Mobile Payment Systems and Services: An Introduction

Mahil Carr
IDRBT
Hyderarbad
mahilcarr@idrbt.ac.in

1. Introduction

Three billion people are expected to own mobile phones in the globe by 2010. There are currently 225 million mobile phones in India and 100 million are added every year. In a few years more than 500 million people are expected to have mobile phones in India (MPFI, 2007).

Mobile commerce is a natural successor to electronic commerce. The capability to pay electronically coupled with a website is the engine behind electronic commerce. Electronic commerce has been facilitated by automatic teller machines (ATMs) and shared banking networks, debit and credit card systems, electronic money and stored value applications, and electronic bill presentment and payment systems. Mobile payments are a natural evolution e-payment schemes that will facilitate mobile commerce. A mobile payment or m-payment may be defined, for our purposes, as any payment where a mobile device is used to initiate, authorize and confirm an exchange of financial value in return for goods and services (Au and Kauffman, 2007). Mobile devices may include mobile phones, PDAs, wireless tablets and any other device that connect to mobile telecommunication network and make it possible for payments to be made (Karnouskos and Fokus, 2004). The realization of mobile payments will make possible new and unforeseen ways of convenience and commerce. Unsuspected technological innovations are possible. Music, video on demand, location based services identifiable through mobile handheld devices – procurement of travel, hospitality, entertainment and other uses are possible when mobile payments become feasible and ubiquitous. Mobile payments can become a complement to cash, cheques, credit cards and debit cards. It can also be used for payment of bills (especially utilities and insurance premiums) with access to account-based payment instruments such as electronic funds transfer, Internet banking payments, direct debit and electronic bill presentment.

Several mobile payment companies and initiatives in EU have failed and many have been discontinued (Dahlberg *et al*., 2007). In Europe and North America with few exceptions such as Austria, Spain and Scandinavian countries the development of mobile payments have not been successful. However, mobile payment services in Asia have been fairly successful especially in South Korea, Japan and other Asian countries (e.g., Mobile Suica, Edy, Moneta, Octopus, GCash). NTT DoCoMo has 20 million subscribers and 1.5 million of them have activated credit card functionality in Japan. There are 100,000 readers installed in Japan (Ondrus and Pigneur, 2007). The main difference between successful implementations of mobile payment services in the Asia Pacific region and failure in Europe and North America is primarily attributed to the 'payment culture' of the consumers that are country-specific.

In this paper we present an overview of the mobile technology landscape and address the concomitant issues that arise with the introduction of mobile payment services.

2. Mobile Payment Characteristics

A mobile payment service in order to become acceptable in the market as a mode of payment the following conditions have to be met (Karnouskos and Fokus, 2004):

a) **Simplicity and Usability**: The m-payment application must be user friendly with little or no learning curve to the customer. The customer must also be able to personalize the application to suit his or her convenience.

b) **Universality:** M-payments service must provide for transactions between one customer to another customer (C2C), or from a business to a customer (B2C) or between businesses (B2B). The coverage should include domestic, regional and global environments. Payments must be possible in terms of both low value micro-payments and high value macro-payments.

c) **Interoperability:** Development should be based on standards and open technologies that allow one implemented system to interact with other systems.

d) **Security, Privacy and Trust:** A customer must be able to trust a mobile payment application provider that his or her credit or debit card information may not be misused. Secondly, when these transactions become recorded customer privacy should not be lost in the sense that the credit histories and spending patterns of the customer should not be openly available for public scrutiny. Mobile payments have to be as anonymous as cash transactions. Third, the system should be foolproof, resistant to attacks from hackers and terrorists. This may be provided using public key infrastructure security, biometrics and passwords integrated into the mobile payment solution architectures.

e) **Cost:** The m-payments should not be costlier than existing payment mechanisms to the extent possible. A m-payment solution should compete with other modes of payment in terms of cost and convenience.

f) **Speed:** The speed at which m-payments are executed must be acceptable to customers and merchants.

g) **Cross border payments:** To become widely accepted the m-payment application must be available globally, word-wide.

3. Mobile Payment Solutions

Mobile payment solutions may be classified according to the type of payment effected, and based on the technology adopted to implement the solution. There are a variety of combinations of these frameworks – technology adopted and mode of payment, a survey of which would constitute a study in itself. There are three different models available for m-payment solutions on the basis of payment (Lim, 2007):

      a) Bank account based
      b) Credit card based
      c) Telecommunication company billing based

3.1 Bank Account based M-Payment

Banks have several million customers and telecommunication operators also have several million customers. If they both collaborate to provide an m-payment solution it is a win-win situation for both industries. In this model, the bank account is linked to the mobile phone number of the customer. When the customer makes an m-payment transaction with a merchant, the bank account of the customer is debited and the value is credited to the merchant account.

3.2 Credit Card based M-Payment

In the credit card based m-payment model, the credit card number is linked to the mobile phone number of the customer. When the customer makes an m-payment transaction with a merchant, the credit card is charged and the value is credited to the merchant account. Credit card based solutions have the limitation that it is heavily dependent on the level of penetration of credit cards in the country. In India, the number of credit card holders is 15 million (Subramani, 2006). Only this small segment of the population will benefit in the credit card based model. Though limited in scope, there may be high demand within this segment for a payment solution with credit cards and also, may provide high volumes of transactions.

3.3 Telecommunication Company Billing of M-Payments

Customers may make payment to merchants using his or her mobile phone and this may be charged to the mobile phone bills of the customer. The customer then settles the bill with the telecommunication company (Zheng and Chen, 2003). This may be further classified into prepaid airtime (debit) and postpaid subscription (credit).

4. Technologies for Mobile Payments

The mobile technology landscape provides various possibilities for implementing m-payments. Essentially, a GSM mobile phone may send or receive information (mobile data service) through three possible channels – SMS, USSD or WAP/GPRS. The choice of the channel influences the way m-payment schemes are implemented. Secondly, the m-payment client application may reside on the phone or else it may reside in the subscriber identity module (SIM). We briefly describe NFC technology as another possibility.

4.1 Short Message Service (SMS)

This is a text message service that enables short messages (140-160 characters) that can be transmitted from a mobile phone. Short messages are stored and forwarded by SMS centers. SMS messages have a channel of access to phone different from the voice channel (Valcourt, Robert and Beaulieu, 2005). SMS can be used to provide information

about the status of one's account with the bank (informational) or can be used to transmit payment instructions from the phone (transactional).

4.2 Unstructured Supplementary Services Delivery (USSD)

Unstructured Supplementary Service Data (USSD) is a technology unique to GSM. It is a capability built into the GSM standard for support of transmitting information over the signaling channels of the GSM network. USSD provides session-based communication, enabling a variety of applications. USSD is session oriented transaction-oriented technology while SMS is a store-and-forward technology. Turnaround response times for interactive applications are shorter for USSD than SMS.

4.3 WAP/GPRS

General Packet Radio Service (GPRS) is a mobile data service available to GSM users. GPRS provides packet-switched data for GSM networks. GPRS enables services such as Wireless Application Protocol (WAP) access, Multimedia Messaging Service (MMS), and for Internet communication services such as email and World Wide Web access in mobile phones.

4.4 Phone-based Application (J2ME/BREW)

The client m-payment application can reside on the mobile phone of the customer. This application can be developed in Java (J2ME) for GSM mobile phones and in Binary Runtime Environment for Wireless (BREW) for CDMA mobile phones. Personalization of the phones can be done over the air (OTA).

4.5 SIM-based Application

The subscriber identity module (SIM) used in GSM mobile phones is a smart card i.e., it is a small chip with processing power (intelligence) and memory. The information in the SIM can be protected using cryptographic algorithms and keys. This makes SIM applications relatively more secure than client applications that reside on the mobile phone. Also, whenever the customer acquires a new handset only the SIM card needs to be moved (Card Technology, 2007). If the application is placed on the phone, a new handset has to be personalized again.

4.6 Near Field Communication (NFC)

NFC is the fusion of contactless smartcard (RFID) and a mobile phone. The mobile phone can be used as a contactless card. NFC enabled phones can act as RFID tags or readers. This creates opportunity to make innovative applications especially in ticketing and couponing (Ondrus and Pigneur, 2007). The 'Pay-Buy Mobile' project launched by the GSM Association (fourteen mobile operators are part of the initiative) targets 900 million mobile users with a common global approach using NFC (Card Technology Today, 2007).

4.7 Dual Chip

Usually the m-payment application is integrated into the SIM card. Normally, SIM cards are purchased in bulk by telecom companies and then customized for use before sale. If the m-payment application service provider has to write an m-payment application in the SIM card, this has to be done in collaboration with the telecommunications operator (the owner of the SIM). To avoid this, dual chip phones have two slots one for a SIM card (telephony) and another for a payment chip card. Financial institutions prefer this approach as they can exercise full control over the chip and the mobile payment process (Karnouskos and Fokus, 2004). But, customers would have to invest in dual chip mobile devices.

4.8 Mobile Wallet

A m-payment application software that resides on the mobile phone with details of the customer (and his or her bank account details or credit card information) which allows the customer to make payments using the mobile phone is called as a mobile wallet. Customers can multi-home with several debit or credit payment instruments in a single wallet. Several implementations of wallets that are company-specific are in use globally.

5. A Generic Architecture for M-Payments

This is a simple, illustrative conceptual model that describes the relationship between the major participants in an m-payment scenario (Fig. 1). There is the customer and the merchant who would like to use an m-payment service. The M-Payment Application Service Provider (MASP) provides the necessary technical infrastructure (hardware and software) to facilitate m-payments and acts as an intermediary between the financial institutions and mobile network operators. The MASP registers users who would like to avail of the m-payment service. The users (customers and merchants) have to be registered with the MASP prior to using the service. At the time of registration the MASP collects the bank account details (or credit card details) of the customer and merchant as well as their valid digital certificates. The mobile phone numbers of the customer and the merchant are mapped to their respective bank accounts and this mapping is maintained by the MASP. The users are provided with a client m-payment application (mobile wallet) that is either resident on their phones or else in the SIM card. This application may be provided over the air to the uers. The mobile wallet will normally interact with the MASP server.

A mobile phone user communicates with a merchant and makes an economic transaction (e.g., buying a ticket from an airline over the phone). The merchant obtains the phone number of the customer and initiates the m-payment transaction request stating the amount for which payment is required. The customer confirms the request and authorizes payment. The MASP receives the authorization and verifies the authenticity of the customer. The MASP then debits the customer account and credits the merchant account by interacting with the bank. Once the electronic funds transfer is successful a

confirmation message is sent to the customer and the merchant advising them of the debit and credit respectively. The Certifying Authority also shown in Fig. 1 supplies digital certificates for the users in the system to provide security (see section below). This model can be extended to handle the interaction between the MASP and the financial system taking into account inter-bank payments and settlement.
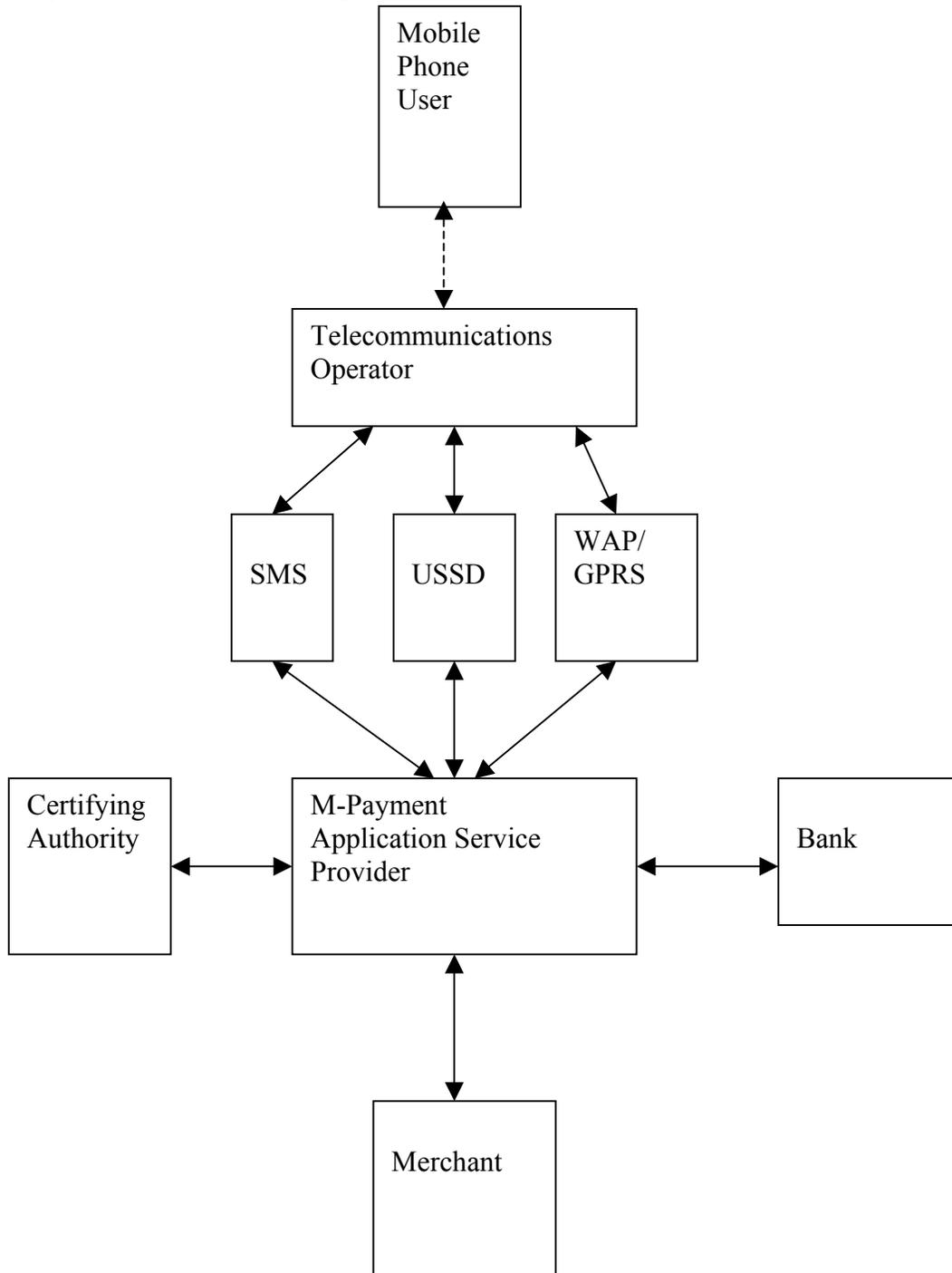

Figure 1 : A Generic Model for M-Payments Application Service Provider

6. Security Issues

For widespread use and customer acceptance of m-payment services, both perceived and technical levels of security should be high. For customers, privacy should not be compromised and there should be no possibility of financial losses. For businesses, customer authentication is important. As per the general framework of any secure messaging system - confidentiality, integrity, non-repudiation and authentication should be guaranteed by the m-payment services (Misra and Wickamasinghe, 2004). The transport layer security offered by GSM/CDMA networks sufficiently guarantees confidentiality (that messages cannot be read by anyone else) and message integrity (the assurance that the message has not been altered in transit). Authentication (identifies the author of the transaction) and non-repudiation (makes sure that any of the users in the system cannot later deny the message they sent) can only be guaranteed with the help of wireless public key infrastructure (WPKI) and digital certificates. Hassinen, Hyppönen and Trichina (2007) suggest that secure mobile payment transactions can be implemented using existing national public key infrastructure, which is independent of financial institutions, mobile network operators and mobile payment application service providers but can be used by all of them. Their proposed technological solution to provide secure mobile payment transaction is briefly described below.

6.1 Public Key Infrastructure and SIM cards

Every user of the system is listed in a publicly available directory. Aruna would like to send a message to another user Bob. Aruna first obtains Bob's public key from the directory and encrypts the message using it. Since only Bob has the private key only he can read the message (after decryption) and no one else. Further Aruna can digitally sign the message. In this scheme anybody can verify that Aruna did indeed send the message and the message was not altered during transmission. A Certification Authority (CA) maintains the publicly available directory, which is responsible for issuing and revoking digital certificates. A digital certificate contains the public key of a user in the system. This framework is known as public key infrastructure (PKI).

A user normally maintains his or her private key confidentially in a personal secure environment. SIM cards have the ability to store and process private keys. In terms of key management, there must be an administrative system to issue key pairs to genuine citizens in a country.

6.2 Protocols

A sample protocol that describes the transaction between a customer and a merchant, each using his or her mobile phone and a m-payment application service provider as an intermediary (cf. generic architecture for m-payments in section 5 above) is outlined in this section. It is assumed that customer and merchant are registered as users with the m-payment application service provider (with their respective bank account details) and both of them have valid digital certificates. The transactions are detailed below.

1. Service Request

Customer → Merchant
Customer makes a service request to the merchant

2. Product Options

Merchant → Customer:
Merchant sends his product options and his certificate

3. Product Selection

Customer → Merchant:
Customer selects a product; the selection is signed by the customer's private key

4. Payment Request

Merchant → M-payment Application Solution Provider (MASP) → Customer:

The payment request (containing the invoice amount) is signed using merchant's private key. Customer can verify that the merchant is genuine by using his certificate (sent earlier in step 2). The MASP also authenticates the merchant before passing the payment request to the customer.

5. Payment Authorization

Customer → MASP:

The customer authorizes the payment request by digitally signing the authorization using the customer's private key. The MASP transfers the money from the buyer's account to the seller's account by communicating to the bank(s).

6. Payment Confirmation

MASP → Customer:
MASP confirms payment made to merchant

MASP→Merchant:
MASP informs merchant of successful payment

The customer and the merchant can verify their respective bank accounts as to whether payment has been made.

The Institute for Development and Research in Banking Technology (IDRBT) has an experimental, proof–of-concept project where PKI enabled m-payment applications have been demonstrated to be feasible.

7. Stakeholders

There are many different stakeholders in the process of implementing mobile payments. They are (Karnouskos and Fokus, 2004):

a) Consumers
b) Merchants
c) Mobile Network operators
d) Mobile device manufacturers
e) Financial institutions and banks
f) Software and technology providers
g) Government

Each player has different incentives and strategies. Sometimes these interests and strategies between different players may be in conflict e.g., the telecommunications network provider would like to maximize revenues through each m-payment transaction whereas customers and merchants would like to minimize costs for each m-payment transaction. The expectations of each of the stakeholders is outlined below.

7.1 Consumer Expectations
- Personalized service
- Minimal learning curve
- Trust, privacy and security
- Ubiquitous – anywhere, anytime and any currency
- Low or zero cost of usage
- Interoperability between different network operators, banks and devices
- Anonymity of payments like cash
- Person to person transfers

7.2 Merchant
- Faster transaction time
- Low or zero cost in using the system
- Integration with existing payment systems
- High security
- Being able to customize the service
- Real time status of the mobile payment service

7.3 Banks
- Network operator independent solutions
- Payment applications designed by the bank
- Exceptional branding opportunities for banks
- Better volumes in banking – more card payments and less cash transactions
- Customer loyalty

7.4 Telecom Network Providers
- Generating new income by increase in traffic
- Increased Average Revenue Per User (ARPU) and reduced churn (increased loyalty)
- Become an attractive partner to content providers

7.5 Mobile Device Manufacturer
- Large market adoption with embedded mobile payment application
- Low time to market
- Increase in Average Revenue Per User (ARPU)

7.6 Government
- Revenue through taxation of m-payments
- Standards

8. Challenges for M-Payments

8.1 Standards

M-payments lack cohesive technology standards that can provide a universal mode of payment. Consolidation of standards in the mobile commerce arena is critical and it will enable producers and consumers to make investments that produce value. The lack of standards will give rise to lot of local and fragmented versions of m-payments offered by different stakeholders (network operator centric models and bank centric models). Standards need to address security and privacy concerns of consumers as well as interoperability between various implementations. Standards formation is a process of negotiation between various stakeholders; it is rather more political negotiations in nature rather technical discussions. First movers benefit from this situation by creating *de facto* standards and major market share. There is no consensus among the players in terms of m-payments standards setting. Certain start up companies have proposed standards and they hope to make these *de facto* by being first movers with strategic advantage and early market selection. The battle over standards occurs at the firm level and at the inter-consortia level (Lim, 2007).

8.2 Business Models

Since there are several stakeholders in the system, a viable and sound business model needs to be developed that will provide a framework for revenue sharing.

8.3 Regulatory Issues

Although m-payments may allow parties to make economic exchanges, it is not *legal tender* in the sense it lacks the status of other payment instruments such as cash, which is a medium of exchange that is authorized, adopted and guaranteed by the government (Au

and Kauffman, 2007). At best m-payments will have to be backed by the issuer's promise to pay. To overcome this problem legislation has to be put in place that will make m-payments legal tender.

The regulations for players in the financial industry are different from those governing the telecommunications industry, which means that each industry has its own particular standards body (Lim, 2007) to comply with.

9. Conclusion

The Mobile Payment Forum of India (MPFI) has been formed with Institute for Development and Research in Banking Technology (IDRBT) and Rural Technology Business Incubator (RTBI), IIT Madras taking the lead role. It has members and representatives from the telecommunications industry, financial institutions (banks and microfinance institutions) as well members from the Reserve Bank of India. Three sub-committees have been formed – on technology, on business models and on regulatory issues. The first meeting of MPFI was held in Hyderabad on the 15th of September 2007. The sub-committees are expected to go over their particular concerns in depth and submit a report shortly.

Lots of challenges are to be overcome for a successful implementation of mobile payments to be widely accepted as a mode of payment. Businesses, merchants and consumers have to come forward and make value-producing investments. A regulatory framework and widely accepted standards will be the pillars on which mobile payment applications will be built.

The way forward is summarized below:

a) Undertake research not in isolation as government agencies or as corporate initiatives but in collaboration as partners (establish consortia) for each of the possible technical solutions. There has to be symbiosis between application service providers, mobile network operators and banks.
b) Study already existing solutions in various countries (especially Asia Pacific countries and Europe) for any specific problems and unmet challenges.
c) Implement a pilot project in a small real time environment.
d) Frame policy and regulatory guidelines.
e) Publish industry wide standards for mobile transactions.
f) Work out the details of the business models in consultation with industry consortia.
g) Allow (license) stakeholders to implement standard solutions that have been pilot tested.
h) Establish a redressal mechanism to handle customer grievances.

Research so far has outlined a diversity of thinking and innovation that exists in the m-payments arena. Numerous solutions have been tried and failed but the future is promising with potential new technology innovations (Dahlberg *et al*., 2007).

References

Mobile Payment Forum of India (MPFI) http://www.mpf.org.in/

A. Subramani Attention credit card holders, The Hindu, 16th Nov 2006, http://www.hindu.com/2006/11/16/stories/2006111614040200.htm

Y.A. Au & R.J. Kauffman, (2007). The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application, Electronic Commerce Research and Applications, doi:10.1016/j.elerap.2006.12.004

T. Dahlberg et al., (2007). Past, present and future of mobile payments research: A literature review, Electronic Commerce Research and Applications, doi:10.1016/j.elerap.2007.02.001

M. Hassinen et al., (2007). Utilizing national public-key infrastructure in mobile payment systems, Electronic Commerce Research and Applications. doi:10.1016/j.elerap.2007.03.006

S. Karnouskos & F. Fokus (2004). Mobile Payment: a journey through existing procedures and standardization initiatives, IEEE Communications Surveys and Tutorials. 6(4) 44-66.

A.S. Lim (2007). Inter-consortia battles in mobile payments standardisation, Electronic Commerce Research and Applications (2007), doi:10.1016/j.elerap.2007.05.003

S.K. Misra & N. Wickamasinghe (2004). Security of mobile transaction: A trust model, Electronic Commerce Research 4(4) 359-372.

J. Ondrus & Y. Pigneur, (2007). An Assessment of NFC for Future Mobile Payment Systems. International Conference on the Management of Mobile Business, 2007, 9-11 July 2007 Page(s):43 - 53 Digital Object Identifier 10.1109/ICMB.2007.9

E. Valcourt, J. Robert, & F. Beaulieu, (2005). Investigating mobile payment: supporting technologies, methods, and use. IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, (WiMob'2005), Aug. 2005 Page(s):29 - 36 Vol. 4 Digital Object Identifier 10.1109/WIMOB.2005.1512946

X. Zheng & D.Chen (2003). Study of mobile payments systems. IEEE International Conference on E-Commerce, CEC 2003, June 2003 Page(s):24 – 27 Digital Object Identifier 10.1109/COEC.2003.1210227

GSM Association aims for global mobile payments using NFC Card Technology Today, Volume 19, Issue 2, February 2007, Pages 1, 3

Visa and SK Telecom to launch mobile payments Card Technology Today, Volume 19, Issue 2, February 2007, Page 6