Introduction to
Merchant Integration with National e-Payment Gateway System

1. Background

Information Technology Authority (ITA) has engaged MasterCard to implement a National e-Payment Gateway system for Oman. MasterCard will provide its MasterCard Internet Gateway Service, also known as "MiGS" for the implementation. The MiGS is a modern, high performance and highly reliable e-Payment Gateway system which is operating worldwide to provide payment services for e-Commerce industry.

The National e-Payment Gateway (e-PG) system as implemented using the MiGS system will provide access by any merchants in Oman who would like to offer online shopping or ecommerce services via Internet. ('Merchant' in this context includes both Government ministries and private sector merchants). ITA will provide the technical support to merchant to establish access to the MiGS system and adopt the MiGS e-payment services for payment processing of the merchant online transactions.

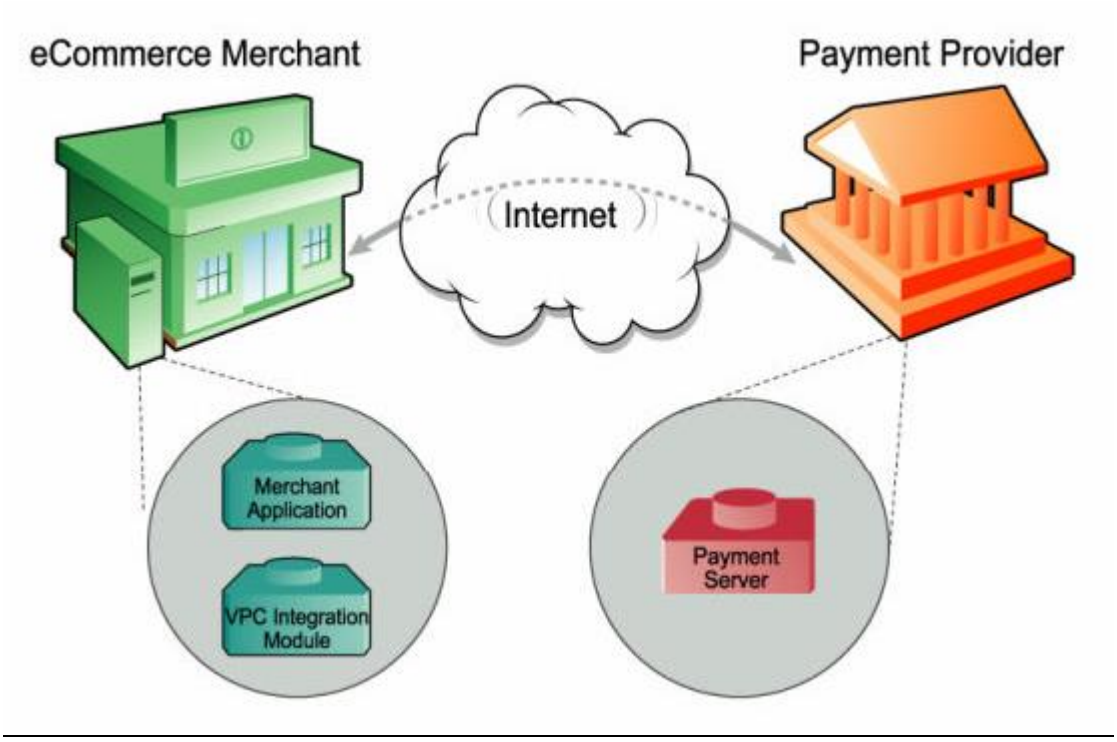
ITA will provide the technical support for merchant to perform integration of the merchant websites to the National e-PG system.

This paper is an introduction of the services provided by the National e-PG system, and the technical information for merchant to perform integration of their websites with the National e-PG system.

2. What are e-Payments?

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

E-Payments are represented in the following diagram:



2.1 The Components of an e-Payment Solution

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

- The Merchant application is a business application/website on the merchant's system that uses Virtual Payment Client to process payments.
- The Integration module is a Virtual Payment Client which communicates between the merchant application and the Payment Server.
- Virtual Payment Client provides secure communication between the merchant application and the Payment Server.
- Payment Server processes merchant Transaction Requests.

- The Payment Provider enables the merchant to accept payments online.

In the National e-PG system, the Payment Server is the MasterCard MiGS system. The Payment Provider is ITA which offers the e-Payment solution with support from MiGS and an acquiring bank for merchants.

3. Integration via Virtual Payment Client

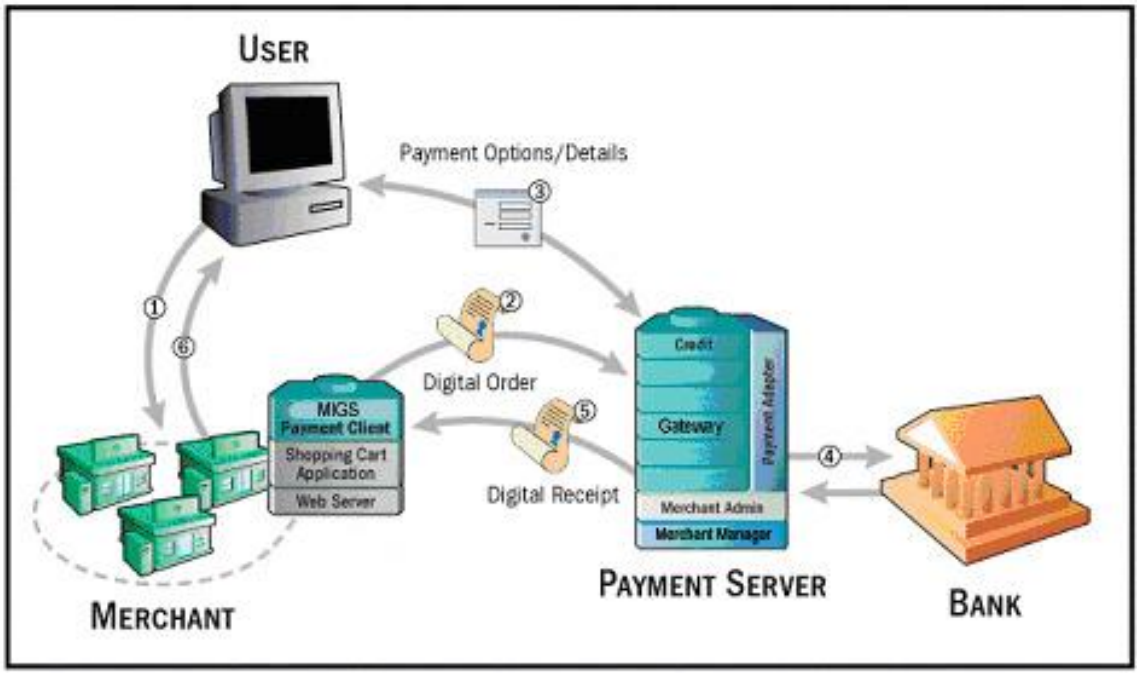
MiGS provides an effective payment enablement of merchants via the MiGS Virtual Payment Client (VPC) which uses a Web Services interface.

The merchant simply integrates the MiGS VPC scripts with the merchant's Web site. The MiGS VPC provides the required formatting, encryption and digital signing of messages to ensure payments are securely received from customers. The VPC enables merchants to payment enable websites by providing a low integration effort solution. It is suitable for most website hosting environments as merchants can integrate payment capabilities into their application without installing or configuring any payments software.

3.1 Information Flow for e-Payment Solution

MiGS 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 Virtual Payment Client encrypts transaction data sent from the shop and buy application to the MiGS Payment Server to prevent alteration in transit as it is redirected via the customer's browser.

Server Hosted Pages - Information Flow



1. A customer ❶ and ❻ decides to purchase goods and enter details into the merchants 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 card details ❸ and displays a series of screens. The first screen displays the cards supported by the processor supports, for example MasterCard, Visa, and American Express. 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 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, and 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 user for their records ❻

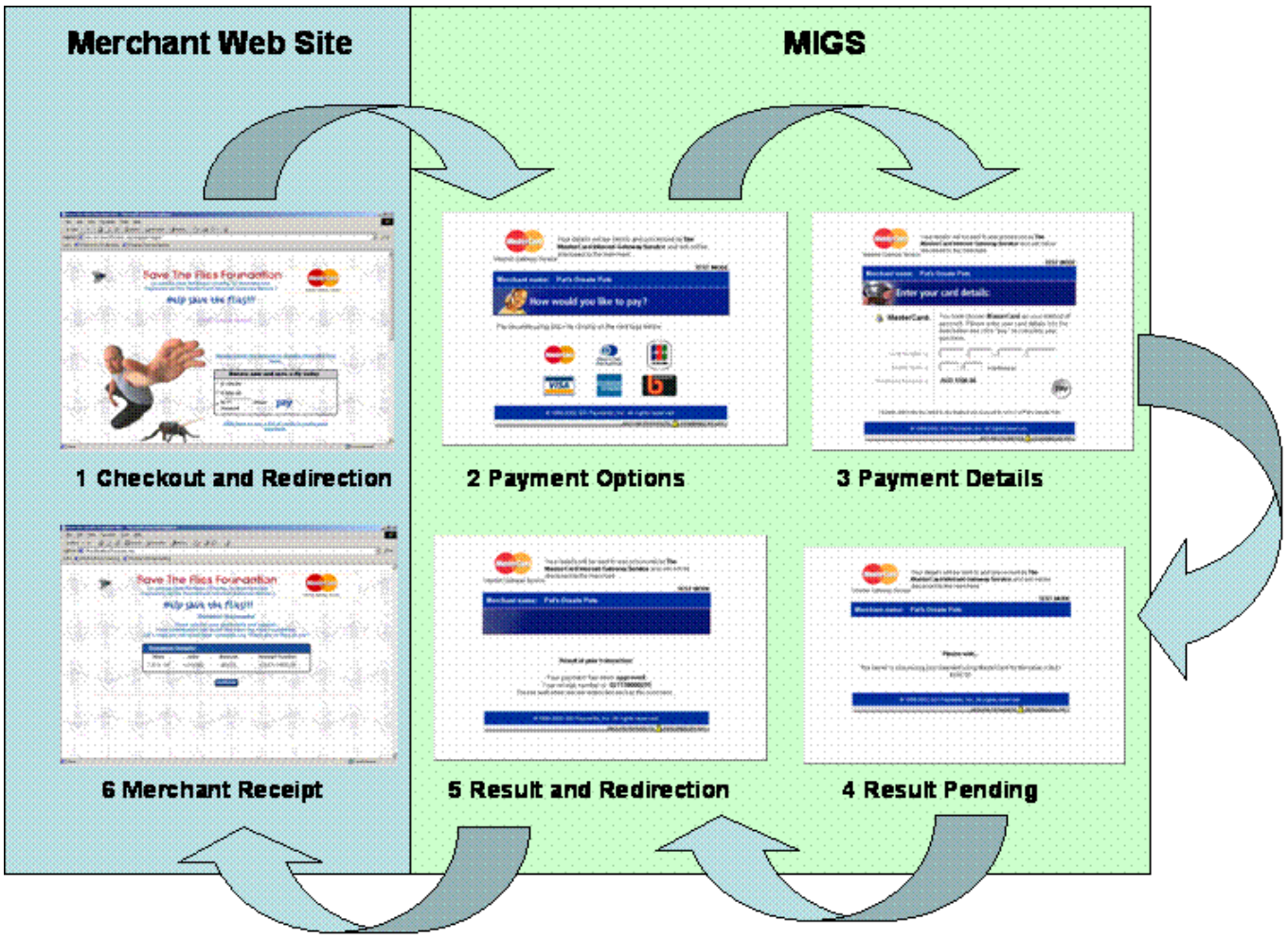
The MiGS Virtual Payment Client constructs and sends an encrypted Digital Order to the MiGS Payment Server, and then decodes the encrypted Digital Receipt from the MiGS Payment Server via browser redirects.

What the Cardholder Sees

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

1. The shop and buy's checkout page
2. The MiGS Payment Server's Payment Options page
3. The MiGS Payment Server's Payment Details page
4. The MiGS Payment Server's Payment Pending page
5. The MiGS Payment Server's Redirection page
6. The shop and buy's receipt page.

Examples of these pages are shown in the diagram on the next page:



4. Authentication Gateway

MiGS supports the MasterCard Authentication initiative Secure Code, and the Visa Authentication initiative Verified by Visa.

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

4.1 What are Payment Authentications?

Authentication is a process that can be performed ahead of the payment request for internet transactions. If the cardholder's bank supports Authentication for their cardholder, then the cardholder is transferred to that bank's Authentication server before processing the payment for the entry of a secure password. The payment can only proceed if the bank's Authentication server confirms a correct password was entered. 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).

4.2 Authentication Implementation on MiGS

MiGS performs cardholder authentication for MasterCard and Visa cardholders without requiring any interaction or special support from the merchant.

The merchant will be provided extra authentication result fields in the Payment Client Digital Receipt and these details are also recorded in Merchant Administration.

5. Security

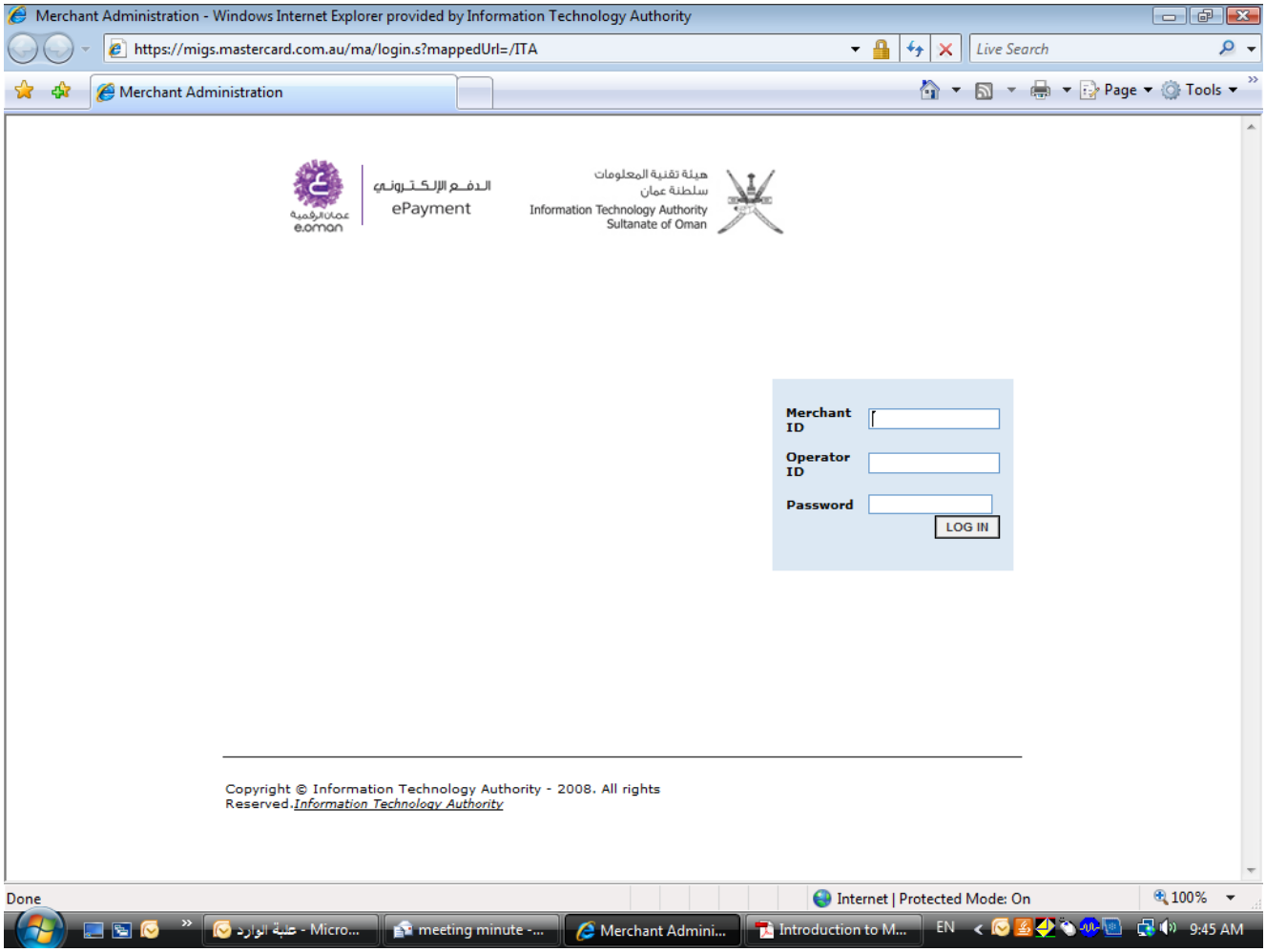
The MiGS system has been designed to ensure maximum security for payment transactions. Key security features include:

- All MiGS system components are housed within the MiGS processing center secure computer facility. The MiGS processing center is routinely audited in accordance with MasterCard's global security procedures.
- The MiGS connection to the Internet is protected by industry strength firewalls.
- The servers running the MiGS software are configured as non-routing to prevent any access to the MiGS systems from the Internet.
- Card details submitted from the cardholder to MiGS will be secured. Each request and response message exchanged with MiGS contains the Merchant ID, Merchant Transaction Reference, other relevant parameters for the call as well as a hash map containing any number of extended fields. The Payment Client uses Java serialization to produce a byte string, which

is then signed and encrypted using RSA to ensure the data is secured and the merchant can be verified as the originator.

- The payment page displayed to the cardholder can originate directly from the MiGS system, which would collect the card details directly from the cardholder using 256 bit encryption. In this way, the e-PG system can shield the merchant from all credit card details collected.
- The credit card authorization message sent to the card issuer is secured using MasterCard's global Bank Net system and other card scheme private global secure networks.
- The MiGS platform is fully PCI DSS (Payment Card Industry Data Security Standards) compliant as certified by Cyber trust. All data is stored and presented in line with the PCI standards.

6. Merchant Administration



Merchant Administration Log-in Screen – (default branding)

Enablement for on-line authorizations is only part of what a merchant requires from a complete payment solution. The merchant also wants to perform other payment functions such as processing voids and refunds, checking transaction details and totals, and creating reports.

The Merchant Administration facility of MiGS provides the merchant with secure browser access to the MiGS central transaction database to perform day-to-day merchant functions. The merchant is

provided with comprehensive and powerful tools for searching, reporting and further processing of transactions.

The key features of Merchant Administration include:

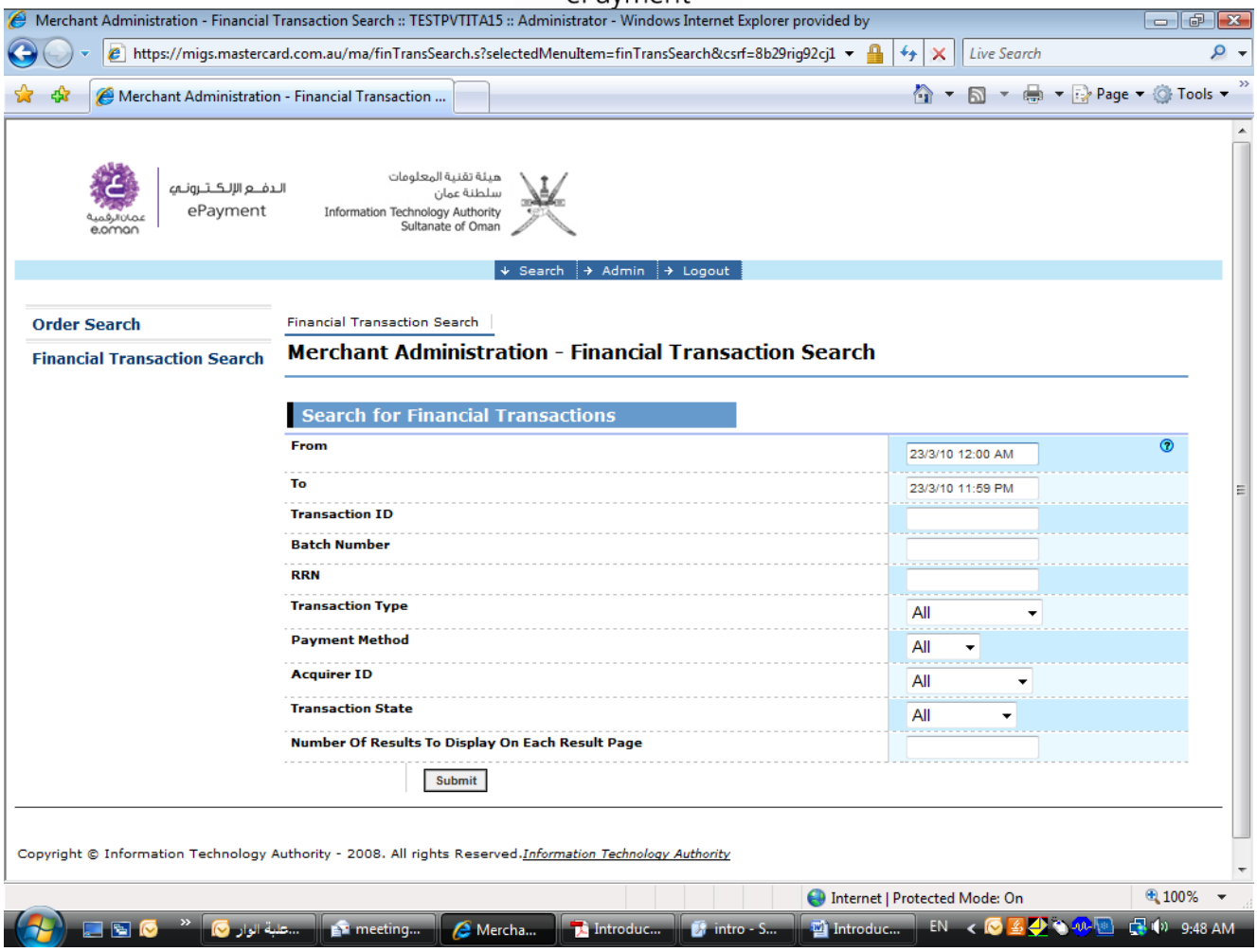
- Merchants may perform interactive searches of their own transaction logs and perform capture, refund or void operations on any transaction. Searches can return a single transaction or a range of transactions.
- Full or partial capture and refund transactions are supported. Multiple partial captures can be used to facilitate split shipments.
- Refund and void operations can be set to require an additional (e.g. supervisor) password to complete. The ability to do refunds and voids is granted at the discretion of ITA and bank, and refunds cannot be performed unless linked to the original transaction. Refund amounts can only be less than or equal to the original transaction amount.
- Each transaction has a drill-down function to show the full detail (e.g. RRNs, Auth codes etc). The credit card details can be masked (as determined by the bank) for both Merchant-Collected and Server-Collected transactions as follows –
    - No Display
    - 0.4 (e.g. xxxxxxxxxxxx7657)
    - 6.3 (e.g. 543212xxxxxx7567)
- Transactions are shown as a linked set of transactions deriving from an initial "shopping transaction", with subsequent financial transactions (i.e. captures, refunds or voids) linked. In this manner a full audit history of each "shopping transaction" can be viewed using drill-down techniques.
- A number of standard report formats are available for the merchant's use including:
    - Transaction count for a selectable period.
    - Transaction dollar volume for a selectable period by merchant, transaction type or card type.
    - Total transactions reconciled for a selectable period, total or by merchant.
- Merchant access is secured using 128-bit SSL. The merchant is identified by an ID and user/password combination disclosed to the authorized merchant user.

- Multiple merchant operators can be created and granted various privileges based on responsibility levels.

To access the administration functions the user must enter their merchant number, user name and a password.

Data that can be displayed in Merchant Administration is transaction history data which is stored up to 12 months after the transaction was processed.

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



Financial Transaction Search Screen

MiGS provides both on-screen and transaction downloads reports. All data available for the merchant is for that merchant only.

7. Settlement of e-Payments

The acquiring bank will perform settlement with the customer's banks via the international card network. The settlement funds net all fees will be credited to the merchant's account with the acquiring bank.

8. Hardware, software and telecommunication network requirements

The following are the hardware, software and telecommunication facility which the merchant needs to provide to perform integration with the MiGS e-PG system:

Hardware and Software

- Web server hardware which hosts the merchant online shop website. Any common Web server software which can run one of the ASP/JSP/PHP programs for the sample codes of MiGS VPC can be used. Examples are Microsoft IIS, Apache/Tomcat Jakarta, Web sphere, Cold Fusion.
- Any PC with Internet browser for merchant users to connect to MiGS system for performing merchant administration

Telecommunication Facility

Any Internet connection through which the merchant Web server can connect to the MiGS system using a URL redirect mechanism.

9. Steps for Merchant Integration with National e-PG System

The above sections provide a basic understanding of the technical information for merchant to integrate with the ITA National e-PG system.

Should merchant wish to proceed with the integration work and implement e-payment solution for their website, the steps to be taken are as follows:

1. Merchant should contact ITA e-PG team to sign-up for merchant agreement to adopt the ITA provided National e-PG payment services.

2. ITA will prepare agreements to be signed between ITA and merchant, this includes Non-Disclosure Agreement, Membership Agreement and Software access license agreement. In

addition, ITA will provide internet acquiring card transaction merchant agreements to be signed between merchants and the acquiring bank. ITA will send signed agreement to Bank on behalve of merchant and get the signed copy back to merchant.

3. ITA will provide the Virtual Payment Client (VPC) Sample Script (in one of ASP/JSP/PHP context) with the VPC Integration Guide manual document to the technical team of the merchant,

4. The technical team of the merchant should adopt the VPC Sample Scripts API in their online shop web pages.

5. For testing the VPC and payment processing with MiGS system, ITA will provide the Merchant Id and Internet URL of the MiGS Test environment. The merchant will then be able to connect to the MiGS test environment. ITA will provide the test plan for merchant to test with the MiGS system.

6. Upon completion of testing with the gateway, merchant has to sign a Test declaration form which will be provided to merchant along with test details. ITA will then switch merchant to live after review of the website

10. Fees

- One-time joining fee – OMR50
- Single transaction fee at 3.5 % of transaction value per transaction, inclusive of fees to (issuing banks, acquiring bank & Visa/MasterCard net).
- Monthly Merchant Maintenance Fee – OMR50 per month.