AN INTEGRATED MECHANISM FOR MOBILE COMMERCE

Mohammad M. R. Chowdhury
UniK – University Graduate Center
P.O. Box 70, N-2007 Kjeller, Norway.
mohammad@unik.no

Josef Noll
UniK – University Graduate Center
P.O. Box 70, N-2007 Kjeller, Norway.
Josef@unik.no

ABSTRACT

Ubiquitous access and pervasive computing have given rise to many new innovative services and service access in every situation. One of the most popular applications can be mobile commerce. SMS based micro payment and remote banking solutions are already available. Smart card based contactless payment solutions have been introduced. But most of these efforts lack macro-level remote payments capability. User also expects easy-to-use and secure mobile commerce solutions. This paper proposes a mobile commerce mechanism which integrates both the local payments and remote payments provisions of any amount. A customized PKI-SIM card contains various payment means and the necessary security infrastructure. Users have to use a secret PIN code to activate the chosen payment provision. NFC is proposed as the secure short range communication technology for local payments. The paper includes a remote payment application example and the whole concept is evaluated from the security point of view. It is expected that the mechanism can provide strong security in mobile commerce.

KEYWORDS

m-commerce, local payment, remote payment, security.

1. INTRODUCTION

Mobile-commerce (m-commerce) is a potential killer application in future mobile network. The goal is to broaden service provisions to mobile subscribers by providing new payments solutions with the hope to increase revenues for operators and service providers. Now, there are more mobile users in this world than people having a bank account [1]. Richard Fletcher, head of MasterCard's mobile wireless group says, "People carry their phone more often than their wallet these days," [2]. PayPal, MasterCard and wireless operator Cingular are betting that the cell phone is about to become king of small, on-the-go, cashless transactions. All these upheld the prospect of m-commerce. Growing number of mobile Internet users are expected use mobile payment solutions over the Internet. Many financial institutes like credit card companies in association with the mobile phone producers, operators and banks came forward to access this market and already initiated various trials in m-commerce. Total worldwide mobile payments market has reached $24 billion in 2006 and will reach $55 billion by 2008 [2].

Mobile phone along with the SIM card has the potential to provide the necessary infrastructure for m-commerce. High capacity network and ubiquitous computing make various remote service accesses like, remote payment and banking possible from mobile phone. Payments based on SMS messages are already available. With the introduction of near field communication (NFC) technology, plenty of local payment solutions using mobile phones are evolving. It is easier for a user to make payment in vending machine having mobile phone in pocket, rather than using suitable set of coins. Vending machines that accept cash have mechanical parts and thus require regular maintenance. Removing money regularly also requires

additional manpower. Therefore, Mobile payment not only can be an attractive service for mobile users but also provide benefits to service providers. However, providing strong security during payment transactions especially over the open Internet environment is a big challenge. Currently several security mechanisms and infrastructures are available to support the m-commerce. In addition to proposing an integrated m-commerce mechanism, this paper presents an analysis on related security features.

M-commerce is also critical from user identity handling perspective. Currently every person carries numerous physical identities in his/her wallet. Many of these identities (for example, credit card, bank cards etc.) are responsible to deal with financial services. [3] introduced a distributed identity mechanism where most sensitive user identities are proposed to be stored in the SIM card. The proposed m-commerce mechanism suggests including these user identities into the mobile phone SIM card infrastructure. It provides solutions for both the local payments and the remote payments by bringing credit card functionality in the phone. It also facilitates the mobile banking. Instead of carrying hard cash, virtual cash can also be loaded into the phone. Through this mechanism, a user can choose from several of the payment options for different types of purchases. We propose NFC as the secure short range communication technology for local payments. The paper shows an example on how a remote mobile payment application can be realized using the proposed m-commerce mechanism.

The next section discusses various works related to m-commerce in brief. The following section describes the current mobile payments provisions. Descriptions of the proposed mechanism and a payment application example are illustrated in the next two sections. Evaluation of the proposed concept comes next. Finally, the paper concludes with the summary of the mechanism and future challenges.

2. RELATED WORKS

The elementary mobile payment schemes are based on *SMS* messages (sending premium SMS message). The amount of payment is then charged on the phone bill. The drawbacks of the approach are, there is no payer authentication mechanism and the system does not provide any kind of non-repudiation service. This is why; it has been limited to products with small monetary values (mobile ring tones, candies etc.). The risks related to poor authentication and non-repudiation are mitigated in many schemes by introducing mobile payment providers. *PayMate* [4] has introduced voice and SMS-based mobile payment solutions in India with user authentication provisions. Merchants send the shopping bill to PayMate data centre and it then sends SMS reply or automated call to customer asking for payment confirmation. *Paypal* [5] users can transfer micro-payment to another paypal account of any individual or merchant through SMS message. A unique mobile PIN created beforehand confirms the payment. Also, many other SMS-based services, such as account balance and latest transaction request, have been deployed successfully in various markets. These services support micro-payment only. Sending SMS messages for payments are also inconvenient for many users.

CAFÉ [6] project developed a pocket sized stand-alone electronic wallet. The prototype transacts via infrared link either directly with service points or with wallets held by other individuals. The principal drawback is, it has no embedded facilitation for mobile on-line data communication. It can transact over Internet when connected through another on-line device. Thus the system introduces additional inconvenience and complexity, especially for remote payment. In order to make both off-line and on-line mobile payment and manage multiple credentials, S. F. Mjølsnes and C. Rong proposed an *On-Line E-Wallet* system [6]. It contains a credential keeper, physically connected to an on-line residential server; and a keeper's agent, a smart card mounted in the user's dual-slot mobile phone. User has to make two simultaneous communication sessions (both with credential keeper and on-line or off-line service points) to transfer the required credentials. The server has to be on-line always and needs strict protection against sophisticated attacks. The mobile-credential keeper communication link also contributes additional security threats. Any malfunctioning of this link can make the user incapable of payment. The proposed mechanism overcomes these problems storing these credentials in the SIM card itself. The suggested system with two SIM card holders is not feasible. The holder costs as much as the radio frequency unit in the phone and adds an additional source of failure due to the mechanical connection.

Another mobile payment system *SmartPay (Mobilhandel)* [7] is using mobile public key infrastructure (PKI) built-in SIM card for user authentication and non-repudiation. In this system, orders are created by SMS messages or by browsing merchant's WAP pages. The PKI-server generates an SMS request to the

user's phone for signing the purchase with appropriate means of payment. Here the network operator is the trusted third party for handling these payment services and credit card information has to be registered in the system if user wants to use it. These might not be accepted by many. The system is not user friendly and too cumbersome to use multiple SMS messages to perform a signed purchase. It also cannot handle local payments.

The objective of our mechanism is to integrate both local and remote payments of micro-, mini- or macro- level into a single platform which is independent of mobile terminals. Payment means and infrastructures are maintained in a custom-made SIM card. Access to this platform requires both *something you have* (mobile phone with SIM card) and *something you know* (a separate PIN code). This strengthens the security of the system. The ultimate goal is to broaden the reach of m-commerce and to make it more accessible to normal customers.

3. PAYMENT PROVISIONS

This section illustrates various types of mobile payments and ongoing efforts in these areas by different organizations. According to Mobey forum [8], payments can be categorized into several types depending on the amount of transaction. A transaction below 10€ can be said as *micro-payment*. Any transaction between 10 and100€ can be termed as *mini-payment*. *Macro-payment* may go above 100€. Most of the current payment provisions of mobile payment support micro-payment (also mini-payment somewhere) with little or no customer's authentication. Macro-payment requires stronger security requirements.

A distinguishing feature in mobile payment schemes has become *off-line* versus *on-line* payments. In off-line payments, the transaction between payer and payee can be completed without communicating a third party. An on-line (or remote) payment implies that a third party must mediate to complete the transaction. *Local payments* happen in close proximity of payer and point of sales (POS) of service providers/payee. Here no third party is involved because customer can show credentials right away. If the transactions with POS require third party mediation, it can also be said as on-line payment. Mobile banking service includes account transfer, checking current account balance, checking last several transactions, SMS-alert (deposit/transfer, stock trading) etc. Some of these are already available in many markets.

Common examples of off-line payments are cash or cheque payment. One of the objectives of m-commerce is to abolish the necessity of carrying cash. Now-a-days numerous developments are going on in mobile local payment areas through the initiatives taken by mobile operators, mobile phone manufacturers, credit card companies and banks mainly using NFC [1]. Nokia has offered wallet capabilities in some of its handsets since 2003. On the service side, NTT DoCoMo launched its "Felicia" electronic wallet service in 2004, allowing for banking and retail transactions using phones equipped with smartcards from Sony [9]. In 2006, it announced the launch of world's first mobile handset with a built-in credit card chip. Last year, Motorola also announced plans for a system called M-wallet that will let consumers using their cell phones as credit cards. It is designed for both banking and shopping. M-wallet will support NFC. There have been U.S. trials of local payment in individual retail outlets. In December 2005, Cingular Wireless, Nokia, Visa and Philips together announced an NFC trial in Atlanta's Philips Arena. Sports fans who have Cingular service, a Visa account, and a Nokia 3220 phone equipped with Philips' NFC chip can buy food, t-shirts and tickets with the flash of a phone [10].

Tap N Go is the name of a contactless payment trial powered by MasterCard *PayPass* in US started in 2006 [11]. The phone securely transmits and receives payment details wirelessly using NFC. *Paypass* can be used to buy goods and services in various stores, restaurants; pay parking tickets and subway fares etc. In 2006, Visa completed contactless based mobile pilots in Malaysia and the United States, using NFC-enabled phones, complementing existing programs in Japan and Korea. In February 2007, Visa International and SK Telecom of South Korea announced the world's first contactless payment application on a universal SIM card which is personalized over-the-air based on Visa's recently introduced mobile platform [1], [10].

It is evident that NFC will play a vital role in ever growing mobile local payment markets. GSM association's (GSMA) announced initiatives to define common global approach to enabling NFC to link mobile devices with payment and contactless systems. Following its progression, fourteen mobile operators are participating in the 'Pay-Buy Mobile' [1] initiative to bring payment capability into devices on which seamlessly interoperable services will be provided. In 3GSM world congress 2007, GSMA and MasterCard

announced a pilot on mobile-based global money transfer initially to enable the world's 200 million international migrant workers to easily and securely send remittance to their dependence [1]. This might be a significant milestone in cross-country mobile banking, especially in account transfer.

Mobey forum [8] also believes that virtual cards residing in a phone's memory (mobile wallet) or in a security element supported by the phone (removable hardware like SIM/USIM or non-removable hardware like embedded chip) will be an important implementations step to make the user experience convenient and secure. Embedded chip into mobile phone provided by the credit card companies will not make the m-commerce terminal independent if these chips are not removable.

Remote mobile transactions span from the purchase of ringing tones and logos sent to the mobile phone, to purchasing goods, services and content during a browsing session with online mobile merchants sites. SMS services constitute majority of the remote transaction today, but the availability of new browsing and Java technologies, and "always-on" packet radio services have facilitated the fast development of remote purchasing of goods, services and contents. By launching visa mobile platform in January 2007 [10], visa expects to provide integrated customer experience ranging from local payment to remote payment. Most of these ongoing mobile local payment efforts fall under micro- or mini-payment category. Very few macro-level remote mobile payments initiatives are there in the market. Several technical, regulatory and political issues are hindering its development. In case of Macro-payment, providing strong end-to-end security over the mobile Internet is critical. Security scenarios of remote payments are also covered in this paper.

4. INTEGRATED M-COMMERCE MECHANISM

The proposed mechanism deals with the m-commerce infrastructure of client side only. It consists of different payment methods suited to different real life payment scenarios. This section gives the detail descriptions of requirements of such a system, its various components and architecture.

4.1 Requirements

The proposed m-commerce platform is based on the proposition of distributed identity mechanism made in [3]. People consider their payment credentials as the most sensitive identity information. These should be maintained securely. Chowdhury in his paper [3] proposed to store and manage these identities in user's personal device. These credentials are issued by trusted third party identity providers. Banks are the most potential candidate to play such roles. A good payment solution should be both convenient and secure. Security of such a system should provide mutual authentication (user-service provider), confidentiality, integrity and non-repudiation during transactions. User also expects privacy or anonymity in some financial dealings. An effective m-commerce mechanism should handle micro-, mini- and macro-payments both locally and remotely. User currently carries both the mobile phone and the wallet. The proposed m-commerce mechanism intends to integrate the payment provisions into a single mechanism so that user requires carrying the mobile phone only.

4.2 Components

Extended SIM card Considering the reach, acceptability and the fact 'a potential user rarely found without it', mobile phone is having the full capability to be the proposed user personal device. It has a PKI-enabled smart card, an *extended SIM card* (ESIM) which is a modified and customized version of the current SIM card. Certificates and necessary public/private keys are stored in it. With PKI and secret keys, this infrastructure can ensure *mutual authentication*, *confidentiality*, *integrity* and *non-repudiation* in financial transactions. ESIM is issued by a mobile operator in association with the proposed identity provider (banks). 'BankID' partnership (Norwegian banks with a mobile operator) [12] is a good example of such initiative. ESIM might have several modules; one provides the access to mobile operator's services and the other modules may act as the infrastructure of providing identity handling services. To activate the later requires an additional authentication mechanism using a separate PIN code and it holds the m-commerce mechanism.

NFC Near Field Communication is a technology that offers short-range communication between two devices. Introduction of NFC adds intelligence and networking capabilities to the phone and creates many

new opportunities like digital transactions in very good proximities. It can make mobile phone an ideal device for payments. Therefore, the proposed m-commerce mechanism decides NFC as the short range communication technology for local mobile payments. To establish secure channel between devices, various cryptographic protocols (RSA, 3DES, AES etc.) can be used. Almost all the trials in local payments are going on using NFC. Market analyst firm ABI Research, of Oyster Bay, N.Y., predicted that more than half of mobile handsets will be equipped with NFC chips by 2010 [13].

Mobile banking An *ESIM* will be issued to the user when registered for mobile banking. It contains the certificate to authenticate the user to banks. User can make account transfer, check the balance, view and pay the bills, order credit card to use from mobile phone, subscribe for digital cash and thereby load the mobile phone with it etc. Traditional SMS banking is also possible. Use can set various SMS alerts in the account and can make enquiries. Therefore, mobile banking is a way to realize payments ranging micro to macro remotely.

Credit card Most of the remote payment requires credit card but most mobile users do not own credit card. Number of people using mobile phones is increased many fold than the people having credit cards. These motivate including easy-to-use credit card solutions into the proposed mechanism. Upon registering for mobile banking user can also subscribe for credit card. Bank then issues a separate certificate to the user for using credit card facilities from mobile phone. The certificate will be stored in the SIM card. This credit card can be used both for local payment and remote payment in macro, mini and micro level. The major advantage of the proposed solution compared to [10], [11] is, credit card can also be used for macro- level remote payments without compromising user's security (besides local micro-level payment provisions).

Digital cash (DigiCash) Traditional physical cash provides the user a high degree of privacy, as it is not traceable to a single user. User expects the similar privacy provision in mobile commerce. In the proposed mechanism, initially user receives an inactive digital wallet during subscription. Through online mobile banking, user can subscribe and thereby activate the wallet. Afterwards, user can load the cash in the digital form to this wallet from his/her bank account. The solution used in [14] can be employed for digital cash creation, negotiation and payment. The vendor's POS requires the similar digital cash handling capabilities. This is how the proposed mechanism ensures privacy and anonymity to a mobile user in m-commerce. The digital cash serves the local payment only.

4.3 System architecture

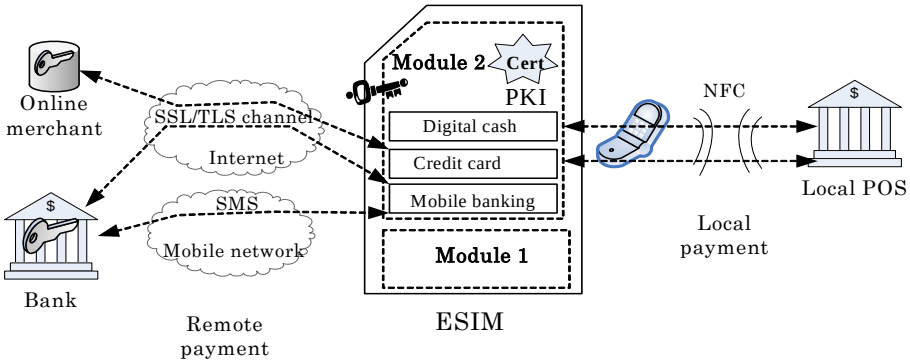

Figure 1. The integrated mechanism for m-commerce.

Figure 1 illustrates the organization of different components of proposed integrated m-commerce mechanism. It is to be noted that this solution is presented from individual client's (user's) point of view. Payee architecture details have not been touched here. It is assumed that banks, on-line/off-line merchants have appropriate mechanisms in place. Proposed *ESIM* comprises two modules; module 1 is responsible for providing mobile operator's services and module 2 contains the necessary m-commerce infrastructures. The later holds the sensitive user's credentials such as several digital certificates (for mobile banking and credit cards), user private key and also the digital cash. User must use a separate PIN code to make these mechanisms available. Then, the user can use installed credit card and mobile banking infrastructures for remote payments. User might choose two different channels for mobile banking; over the mobile Internet and using SMS over mobile network. The former provides the on-line banking. Built-in PKI provides the overall

security during transactions over Internet. The certificate and private key establish a mutually authenticated SSL (secure socket layer)/TLS (transport layer security) channel between the user terminals and banks/online merchants. Loaded digital cash and credit card can be used for local payment. NFC technology provides the secure short range communication between the mobile terminal and local POS for message exchange. Thus, the proposed solution integrates several local and remote payment provisions of micro- and macro-level into a single mechanism.

5. APPLICATION EXAMPLE

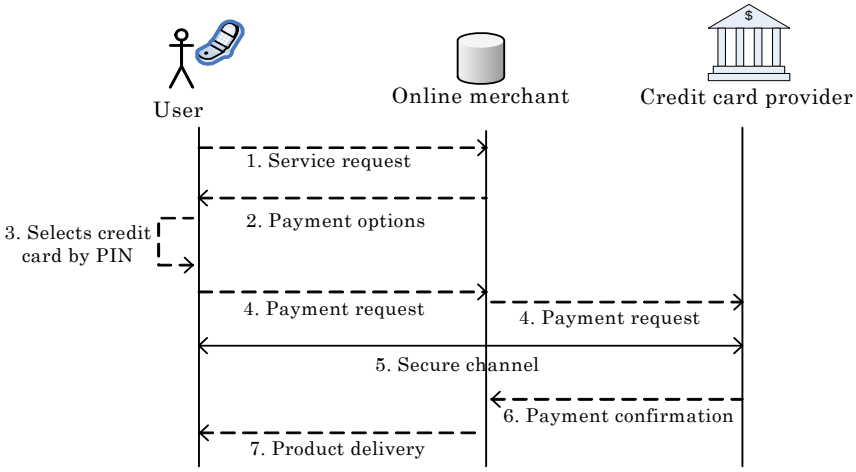

Figure 2. Remote payment in m-commerce.

Figure 2 depicts a remote payment application example using the proposed m-commerce mechanism. The application requires exchange of some messages between the involved parties. These are explained in brief.

1. *Service request.* Customer initiates the m-commerce with the merchant by requesting the products.
2. *Payment options.* Merchants send a list of payment options to the customer's terminal.
3. *Select the payment option.* Customer then selects the appropriate payment option, here the credit card and makes the chosen credential available using a separate PIN code.
4. *Payment request.* Customer sends the payment request to the merchant which then forwards the request to the credit card provider. This message contains the customer's initial credential details.
5. *Secure channel.* After initial handshake, a secure SSL/TLS channel is established. Payment details with customer's signature are transmitted through the channel.
6. *Payment confirmation.* Credit card provider sends the payment confirmation receipt to the merchant.
7. *Product delivery.* Upon receiving the receipt, merchant delivers the product.

Similar application example can be built for local payment using secure NFC interface. The next section will evaluate the system architecture from security point of view.

6. EVALUATION OF CONCEPT

This section makes detail analysis on various security protocols and technologies used for remote and local mobile payments. Strong authentication is preferred for macro-payments; while for transactions of a smaller amount (micro- or mini-payment) could use a less robust form of authentication. Remote mobile payments demand strong end-to-end security especially in open Internet environment.

6.1 Device Security

A customized SIM card holds the proposed m-commerce infrastructure. Therefore, the mobile device security is critical. Here, the system uses two-factor authentication to make financial transactions from the mobile phone. It contains *something you have* (having mobile phone with ESIM) and *something you know* (knowing a PIN code). Security of this mechanism is not compromised when the phone is lost or stolen. The unauthorized person still needs to know a PIN (an additional one) to make use of its m-commerce functionality. Traditional hard cash once lost or stolen cannot be revoked, but digital cash loaded into the phone can be revoked when lost or stolen. The amount can be re-loaded later.

6.2 Remote payment security

To be considered entirely secure, any method of communication must offer several features, such as, confidentiality, integrity protection, authentication and non-repudiation. SSL/TLS are public key cryptographic protocols which provide these security features in traditional Internet transactions. Therefore, we suggest using SSL/TLS for remote payment over the Internet. There are some weaknesses in the authentication mechanism of SSL/TLS. In this mechanism, client (browser) authenticates the server though its effectiveness is questioned. In most cases, consumer authentication is not used at all. Deployment of PKI can mitigate weaknesses of authentication mechanism by SSL/TLS. Mobile terminals are incapable of verifying a X.509 certificate (used in PKI) because of some constraints like less powerful CPUs and restricted power consumption. Wireless versions of TLS (WTLS) and PKI (WPKI) have been evolved to mitigate these problems. WPKI supports client-server mutual authentication through modified WPKI certificate. [15] proposed a User Authentication Server (UAS) to act as a trusted third party to assist the mobile client to authenticate and exchange keys with the service providers to mitigate certificate handling problem. Communication via radio signals is particularly vulnerable to ‘tapping’ by third parties. To protect this, WTLS can allow the change of session key regularly over the course of a session, without the need for a clean handshake.

Providing end-to-end security is a critical issue. WAP1.x (WAP is the mobile equivalent of traditional Internet) presents a security risk because data is momentarily held unencrypted inside WAP gateway. WAP 2.0 addresses the end-to-end security by introducing wireless optimized TCP/IP, TLS and HTTP. Through this protocol, TLS tunnel is enabled through an intervening WAP proxy permitting secure end-to-end HTTP transaction. The TLS used by WAP 2.0 is having some of the weaknesses of WTLS such as, no obligation to exchange certificates, no obligation to verify certificates and authenticates owners. Introduction of PKI will strengthen the security of the proposed mechanism by providing mutual authentication service. C. M. Ou and C. R. Ou proposed a high-level 3G wireless PKI solution [16]. According to this, mobile equipment will contain two pairs of public-key/private-key; one is used for encryption/decryption, the other is used for digital signature generation and verification.

In mobile commerce, it is important to maintain ongoing session even after the RF connection is dropped. K. Kawamoto and N. Nakamura proposed a solution to this [17]. It suggested managing the state of the certificate both at SIM side and Certificate Authority (CA) side. By setting the correspondence between the PKI states in USIM with the state of certificate in CA, it is possible to restart the process of certificate issue application even if the connection is dropped. The proposed m-commerce mechanism can implement this.

Public key security system used in the proposed m-commerce solution provides the critical security services (authentication, integrity, confidentiality and non-repudiation) in highly distributed systems, making it preferred security system for important *remote payment* over Internet. But as is the case with any technology, those features and functions come at the price of additional complexity.

6.3 NFC security

Bluetooth broadcasts its data promiscuously and at greater distances (10-100m) than NFC. Besides, there are various security weaknesses of Bluetooth communications. NFC phones are only intended to make connections with authorized device at close range. The read range of NFC's RFID technology is 10 centimeters or less. That short read range should mitigate the risk of eavesdropping by other reader devices. Still it is a threat. A research paper on security in NFC says that when a device is sending data in active mode

eavesdropping can be done up to a distance of about 10 m, whereas when the sending device is in passive mode, the distance is reduced to 1 m [18]. Data modification and denial of service attacks are also possible. But it is practically impossible to do man-in-the-middle attack on an NFC link. Establishing a secure channel using cryptographic protocol between two NFC devices, which is proposed here, is clearly the best approach to protect against any kind of eavesdropping and data modification.

7. CONCLUSION

In this paper, we have introduced an integrated mobile commerce mechanism that can handle both local and remote payments of any amount. Most current remote payment and banking solutions are SMS based and allow only the micro-level payments remotely from mobile phone. Credit card companies in association with mobile operators, equipment vendors and banks have recently initiated various trials in m-commerce. But these efforts are mostly concentrated in local payments. It is expected that the suggested mechanism can combine both the local and remote payments into a single platform. A customized SIM card is proposed as the storage place for several payment provisions. Built-in PKI SIM can ensure the security of macro-level remote payments. Secure NFC technology works for the local payment with local POS. The goal of this paper is to extend the reach of mobile commerce by making it convenient and secure. Building user confidence on remote macro-payment will be a big challenge. This work is also important for on-going research in user's identity handling.

REFERENCES

[1] Payments news, http://www.paymentsnews.com

[2] http://money.cnn.com/2006/07/10/magazines/business2/mobilecommerce.biz2/ [Retrieved on Feb 09, 2007]

[3] Mohammad M R Chowdhury, J.Noll, 2007, "Distributed Identity for Secure Service Interaction.", in press, *The Third International Conference on Wireless and Mobile Communications, ICWMC07*, Gaudeloupe, French Caribbean.

[4] PayMate, India, http://www.paymate.co.in/

[5] PayPal, http://www.paypal.com

[6] Stig Frode Mjølsnes and Chunming Rong, 2003, On-Line E-Wallet System with Decentralized Credential Keepers, *Mobile Networks and Applications 8*, pp. 87-99, Lkuwer Academic Publishers, Netherlands.

[7] Marko Hassinen, Konstantin Hyppönen, and Keijo Haataja, 2006, An Open, PKI-Based Mobile Payment System, *Lecture Notes in Computer Science* 3995, pp. 86-100, Springer-Verlag Berlin Heidelberg.

[8] Mobey Forum, Mobile Financial Services, http://www.mobeyforum.org

[9] http://digital-lifestyles.info/2004/08/10/felcia-payment-system-goes-live [Retrieved on Feb 14, 2007]

[10] VISA, www.visa.com

[11] http://www.mastercard.com/us/paypass/mobile/ [Retrieved on Feb 09, 2007]

[12] www.cybertrust.com/media/case_studies [Retrieved on Feb 22, 2007]

[13] http://www.eweek.com/article2/0,1895,1923242,00.asp [Retrieved on Feb 09, 2007]

[14] Ranjit Abbadasari, Ravi Mukkamala and V. Valli Kumari, 2004, MobiCoin: Digital Cash for M-commerce, *Lecture Notes in Computer Science 3347*, pp. 441-451, Springer-Verlag Berlin Heidelberg.

[15] Samuel T. Chanson and Tin-Wo Cheung, 2001, Design and Implementation of a PKI-based End-to-End Secure Infrastructure for Mobile E-commerce, *World Wide Web Journal*, Vol. 4, No. 4, pp. 235-253, Springer Netherlands.

[16] Chung-Ming Ou and C. R. Ou, 2006, A High-Level 3G Wireless PKI Solution for Secure Healthcare Communications, *EuroPKI 2006, Lecture Notes in Computer Science 4043*, pp. 254-256, Springer-Verlag Berlin Heidelberg.

[17] K. Kawamoto and N. Nakamura, 2002, Study of Management on the Mobile Public Key Infrastructure, *Network Operations and Management Symposium, NOMS 2002*, Florence, Italy, pp. 955-957.

[18] Haselsteiner, Ernst and Breitfuss, Klemens, 2006, Security in Near Field Communication (NFC) Strengths and Weaknesses, *Workshop on RFID Security - RFIDSec 06*, Graz, Austria.