

The
Authority
on Payment
Solutions

Issue 12 / June 07



The Goldfinch Report

GFG
GROUP

PAYMENT
SOLUTIONS
YOU CAN
BANK ON

Mobile - Current Positioning for the Developing Economies

Mobile devices such as cell phones are now being used as an extension of the ATM and eftpos channels, writes Peter Goldfinch - GFG Group's General Manager for South East Asia. Peter's credentials have been earned over 23 years experience in electronic payments, including pioneering work on ATMs and EFTPOS, and the introduction of credit and debit cards in a range of countries.

Mobile handsets are the new payment delivery channel. They can be positioned as either an extension of the ATM and eftpos (with PIN) networks as well as being seen as the small screen version of the Internet, supporting m-commerce applications. Mobile handsets' versatility is what makes them a powerful payment channel.

With the development of the mobile network capability and the capacity to handle data, mobile is being promoted in some markets as an alternative access device for the Internet. Internet commerce and banking services can now be accessed using existing processes with a mobile device. It is largely big screen vs. little screen. The transaction security is equally weak on both services - even with the introduction of 3D secure and 2 factor authentication processes.

“MOBILE’S
VERSATILITY IS
WHAT MAKES
IT A POWERFUL
CHANNEL.”

“INTERNET
COMMERCE AND
BANKING SERVICES
CAN NOW BE
ACCESSED WITH
A MOBILE DEVICE.”

This paper concentrates on the use of mobile handsets as an extension of the ATM and eftpos channels. This is where the mobile device supports the same security and messaging standards as those two debit account access services. In these areas the concept of non-repudiation is realizable.

In addition mobile enables banking and payment services to be delivered to a sector of the population not currently covered. The low cost of mobile delivery for the financial sector allows it to target the unbanked without the need to build an expensive infrastructure associated with branch banking and ATM networks.

The handset as surrogate payment card

There is a pre-requirement that users be mobile subscribers. There must be mobile coverage where the user resides. In reality not all potential users are in this situation. As the reasons for having a mobile handset become more compelling, the business case for operators to extend their service – and subsidize handsets – will ensure more individuals become users of the service.

The key point is that banks and Telcos will not need to invest in the infrastructure required to support the mobile payment channel. The operator’s business case, based on current subscriber fee structures, will ensure the infrastructure grows with market demand. The revenue derived from the payment service is only one revenue line item in the business model.

The proposition is that the handset becomes a surrogate payment card. This means the mobile handset has the ability to access a bank account, and can be used by account holders to send payment instructions to their bank. For the unbanked the payment channel will need to be supported by a prepaid card/account base. This will deliver an end-to-end service where the unbanked person no longer needs to deal only in cash, and can receive and make payments electronically, plus build up a history of both savings and fiscal responsibility.

Micro loans can also be delivered across mobile, with the potential to both control the spending and provide a method to receive repayments electronically. There are optional methods of managing the user interface for the illiterate person through three dimensional bar coding.

The types of transactions that can be supported by a mobile payments service are:

Person to Person: This is the cornerstone of the mobile payment service as it allows account holders to transfer funds in real-time and at a low cost. Typically this process facilitates domestic remittances without geographical or service access constraints.

Person to person payment also facilitates ad hoc payments to small businesses and merchants.

Bill Payments: The ability to pay regular bills on demand where the amount may vary.

Either party can initiate payment requests.

Remote Purchases: Typically referred to as the ‘card not present’ situation. A request is sent to the mobile handset by the merchant, for acceptance by the purchaser of payment.

These payments can also be initiated from the handset. This is the case when the handset is used to initiate the purchase of airtime.

Non-Financial: Balance enquiries and transaction listings are two support transactions. These are required to complete the services.

“MICRO LOANS CAN BE DELIVERED ACROSS MOBILE, WITH THE POTENTIAL TO BOTH CONTROL THE SPENDING AND PROVIDE A METHOD TO RECEIVE REPAYMENTS ELECTRONICALLY.”

“THE ACCOUNT OR ACCOUNTS ARE LINKED TO EITHER A VIRTUALLY OR PHYSICALLY ISSUED PAYMENT CARD. THE BANKED POPULATION MAY USE THEIR EXISTING ATM OR DEBIT CARD.”

Account holder authentication

As with any payment transaction, it is critical to authenticate the transactor as having the authority to access the funds. For this reason, the service is recommended to be restricted to one account holder per handset. That is, the account holder can only perform transactions on his own registered handset and a handset is not to be used by multiple account holders. This is not a technology restriction, but rather a recommended imposed business restriction to support the integrity and security of the payment channel.

The registration process needs to meet banking standards concerning identification of the account holder. The handset phone number and SIM is then cross-referenced and linked to the subscriber's payment card. This affects the surrogate payment card concept. The account or accounts are linked to either a virtually or physically issued payment card.

Physical means a plastic card is issued. The card may also be issued to provide the account holder with access to ATMs for cash withdrawals or to perform card-present purchases at the point of sale. A virtual card exists only in the system. No plastic is issued, and the account holder does not need to know of its existence.

This payment card for the banked population may already be issued. It may be their currently held ATM or debit card. It may be branded or proprietary, and it may be their credit card. The point is it does not need to be specially issued or unique to the mobile service. The requirement is that the card provides the relationship of the account holder to their accounts. It is also the basis for account holder authentication, as it is in the ATM network.

When a transaction is initiated on the handset, it is not necessary for account information to be sent over the air. Put another way, it does not have to be contained in the payment instruction. If multiple accounts are supported then a default account can be used in the same way as an ATM fast cash transaction, or the option to select from a list of accounts can be supported. Again, this is done by many ATM services.

The mobile payment server, (resident in the network or with the bank) links the handset phone number to the account holder's profile, (established at the time of registration). It is this profile that holds the details of the payment instruments.

At this point in the development of mobile payments, the recommendation is for this account information to be held only on the network server, (securely) and not downloaded to the mobile device. In the future, for mobile handsets to support NFC payments the card detail will be downloaded and maintained over the air, (OTA). As payment instrument, details will need to be supported on the handset.

The account holder when initiating a transaction is required to enter a PIN. The PIN is validated in the same manner as an ATM PIN, using a banking standard algorithm such as the IBM or PVV method. The PIN is based on the card number. Optionally the PIN keys can be the same as those used for a physical card (if issued) or a unique set so the derived PIN for the handset is different from the derived for the plastic. Customer PIN select may mean the account holder elects to have a common PIN.

If the PIN fails validation a transaction is denied and if 'X' attempts fail then the handset and physical card, (if issued) should both be blocked.

Payment security

This approach to mobile payments requires a robust level of security. Security should be based on the following:

1. The deployment of triple DES or PKI encryption on the SIM. Each handset should hold three unique triple DES keys. A key each for PIN block encryption, transaction data encryption and over the air, (OTA) data encryption. The recommendation is for the OTA key to be injected at manufacture with the other two downloaded on service initialization. For the data encryption the preferable option is to use a DUKPT generated key.

About Peter

Peter Goldfinch, GFG Group's General Manager South East Asia, is a respected analyst and commentator on global trends in payment technology.

One of the original founders and shareholders in GFG Group, Peter has a background of more than 23 years in the information technology industry, most of which has been involved with consulting and systems development for banking and finance customers in 25 countries.

He has particular expertise and experience in payment systems, including mobile payment systems. His career highlights include pioneering work on the first ATM and EFTPOS networks.

In the mid-1990s, he played a key role in the introduction of credit and debit cards into the Russian market, working with GFG's customer SBRF.

About GFG

32 million consumers in 39 countries use GFG software applications. More than 20 years of payments experience stands behind the company's worldwide leadership in integrated Card and Mobile-based payment products.

Accredited by the World Bank, GFG's solutions are based on a single, integrated architecture comprising two key products:

Simfonie™ A proven, market-leading product which enables a mobile handset to operate as a fully mobile payment device.

Cadencie™ A full-function, real-time, credit, debit and charge card management system.

GFG Group operates from offices in Auckland and Wellington New Zealand, Melbourne Australia, Manila in the Philippines, Singapore and Toronto. The company's core research and development team is based in Auckland, with consultants and technical staff located in the international offices to provide front line 24/7 support for customers in multiple geographies.

GFG Group Ltd
Level 10
Qantas House
191 Queen Street
Auckland
P O Box 5825 Wellesley Street
Auckland 1141

Telephone: +64 9 966 7041
Facsimile: +64 9 966 7070
E-mail: info@gfg-group.com

2. Security is enhanced if the transaction does not hold any payment card details. An alternative to using the phone number as suggested above is to download at initialization a card proxy generated by a one-way hash algorithm. The proxy – if compromised, or as a precaution – can be re-generated at set intervals without the need to change the card number.
3. Industry standard key management practices must be deployed with the implementation of host security modules. Key generation practices employed for ATM and eftpos should be used for mobile. Keys should not be transported or stored in the clear and not be known by any one individual.
4. Data such as card numbers held by the network server in the network must be either encrypted or truncated.
5. The utilization of transaction permissions, limits and velocity checks is suggested. This is standard practice for eftpos and ATMs.

A key element of security is to ensure if a single handset is compromised then the risks are contained to only that handset. What has been described above will achieve this goal.

Transaction integrity

Transaction processing must be in compliance with payment practices as outlined in standards such as ISO8583. This means the processing for every transaction must be completed, even if unsuccessful from a business perspective.

Time limits are required to be placed on message responses. If responses are not received within these limits then reversal processing needs to take place. If a system link is down then store and forward processes should be instigated to ensure transactions are completed once the link is re-established.

These are the same processes as those used for ATM and eftpos systems.

In summary a mobile payment solution needs to:

1. Be considered as another delivery channel similar to ATMs and EFTPOS, (with PIN).
2. The handset should be treated as a surrogate card.
3. Restrict the amount of data held on the handset to a minimum, using proxies if appropriate.
4. Deploy key management functions, same as for ATMs and EFTPOS (with PIN) networks.
5. Utilize 3DES keys for PN block, transaction and OTA encryption.
6. Deploy standard message integrity processes.
7. Deploy velocity and transaction risk management techniques.