integration errors. Additionally, a list of frequently asked questions (FAQs) has been included.

Contact Us

Customers with questions about integrating with MiGS should contact MasterCard using the appropriate email address.

For customers in this region...	Send an email message to...
Asia/Pacific	migs_support@mastercard.com
Middle East/Africa	migs_support_mea@mastercard.com

Common Integration Errors

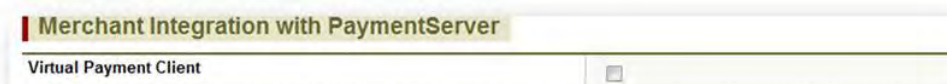
vpc_Message=E5000: Merchant xxxxx does not have the required privilege to use the VirtualPaymentClient API

VPC Transaction Response Code:	7
Transaction Response Code Description:	Payment Server System Error
Message:	E5000: Merchant [REDACTED] does not have the required privilege to use the VirtualPaymentClient API.

Solution performed by: Merchant Services Organization (MSO)

Solution steps:

Go to **Merchant Manager > Merchant Configuration page > Merchant Payment Details > Merchant Integration with Payment Server**. Then enable the option: **Virtual Payment Client**.



vpc_Message=E5000: Cannot form a matching secure hash based on the merchant's request using either of the two merchant's secrets

VPC Transaction Response Code:	7
Transaction Response Code Description:	Payment Server System Error
Message:	E5000: Cannot form a matching secure hash based on the merchant's request using either of the two merchant's secrets

Solution performed by: Merchant/PSP

Solution steps: There are multiple conditions that can cause this error. Consider the following when determining the appropriate solution.

1. This error can occur if you are not using the same Hash Secret in both the Digital Order and Digital Receipt integration code files. You can get your Secure Hash Secret from the Merchant Administration portal, under the Admin tab. Pay attention to white spaces that might exist while copying and pasting the string.

```
// To not create a secure hash, let SECURE_SECRET be an empty string - ""
// $SECURE_SECRET = "secure-hash-secret";
$SECURE_SECRET = "BxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxF";
```

2. Confirm that you are using the Secure Hash Type command **vpc_SecureHashType** when you are using the SHA-256 hashing method. It is not necessary to use this field with MD5 because MD5 is the default type.
3. Ensure that you are using the test Secure Hash Secret when sending your transactions to the Member Test Facility URL, and use the production Secure Hash Secret when sending your transactions to the production URL.
4. Keep in mind that the Access Code and the Secure Hash Secret of the production MID are different from the TESTMID, so mixing them will cause this Hash Mismatch error.
5. Before passing the parameters string to the hashing function, verify that the field names are sorted in ascending order of parameter name. Specifically, the sort order is as follows:
 - a. Ascending order of parameter name using the ASCII collating sequence; for example, "Card" comes before "card".
 - b. 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".

For more information about how to generate the Secure Hash, refer to the *MiGS Virtual Payment Client Integration Reference* that you were provided in the starter pack.

vpc_Message=E5000: No bank links are configured for merchant xxxxx

Solution performed by: Merchant Services Organization (MSO)

Explanation:

This error can occur when the acquirer link has not yet been configured for that Merchant ID or the acquirer link is disabled.

Solution steps:

Check the Acquirer Link Status.

Go to **Merchant Manager > Merchant Configuration page > Acquirer Link Details**. Then change the **Acquirer Link Status** option to either **Test only** or **Test and Production**.



vpc_Message=E5009: Invalid Digital Order

When performing an authorization request, you receive the following response:



Solution performed by: Merchant Services Organization (MSO)

Explanation:

This error occurs as a result of sending the same Merchant Transaction Reference for more than one transaction when the setting in Merchant Manager requires a unique Merchant Transaction Reference. This also applies for Order Reference, as shown in the following example.



Solution steps:

The merchant must send unique values, or the acquirer has to disable these settings.

vpc_Message=Unspecified Failure

When performing an authorization request, you receive the following response:

VPC Transaction Response Code:	1
Transaction Response Code Description:	Unknown Error
Message:	Unspecified Failure

Solution performed by: Merchant Services Organization (MSO)

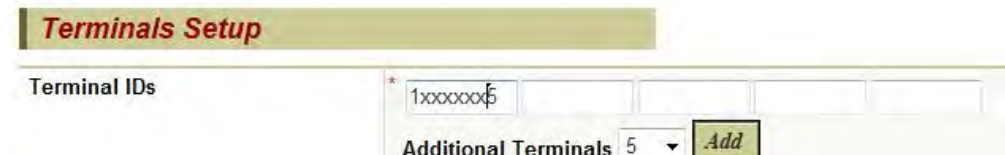
Explanation:

The most likely reason for this error is that the Terminal ID used for that merchant is wrong.

Solution steps:

Go to **Merchant Manager > Acquirer Link Details > Terminals Setup**.

Ensure that the Terminal IDs used are within the range of Terminal IDs assigned by MasterCard. If not, make the necessary changes where applicable, and approve the change.



The screenshot shows the 'Terminals Setup' section of a web application. It features a table with the header 'Terminal IDs' and several rows. The first row contains the text '1xxxxxx'. Below the table, there is a label 'Additional Terminals' followed by a dropdown menu showing the number '5' and an 'Add' button.

Acquirer Response Code: 30

When performing an authorization request, you receive the following response:

Declined

Response Code: 1 — Unspecified Failure

Acquirer Response Code: 30

Solution performed by: Merchant/Merchant Services Organization (MSO)

Explanation:

There are several reasons that you receive acquirer response code 30. Refer to the following.

Solution steps:

- **Format error:** Here the merchant is sending a value for a field in the wrong format. Check the format of your fields' values.
- **Terminal ID problem:** Check the Terminal IDs configured for your merchant ID in Merchant Manager
- **Issue in the Visa 3 Exponent Currency:** A VISA mandate says that you are not allowed to have any value other than 0 in the third decimal location of the currency for currencies that have three decimal places. For example, for the Kuwaiti Dinar, you are not allowed to send a value such as 10.123 KWD; instead, this currency should be expressed as 10.120 KWD.

For currencies with 3 decimal places, the last digit of the amount in fields 4, 28, 61.1, and 95.1 must be zero; that is, the amount must be rounded to two decimal places with a trailing zero.

NOTE

This rounding maintains compatibility with BASE II clearing messages, which do not support amounts with 3 decimals.

vpc_Message=E5432: Internal Error: Failed to perform transaction via payment engine

Solution performed by: Merchant

Explanation:

This error usually appears because either of the following issues have occurred.

- The merchant is sending data in some unexpected fields or not sending data in some required fields; for example, the option “Enforce CSC Entry” is enabled, but the merchant is not sending the Card Security Code value.
- The merchant is changing the transaction source without having the privileges to do so or is setting the source of the transaction to a value that is not allowed; for example, the merchant is specifying CardPresent as the transaction source when it is not an allowed source.

Solution steps:

Ensure that the fields are populated correctly and that the transaction source is allowed.

vpc_Message=No Value Returned

When performing a query for a transaction using the QueryDR function, you receive the following response:

VPC Transaction Response Code: No Value Returned
Transaction Response Code Description: Unable to be determined
Message: No Value Returned

Solution performed by: Merchant

Explanation:

There are three reasons that cause this error message:

1. You have entered an invalid Merchant Transaction Reference when you submitted your queryDR message.
2. The transaction you are searching for doesn't exist in the MiGS database.
3. You are searching for a transaction that is older than 5 days. Please note that the queryDR can retrieve transactions that are not older than 5 days.

Solution steps:

Please ensure that the Merchant Transaction Reference is valid and that the transaction is not older than 5 days.

vpc_Message=E5028: Invalid Digital Receipt Delivery URL

When performing an authorization request, you receive the following response:



An error has occurred processing your payment.

Undefined System Error
E5028-06182106: Invalid Digital Receipt Delivery URL

Solution performed by: Merchant/Developer

Explanation:

This error occurs as a result of supplying the wrong delivery return URL value in the field **vpc_ReturnURL** or by not including the prefix (http://) in front of the domain name. (For example, http://www.mastercard.com.)

Solution steps:

The merchant or developer must ensure that the delivery return URL value is correct and that the prefix is included in the domain name if appropriate.

Merchant ID must be unique, a merchant ID cannot be re-used if it has been previously deleted



Solution performed by: Merchant Services Organization (MSO)

Explanation:

The Merchant ID must be unique across the entire MiGS system. MasterCard recommends that you use a prefix that identifies your organization for all Merchant IDs. For example, if the MSO is called ANYBANK, the Merchant IDs could all begin with AB, such as AB0012345.

Solution steps:

Amend any Merchant IDs that are not unique.

vpc_Message=I5433: Invalid Permission: CardNum

When performing an authorization request, you receive the following response:

&vpc_Message=I5433: Invalid Permission: CardNum

&vpc_TransactionNo=0

&vpc_TxnResponseCode=7

Solution performed by: Merchant Services Organization (MSO)

Explanation:

This error may appear because the merchant is sending the card details in the request message while not having given the Card Details in Digital Order privilege to that Merchant ID.

Card Details In Digital Order



Solution steps:

Go to **Merchant Manager > Merchant Configuration page > Merchant Payment Details > Advanced**. Then enable the option: **Card Details In Digital Order**.

vpc_Message=I5433: Invalid Permission: MOTO

When performing an authorization request, you receive the following response:

&vpc_Message=I5433: Invalid Permission: MOTO

&vpc_TransactionNo=0

&vpc_TxnResponseCode=7

Solution performed by: Merchant Services Organization (MSO)

Explanation:

This error may appear because the merchant is performing a 2-party transaction (for example, void, refund, QueryDR, or capture) when the MOTO option (which allows the merchant to send to <https://migs.mastercard.com.au/vpcdps>) is not enabled.

Solution steps:

Go to **Merchant Manager > Merchant Configuration page > Merchant Payment Details > Gateways**. Then enable the option: **MOTO**.

vpc_Message=E5416: VoidCaptureError: Field in error: 'initialTransaction.orderNumber', value 'xxxxxxx' reason: Not a capture transaction

Solution performed by: Merchant

Explanation:

This error usually appears because the merchant is voiding a transaction that is not a capture transaction by providing the Transaction Number of some other transaction type.

Solution steps:

Ensure that the Transaction Number is correct for the Capture Transaction that you are trying to void.

vpc_Message=E5431: Invalid Field: Card Security Code

When performing an authorization request, you receive the following response:

vpc_Message=E5431: Invalid Field: Card Security Code

Solution performed by: Merchant

Explanation:

This error occurs as a result of sending the CSC number in a way that is incompatible with the card scheme. For example, sending a 3-digit CSC value for an AMEX card will return this error because AMEX has a 4-digit CSC.

Solution steps:

The merchant or developer must ensure that the CSC number value and format are correct.

vpc_Message=E5431: Invalid Field: No CSC Value Was Provided

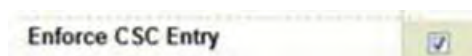
When performing an authorization request, you receive the following response:

vpc_Message=E5431: Invalid Field: No CSC value was provided

Solution performed by: Merchant Services Organization

Explanation:

This error occurs when the option **Enforce CSC Entry** is enabled, but the merchant does not send the CSC entry to MiGS in the digital order.



Solution steps:

Either the merchant must send the CSC number value, or the acquirer must disable this option.

To disable this option, go to **Merchant Manager > Merchant Configuration page > Merchant Payment Details > Advanced**. Then enable the option: **Enforce CSC entry**.

vpc_Message=E5411: Unknown Administration Method: Invalid command: null vpc_TxnResponseCode=7

When performing a Stand Alone Refund, you receive the following response:

vpc_Message=E5411: Unknown Administration Method: Invalid command: null vpc_TxnResponseCode=7

Solution performed by: Merchant Services Organization (MSO)

Explanation:

This error occurs when a merchant is trying to make a Stand Alone Refund, but the merchant does not have the Stand Alone Refund privilege enabled.

Solution steps:

Go to **Merchant Manager > Merchant Configuration page > Merchant Payment Details > Advanced**. Then enable the option: **Stand Alone Refunds**.



This feature may not be enabled by default for the Merchant Services Organization (MSO). The MSO can make a request for this feature to be enabled by contacting local MiGS support.

vpc_Message=E5415: Refund Error: Field in error: 'transaction amount', value '3500'—reason: Excessive refund attempted

When performing a Refund request, you receive the following response:

vpc_Message=E5415: Refund Error: Field in error: 'transaction amount', value '3500'—reason: Excessive refund attempted

Solution performed by: Merchant

Explanation:

This error occurs when a merchant is trying to process a refund, but the refund amount is greater than the transaction amount and the merchant does not have the Excessive Refund privilege enabled.

Solution steps:

Go to **Merchant Manager > Merchant Configuration page > Merchant Payment Details > Advanced**. Then enable the option: **Allow Excessive Refund**.

This feature may not be enabled by default for the Merchant Services Organization (MSO). The MSO can make a request for this feature to be enabled by contacting local MiGS support.

vpc_Message=E5408: Failed to process transaction

When performing a Void Authorization operation, you receive the following response:

vpc_Message=E5408: Failed to process transaction

Solution performed by: Merchant Services Organization (MSO)

Explanation:

This error occurs when a merchant is trying to void an authorization, but the merchant does not have the Void Authorization feature enabled.

Solution steps:

Select the option to enable Void Authorization.

This feature may not be enabled by default for the Merchant Services Organization (MSO). The MSO can make a request for this feature to be enabled by contacting local MiGS support.

vpc_Message=Merchant [xxxxxxxx] does not exist

When performing an authorization request, you receive the following response:

vpc_Message=Merchant [xxxxxxxx] does not exist

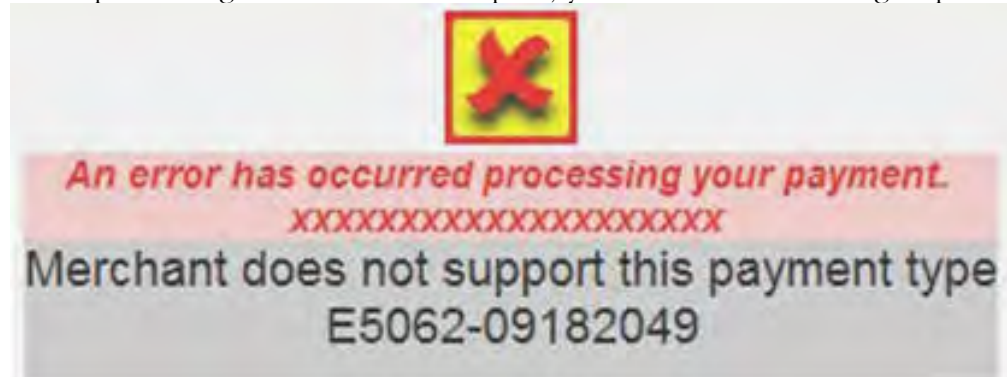
Solution performed by: Merchant Services Organization (MSO)

Explanation:

This error occurs when the Merchant ID (MID) sent in the message is incorrect or the acquirer has not yet created the Merchant ID.

vpc_Message=E5062: Merchant does not support this payment type

When performing an authorization request, you receive the following response:



Solution performed by: Merchant Services Organization

Explanation:

This error usually occurs because the merchant ID does not have the appropriate privilege enabled to use the particular payment type. For example, a merchant sending transactions as 3-party integration mode will receive this error if the merchant does not have the 3-party privilege enabled.

Solution steps:

Go to **Merchant Manager > Merchant Configuration page > Merchant Payment Details > Gateways**. Then enable the option: **3-party** or **MOTO** depending on the payment type used by the merchant.

Authentication State: A—Authentication Failed; Error Description: Merchant Not Participating

When performing an authentication request, you receive the following response:

Payment Authentication Details	
Authentication ID	3108811136
Date	20/11/12 3:14 PM
Order Reference	IN1111801655P700
Card Number	XXXXXXXXXXXXXXXXXX
Amount	USD \$1.00
Message Type	MasterCard SecureCode
Authentication State	A - Authentication Failed
Verification Security Level	07

Response Details	
Source	Directory Server
Message Type	Error Message
Error Message Version	1.0.2
Error Code	51
Error Detail	
Vendor Code	ARCOT SYSTEMS;
Error Description	Merchant not participating

Solution performed by: Acquirer

Explanation:

The error appears when the merchant is not registered with MasterCard *SecureCode* or is registered with incorrect details.

Solution steps:

The acquirer should register the merchant for MasterCard *SecureCode* using the merchant upload template. To request the merchant upload template, contact local MiGS Support.

Go to **Merchant Manager > Acquirer Link Details > MasterCard SecureCode Authentication Credentials**.

Ensure that the Merchant ID value provided on the *SecureCode* merchant upload template is the same value configured in MiGS.

Frequently Asked Questions (FAQs)

Why does the browser display a blank page?

Solution performed by: Merchant Services Organization (MSO).

After clicking the check-out page on the merchant website, the browser displays a blank page. There are two reasons for this issue.

- The Acquirer Link Status for this Merchant ID is set to **Test Only**.

A screenshot of a dropdown menu titled "Acquirer Link Status". The menu is open, showing a list of options. The option "Test Only" is highlighted in a light yellow color, indicating it is the selected status.

- The cardholder's browser does not support redirection.

The acquirer should set the Acquirer Link Status to **Test and Production** and ensure that the browser being used supports redirection.

Why can't I see the void capture button on the Merchant Administration page? I'm sure that the void privilege is enabled.

A merchant can perform voids only on transactions that have not yet been sent to the acquirer for settlement. If the transaction has been sent for settlement, the void option is no longer displayed.

Why can't I see the void authorization button on the Merchant Administration page? I'm sure that the void privilege is enabled.

A merchant cannot void an authorization that has already been captured.

How do I release the amount reserved or on hold in the cardholder's account after a successful authorization, when the transaction needs to be cancelled but settlement has not yet occurred?

Within the Merchant Administration portal, the **Void Authorization** feature is used to void an authorization and release the reserved amount in the cardholder account.

If you do not have this feature enabled, then the cardholder must wait until the issuer releases the hold on the authorized amount after a period of time specified by the issuer.

This feature may not be enabled by default for the Merchant Services Organization (MSO). The MSO can request that this feature be enabled by contacting local MiGS support.

How can a single merchant support multiple currencies?

Multicurrency processing for a merchant is supported in MiGS depending on (a) if the acquirer's system is able to support settling and clearing of the required currencies and (b) the business requirements of the merchant.

The following options are available for multicurrency processing:

- A different merchant ID (MID) can be set up for every currency. The merchant must identify the required transaction currency and to use the related MID for that currency, for example, using Bank-USD for USD and Bank-QAR for QAR, and so on.
- A single MID can be created with multiple acquirer links. Each acquirer link has its unique Card Acceptor Identification Code (CAIC) and currency.
- A single MID and a single CAIC combination can be created with multiple currencies linked to it. However, some card management systems do not support this option.

In the Draft Capture File (DCF), the acquirer will receive the CAIC and the currency code in every transaction.

NOTE

Card Acceptor Identification Code (CAIC) is the same as the MID of the acquirer's card management system.

How do I obtain a member's Verified by Visa certificate on MiGS?

Enabling Verified by Visa involves the following process.

1. The acquirer contacts Visa and obtains the form that includes the needed details.
2. The acquirer completes the form and sends it to the local MiGS support team.
3. The MiGS support team generates a certificate, and then sends the certificate back to the acquirer.
4. The acquirer sends the certificate to Visa for signing.
5. Visa signs the certificate and sends it back to the acquirer.
6. The acquirer sends the certificate to the local MiGS support team.
7. The MiGS support team implements the signed certificate on the test profile for the acquirer.
8. The MiGS support team implements the certificate on production after acquirer confirmation.

NOTE

When requesting the VbV certificates from Visa for use on MiGS, the acquirer should ensure that the certificate Subject DN Information section contains the following:

CN=migs.mastercard.com.au

OU=MIGS

The O, L, and C components are relevant to the specific customer; however, all MiGS certificates to Visa must contain the CN and OU as indicated.

How can a merchant provide a refund to a cardholder for a transaction that occurred through MiGS more than one year ago?

MiGS enables a merchant to search for transaction data within only a one year time frame. For a merchant to refund to the cardholder the value of a transaction that occurred on MiGS after a time period of more than one year, the merchant must perform a Stand Alone Refund.

A Stand Alone refund can be performed using API commands; it cannot be performed through the MiGS portal interface.

To perform a Stand Alone Refund in MiGS, use the following API commands:

- Vpc_Command=doRequest
- Vpc_RequestType=credit
- Vpc_Command=doStandAloneRefund

For more information about how to perform the Stand Alone Refund, refer to the *MiGS Virtual Payment Client Integration Reference* that you were provided in the starter pack.

Why are some user IDs created for a Merchant ID unable to login to the Merchant Administration portal?

User IDs that are created with **Enable Advanced Merchant Administration Features** selected will be able to communicate with MiGS through API calls. For security reasons, these user IDs are restricted from accessing the portal.

- To provide access to the portal, create one user ID and **do not select** the **Enable Advanced Merchant Administration Features**.
- To allow for API Advanced Merchant Administration (AMA) calls such as QueryDR, void, refund, and so on, create another user ID and **select** the **Enable Advanced Merchant Administration Features**.

How can a merchant use dynamic descriptors—for example, type of service provided or other details—for inclusion in the cardholder statement?

A merchant may choose to provide transaction details for an issuer to use in the cardholder statement. For example, a telecommunications company may want to include the type of service (such as top-up, transfer, or Internet) for inclusion in the cardholder statement. For another example, a car rental company may want to provide the rental agreement number and the renter's name so those details can appear on the statement.

To include data sent by the merchant for the cardholder statement, the issuer of the card must receive the data in the clearing message from the acquirer. For the issuer to receive the data in the clearing message from the acquirer, the acquirer must populate the clearing message with the Dynamic Descriptor field provided in the Draft Capture File (DCF).

The Order Reference field in the DCF maps to the VPC attribute: vpc_orderinfo in the MiGS API.

Positions in the record	Attributes	Subfield	Values
198–231	ans-34	Subfield 1	Order Reference

The acquirer should add the “order reference” value to Data Element (DE) 43 in the clearing message.

Example

A car rental merchant, MerchantA, wants their agreement number with the customer to appear in the customer’s bank statement. The process would be as follows.

1. MerchantA sends the additional data in the **Order Reference = vpc_orderInfo** field.
2. DE 43 in the authorization message contains the **Merchant Name= MerchantA**.
3. MiGS returns the **Order Reference = vpc_orderInfo** in the DCF at the end of that day.
4. The Acquirer will append/add the **Order Reference** field received from MiGS DCF to DE 43 in the clearing message.
5. DE 43 in the Clearing message will look like: (MerchantA – **agreement No – Name**, given that the Order Reference field contained the value of (**agreement No - Name**).
6. The issuer receives the clearing message with DE 43 = MerchantA – **agreement No - Name**
7. Cardholder’s statement will show the additional data because the data in DE 43 should be included in the statement.

How can a merchant generate different responses in the test environment to test the system for all possible cases?

When using the TESTMID in production environment, the decimal value of the amount (the last two digits of the field vpc_amount) will determine the Issuer/Acquirer Response Code. This is to allow the merchant to test the merchant system against any possible response. For a list of all possible responses, refer to the *MiGS Virtual Payment Client Integration Reference* that you were provided in the starter pack.

Payment Method	Credit
Amount	BHD BD0010
Order ID	20371
Batch Number	2012
RRN	2333
Response Code	1 - Unspecified Failure
Acquirer Response Code	10
Authentication Code	