ANZ eGate™ | ANZ

Product Guide

Australia and New Zealand Banking Group Limited ABN 11 005 357 522

ANZ Consumer Finance

10/75 Dorcas Street

South Melbourne VIC 3205

Australia

1800 039 025

69 Tory Street

Wellington

New Zealand

0800 EFTPOS (338767)

Summary of Changes

***MIGS Product Guide*, March 2004**

Change Summary	Description of Change	Where to Look

Information about this Manual

Contents

This document outlines the ANZ eGate product, as an overview for merchants who wish to use this service.

The guide outlines the offering and the business logic of functionality provided by ANZ.

Please refer to "Using this Manual" for a complete list of the contents of this manual.

Questions?

If you have questions about this manual, please contact the Customer Operations Services team or your regional help desk. Please refer to "Using this Manual" for more contact information.

ANZ is Listening…

Please take a moment to provide us with your feedback about the material and usefulness of the *ANZ eGate Product Overview Guide* using the following e-mail address:

Australia: anzegate@anz.com

New Zealand: egate@eftpos.co.nz

We continually strive to improve our publications. Your input will help us accomplish our goal of providing you with the information you need.

Using this Guide

This chapter contains information that helps you understand and use this document.

Purpose

The ANZ eGate *Product Overview Guide* helps to provide merchants with a wide understanding of the MasterCard Internet Gateway Service (MIGS), and the business logic associated with its use.

Audience

ANZ provides this manual for merchants and their authorized agents. Specifically, the following personnel should find this manual useful:

- Merchant business owners.
- Merchant administration personnel.

Overview

The following table provides an overview of this manual:

Chapter	Description
Table of Contents	A list of the manual's chapters and subsections. Each entry references a chapter and page number.
Using this Manual	A description of the manual's purpose and its contents.
Introduction	An overview of Merchant Administration.
Architectural Overview	Describes the MIGS components and their relationship.
Glossary	A dictionary of terms and acronyms used in the MasterCard Internet Gateway Service.

Revisions

ANZ periodically will issue revisions to this document as we implement enhancements and changes, or as corrections are required.

With each revision, we include a Summary of Changes describing how the text is changed. Revision markers (vertical lines in the right margin) indicate where the text is changed and the date of the revision appears in the footer of each page.

Occasionally, we may publish revisions or additions to this document. Revisions announced in another publication, such as a bulletin, are effective as of the date indicated in that publication, regardless of when the changes are published in this manual.

Related Information

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

- *ANZ eGate Merchant Manager Manual*
- *ANZ eGate Bank Administration Manual*
- *ANZ eGate Merchant Administration Manual*
- *MIGS Payment Client Integration Manual*
- *MIGS Payment Client Reference Manual*
- *MIGS Virtual Payment Client Manual*

Table of Contents

Quick Reference Guide

Overview of the Service

- **What is ANZ eGate?**
  ANZ eGate is the brand offered to merchants which utilizes MIGS (MasterCard Internet Gateway Service) technology as the payment gateway platform.

- **What is the 'MasterCard Internet Gateway Service' (MIGS)?**
  MIGS is a hosted service providing **Card-Not-Present** (C-N-P) transaction support for eCommerce, Call Centre, and all C-N-P channels. In addition, MIGS provides a range of administration functions to the merchant and bank to provide full control of all aspects of their C-N-P business. It is a high-availability service operated by MasterCard International and is offered to banks to support their merchant's C-N-P requirements. Please see the 'Introduction' section for more details.

- **What is Merchant Manager (MM)?**
  Merchant Manager is an internet portal available to ANZ or ANZ's agent to allow the implementation and control of MIGS merchants. Please see the 'MIGS Merchant Manager Manual' for more detail.

- **What is Merchant Administration (MA)?**
  Merchant Administration is an internet portal available to merchants to view and administer their transactions processed on MIGS. Please see the 'MIGS Merchant Administration Manual' for more detail.

- **What is Bank Administration?**
  Bank administration is an internet portal for ANZ or it's agent to support real-time transaction queries on MIGS. It also allows login message to be set for the merchant and bank staff, and provides bank- and merchant-level reports. Please see the 'MIGS Bank Administration Manual' for more detail.

Transactions

- **What types of transactions does MIGS support?**
  MIGS supports 2 types of transactions. Purchase (also known as 'Sales') transactions allow the merchant to get authorisation and request payment in one message to MIGS. Authorisation/Capture (also known as Pre-Auth/Completion) provides support for merchants who require real-time authorisation, but provide a separate message to request capture of the funds from the payment (normally triggered by fulfillment of the goods or service office).

- **What options does a merchant have in accepting payments on their web-site?**
  MIGS provides a hosted payment option to the merchant to facilitate secure acceptance of payment on the internet. With this option, ANZ provides a bank-branded payment screen that can provide additional consumer confidence during the payment process, decreasing consumer 'drop-out'. With this option the merchant may not require a site certificate for the acceptance of payments and negates the need to specifically protect their systems from hackers searching for credit card numbers.

By default, MIGS can be configured not to disclose credit card information to merchants who use server-hosted payments.

Alternatively, ANZ may elect to allow the merchant to accept the credit card details on their site directly, with MIGS providing the authorisation back-end. This is the only option for non-internet transactions.

- **What are Authentication, MasterCard SecureCode™ and Verified by Visa™?**
  MasterCard International and Visa International have introduced new authentication schemes to substantially reduce credit card fraud on the internet by virtue of authenticating the cardholder during the payment process. The aim is to reduce the rate of 'Cardholder Not Authorised' chargebacks by the cardholder, the risk of which has traditionally been borne by the merchant. MIGS supports MasterCard's SecureCode™ and Visa's Verified by Visa™ protocols which facilitate liability shift when a merchant is registered with these schemes on MIGS. In addition, the merchant does not need to add any additional checks or functionality to their website when using MIGS for customer eCommerce payment authentication.

- **Can I perform refunds on MIGS?**
  ANZ is in control of what privileges are granted to any merchant. The ability of refunding payments (in part or full) can be performed by the merchant subject to the privileges being set by ANZ. Refunds can only be performed on transactions registered through MIGS and only on the card number used in the original payment transaction.

- **How do I find a transaction I have processed on MIGS?**
  Merchants can locate transactions via the Merchant Administration portal (MA), which will display all details associated with that transaction. Subsequent action history (refunds) can be performed if the appropriate privileges are granted by ANZ. ANZ can also determine what, if any, of the credit card details are subsequently visible to the merchant for any transaction.

Mail Order / Telephone Order Payments

- **How do I use MIGS to process my Mail Order and Telephone Order transactions?**
  MIGS supports Mail Order and Telephone Order transactions (where the card details are provided to the merchant). For small volume merchants processing a few telephone or mail order transactions, MIGS provides an internal order screen through Merchant Administration. To perform a MO/TO transaction, you will need the cardholder's details, including card number, expiry date, Card Security Code if applicable, and all the details of the transaction (i.e. order number, merchant references if applicable).

- **How do I use MIGS to process my Call Center transactions?**
  The MIGS Payment Client can be integrated into most business systems. The Payment Client can be integrated into a merchant's Call Centre application to provide back-end transaction processing. For merchants who have Call Centre and eCommerce payments, MIGS provides a single solution for all payment needs.

Introduction

An overview of the MasterCard's Internet Gateway.

Background

ANZ has partnered with MasterCard to provide its merchants with a platform to perform Card not Present (Internet and MOTO) transaction processing. MasterCard refer to the platform as MIGS (MasterCard Internet Gateway Service).

Product Architecture

The MIGS Payment Server is a comprehensive and scalable ePayments Architecture that is designed to process Business to Consumer (B2C) Credit Card, Mail Order/Telephone Order (MOTO) payment and general Card-Not-Present (C-N-P) transactions.

The MIGS Product Architecture is based on client-server product architecture as follows:

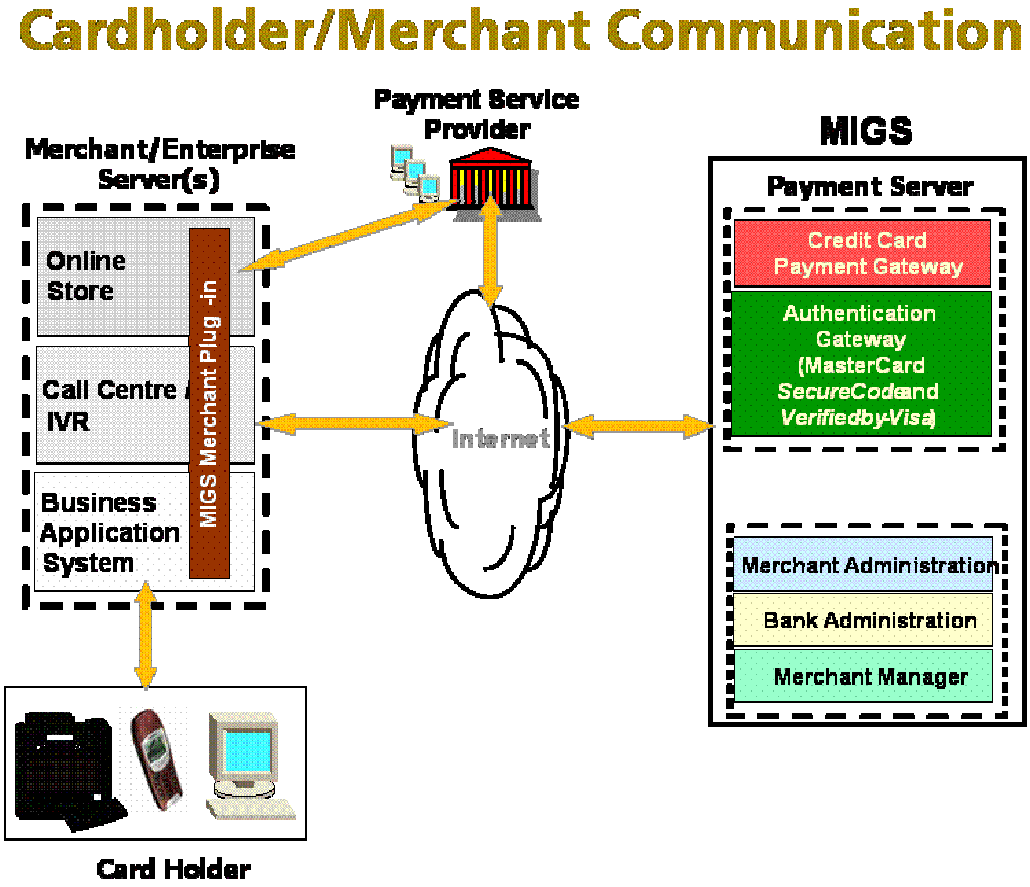


Figure 1 - Cardholder/Merchant Communication

Functional Elements

The components of a payment server system can be viewed at 3 levels:

1. MIGS Payment Server

The MIGS Payment Server consists of a core Payment Adapter that communicates with ANZ via the MasterCard Processing Centre. The adapter is configurable to support multiple Payment Gateway "plug-ins" such as Payment and Authentication.

2. MIGS Payment Client

The **MIGS Payment Client** is a distributed piece of software, which integrates with the Merchant web "store-front" site, Corporate ERP System or other merchant application.

Any Merchant application that integrates to the payment client using the ASP interface or involves the serving of web pages will require a Web Server (Windows NT, 2000 based (e.g. Microsoft IIS) or Unix based (eg. Apache/Tomcat)) to operate the Payment Client, and for a web 'store-front', a 3rd party "Shop & Buy" package (e.g. MS Site Server). The Merchant may "self host" or outsource to an ISP host. MIGS has integrated its Payment Client software with leading shop & buy applications and is therefore easy to install using the "Installshield" process.

Alternatively, web merchants can use a **MIGS Virtual Payment Client** to connect to the MIGS Server. This connection option does not require distributed software or a Web Server to operate, but requires more programming from the site developer.

Non web merchants who do not which to employ a web server can integrate with the payment client via either the Java or Sockets interface.

3. Consumer/Buyer - Internet Browser access

Consumers and/or Business buyers will access Merchant web sites in order to purchase Products & Services. For credit card payments over the Internet using MIGS, the consumer does not require any MIGS software. However, they will require MS-Internet Explorer or Netscape Navigator (Vers. 4.5 or above).

Functional Sub-Elements

The server infrastructure consists of a Payment Gateway to receive and send authenticated HTTPS credit transactions over the Internet and a Payment Adapter that converts and routes the HTTPS transactions into the MasterCard Processing Centre for distribution to the acquirer. All payments processed for ANZ on behalf of the merchant will be settled at the end of each day by normal bank processes.

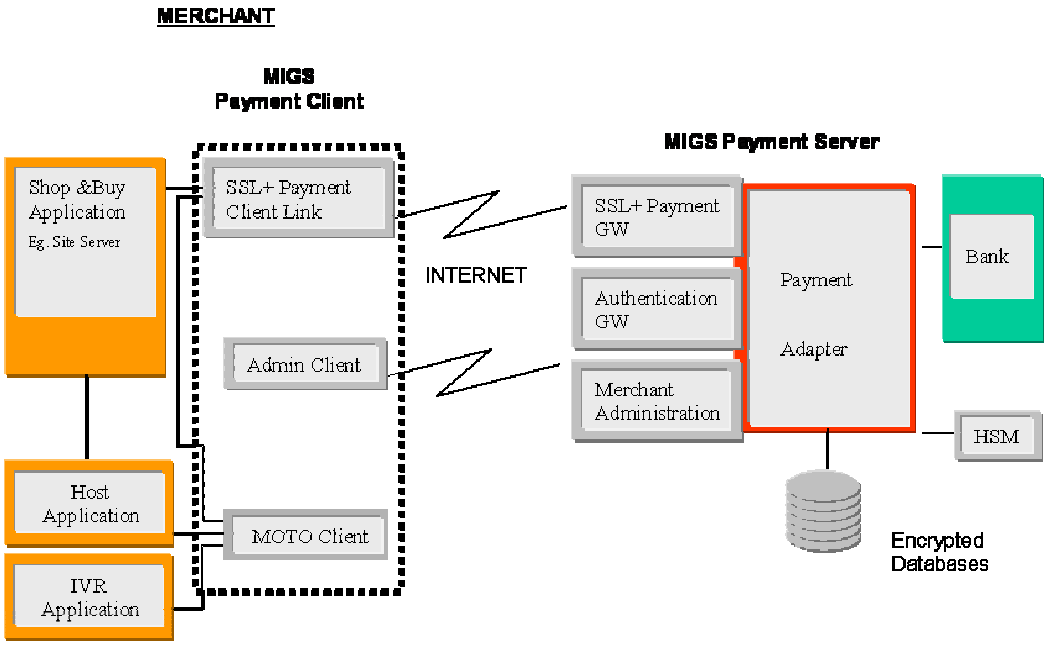


Figure 1. eGate Payment Server - Functional Components

Merchant Manager (MM)

The Merchant Manager module automates the registration process for both existing and new merchants and enables the mass deployment of the Merchant payment software (Payment Clients). MM is also used to set privileges for the merchant and facilitates the control of TEST and LIVE links for the merchant. The Merchant Manager module is for bank use only.

Merchant Administration (MA)

MIGS Merchant Administration is an Internet-based portal that allows merchants to monitor and manage their on-line processing and administration of payments through a series of easy to use pages. Merchant Administration can be accessed via an Internet browser, the appropriate URL will be provided by ANZ.

To use Merchant Administration, a merchant profile is required. This profile is setup by ANZ via Merchant Manager. The profile is a record of the merchant's details and the permitted functionality that the merchant has within MA. Two types of merchant profile are created through the enrolment process:

- **TEST** merchant profile – this allows merchants, within the test facility, to perform transactions against an emulator of ANZ's transaction processing system. This profile will always exist for testing purposes.
- **PRODUCTION** merchant profile – enables merchants in the production system, allowing them to perform transactions directly against the MIGS live transaction processing system. This profile is only activated once testing has been deemed sufficient by ANZ.

Architectural Overview

Unique Benefits

Role of the MIGS Payments Server

The MIGS Payments Server provides a secure, virtual point of sale (POS) Gateway to accept and process Internet payment transaction from ANZ's merchants.

MIGS will accept consumer and business originated credit payment transactions over the Internet. For transactions processed by the MIGS Payment Client, MIGS will protect these transactions from third parties by encrypting and digitally signing each transaction with strong cryptographic technology. In addition, the Gateway provides an option (Server-Hosted Pages) whereby all card details are processed on the Payment Server and NOT on the merchant's shop-and-buy application as with other systems. The server will also encrypt card numbers, making it impossible for unauthorized persons to use them for fraudulent purposes.

Critical Deployment Issues

MIGS has anticipated and addressed the many shortcomings of the e-commerce schemes and solutions, which are currently being delivered to acquiring financial institutions. Shortcomings in competitive offerings arise in three primary areas for Merchants:

Deployment & Manageability Issues	Explanation of the Issue	Typical Alternative	MIGS Solution
Installability	The time taken to integrate enabling software 'plug-ins'.	Difficult platform-specific (esp.Unix variants) software plug-ins required. Crypto programming often required by developer. Complex programming calls used. Lack of complete support for many popular application environments.	MIGS provides Merchant setup control, and key generation which eliminates need for crypto-programming by developer. The **Payment Client** can be integrated with 2 simple calls and is supported on all popular NT/UNIX web application environments.
Upgradability	The ability to upgrade the client solution to support multiple payment instruments	Many designed for simple SSL-encoded transmissions of credit card details to Bank gateways. Unable to be re-architected for sophisticated or for multiple payment instruments.	**Instrument-independent Server-Hosted Messaging Architecture -** uses Dynamic Server-side templates to ensure support for sophisticated or for multiple payment instruments, which can be managed centrally without changing each merchant plug-in/web site.
Maintainability	The ability to provide reporting, reconciliation, advanced transactions and self-help without calling on bank personnel.	Merchants have to call their acquirer's call centre for reporting, reconciliation or performing advanced transactions or alternatively do so with limited functionality only for credit cards payments.	**Merchant Administration** - This browser-based portal enables merchants to reconcile their transactions, perform advanced transactions (eg. voids, refunds) and run reports - all without requiring personnel or help-desk support from the bank.

Figure 2. Critical Deployment Issues & MIGS Solutions

MIGS has addressed each of these critical deployment issues by a specific technology solution, which is unique to the MIGS Payment Architecture, and each confers a benefit that is measurable in dollars of avoided cost.

MIGS Advantages

A summary of the core competitive advantages offered by MIGS Payment Server Architecture follows:

Security

The MIGS messaging technology supports secure, independent communications between the cardholder and MIGS, and between MIGS and ANZ. Sensitive cardholder data is managed independently of the merchant data. This capability ensures that data cannot be compromised in transmission to ANZ, nor can it be stored at the merchant or ISP site.

Authentication

The MIGS encryption and digital signature technology authenticates merchant-to-bank and bank-to-merchant communications. These functions validate the

merchant / financial institution (bank) relationship by guaranteeing the identification of both parties in the internet environment. MIGS also supports cardholder authentication mechanisms such as **Verified-by-Visa™** and **MasterCard SecureCode™**, which allow MIGS to identify all parties in the transaction, alleviating merchant chargeback risk and increasing consumer confidence.

Architecture

The MIGS Product Architecture supports a wide range of payment schemes through a family of payment gateway products. This provides the ability to incrementally add new payment types for the merchant as supported by MIGS users.

Deployment

The MIGS secure payment technologies provide a web-based sample code to deliver software configurations specific to each merchant and their internet environment.

Management

The MIGS secure payment technologies provide effective administrative tools to enable ANZ to manage deployment and merchant acceptance. These tools allow ANZ and merchant to control key functions of their business.

Differentiators	Feature	Function	Benefit
Security	Independent messaging schema	Separates cardholder and merchant communications	Prevents hacking and eliminates merchant or ISP fraud
Authentication	Encryption and digital signature software technology Visa 3D Secure and MasterCard SecureCode™	Validates merchant and cardholder to Bank	Guarantees all parties to the transaction
Architecture	Family of payment gateways	Ability to add new payment types	Minimizes disruption when adding new payment types
Deployment	Automated web-based merchant registration tools	Registration and enablement of merchants	Lowers the cost of fulfilment in a diverse internet environment
Management	Administrative tools for the Bank and Merchant.	Supports deployment, and acceptance.	Controls key business functions.

Figure 3. Unique Features of the MIGS Architecture

Payment Gateway

Payment Adapter

Beginning with the Payment Adapter, this system facilitates the connection to the MasterCard Regional Service Centre (RSC), which operates in the MasterCard Australian Processing Centre (APC) in Sydney. This provides global authorization capability and direct bank links for traditional acquirer processing. The Payment Adapter also takes advantage of strong hardware based cryptographic and public key modules, therefore providing the highest security standards currently available.

The Payment Adapter is a multi-threaded transaction processing environment designed to manage transaction integrity for a wide variety of traditional and e-commerce payment schemes. The Payment Adapter design provides a flexible, scaleable and supportable solution.

The Payment Adapter supports all traditional transactions as well as newer payment transaction protocols and payment schemes.

The Adapter is an on-line, multi-processing system, which runs on the Sun Solaris platform. Coupled with the MasterCard RSC environment, which includes 24x7 operational support for ANZ, a high-availability service is ensured, with industry best practices deployed including a fully replicated remote-site Disaster Recovery server.

Dynamic Gateway Support for Multiple Payment Instruments

MIGS' flexible messaging architecture provides a payment instrument-independent messaging schema between multiple trading partners, including the financial institution.

Each merchant's payment options can be delivered to consumers in the form of a dynamic server-side template from the MIGS Gateway. This means that upgrading merchant payment options can be done automatically and immediately. This contrasts greatly with present systems that require hands-on changes and additional integration.

Transaction Types

There are two transaction styles supported by MIGS:

Merchant Hosted Pages
Used for any merchant application, such as a merchant web shop & buy application or a call centre operation, where the merchant collects the card details. Authentication with MasterCard SecureCode™ and Verified by Visa™ can be supported for Merchant Hosted Pages.
NB: Includes Non Web Merchant Applications

Server Hosted Pages (with Authentication)
Only possible from a web application, such as a merchant shop & buy application, as the customer can only input their credit details direct to MIGS via a web page that is displayed from the MIGS web server. As MIGS has control of the cardholder's browser during this process, authentication with MasterCard SecureCode™ and Verified by Visa™ can be made an integral part of the transaction.

Server-Hosted Payment Pages

Server-hosted transactions use the SSL protocol to provide secure transmission of sensitive data between a customer's web browser and the MIGS Payment Server. In addition to SSL channel encryption, the Payment Client encrypts transaction data sent from the shop & buy application to the MIGS Payment Server to prevent alteration in transit as it is redirected via the customer's browser.

One of the benefits of a Server-Hosted Payment Page is that the merchant does not carry the legal responsibility of having to secure card details from hackers and misuse.

Server Hosted Pages - Information Flow

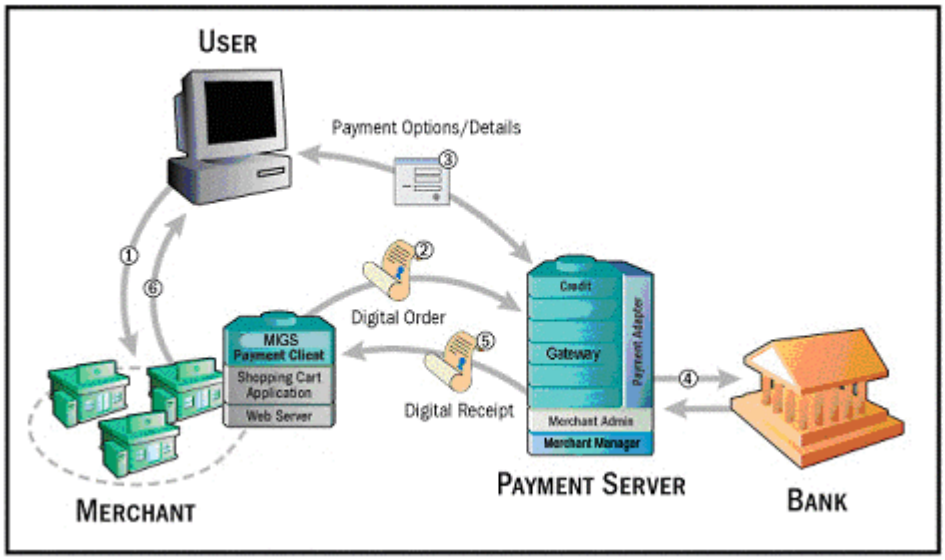


Figure 4. Information Flow in Server Hosted Payment Page

1. A customer ❶ and ❻ decides to purchase goods and enter the details into the merchant's shop and buy application software at the checkout page.
2. The customer pays for the goods and the merchant software sends an encrypted Digital Order to the MIGS Payment Server❷.
3. The MIGS Payment Server receives the customer's order details ❸ and displays a series of screens. The first screen displays the cards supported by the merchant, for example MasterCard and Visa. The customer chooses the card type they want to use for the transaction. The second screen accepts the details for the chosen card such as card number, card expiry, a card security number if required.
4. The MIGS Payment Server passes the details directly ❹ to ANZ who then switches the transaction to the card issuing institution. When the payment has been processed, the MIGS Payment Server temporarily displays the result of the transaction before displaying the final screen, which asks the customer to please wait while they are redirected back to the merchant's site. The MIGS Payment Server passes an encrypted Digital Receipt back to the merchant's site detailing the result of the transaction❺. This information is then passed back to the cardholder for their records ❻.

The MIGS Payment Client constructs and sends an encrypted Digital Order to the MIGS Payment Server, and then decodes the encrypted Digital Receipt from the MIGS Payment Server via browser redirects.

What the Cardholder Sees

In a Server-Hosted transaction the cardholder is presented with six pages:

1. The merchant's checkout page
2. The ANZ eGate Payment Options page
3. The ANZ eGate Payment Details page
4. The ANZ eGate Payment Pending page
5. The ANZ eGate Redirection page
6. The merchant's receipt page.

Examples of these pages are shown in the following pages.=

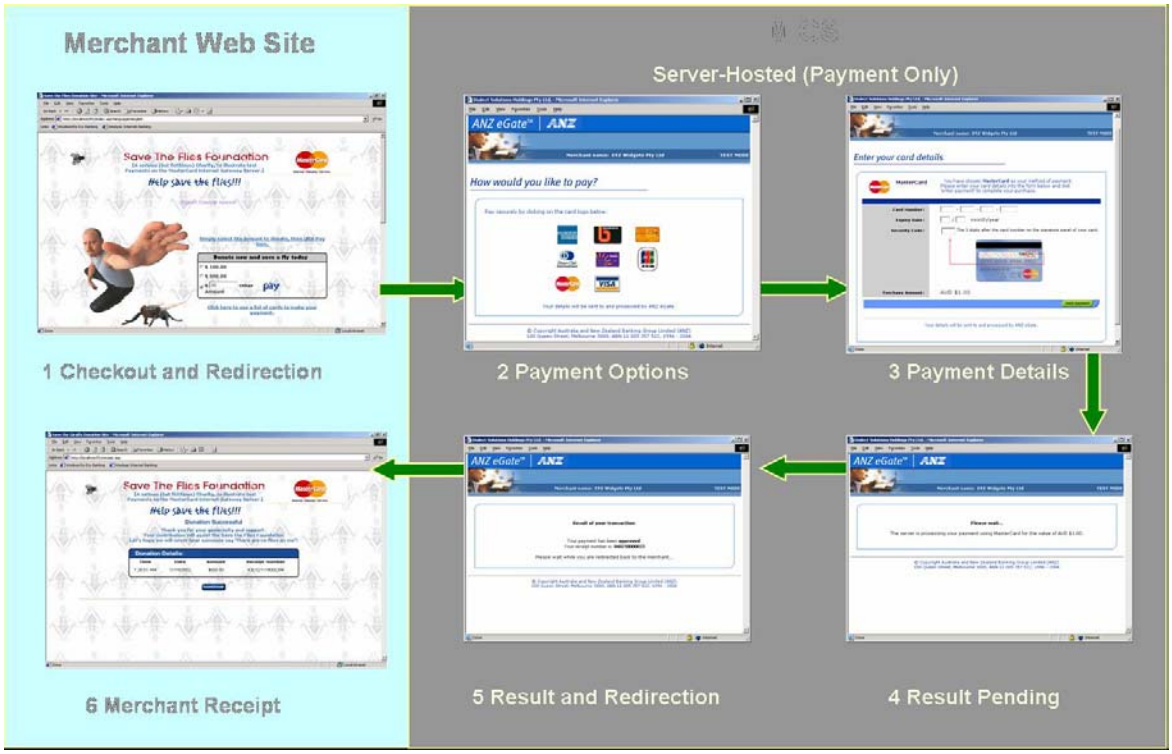


Figure 5. What the Customer sees in a Server-hosted transaction.

The Shop & Buy Checkout Page

The Checkout page displays the line items that the customer wants to purchase and the total amount to pay, including any delivery charges and taxes. The customer accepts the amount and proceeds to the MIGS payment pages to enter their card details.

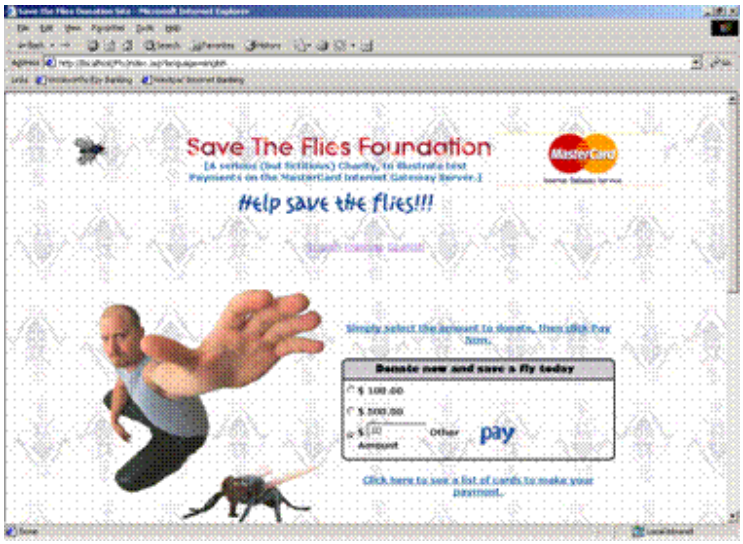


Figure 6. The Shop & Buy Check Out Page

The ANZ eGate Payment Options Page

The Payment Options page presents the customer with the card types that the merchant accepts. The customer clicks a card type and proceeds to the Payment Details page. The merchant can bypass this first screen by supplying the card type previously.

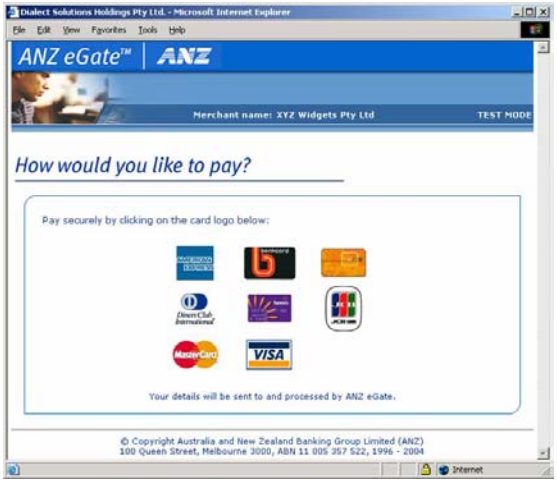


Figure 7. ANZ eGate Payment Options Page

The ANZ eGate Payment Details Page

On the Payment Details page, the customer enters their card details, including the card number and expiry date, and clicks the pay button. MIGS then processes the payment.

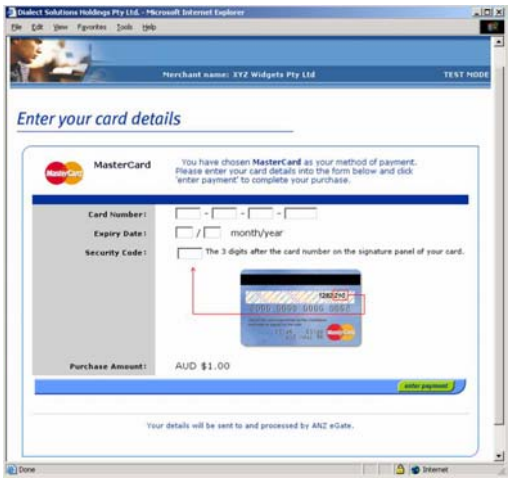


Figure 8. ANZ eGate Payment Details Page

The ANZ eGate Payment Pending Page

As the payment processor is processing the payment, a payment pending page is displayed to the cardholder.

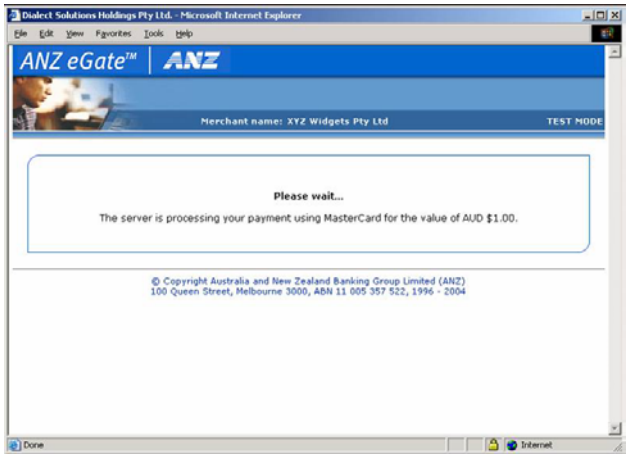


Figure 9. ANZ eGate Payment Pending Page

The ANZ eGate Redirection Page

The redirection page is displayed in the customer's browser and the Digital Receipt is passed to the merchant's shop-and-buy application.

Figure 10. ANZ eGate Receipt Page

The merchants Shop & Buy's Receipt Page

The shop and buy receives the Digital Order and creates a Digital Receipt as a receipt page is displayed to the customer.

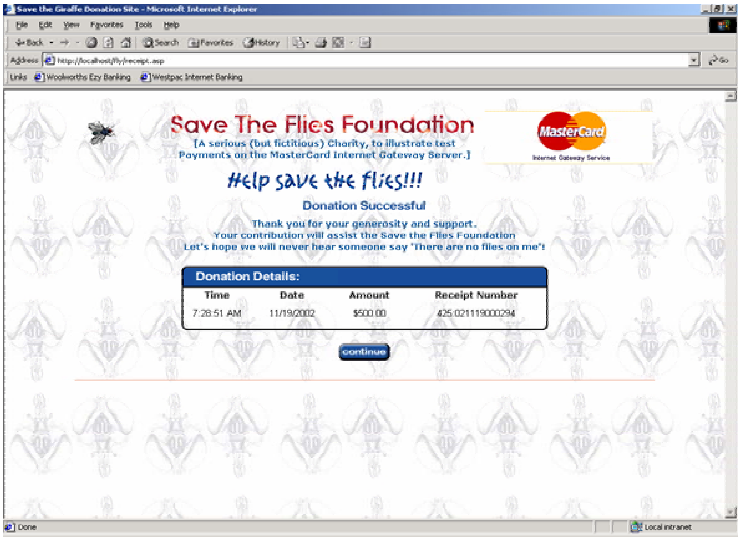


Figure 11. The Merchant's Receipt Page

Merchant Hosted (MOTO) transactions

Merchant Hosted transactions are purchase/auth transactions orders where the customer provides their card details to a merchant, via mail order or by telephone (including Interactive Voice Response (IVR) systems) or web based shopping applications.

The customer provides their payment details (card type, card number and expiry date) directly to the merchant.

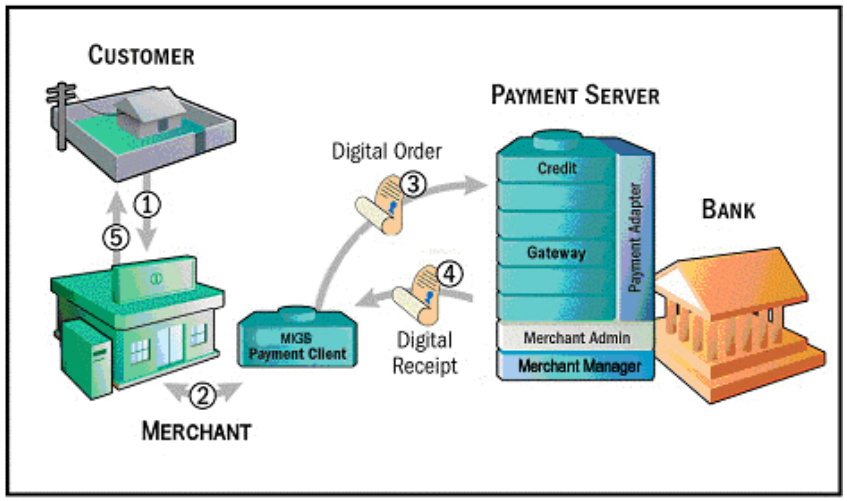


Figure 12. Information Flow in Merchant-Hosted Transaction

Merchant-Hosted Information Flow (using Payment Client)

1. A customer ❶,❺ purchases goods or services.
2. The merchant collects the card details using the Internet, IVR, mail order or telephone order and submits the details to be processed via the Payment Client ❷.
3. The Payment Client generates an encrypted Digital Order and sends it over the Internet to the MIGS Payment Server ❸. The Digital Order includes the purchase amount, card details (submitted to the merchant), and a merchant-specified transaction reference.
4. The issuing bank processes the information and passes the result back to the MIGS Payment Server, which forms an encrypted Digital Receipt. This receipt, which includes the transaction results and payment reference details, is sent from the MIGS Payment Server back to the Payment Client❹ where it is decrypted. The decrypted results are sent back to the merchant❷ and stored for future reference. A receipt is also passed back to the customer for their records❺.
5. A Merchant-Hosted transaction is a multi command function that uses the following commands:

6. Echo test – to check if the shop and buy application has access to the Payment Client.
7. Add additional data fields like Card Number and Card Expiry to the transaction.
8. Send the Digital Order.
9. Check if there is a receipt result.
10. Get the individual receipt results

What the Cardholder Sees – Web Merchants Only

In a Merchant-Hosted transaction the cardholder is presented with two pages:

1. The merchants shop and buy checkout page.
2. The merchants shop and buy receipt page.

The MIGS Payment Server does not display any pages in a Merchant-Hosted style transaction, as all pages are displayed by the merchant's application.

Authentication Gateway

MIGS fully supports the MasterCard Authentication initiative SecureCode™, and the Visa Authentication initiative Verified by Visa™.

Once a merchant has enrolled for SecureCode™ and Verified by Visa™ authentication can be performed automatically as part of an internet Server-Hosted or Merchant-Hosted transaction.

For full details on both of these authentication initiatives, please contact ANZ representative.

What are Payment Authentications?

Verified by Visa™ and MasterCard SecureCode™ were designed to alleviate online security concerns. When a cardholder makes a payment on a web site, he or she is required to enter their special code (password) in a pop-up box from his or her card issuer. If the correct code is entered, the cardholder's identity is authenticated and the transaction can then be sent normally for authorisation. It is a small additional step in the payment process which verifies the identity of the cardholder. The process is similar to the authentication of a debit cardholder with a PIN at an Automatic Teller Machine (ATM).

Many chargebacks in electronic commerce are 'No Cardholder Authorisation' chargebacks - the cardholder either denies responsibility for the transaction or the merchant lacks evidence of the cardholder's authorisation of the transaction. With MasterCard SecureCode™ and Verified by Visa™, the liability for electronic commerce transactions will shift from the merchant to the card issuer when:

A The merchant is fully enabled for Verified by Visa and/or MasterCard SecureCode
B The issuer authenticates the cardholder using Verified by Visa and/or MasterCard SecureCode
C Following cardholder authentication, the issuer authorises the transaction and the merchant receives a response code from the acquirer confirming approval.

Authentication Implementation on MIGS

To facilitate authentication on MIGS, MIGS needs to be in control of the customer payment process. This happens naturally during a Server-Hosted payment as MIGS controls the card detail collection from the cardholder. In order to facilitate authentication in Merchant-Hosted mode, MIGS requires a new type of request, which is similar to Server-Hosted but where the previously collected card details are passed in the message.

In either case MIGS performs cardholder authentication for MasterCard and Visa cardholders without any interaction or special support from the merchant.

The merchant will be provided extra authentication result fields in the Payment Client Digital Receipt which can be stored by the merchant to defend a chargeback, but this is not necessarily required as these details are also recorded in Merchant Administration.

MasterCard SecureCode™ and Verified by Visa™

Introduction

MIGS performs the authentication using a Server-Hosted redirect. The cardholder is redirected to the Issuer's Authentication site, where they enter their password into the Issuer's Access Control Server (ACS)

In MIGS, the Payment Server performs both the authentication and payment in the one transaction.

From a cardholder's experience, there is simply a new step added – the cardholder is redirected to the Issuer's Access Control Server (ACS) where they have to enter a password. If this matches, the password selected by the cardholder at the point of enrolment in their Issuers Authentication program, then the transaction is considered authenticated and payment can proceed.

If the cardholder does not enter the correct password, and therefore cannot authenticate themselves, MIGS will not proceed with the payment.

Other failures (for example, communication errors) may result in the authentication attempt failing, but the payment going ahead. The general rule is that if authentication is possible it will be performed, but if it is performed it must succeed otherwise the payment will not be processed.

Process Flow

It is beyond the scope of this document to fully outline both SecureCode™ and Verfied by Visa™, but the process flow in MIGS will be described in this section. The MIGS interaction with any other entity apart from the cardholder or merchant is described for information only, as the merchant will only witness passing of control to MIGS and the return of authentication data if authentication was attempted.

It is important to note that the merchant has no control over an authenication attempt if he is configured for SecureCode™ or Verfied by Visa™. MIGS will detect the submission of a MasterCard or Visa Card by the cardholder and, if the merchant has been enabled for SecureCode™ or Verified by Visa, MIGS will interrogate the MasterCard or Visa Directory Service to check if the cardholder is enroled in their Issuer Authentication program.

If the cardholder is not enroled, or the issuer does not support SecureCode™ or Verified by Visa™, authorisation is performed as normal.

It the cardholder is enroled, the Directory Service will return the URL of the Issuer's ACS, and MIGS will redirect the cardholder's browser to this ACS to allow the issuer to authenticate the cardholder. The ACS then returns the cardholder's browser back to

MIGS, along with the result of the authentication attempt.

MIGS will continue with the authorisation of the transaction if the authentication was sucessful.

Server-Hosted Pages - Process Flow

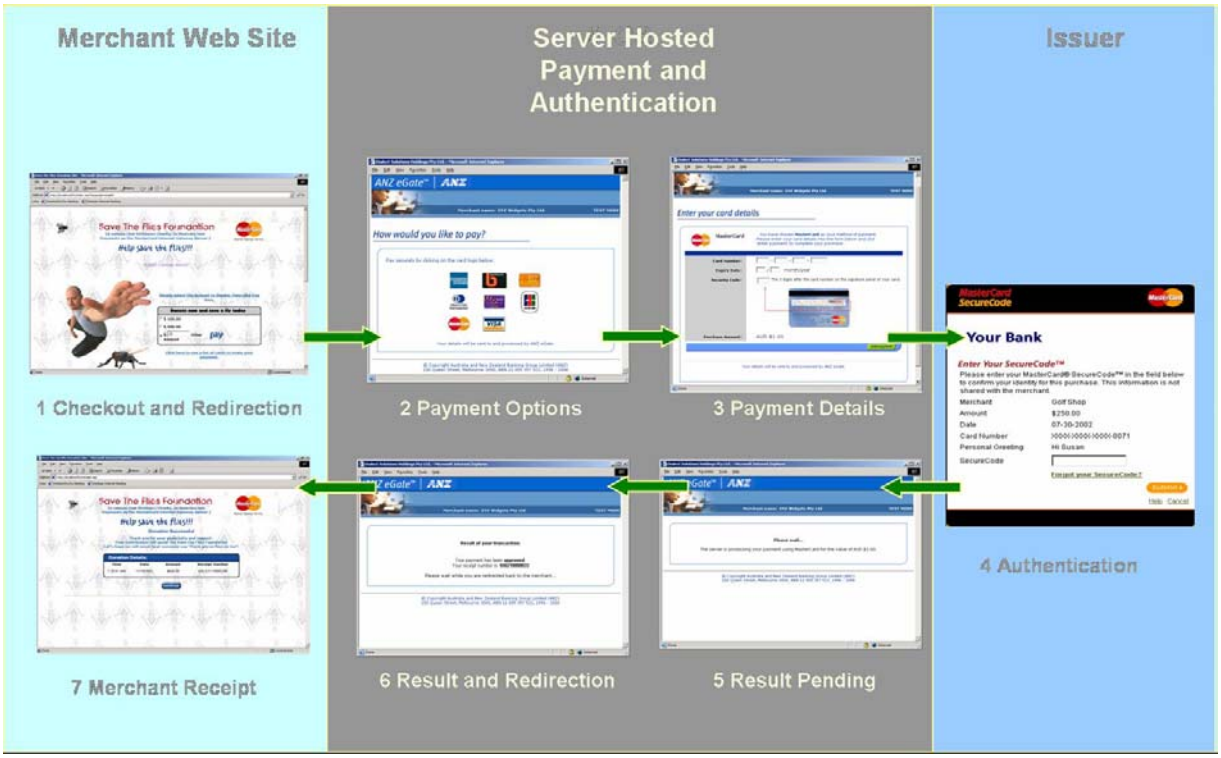


Figure 13. Server-Hosted SecureCode/ Verified by Visa Process Flow

For a Server-Hosted transaction the merchant has no extra considerations on the submission of the payment request.

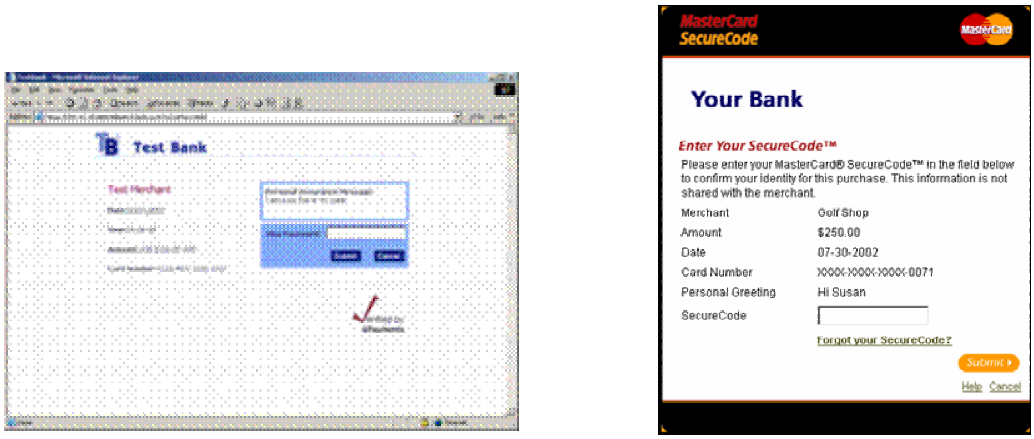


Figure 14. Examples of Issuer Access Control Server Screens

Process Flow for Merchant-Hosted Payment Pages

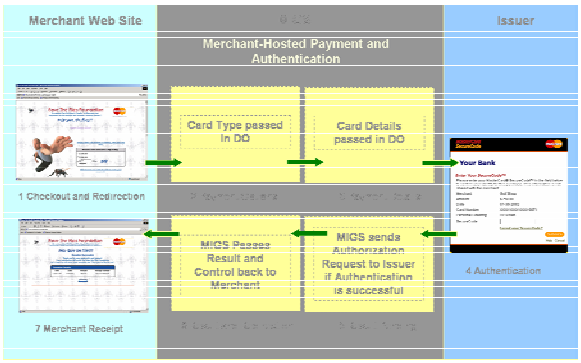


Figure 15. Merchant-Hosted Payment - Authentication Process Flow

Authentication for a Merchant-Hosted transaction is performed by using the standard Server-Hosted Payment Client call, but providing the credit card type, number, and expiry date as extended fields, allowing the credit card entry screens to be bypassed.

The cardholder experiences the process above, where control appears to be passed straight from the merchant website to the Issuer ACS, where in fact, control has been passed to MIGS, who silently detects the card details in the digital order, interrogates the Directory Service and redirects the cardholder to the issuer ACS.

Product Functions & Features

Payment Client

Merchant software can communicate with the Payment Server using a downloaded thin secure Payment Client. The Payment Client can run on a Windows or Unix system that supports Java. The payment client software self-installs and contains self-test code, which provides visible results to the user for standard shop-and–buy applications such as MS Site Server, Inter-Merchant, InterShop, etc. Some user-level configuration is required with bespoke applications.

In operation, merchant software makes two calls to the Payment Client. One call to generate a Digital Order, (DO) the second, when a Digital Receipt (DR) is received, to validate and disassemble the DR into its components. Additional calls to the Payment Client retrieve each component of a Digital Receipt by name.

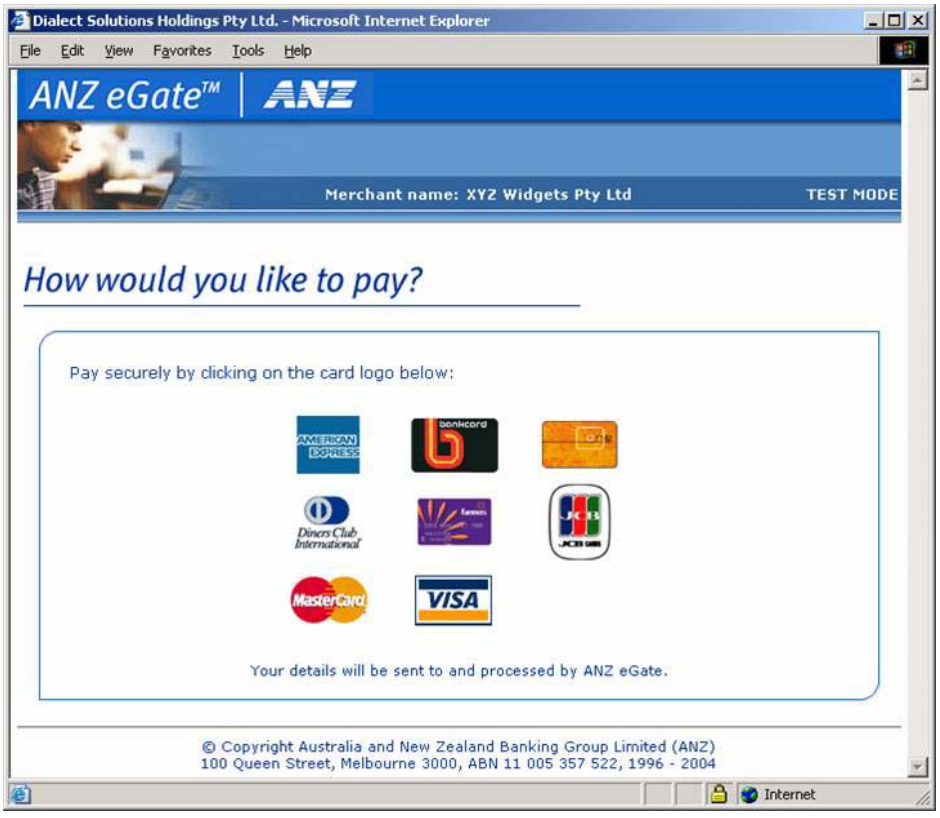


Figure 16. Payment Server Payment Options Display Format

The Payment Options screen is triggered by the DO. The Credit Gateway receives the DO and serves the payments option screen to the cardholder. The merchant's payment options are stored in the payment server database. Once the cardholder has selected the payment instrument option required a second payments details screen will be served.

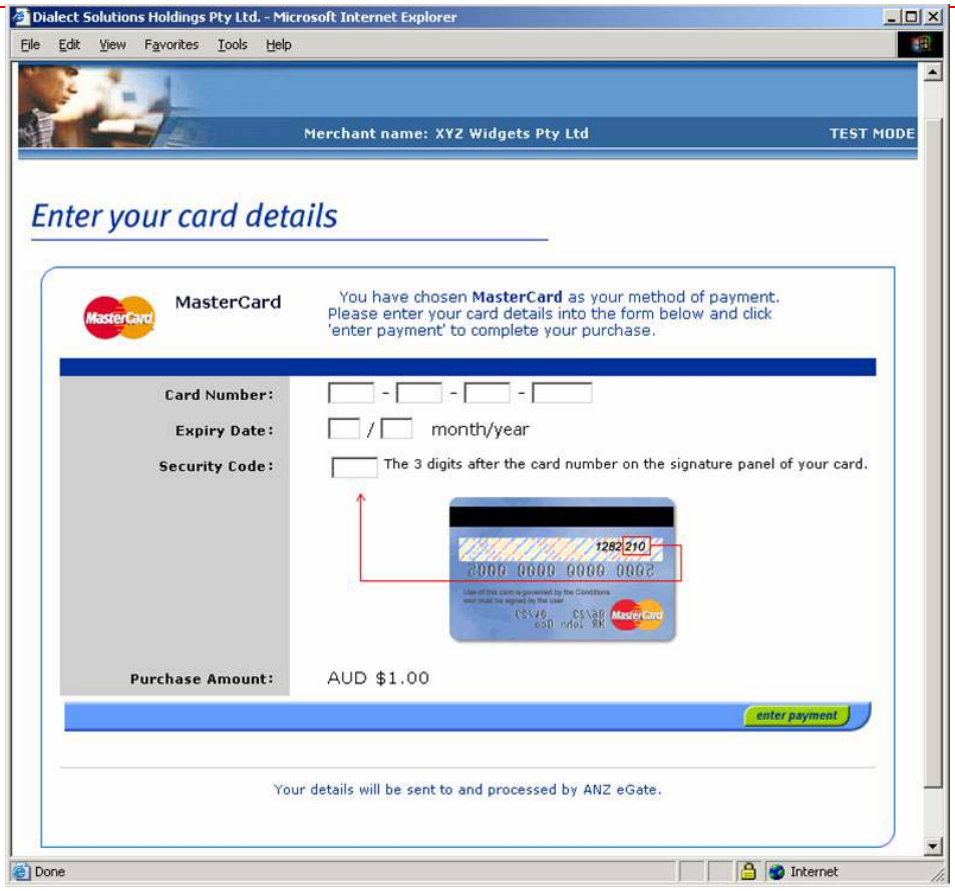


Figure 17. Payment Server Payment Details Display Format

The payment details screen will capture the cardholder's card detail and any additional information required e.g.: order number, additional references etc.

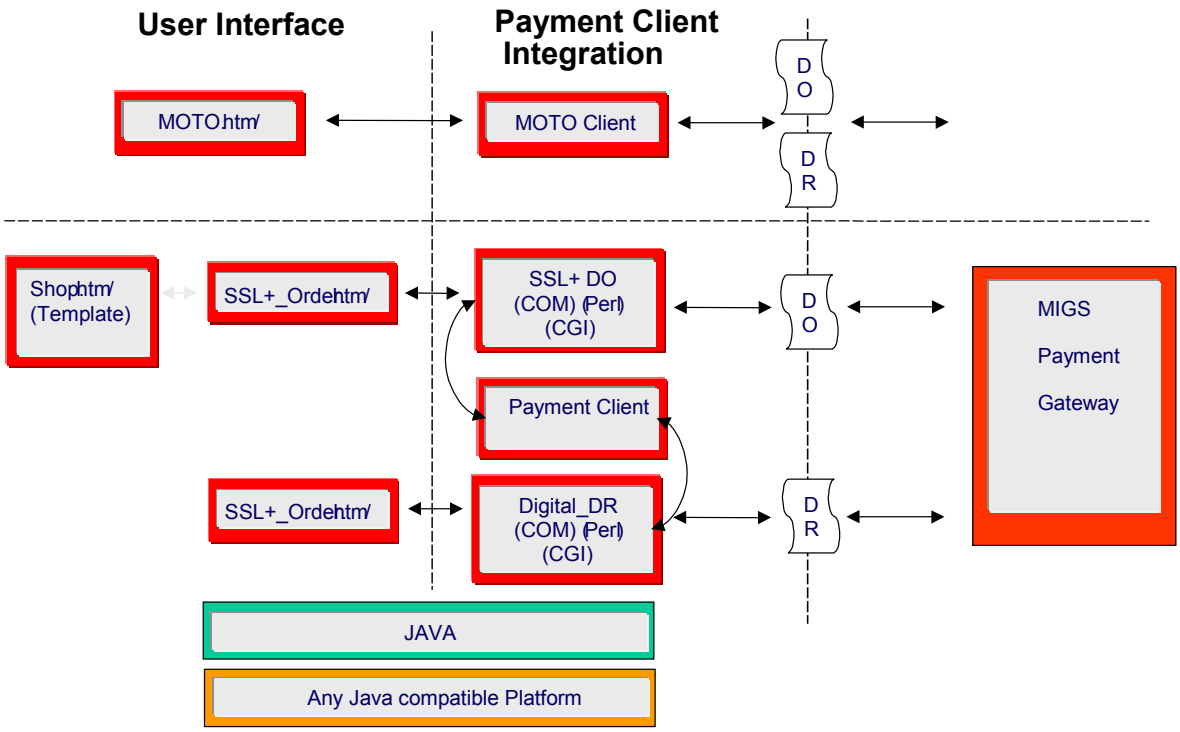


Figure 18. Merchant Payment Client Infrastructure

Merchant Payment Client Infrastructure above shows the Payment Client components. All clients share a common set of functions as described above. The payment client interface to the merchant catalogue or web store applications is provided using Java, C, C++ or Visual Basic languages via COM, ASP, CGI, Sockets, Perl or JAVA interfaces.

Support for payment types includes:

- Accepting requests to make payments
- Validations and approvals
- Issuing the payment message via a payment adapter
- Issuing receipts
- Tracing, error handling and correction
- A single daily transaction credits to the merchant's account.

Server-Hosted Payment Gateway

The primary function of the Server-Hosted Payment Gateway is to manage the secure messaging schema between cardholder, merchant MIGS and Issuer ACS if the cardholder and merchant are both enrolled for Authentication. It also serves a number of other secure functions including -

1. The Gateway is a protocol translation engine converting and re-mapping HTTP/S communication to and from ISO8583 formats (in conjunction with the Payment Adapter). All HTML pages are generated from JHTML files.

2. The Gateway also routes the transactions to all other Gateway sub systems and the Payment Adapter Transaction Processing Engine (TPE) mentioned below.

3. The Gateway also serves the payments HTML pages. The pages generated are internationalised, specifically including both visible text and GIFs. Internationalised text is drawn from a set of gateway resource bundles. Internationalised GIFs are handled by appending the locale descriptor to the basename of the GIF. For example, image2_ja.gif may be a Japanese version of the GI image2.gif.

4. The Gateway manages the transaction integrity of internet communications between all parties.

   All HTML pages generated by the gateway provide a common look-and-feel through the use of JHTML template files. In typical usage, these files provide a common header, footer and background from the gateway pages. A template is chosen as follows:
   - use a merchant-specific template if available; else
   - use a acquirer-specific template if available; else
   - use the MIGS default template.

   JHTML templates are internationalised through the same naming conventions as used for GIFs, mentioned above. Locale-specific templates are preferred to generic templates. Each template incorporates the substitution tag ${MIGS_payment_block}, which marks the position where the page body is inserted. The gateway provides separate JHTML blocks for each of the generated pages, include gateway error pages.

   Furthermore, Gateway Templates enable new merchant's payment instruments to be configured on an as needed basis. This approach effectively:
   - eliminates the need to distribute new software to each Merchant
   - reduces the software version control requirement
   - reduces help-desk support requirements

Communications Protocols

The Payment Client to Gateway communications services use HTTPS to provide the real-time advice for authorisations and sales. Historical enquiries of sales and reconciliation data are provided through the merchant administration portal, which provides either browser-based or server-based access to such data.

Test Host Simulator

The Host Simulator module provides a comprehensive transaction testing facility for the payment client software. The merchant receives the payment client software via ANZ or an authorised Payment Service Provider. Once the payment client and the merchant key pairs have been installed into the merchant's test application environment, testing with MIGS can commence.

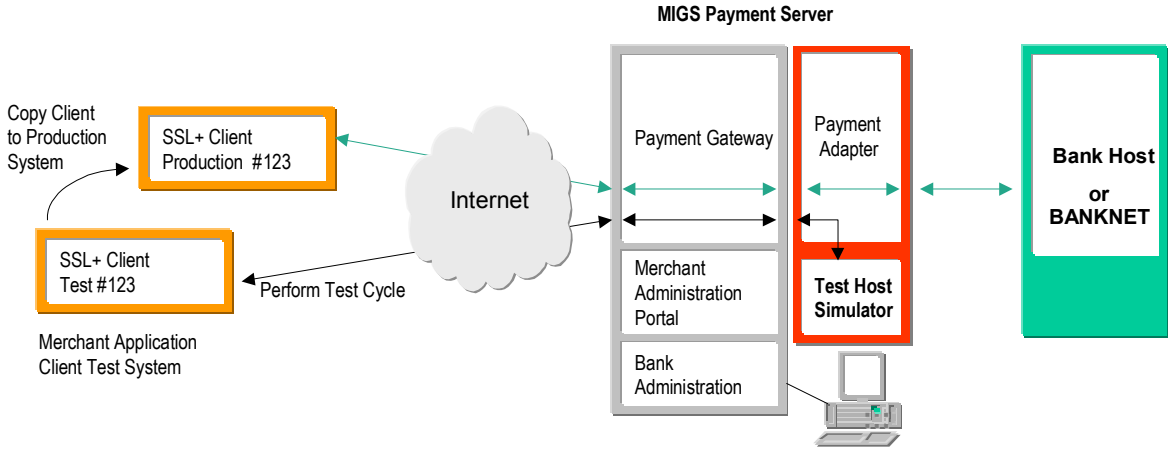


Figure 19. Merchant Payment Client Test Simulator Infrastructure

Bank merchant services staff can set the Test Link for the merchant. The merchant simply prefix's their merchantID with the word 'TEST' to initiate the routing of all transactions received from the payment client to the Test Host Simulator module. Full sets of test logs are written to the Merchant Administration Portal so that both the Merchant and Bank Help-Desks can view and validate test results.

Once the transaction testing cycle has been completed successfully the Payment Client software will be copied to the merchant's production system application. Once installed in the production system and all necessary bank processes have been completed, ANZ or approved agent will set-up the merchant's Live Link. The merchant can access this link by simply removing the word 'TEST' from their merchantID. The merchant's test profile will remain and can be accessed at any time for further testing.

All transactions on the Live Link will be routed to the MasterCard RSC and logged in the MIGS administration systems as live production transactions.

It is important to summarize that the merchant cannot perform live transactions unless specifically configured by ANZ to do so.

Merchant Administration (Portal)

A Merchant can use two methods to administer their transactions:

1. Manual - the merchant can use a browser (with 128-bit SSL encryption capability) to interactively perform historical searches; perform captures, and refunds.
2. Automated - the merchant can use the Payment Client to directly access MIGS from a merchant application to perform most transaction-related functions (capture, refund, etc) suited to automate merchant software interfaces. This is useful for merchants who wish to integrate payment administration functions into their host applications.

Both methods allow use of a common merchant administration process. All transactions are presented in one database (but tagged as to their originating payment type).

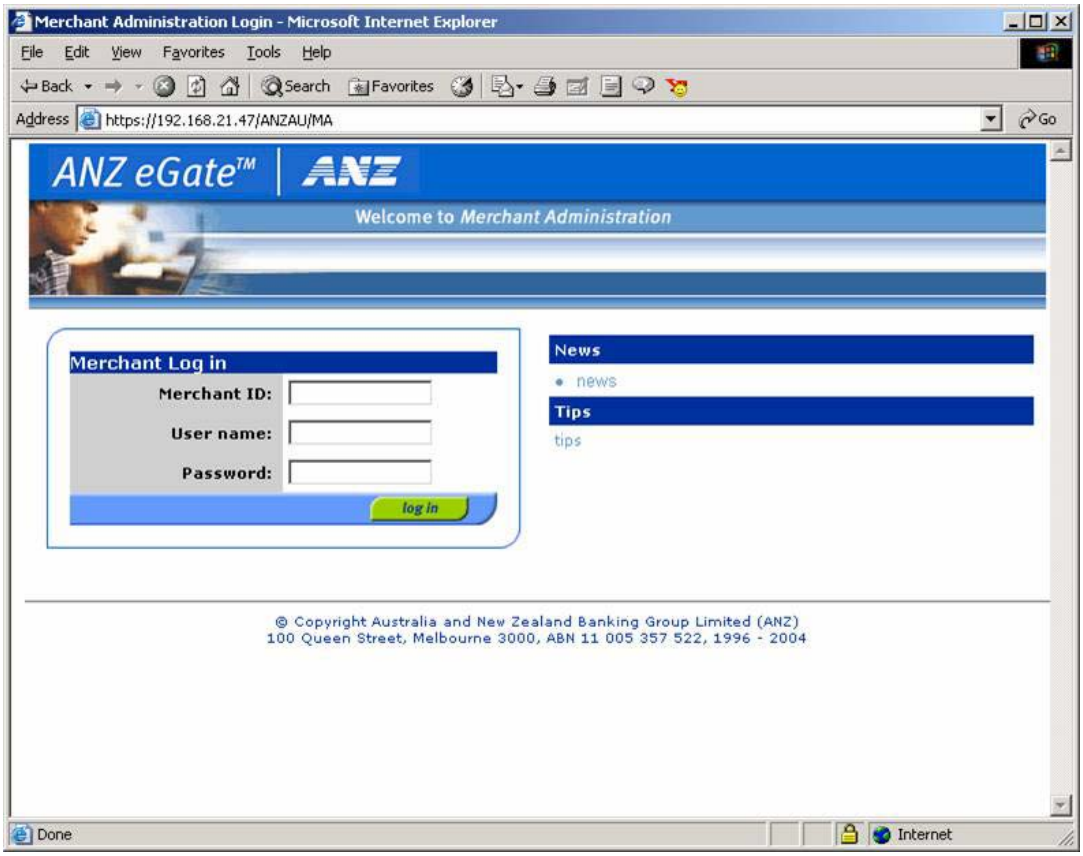


Figure 20. Merchant Administration Login Screen Interface

To access the Merchant Administration functions the user must enter their MerchantID, user name and a strong password. The screen provides a browser interface that provides direct access to the payment administration facilities on MIGS. The screen is divided into quadrants for the brand and bank logos, bank and third party advertising rollovers, news articles and user tips.

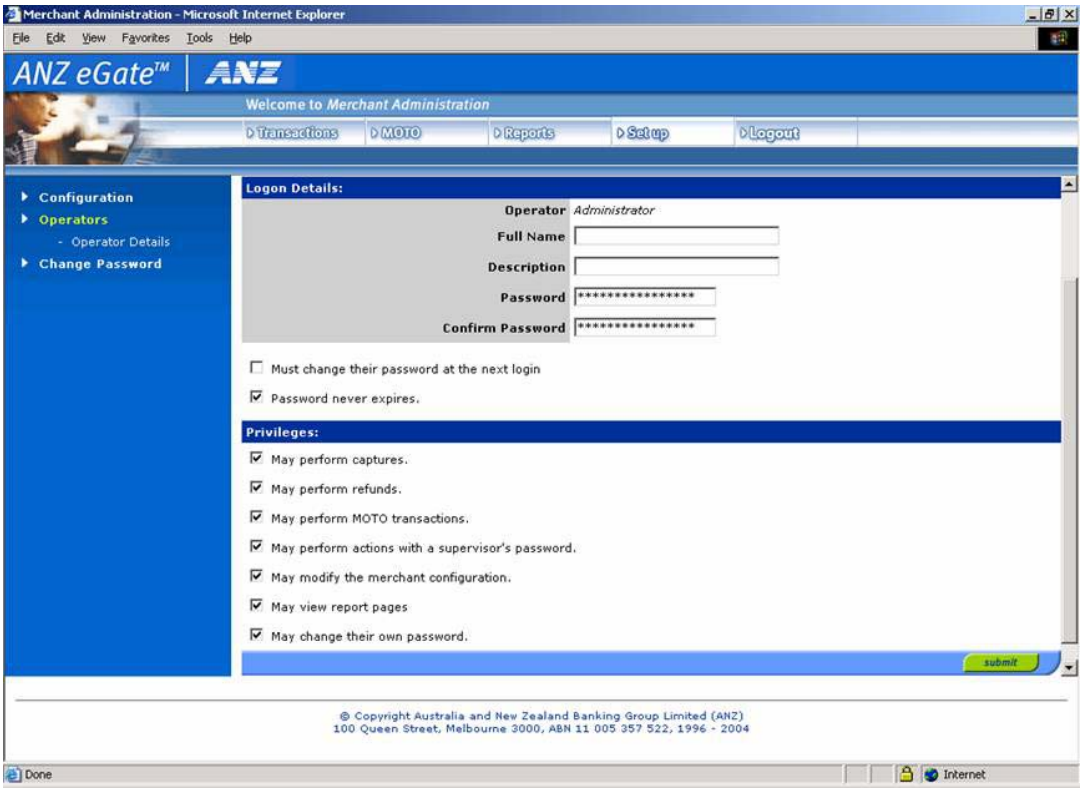


Figure 21. Merchant Administration Graphic User Interface

The Merchant Administration portal process can use a browser or application interface to access the MIGS administration database. The merchant administration log-on process requires a user name and strong password authentication over a 128bit SSL encrypted communication link. The administration interface will display the transaction state and a fully auditable transaction log file to the user.

The merchant interface allows the administration user to locate specific transactions using the date, time or order number as the transaction identification key as shown above.

MIGS provides the means for the various gateway and administration facilities to perform financial transactions to the acquiring banks through the Payment Adapter.

Supported payment transactions are listed below:

1. Authorisation
2. Capture
3. Partial Captures
4. Purchase (Sale)
5. Refund

Transaction Detail

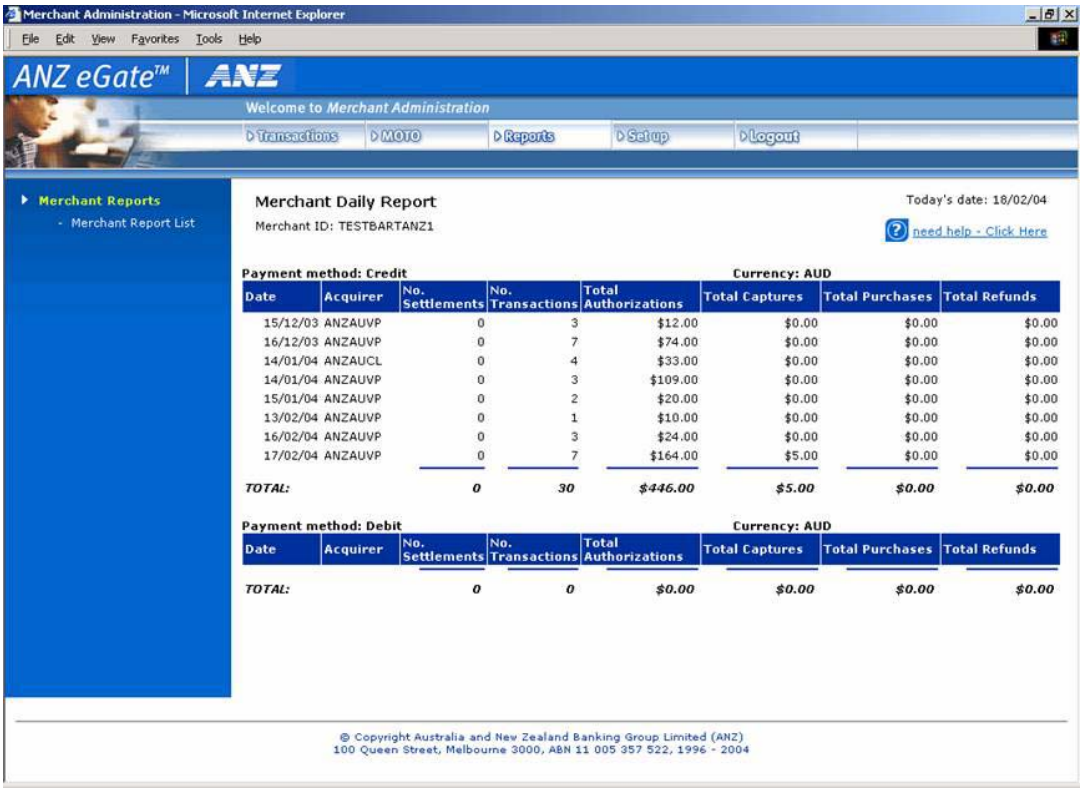
- The full detail for all transactions can be displayed to the merchant with the exception of the credit card number. ANZ may elect to perform some 'masking' of the card number depending on the transaction type.

Authorisation, capture, purchase, refund

Authorisations, captures, purchase and refunds can be performed at any time.

Reports

Figure 22. Transaction Summary Report Screen



Standard transaction summary screens are available in daily, weekly, monthly and yearly formats.

Other Features

Application Service Provider (ASP) Hosted Merchants

Multiple merchants using the same shop-and-buy application or multiple merchant shop-and-buy applications hosted at one ASP site may use a single copy of the Payment Client. It is not necessary to provide a separate copy of the Payment Client to each merchant.

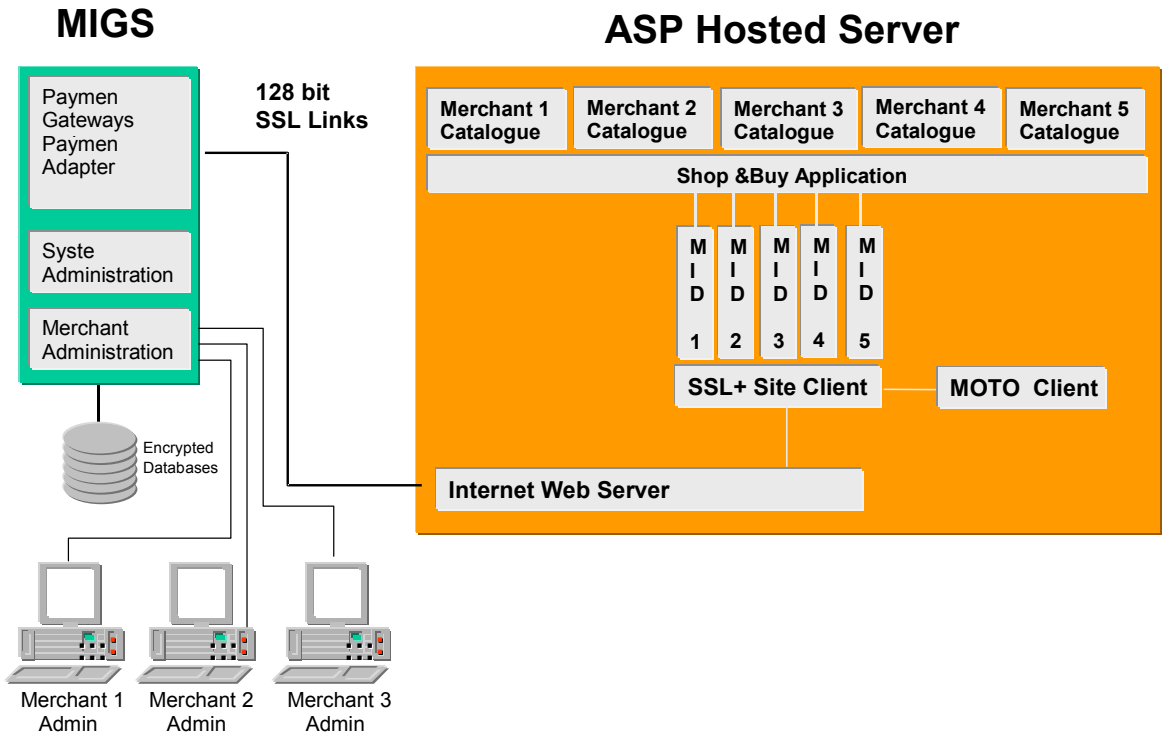


Figure 23. ASP Hosted Merchant Architecture

Each merchant will be provided with a merchantID and have an administration system set-up in the MIGS Merchant Administration facility. The merchant will be able to access the Merchant Administration system via a browser or an application interface.

Glossary

This chapter defines various terms, concepts, acronyms, and abbreviations used in this document. These definitions appear for convenience only and are not to be used or otherwise relied on for any legal or technical purpose. ANZ specifically reserves the right to amend any definition appearing herein and to interpret and apply all such definitions in its sole discretion as ANZ deems fit.

In addition, the description of terms in this section are in the context of what they mean within the MIGS service, rather than any generic meaning.

Acquirer (or Acquiring Bank)

ANZ that maintains the merchant relationship and facilitates the processing of payments on behalf of the merchant.

Advanced Merchant Administration

A special privilege which can be granted to a MIGS Merchant Administration user, allowing a merchant to perform administrative functions (such as captures and refunds) via their host system, as an alternative to performing these functions via the Merchant Administration Portal.

ANZ eGate

ANZ has partnered with MasterCard to provide its merchants with a platform to perform Card not Present (Internet and MOTO) transaction processing. MasterCard refer to the platform as MIGS (MasterCard Internet Gateway Service).

Authorisation

The process of a transaction by or on behalf of the cardholder's bank (the *issuer*) according to defined operations regulations. MIGS will return the response to the authorisation request, to indicate approval or reason for decline.

Batch

A batch refers to the grouping of transactions by MIGS into payment groups. MIGS stops each days processing batch at a set time, opening a new batch for the next day's transactions. It should be noted that the cut-over time of the batch may not be in line with the merchant's business hours. Contact ANZ for details of the cut-over time. Batch number is effectively the same as Settlement Date.

Capture Transaction

A capture is only relevant to merchants who perform split Authorisation/Capture combinations. Most merchants will not use this function as capture of funds will be performed automatically with a cardholder's authorisation on MIGS.

If Authorisation/Capture is used, a separate request by the merchant is performed to capture the funds from the cardholder.

Cardholder

The customer to whom a card has been issued or the individual authorized to use the card. This is the customer of the merchant or purchasing goods on behalf of the customer.

Issuer

The issuer is ANZ or institution which issues the card to the cardholder. In MIGS, the issuer or their agent decides on approval or decline of a cardholder request for payment of goods or services from the merchant. If a transaction is declined by the issuer, the cardholder generally needs to contact their issuing bank.

Mail Order/Telephone Order (MOTO)

A generic term referring to any 'Card Not Present' transaction. When the cardholder's card is not present, the merchant may be allowed to accept the card details from the cardholder by mail or telephone. In this type of transaction, the merchant collects the card details and supplies all of this information to MIGS in the request.

MasterCard Internet Gateway Service (MIGS)

MasterCard Internet Gateway Service is the trademark name for the MasterCard Regional Service Centre and the Internet Payment Gateway front-end.

MasterCard SecureCode™

MasterCard SecureCode™ is a program designed to provide online retailers the added security of having issuing banks authenticate their MasterCard SecureCode™ enabled cardholders and qualify their online transactions for protection against "cardholder unauthorized" chargebacks.

Merchant

A retailer, or any other person, firm or corporation that (pursuant to a merchant agreement) agrees to accept credit cards. Merchants can only operate on MIGS if they have signed agreements with their bank

Merchant Administration

An internet web browser-based portal which allows merchants to monitor and manage their online processing. It also provides access to administrative functions on payments.

MIGS

See MasterCard Internet Gateway Service

MOTO

See Mail Order/Telephone Order.

Payment Authentication

A process whereby the cardholder authenticates their identity with the issuing bank during the online transaction process. This is made possible by a MasterCard SecureCode™ or Verified by Visa™ password which is requested upon each transaction; a similar concept to the use of a Personal Identification Number (PIN) on Automatic Teller Machines (ATMs).

Payment Client

A back-end processing tool integrated into the merchant's website which allows the real-time sending of secure transactions (digital orders) to MIGS and the receipt of transaction results (digital receipts).

Payment Server

The MIGS payment gateway service hosted by MasterCard International which provides an interface into the authorisation and authentication networks. The Payment Server accepts incoming secure transactions from the Payment Client and processes transactions in real-time.

Purchasing Transaction

A purchase transaction is the most common of MIGS payments. Transactions of this type both authorize the payment request (via the Issuer) and facilitate payment to the merchant (via the Acquirer) in one single message.

Refund

A transfer of funds from the merchant back to the cardholder; example usages are when goods are returned or unable to be delivered. On the MIGS system, refunds must be matched to a purchase/capture transaction and must not exceed the original value of the transaction.

SSL

Secure Socket Layer (SSL) developed by Netscape Communications Company, is a standard that encrypts data between a Web Browser and a Web Server. SSL does not specify what data is sent or encrypted. In an SSL session, all data sent is encrypted. MIGS only supports SSL connections of 128bit encryption from the cardholder or merchant browser.

Verified by Visa™

Verified by Visa™ is a program designed to provide online retailers the added security of having issuing banks authenticate their VbV enabled Visa cardholders and qualify their online transactions for protection against "cardholder unauthorized" chargebacks.

Virtual Payment Client

Enables merchants to connect to MIGS without the distributed Payment Client software. This method requires more work for the developer and is less secure than the Payment Client connection option.