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

INFINITIUM
Securing Payment & Beyond
The Infinitium 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.

Infinitium 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.

Infinitium 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.

Enrolment and Registration has always been the Achillies’ 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 3 secure adoption will be successful.

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.

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

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**

Infinitium 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.

**Mass Enrolment**

Enrolment and Registration has always been the Achillies’ 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.

**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.

**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.

**Expansion to Multi Payment Channel**

Issuer can extend IMS’s authentication capably 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.

**Full Compliance**

Infinitium IMS is designed to be fully compliant with payment standards in mind. IMS supports both Visa’s 3D Secure and Mastercard SPA-UCAF standards. Infinitium IMS is in compliance with PCI-DSS. In addition, Infinitium 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.

Infinitium 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:-

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>ACS Window</th>
<th>SMS Fraud Alert</th>
<th>PIN Displayed</th>
<th>Authentication Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>USSD OTP</td>
<td>Notification</td>
<td>Yes</td>
<td>Mobile Phone</td>
<td>Mobile Phone</td>
</tr>
<tr>
<td>USSD B</td>
<td>Enter Pin</td>
<td>Yes</td>
<td>Mobile Phone</td>
<td>Web Browser</td>
</tr>
<tr>
<td>SMS OTP</td>
<td>Enter Pin</td>
<td>Yes</td>
<td>Mobile Phone</td>
<td>Web Browser</td>
</tr>
<tr>
<td>VBV/SecureCode Password</td>
<td>Enter PIN</td>
<td>No</td>
<td>None</td>
<td>Web Browser</td>
</tr>
</tbody>
</table>

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 result 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 issuer 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

Sample Screen Shot of IMS

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.
Sample Screen Shot of Various Authentication Methods

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

**Virtual Hotel KL**

RM1748.00
28/03/10
xxxx xxxx xxxx 7663
125874
From: 663021

Your Netbank Bank’s One-Time-PASSWORD is 125874 for the purchase at Penang Hotel amount RM1725.00. It will expire in 5 minutes.

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

**Penang Hotel**

RM1725.00
28/03/10
xxxx xxxx xxxx 7663
125874
From: 663021

Netbank Bank VISA Pymt Request Name: Virtual Hotel KL Amt: RM1748.00
P1 to accept 2 to reject 9 to report fraud

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

**Incoming Authentication**

<table>
<thead>
<tr>
<th>Process</th>
<th>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</th>
</tr>
</thead>
</table>

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

**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.

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

**The Transaction Is Authorized By Bank.**

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

**The Transaction Is Authorized By Bank.**

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

**The Transaction Is Authorized By Bank.**

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