

Integrated Mobile Secure (IMS)

Enhanced 3D Secure Add-on for Issuer with

2 Factor Authentication • OTP (One Time Password) • Dynamic Authentication Method
Out Of Band Authentication • Transaction Alert • Fraud Notification • Multi Payment Channel

A man in a grey pinstriped suit and light blue shirt is sitting in a dark wooden chair, looking at a smartphone. The background is a blurred green and blue bokeh.

INFINITIUM
IMS



The Infinetium Integrated Mobile Secure (IMS) is a payment server product designed for Issuer to provide a comprehensive payment verification and authentication capability for their Card-Not-Present (CNP) transactions.



The Infinetium Integrated Mobile Secure [IMS] is a payment server product designed for Issuer to provide a comprehensive payment verification and authentication capability for their Card-Not-Present (CNP) transactions.

Authentication for CNP payment such as E-commerce, Mobile Commerce and MOTO (Mail Order Telephone Order) remains one of the main challenges facing the Payment Industry affecting all the parties in the ecosystem - Acquiring Bank, Merchant, Issuing Bank and Card Holder.

The 3D Secure Framework is widely recognized as the standard for Verification and Authentication under VISA's VBV and Master's SecureCode program that was introduced largely to address the E-commerce channel.

Infinetium IMS solution is designed as an extension of the 3D Secure Framework to enhance the verification and authentication process with mobile based 2FA and capability to extend to other payment channel such as MOTO, IVR, Mobile Commerce. Some of the key benefits includes:-

- 2 Factor Dynamic Authentication to address Phishing, Trojans, Man-In-Middle, Keyboard logging attacks.
- Utilizes Stronger Security Control with Dynamic Password/One Time Password/Mobile Signature.
- Eliminate the need for customer to register and remember static password.
- Real Time Fraud Notification and Reporting by Card holder.
- Capability to extend to more channels such as MOTO, Mobile Commerce, IVR and EDC Terminal.



The key highlights of IMS is the capability to extends the 3D framework to include other payment channel notably MOTO, Mobile Commerce transactions as well as the elimination of static password with 2FA Dynamic Authentication that is in line with the direction of many security policy set by central bank governing agencies.



Features and Functionalities



Ready To Go Hosted

Infinetium IMS provides a "ready to go" hosted solution model whereby all the infrastructure are ready for deployment. Minimal time to market and eliminates the need to manage the system and maintenance functions.



Elimination of Static Password

One of the most significant enhancements with IMS is the ability to eliminate the need of Static Password. Card Holder does not need to register and remember any password. The challenges of forgetting and resetting the password is also eliminated.



Mass Enrolment

Enrolment and Registration has always been the Achilles' heel of the 3D deployment for the Issuer due to it's complexity and customer participation issues. With IMS, Issuer can proceed with Mass Enrolment without requiring further "action" from cardholder. With these flexibility and simplicity, the 3D secure adoption will be successful.



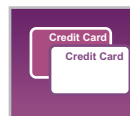
Expansion to Multi Payment Channel

Issuer can extend IMS's authentication capability to handle multiple payment channel such as MOTO, Mobile Commerce, Auto-bill and IVR. This will provide the card holder with a common and seamless authentication methods everytime they used their card regardless of the channel of the merchant.



Transaction Alert

Every time a credit card is been used in CNP scenario, IMS will send an authentication message to the cardholder mobile devices. The cardholder will be able to report a fraudulent transaction in real time if they ever suspect that their card has been compromised. IMS can trigger the bank host to temporarily suspend the card in such event. This will help the bank to further minimize fraud and chargeback.



Full Compliance

Infinetium IMS is designed to be fully compliant with payment standards in mind. IMS supports both Visa's 3D Secure and Mastercard SPA-UCAF standards. Infinetium IMS is in compliance with PCI-DSS. In addition, Infinetium strong in-house R&D team and innovative support ensures that the product stays relevant in today's dynamic world.



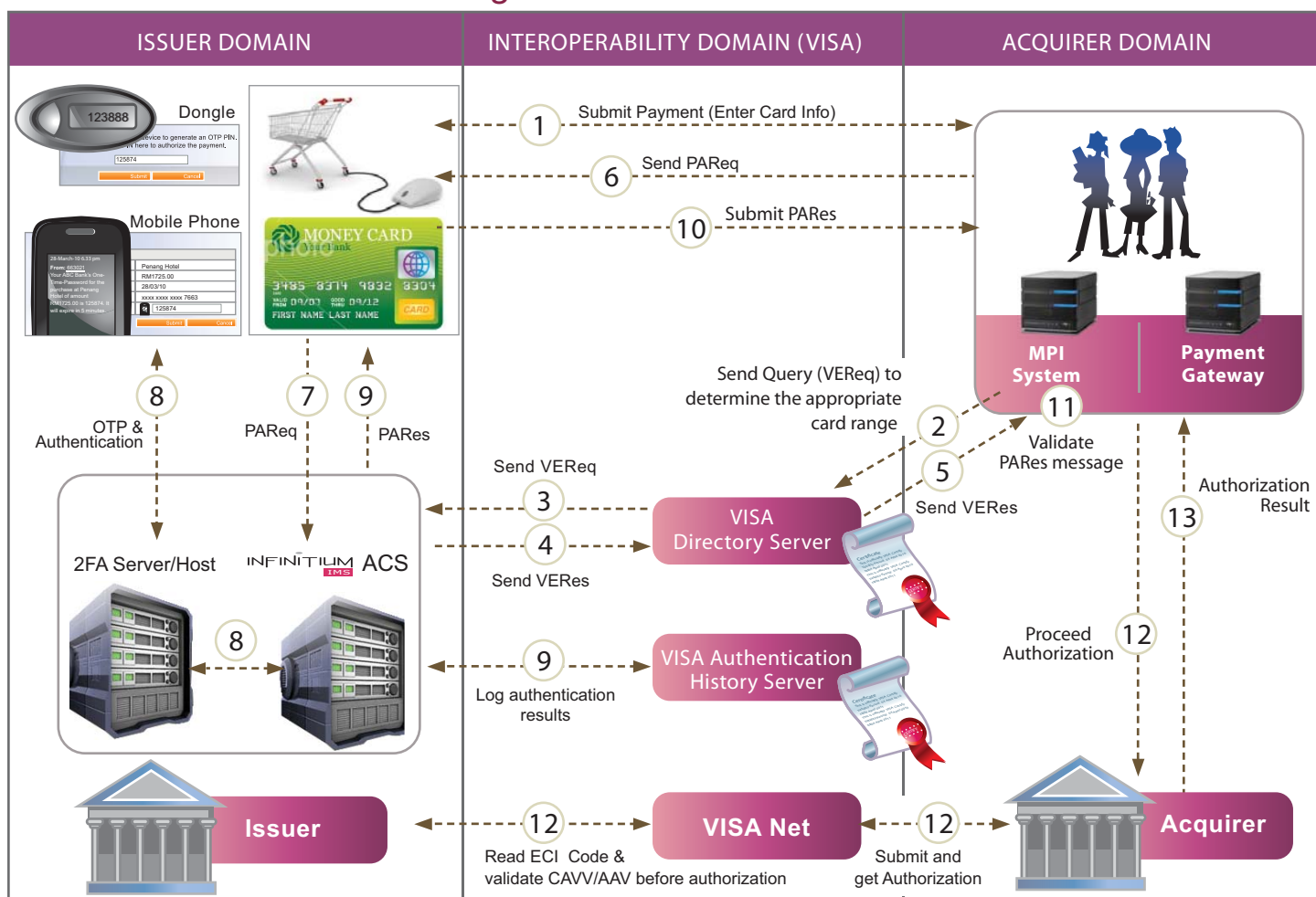
Enhanced Security with Dynamic Authentication

IMS enhances the standard customer authentication protocols such as Visa's 3D Secure and MasterCard's SPA-UCAF with additional processes via the IMS adaptor. The IMS not only offers the capability for 2 Factor "Out of Band" authentication via mobile devices, it also eliminates the threats of Phishing, Trojans, Man-In-Middle attack and keyboard logging.

Infinetium IMS also supports a wide range of authentication methods providing flexibility to Issuer to pick and choose different authentication methods that suits the market demand. Some of the possible authentication methods includes:-

Authentication Method	ACS Window	SMS Fraud Alert	PIN Displayed	Authentication Entry
USSD A	Notification	Yes	Mobile Phone	Mobile Phone
USSD B	Enter Pin	Yes	Mobile Phone	Web Browser
SMS Push A	Notification	Yes	Mobile Phone	Mobile Phone
SMS Push B	Enter Pin	Yes	Mobile Phone	Web Browser
SMS Pull	Display Pin	No	Web Browser	Mobile Phone
OTP Dongle A	Enter Pin	No	OTP Dongle	Web Browser
OTP Dongle B	Notification	No	OTP Dongle	Mobile Phone
Digital Signing	Notification	Yes	Digital Signing PIN	Mobile Phone
VBV/SecureCode Password	Enter PIN	No	None	Web Browser

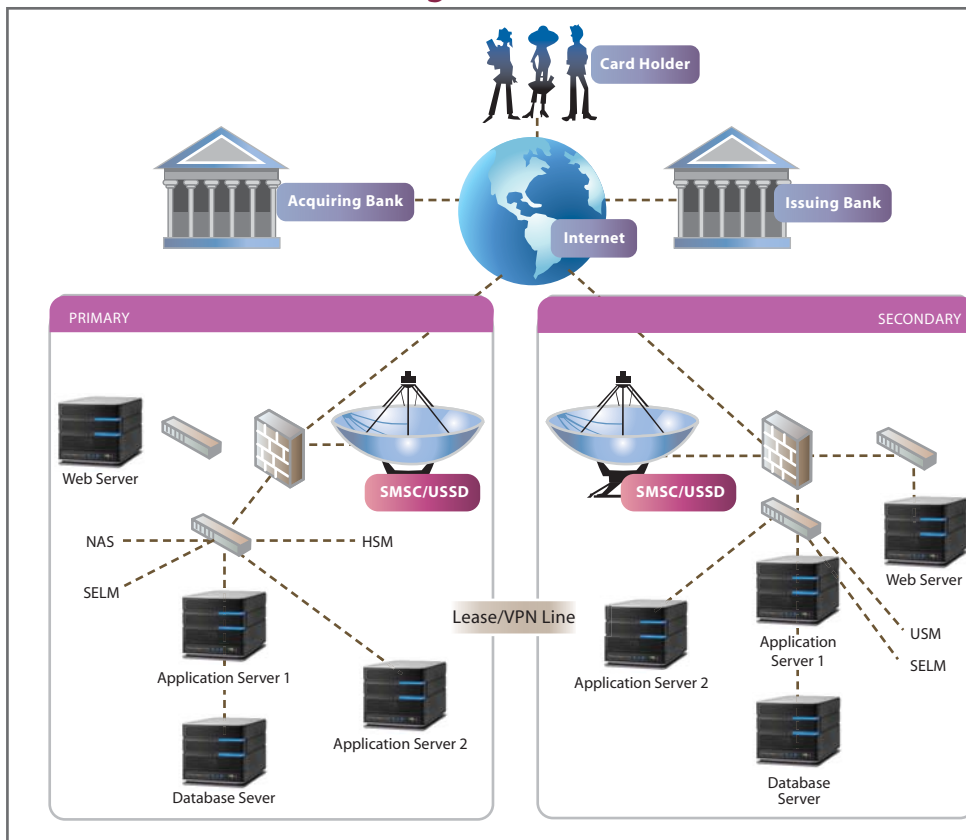
IMS Authentication Processing



1. Shopper browses at merchant site, finalizes a purchase and makes payment. Merchant now has all the necessary data to begin 3D Secure processing, including card number.
2. Merchant Server Plug In (MPI) which may be hosted by the Merchant, the Acquirer or a third party will send card number to Visa/MasterCard Directory Server.
3. If card number is in a participating card range, Visa/MasterCard Directory Server queries appropriate ACS to determine whether authentication is available for the card number. If no appropriate ACS is available, the Visa/ MasterCard Directory Server creates a response for the MPI and processing continue with Step 5.

4. IMS's ACS responds to Visa/MasterCard Directory Server.
5. Visa/MasterCard Directory Server forwards ACS response (or its own) to MPI.
6. MPI sends Payer Authentication Request to ACS via shopper's browser.
7. IMS's ACS receives Payer Authentication Request
8. Cardholder enters password using authentication method which is applicable to the card number. IMS's ACS authenticates shop per for the card number, then formats the Payer Authentication Response message with appropriate values and signs it digitally. The Payer Authentication Response message contains an ECI (Visa)/ UCAF(MasterCard) value indicating the authentication result. The CAVV(Visa)/ AAV(MasterCard) values which serve as a proof that authentication happens.
9. IMS's ACS returns Payer Authentication Response to MPI via shopper's browser. Meanwhile if this is a Visa card, authentication results will be sent to Visa Authentication History Server (AHS).
10. MPI receives Payer Authentication Response.
11. MPI validate Payer Authentication Response signature. (either by performing the validation itself or by passing the message to a separate Validation Server).
12. Merchant proceeds with authorization exchange with its Acquirer. Acquirer processes authorization with Issuer via Visa/MasterCard Net, then returns the result to Merchant. When issuer bank receives authorization request from acquirer bank, the issuer bank needs to validate the ECI/UCAF and CAVV/AAV value. Issuer bank may opt to reject the authorization in case of the 3D authentication is failed or the CAVV/AAV value is not valid. Customization at issuer bank host is required to read the ECI/UCAF value and validate the CAVV/AAV.
13. Acquirer return the authorization result to Merchant.

Hosted Infrastructure Diagram



As part of the hosted infrastructure, we will provide the above system configuration as part of our solution offering for the hosted model. There will be 2 sets of system (Primary and DR) running in two different Data Center with 2 different Internet backbone. The servers is designed with high availability configuration.

The Hosted Platform will consist of the following:-

- Firewalls
- IPS/IDS system
- Web Servers
- Application Servers
- Database Servers
- Monitoring and Fault Reporting System
- SMSC/USSD connectivity
- File Integrity Monitoring system
- System Policy Management system
- Event Log Management system
- Central Antivirus Management Console
- Stringent physical access controls to all servers.



Our system are monitored 24 X 7 and SMS alerts are triggered to our support engineer for critical event. All systems are managed in accordance to recognized standard such as Payment Card Industries Data Security Standards. (PCIDSS)

Sample Screen Shot of IMS

The screenshot shows the IMS web application interface. The top navigation bar includes Home, Card Holder Management, Report, Configuration, and User Management. The main content area displays a table of Card Holder Accounts with the following data:

No.	Card No.	Issuer Id	Status	Authentication Type	Mobile Num.	Last Successful Authentication Date
1	4888880000000201	NET_Visa	Active	One Time Password		
2	4111110000000001	NET_Visa	Active	One Time Password		
3	4888880000000001	NET_Visa	Active	One Time Password	012315069	08/04/2009 11:59:29
4	4111110000000001	NET_Visa	Active	One Time Password		
5	4111110000000011	NET_Visa	Active	One Time Password	012315069	
6	4111110000000001	NET_Visa	Disabled	One Time Password		27/05/2009 11:17:46
7	4888889999999999	NET_Visa	Inactive	One Time Password		27/05/2009 10:53:36
8	4333330000000001	CHB_Visa	Active	One Time Password		27/05/2009 15:50:54

The screenshot shows the details for a specific Card Holder Account. The information is organized into several sections:

- General Information:** Card No: 4888880000000201, Issuer Id: NET_Visa, Status: Active, Authentication Type: One Time Password, Mobile Num.: 60125985421.
- Registration Information:** Registration Date: 27/05/2009 09:05:24, Registration Method: ADS, Personal Message: testing, Password: eJtJYGwyHIzyKNF5QmCO/wzMQXE=.
- Authentication Information:** Last Successful Authentication Date, Last Attempt Date, Fail Count: 0.
- Audit Information:** (Section header visible).

Sample screen on mobile phone when requesting digital from card holder. When cardholder call up, customer service agent will search for cardholder card number for detail information.

Incoming Authentication

Results: 1-48 41-80 81-116 Next » [116 records(s) found]

No.	Payer Id	Txn Date	Issuer Id	Auth Type	Acct Id	Merchant Name	Trans
1	386	08/06/2009 04:10:39	NET_Visa	One Time Password	6093689651040521598	My Hotel	
2	385	08/06/2009 01:51:17	NET_Visa	One Time Password	6093689651031389495	My Hotel	
3	384	08/06/2009 01:49:38	NET_Visa	One Time Password	6093689651031290198	My Hotel	
4	383	08/06/2009 01:38:27	NET_Visa	One Time Password	6093689651030619917	My Hotel	
5	382	07/06/2009 11:02:51	NET_Visa	One Time Password	609368965978148026	My Hotel	
6	381	05/06/2009 06:41:15	NET_Visa	One Time Password	609368965790368537	My Hotel	
7	380	05/06/2009 06:31:56	NET_Visa	One Time Password	609368965789809146	My Hotel	
8	379	05/06/2009 04:13:51	CIMB_Visa	One Time Password	1110793984781525075	My Hotel	
9	378	05/06/2009 04:13:30	CIMB_Visa	One Time Password	1110793984781503388	My Hotel	
10	377	05/06/2009 03:52:52	CIMB_Visa	One Time Password	1110793984780264346	My Hotel	
11	376	03/06/2009 10:23:21	NET_Visa	One Time Password	609368965630177073	Peace Nature Hotel	
12	375	03/06/2009 10:06:50	NET_Visa	One Time Password	609368965629186104	Peace Nature Hotel	
13	374	03/06/2009 10:06:22	NET_Visa	One Time Password	609368965629158151	Peace Nature Hotel	
14	373	03/06/2009 10:05:59	NET_Visa	One Time Password	609368965629135292	Peace Nature Hotel	
15	372	03/06/2009 10:04:59	NET_Visa	One Time Password	609368965629075901	Peace Nature Hotel	
16	371	03/06/2009 10:03:24	NET_Visa	One Time Password	609368965628981058	Peace Nature Hotel	
17	370	03/06/2009 09:57:58	NET_Visa	One Time Password	609368965628654776	Peace Nature Hotel	
18	369	03/06/2009 09:12:03	NET_Visa	One Time Password	609368965625900151	Peace Nature Hotel	

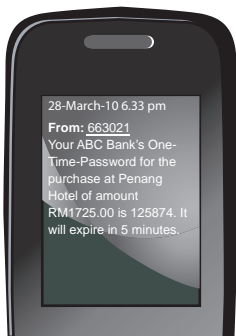
Incoming Authentication - View

General

General Information	
Payer Id	386
Issuer Id	NET_Visa
Transaction Information	
Txn Date	08/06/2009 04:10:39
Auth Type	One Time Password
Installment	0
Transaction Amount	MYR 848.00
Merchant Information	
Merchant Name	My Hotel
Merchant Country	458
Merchant Url	http://www.myhotel.com
Authentication Result	

Sample screen on Incoming Authentication. Customer services agent are able to search and filter Authentication Attempt, Authentication Statistic, Incoming Verification, Registration Attempt report.

Sample Screen Shot of Various Authentication Methods



Enter Your One-Time Passcode

Your mobile phone has been registered for ABC Bank's Secure SMS Service. An SMS has been sent to your mobile phone. Please enter your One-Time Passcode in the field below to verify your identity for this purchase.

Transaction Details	
Merchant	Penang Hotel
Amount	RM1725.00
Date	28/03/10
Card Number	xxxx xxxx xxxx 7663
One-Time Passcode	<input type="text" value="125874"/>

Verified by VISA INFINITIUM TMS

The Transaction Is Authorized By Bank.

Please click on "Print" button on below to print this receipt for your own reference.

Transaction ID	OID201003280001	Payment Ref No.	R8889003
Transaction Date	28/03/2010	Payment Method	Credit Card
Transaction Amount	MYR 1725.00	Approval Code	87716776
Receipt No.	A6663421	Card No.	xxxx xxxx xxxx 7663

RoomType	Check-in Check-out	No. Of Nights	No. of Rooms	Rate(MYR)
Double Bed Room BEST AVAILABLE -INCL BREAKFAST	Check-in 15-04-2010 Check-out 20-04-2010	4	1	1500.00
Government Tax - 5% of Total Package Charge				75.00
Service Charge - 10% of Total Package Charge				150.00
Remaining Amount Payable at Hotel				1725.00

Verified by VISA INFINITIUM TMS

Sms Push B

Receive the One Time Password (OTP) directly on the phone via SMS and key in <ID> on the web for authentication.

Processing...

Waiting for Mobile Authorization Confirmation.

Please do not click on Back, Stop, Refresh buttons, or close window while we are processing your payment..

Sending authorization request to your registered mobile number 012 565 1104

Transaction Details	
Merchant	Virtual Hotel KL
Amount	RM1748.00
Card Number	xxxx xxxx xxxx 7663

Verified by VISA INFINITIUM TMS



The Transaction Is Authorized By Bank.

Please click on "Print" button on below to print this receipt for your own reference.

Transaction ID	OID201003280014	Payment Ref No.	R02099911
Transaction Date	29/03/2010	Payment Method	Credit Card
Transaction Amount	MYR 1748.00	Approval Code	1001092
Receipt No.	A236985	Card No.	xxxx xxxx xxxx 7663

RoomType	Check-in Check-out	No. Of Nights	No. of Rooms	Rate(MYR)
Studio Room BEST AVAILABLE -INCL BREAKFAST	Check-in 01-06-2010 Check-out 05-06-2010	4	1	1520.00
Government Tax - 5% of Total Package Charge				76.00
Service Charge - 10% of Total Package Charge				152.00
Remaining Amount Payable at Hotel				1748.00

Verified by VISA INFINITIUM TMS

USSD A

Receive the One Time Password (OTP) directly on the phone via USSD while the browser waits for mobile authentication, user respond via mobile with 1 to accept transaction, 2 to reject transaction and 9 to report fraud.

Please use your security device to generate an OTP PIN. Then enter the PIN here to authorize the payment

Verified by VISA INFINITIUM TMS



The Transaction Is Authorized By Bank.

Please click on "Print" button on below to print this receipt for your own reference.

Transaction ID	OID201003300784	Payment Ref No.	R02099911
Transaction Date	30/03/2010	Payment Method	Credit Card
Transaction Amount	MYR 1380.00	Approval Code	8541092
Receipt No.	A58754845	Card No.	xxxx xxxx xxxx 1212

RoomType	Check-in Check-out	No. Of Nights	No. of Rooms	Rate(MYR)
Studio Room	Check-in 01-05-2010 Check-out 05-05-2010	4	1	1200.00
Government Tax - 5% of Total Package Charge				60.00
Service Charge - 10% of Total Package Charge				120.00
Remaining Amount Payable at Hotel				1380.00

Verified by VISA INFINITIUM TMS

Dongle

Generate the One Time Password (OTP) directly via dongle. User key in the OTP provided on browser for authentication.

Other Value Added Payment Solutions



INFINITIUM
ePayment

Infinitium ePayment for Acquirer

The Unified Payment Platform that simplifies online payment processing with multi channel, multi payment modes and real time fraud detection for acquiring merchant.

- Support multiple payment modes - credit card/debit card/edebit/loyalty points/ewallet.
- Real time credit card acquiring with multi currency.
- Real Time Fraud Scoring and Profiling.
- Automated Reconciliation System.
- Web based management consoles.



INFINITIUM
RPS

Recurring Payment System (RPS) for Acquirer.

Dedicated system targeted at acquirer who provides payment processing for auto billing merchant for recurring payment such as monthly bills, installment plan, monthly membership, insurance premium renewal and etc.

- Automation of Auto Billing facility with Auto File-Mapping merchant for multiple merchant.
- Web based Management Console.
- Real-time Credit Card Acquiring with multi currency.
- Fully customizable reporting template for multiple bank submission.
- Multi business rules for exception handling of expired or invalid card.



INFINITIUM
E-Mail

Infinitium eMail

Comprehensive online storefront solution for large merchants and banks with online catalog, shopping cart, shipping logic and payment system fully integrated.

- Support multiple biz model for B2C, B2B, Many to Many, One to Many.
- Support multiple Micro sites for sub-merchant/supplier.
- Support product redemptions as well as "money plus point" purchases.
- Various marketing module such as Buy 1 Get 1 Free, Free Shipping, Promotion, Voucher Discount, etc.
- Suggestive selling and up-selling modules
- Ideal for bank's Email with backend integration for On-Us routing.



INFINITIUM
E-MANAGER

Infinitium eManage

Enterprise Outsource Service for large enterprise and bank. We offer outsource service for our whole range of products and solutions. Our eManage client does not need to invest in hardware/software and man-power to manage all these system.

Infinitium eManage are tailor made on a requirement basis for each of our customer. eManage contract are mainly for Online Storefront, Unified Payment Platform and Fraud Detection System.

- eManage of system hardware and software with 24X7 support.
- eManage of Bank's Email with order processing and catalog updating.
- eManage of Airlines's Unified Payment Platform with 24X7 monitoring and support.
- eManage of inbound IVR Call center payment.

Infinitium Offices

Malaysia

Infinitium Group of Companies
No.15-2, Block C1, Jalan PJU 1/41, Dataran Prima,
47301 Petaling Jaya, Selangor, Malaysia.

Tel (+603) 7880 4077
Fax (+603) 7803 5077

Indonesia

PT Infinitium Solutions
Mayapada Tower Lt. 19-02A,
Jl. Jend. Sudirman Kav. 28, Jakarta Selatan,
Indonesia.
Tel (+6221) 525 3389 / (+6221) 522 6751
Fax (+6221) 522 6571

Singapore

Infinitium Solutions Pte Ltd
8 Ubi Road 2,
#04-05 Zervex,
Singapore 408538.

Tel/Fax : (+65) 6383 4346