An Architectural Design for Secure Mobile Remote Macro-Payments.

Article *in* Journal of Next Generation Information Technology · August 2010

DOI: 10.4156/jnit.vol1.issue2.7 · Source: DBLP

2 authors:

Britto Kumar
St. Joseph's College of Tiruchchirappalli
6 PUBLICATIONS **44** CITATIONS

S. Albert Rabara
St. Joseph's College of Tiruchchirappalli
57 PUBLICATIONS **277** CITATIONS

Journal of Next Generation Information Technology
Volume 1, Number 2, August, 2010

An Architectural Design for Secure Mobile Remote Macro-Payments

S.Britto Ramesh Kumar[1] and S.Albert Rabara[2]
[1]*Dept of Computer Applications, Bishop Heber College, Tiruchirappalli – 620 017,*
[2] *Dept of Computer Science, St.Joseph's College, Tiruchirappalli – 620 002.*
brittork@gmail.com, a_rabara@yahoo.com

doi: 10.4156/jnit.vol1.issue2.7

Abstract

The high market penetrations of mobile personal devices including mobile phones, PDAs have paved a way for the development of new application models in Mobile Commerce. Mobile phones are well suited with mobile commerce to reach the customers anywhere and at any time. Mobile Payments are the natural evolution of e-payment schemes that facilitate mobile commerce. The mobile payment markets are categorized into a combination of micro/macro-payments and remote/local mobile payment environments. A study reveals that there are different initiatives have already been launched in mobile remote macro-payment areas such as PayPal Mobile or Google Checkout Mobile. However, those initiatives are focused on a limited number of m-payment opportunities. For example, PayPal focused on P2P payments and mobile shopping via SMS. Also, the existing systems are still suffering from security breaches.

This paper proposes an architectural design for Secure Mobile Payment System that supports remote macro-payments. The main aim of this architecture is to achieve end-to-end security using symmetric operations. Since the development of secure mobile payment system for remote macro payments is a hot research topic in research community, this paper proposes an effective architecture to carry out the payment transactions between the customer and merchant. The proposed architecture ensures high level security in transactions and provides convenient payment mechanism.

Keywords: *Framework, Secure Mobile Payment System, Remote Macro-payments*

1. Introduction

E-commerce is simply the commercial transactions such as buying and selling of products and services conducted over the Internet. The advent of the open network Internet and the explosion of World Wide Web have emerged to expand the area of Business-to-Business (B2B) E-Commerce and Business-to-Consumer (B2C) E-Commerce and Consumer-to-Consumer (C2C) E-Commerce into Wireless E-Commerce i.e. Mobile Commerce. The successful electronic business operations are contributing major advantages with increased efficiency in services and reduced cost by breaking the barriers of geographical and time zone distances to the business people and consumers. However, due to the penetration of wireless and mobile technologies and no support of user mobility in e-commerce, it provides a viable entry for new type of commerce i.e. Mobile Commerce into the new millennium.

There are number of challenges in e-commerce such as failure to understand the customer behaviour, inability to predict environmental reaction, over-estimation of resource competence, failure to coordinate among transactions, and under-estimation of time requirements, in spite of the numerous benefits. While developing the new wireless and mobile applications by using the existing standard e-business strategies, all the above factors are to be considered. There are five value-added attributes of wireless e-commerce to make regular e-commerce such as mobility, convenience, instant connectivity, personalization and localization. In addition to that there are some challenges to be considered at the development stage such as uniform standards, ease of operation, easy of up gradation, security for transaction, minimum screen size, display type and bandwidth, and billing services for the operators.

Several mobile commerce applications such as Mobile Banking, Mobile Entertainment, Mobile Information Services, Mobile Marketing, Mobile Shopping, Mobile Ticketing and Telemetric Services include Remote Diagnosis and Maintenance of Vehicles, Navigation Services, Vehicle Tracking and

Theft Protection, and Emergency Services have emerged in recent years globally with many innovative advantages such as ubiquity, accessibility, personalization, convenience etc. In spite of them, Mobile Payment is one of the services and the mobile phones are used as a payment instrument for services or goods, bills and money transfer [1].

Mobile Payment is an essential service for any mobile commerce applications and which has raised the attention of researchers in the last few years. Mobile Payment services become as the integral part of our lives at the personal level and professional level. Mobile payments can become a complement to cash, cheques, credit cards and debit cards. It can also be used for payment of bills with access to account-based payment instruments such as electronic funds transfer, Internet banking payments, direct debit and electronic bill presentment. M-payment will provide tremendous opportunities for application developers, service providers, telecommunication network service providers and financial institutions in forth-coming years.

A mobile payment or m-payment may be defined 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 [2]. 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 [3]. According to a study conducted by Juniper Research, the Global mobile commerce revenues are expected to grow up to 88 billion USD by 2009 [4]. Moreover, the popularity of mobile commerce applications provide new opportunities for mobile users, application developers, service providers, network providers, financial institutions and researchers and make it more profitable and promising.

Secure mobile payment system for remote macro-payments becomes a major research area in the field of mobile commerce. The payments can be classified into either micro or macro level and each level require different technologies and various security levels. The local micro-payment (€10 or less) for goods and services, such as ring tones and games, is already a mature market. The limitations of local micro-payment schemes are, limited capacity of payment technologies like RFID, IrDA and NFC and need for dedicated and compatible POS terminal.

In the remote macro-payments, the mobile is linked to a payment card such as credit and debit card or bank account via an activation/enrollment process. There are various opportunities for mobile remote macro-payments such as Mobile Shopping, Mobile Banking, Bill payment, Internet Shopping, and P2P mobile payments. A study reveals that there are different initiatives have already been launched in mobile remote macro-payment areas such as PayPal Mobile or Google Checkout Mobile. However, those initiatives are focused on a limited number of m-payment opportunities. For example, PayPal focused on P2P payments and mobile shopping via SMS and Crandy focused on vending and parking solutions. The MOVO focused on P2P and credit transfer payments. Additionally, many mobile payment solutions are fraught with security breaches. The security levels relating to the mobile remote macro-payment do not match the standards required by a bank or card issuer in order to solve risk of payment.

Hence, this paper proposes an architectural design for Secure Mobile Payment System that supports remote macro-payments. The proposed design comprises various functional components and overcomes the problems as limited computational capabilities and limited power of mobile handsets. The aim of this architecture is to achieve end-to-end security using symmetric key operations and to provide convenient payment mechanism.

The paper is organized as follows: Section 2 presents a detailed study on existing mobile payment systems. Section 3 illustrates the proposed architectural design for secure mobile payment system that supports mobile remote macro-payments. The security protocol is presented in section 4. The section 5 analyses system security focusing on realized security procedures. The Use Case diagram for system prototype is presented in section 6. Finally, section 7 is devoted to future work and concluding remarks.

2. Related Works

Several studies have been conducted till recently to build a secure and cost effective mobile payment system. Xiaolin Zheng *et al.* have presented a functional modules graph for SMS-based Mobile Payment System [5]. The graph considers various functional modules such as transaction platform, control of communicating interface, query and statistics for service states, statistic and analysis for business, system monitor and control, charge account, customer service and database, but the important security properties of mobile payment system such as authentication, data confidentiality and etc. have not been supported by the graph.

S. Karnouskos *et al.* have presented architecture and business model for Secure Mobile Payment System (SEMOPS) [6], where the payer-sender, the payer's payment processor, the payee's payment processor and the payee-beneficiary are the key actors. SEMOPS supports micro and macro-payments over SMS, USSD and GPRS. The SEMOPS is a universal and open mobile payment system that supports micro, mini and macro payments. However, there are still some limitations in SEMOPS model. In SEMPOS, the customer prepares a Payment Request (PR) and submits it to the customer payment processor. The customer payment processor then prepares a payment notification and forwards it to the Data Center (DC). Since the payment notification relay through DC and merchant payment processor, the transaction data casts a trail on the way to the merchant. Then the customer and the merchant have to trust the payment processors, but there is no guarantee for comprise-resistant payment processors.

L.Jupco Antovski *et al.* have presented the architecture based on Mobile Network Operators (MNOs)-based payment system and supports micro-payments [7]. The architecture deployed security at the application level using asymmetric key encryption and Public Key Infrastructure (PKI). However there are high possible attacks on data transmission, since the proposed architecture uses HTTP. A study reveals that the server-side HTTP attacks and client-side HTTP attacks are identified as high-risk threats. In 'HTTP Connect Tunnel' attacks, the HTTP-connect-tunnels are used for sending spam emails. In MNO-based mobile payment system, when the payment amount is transferred from one account to another in different mobile operator's networks, it requires additional procedures for validation and clearing. This leads to high cost and does not suit for micro-payments effectively. Also, those systems suffer seriously due to lack of transplant-ability, no compatibility among different MNOs, high demand for privacy, authentication and trust-management protection, and lack of scalability.

Jun Liu *et al.* have presented a new architecture for mobile payments [8] to conquer the limitations of SEMOPS that reduces the trust dependence on payment processors and enhances the security and privacy. To avoid disputes with the customers, the customer payment processor preserves the timestamp and Payment Request (PR). The customer and merchant information resides with respective payment processors. This supports privacy and anonymity for both customer and merchant. The transaction data are hashed before transmission to ensure the integrity. The proposed architecture introduced Certificate Authority (CA) with the combination of Time Stamping (TS) service to ensure the non-repudiation and transaction accountability. However, the architecture uses third party to reduce trust dependency that requires extra processing steps as well as additional transaction cost. The major threats like cracking/hacking, viruses, worms, Trojans, and Spyware are possible to send by the third-party organisations or individuals. Those attackers are classified as insiders, intruders, once-removed parties and their intention is to harm the payment transactions and networks. The method for certificate validation is another major concern for high-level security.

Different mobile payment models such as bank driven, mobile network operator driven and independent payment systems are found in the market [9]. It is understood that there are wide range of mobile payment solutions and models available with the aid of various services such as Short Message Service (SMS), Unstructured Supplementary Service Data (USSD) and Wireless Application Protocol (WAP). Security is the major concern for any mobile payment system. The literature study reveals that the security is applied at various levels in Mobile Payment Systems such as mobile platforms, services or protocols, network technologies and mobile devices to perform the payment transactions successfully. The mobile device contains the user's confidential data, key information, etc. Thus, the client devices are required to protect from unauthorized users. It can be achieved by applying Personal Identification Number (PIN), Personal Unblocking Key (PUK) or passwords as user authentication mechanisms.

In order to achieve secure communications during the payment transaction, symmetric and asymmetric cryptography are used normally among engaging customers. Most of the protocols in recent years are developed on public-key infrastructure (PKI) [10, 11, 12, 13] where as the remaining employ symmetric key operations [14, 15]. However, the security protocols using symmetric-key operations consume lower computations at all the engaging parties and they are good enough to support transaction security properties such as party authentication, transaction privacy, transaction integrity, and non-repudiation. The proposed architecture ensures high level security and convenience using symmetric key operations.

3. Proposed Architectural Design for Secure Mobile Payment System

Based on the study, the proposed architecture is specifically designed for the remote macro-payments through the registered clients using mobile devices. There are five entities involved in this proposed scheme that includes mobile client (MC), Mobile Payment Application Service Provider (MPASP) Server, Client Bank (CB), Merchant Bank (MB), and Merchant. The proposed Mobile Payment System provides the necessary technical infrastructure such as acquiring user information, connectivity, authentication, and secure communication to facilitate m-payments. Furthermore, both Wireless Transport Layer Security Specification (WTLS) and the Internet Secure Socket Layer (SSL) protocol are applied to protect the end-to-end security between the entities. The WTLS is used to provide privacy, data integrity and authentication and which is optimized for small bandwidth and long latency. The proposed architecture is depicted in the figure 1.

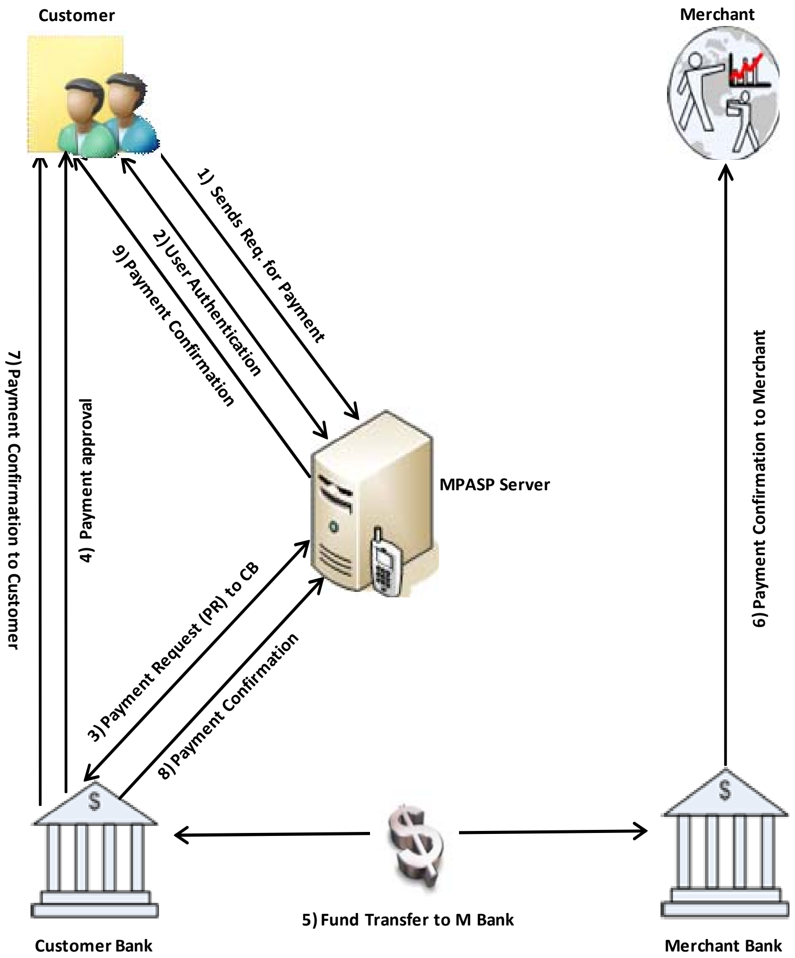
Customer
Merchant
1) Sends Req. for Payment
2) User Authentication
9) Payment Confirmation
7) Payment Confirmation to Customer
4) Payment approval
MPASP Server
6) Payment Confirmation to Merchant
3) Payment Request (PR) to CB
8) Payment Confirmation
5) Fund Transfer to M Bank
Customer Bank
Merchant Bank

Figure 1. Proposed Architectural Design

The users (e.g. customers, merchants) handle a large number of heterogeneous mobile devices, nowadays. The mobile interfaces could be described in the form of voice and data. The application developer has to design the dynamic user interfaces for interaction between the various wireless mobile commerce applications and users with the capability of supporting the heterogeneous environment. The user interface is capable of handling WML, XML and other mobile related communication issues. The client must have an account in a bank and he/she must be registered with MPASP server as well as with the bank. At the time of registration, the bank issues the ID for registered users like client and merchant. The MPASP server may maintain by any bank. When the client registers to the server, MPASP server collects personal details and bank account information. Also, the server gets the answer for secret question from the client. For the registered clients, the server sends client id and mPIN to the respective client mail via Internet. In the proposed architecture, the MPASP server acts as a payment gateway between the client and merchant.

The client initiates the payment request by sending the client id given by the server, merchant id and payment transaction data to the server as an encrypted message using shared mPIN number. The transaction data contains transaction date, transaction amount, merchant id, and merchant bank id. Once the payment request is received by the server, it decrypts the message using same mPIN number. The requester MSISDN number is used to identify the mPIN client. When the requester is identified, the server retrieves the secret question from the server database for the respective client and sends encrypted message to the client using mPIN. The server applies timestamp for the message using the customized sofware. If the client tries to decrypt the message more than 3 times, the message will be deleted at client device. Otherwise, the client views the message and sends the response to server using shared mPIN. The server then, maps the client response with server database. If both of them are matched, the client is authenticated. The proposed architecture employs two-factor authentication mechanism such as mapping of MSISDN and secret answer to identify the mPIN client. The client also authenticates the server by decrypting the secret question using valid mPIN. The mPIN is only known to the client and MPASP server.

Once the client authentication process is completed successfully, the server generates session id for the respective request and creates the Payment Request (PR) on behalf of valid mPIN client. The payment request contains the information like client id, payment amount and transaction data. The server then sends the PR to the Client Bank (CB). The CB identifies the client using client Id where the client id is issued by the bank during registration. After receiving the PR by the CB, it checks the account balance for the respective client. If the balance is insufficient in the client account, the client bank rejects the PR and intimates to the MPASP server. Then the client bank sends the request for payment approval to the client. After getting the payment approval from the client, the CB transfers the requested amount to the Merchant Bank (MB).When the amount is received by the merchant bank, MB sends the payment confirmation to the merchant. Also, MB sends the payment confirmation message to the CB. Now, the client bank confirms the payment with client and with MPASP server. Finally, the MPASP server forwards the same message to the client and the payment transaction is completed successfully.

4. Security Protocol for Mobile Remote Macro-Payment System

This section proposes and explains the workflow of the system in terms of communication protocols. To be a successful payment system, the proposed protocol accomplishes all the security properties such as authentication, confidentiality, privacy, integrity and non-repudiation.

4.1. Notations used in Protocol

The notations used in this proposed scheme are as follows:

$E_{SP}\{M\}_{A\text{-}B}$	:	the message *M* is symmetrically encrypted and by shared mPIN number between parties A and B.
$D_{SP}\{M\}_{A\text{-}B}$	:	the message *M* is symmetrically decrypted and by shared mPIN number between parties A and B.
ID_T	:	the identity of transaction that includes time and date of transaction.
ID_C	:	the identity of the Client.
ID_M	:	the identity of the Merchant.
ID_{CB}	:	the identity of the Client bank.
ID_{MB}	:	the identity of the Merchant bank.
DS_C	:	the digital signature of the Client.
SID_T	:	the session id for each transaction.
T_{EXP}	:	the timestamp when the transaction request expires.
$T_{i\,C}$	:	the *i* th timestamp at Client.
$h(X)$	:	the one-way hash function of message *M*.
SQn	:	the secret question to authenticate the client.
SAns	:	the secret answer to authenticate the client.
$ABal_C$	:	client's account balance.
$AmtInfo_c$	:	the amount yet to be transferred.
$PApp_{Req}$	:	the payment approval request from the client bank to client.
$PApp_{Resp}$	:	the acceptance of payment request from the client to client bank.
Pay_{Ack}	:	payment acknowledgement from merchant bank to client bank
$Pay_{Confirm}$	:	payment confirmation message.

4.2. Security Protocol

```
1) C → MPASP: $E_{SP}\{ID_C, AmtInfo_{c,}\ h(TransactionData)\}_{C\text{-}MPASP}$
2) $ID_T$ = create_TranId($ID_C$)
   MPASP →C: $E_{SP}\{ID_T, T_{i\,S}, SQn\}_{C\text{-}MPASP}$ [where Ti is the timestamp at C for
   which the value is assigned by MPASP]
3) C: $D_{SP}\{ID_T, SQn\}_{C\text{-}MPASP}$ [$T_{EXP}$ ($T_{EXP} > T_{i\,S}$) is the timestamp and it expires
   when the client tries more than the given timestamp value]
4) C → MPASP: $E_{SP}\{ID_T, SAns\}_{C\text{-}MPASP}$
5) MPASP: $SAns = D_{SP}[E_{SP}\{ID_T, SAns\}_{C\text{-}MPASP}]_{C\text{-}MPASP}$
    If SAns is valid then
    {
        $SID_T$ = CreateSession($ID_T$)
        $SID_T$ = GetClientInfo($IDc, ID_{CB}$)
    }
    else
        MPASP →C: send failure_msg1
6) MPASP →CB: $E_{SP}\{SID_T, ID_{C,}\ AmtInfo_c,\ h(TransactionData)\}_{MPASP\text{-}CB}$
        If $ABal_C$ is sufficient then
            CB→C: $E_{SP}\{SID_T, AmtInfo_{C,}\ PApp_{Req}\}_{C\text{-}CB}$
        else
           CB→MPASP: send failure_msg2
7) C → CB: $E_{SP}\{SID_T, AmtInfo_{C,}\ PApp_{Resp}\}_{C\text{-}CB}$
8) CB → MB: $FT[SID_T, ID_{M,}\ ID_{CB}, AmtInfo_{C,}]_{CB\text{-}MB}$
9) MB → M: $E_{SP}\{SID_T, Pay_{Confirm}, ID_{C,}\ AmtInfo_C\}_{MB\text{-}M}$
10)MB → CB: $[SID_T, Pay_{Ack}, ID_{C,}\ , ID_{M,}\ AmtInfo_C]_{CB\text{-}MB}$
11) CB → C: $E_{SP}\{SID_T, Pay_{Confirm}, ID_{M,} AmtInfo_C\}_{CB\text{-}C}$
12)CB → MPASP: $E_{SP}\{SID_T, Pay_{Confirm}, ID_M, AmtInfo_C\}_{MPASP\text{-}CB}$
```

5. Security Analysis

The proposed mobile payment scheme described in this paper satisfies the following security and privacy requirements.

5.1. Customer Requirements

5.1.1. Authentication of MPASP Server is required.

In the proposed mobile payment scheme, the customer authenticates the MPASP server using mPIN while decrypting the secret question. The mPIN number is only known to the client and to the server. Once the client is authenticated the MPASP server, the client sends the answer to the secret question. The reply message is also encrypted using shared mPIN number.

5.1.2. Trust Relationship is required

The customer shares his personal information with MPASP server to carry out the payment transactions. The trust relationship is vital one between the customer and the MPASP server. However, the MPASP server is maintained by the bank, the trust is improved for the customer.

5.1.3. Payment Approval is required

The payment approval is an important requirement with respect to the customer. In the proposed design, the customer bank makes the request for payment approval. The trust relationship is established between the customer and his/her bank. When the customer creates the account to a bank, the secret PIN number is issued by the bank and which is used to have the secure communication between the client and client bank. Since the bank gets payment approval directly from the client, the proposed scheme avoids the possible conflicts between the communicators.

5.2. MPASP Server Requirements

5.2.1. Authenticated and Authorized payment is possible.

The proposed protocol allows the customers to make the payment only after the authentication and authorization. The server authenticates the client using MSISDN number and shared secret number namely mPIN. After authentication, the server authorizes the client for payment services by checking the secret answer. The MSISDN number is also used to authenticate the customer device. If the mPIN is revealed to any unsolicited person, the secret answer is used to authorize the payment.

5.3. Integrity

The protocol employs a hashing algorithm to create a message digest of the message exchanged. The message digest is calculated both at the mobile phone application and at the MPASP server. The integrity check algorithm is incorporated with payment application. If the content is altered during transmission a mismatch digest will occur and the receiver will know that the message has been compromised.

5.3. Privacy

In any payment system, the order information and the identity of the merchant should not reveal to remaining entities involved in the payment system like payment service provider. The confidentiality the payment details should be protected from eavesdropping. The proposed security protocol satisfies these requirements, completely. The customer sends payment details to the MPASP server in an encrypted form and such payment details can only be accessed by the bank than the server. However, the client bank receives the payment details including merchant id, it does not receive any information about merchant's account number. The merchant bank identifies the merchant's account through merchant's id.

5.4. Non-repudiation

The important security property of non–repudiation is ensured through the use of the mPIN that is known only to the client and the MPASP server. If the message is successfully decrypted by the server using the mPIN, then it indicates that the corresponding client must have sent the message. The client cannot therefore deny having sent the message. Besides ensuring non repudiation, answering to the secret question plays an important role in preventing replay attacks.

6. Use Case Illustration

The figure 2 illustrates the use case diagram for the proposed system prototype. In the diagram the client sends the application on his or her mobile phone in order to perform a remote macro-payment transaction. Now, the message is created as secure message and sent via https socket connection to the server. The server decrypts the message, verifies message integrity and carries out account authentication. When this is successfully achieved the MPASP server thereafter performs the requested payment transaction. A confirmation is thereafter sent to the client indicating success of the requested transaction.

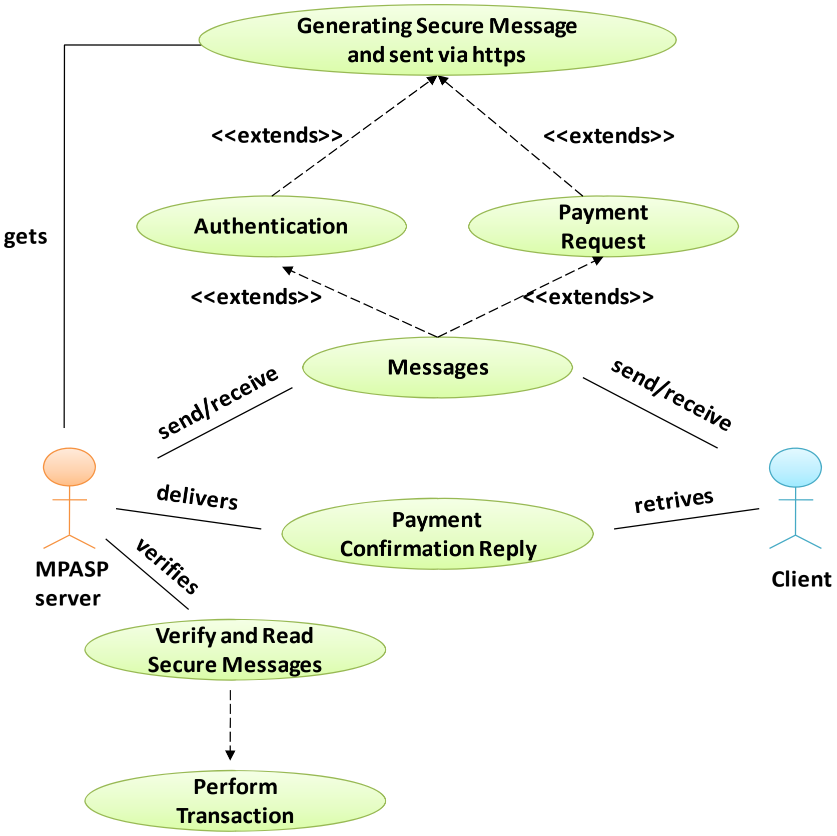

Figure 1. Use Case Diagram of Proposed Prototype

7. Conclusion

The increasing deployment of wireless networks and the widespread popularity of handheld devices have led to numerous mobile commerce applications. The mobile remote macro-payments are going to remain the de facto standard for personal payments in the near future. The Mobile devices are making a big impact on mobile payment systems. In particular, the mobile phones are becoming an increasingly popular way to make all sorts of payments. There are many mobile payment models are found in the market, but none of them has taken a dominant position due to its inherent limitations and due to focused on limited customer base.

This paper proposes an architectural design for mobile payment system that supports remote macro-payments and achieves end-to-end security using symmetric key operations. The proposed architecture is suitable to any kind of financial applications and quite importantly facilitates better understanding on the future development of mobile payments. This architectural design ensures the flexibility, better customer support, and quick response time, since it supports symmetric key crypto-system. The suggested protocol employs two-way authentication scheme to authenticate both the parties. This solution can be implemented within the available resources of a J2ME based devices and it does not require any modification in existing wireless networks or protocol.

The implementation of this security protocol will not increase expenses of users significantly. The proposed protocol can be easily implemented and executed on the current expenses charged by financial institution from the users. Basically, the cost model of the proposed protocol depends mostly on the policies that financial institutions adopt for implementing this protocol.

Future work will focus on developing a new prototype in a simulated environment based on the proposed architecture by using J2ME. The ongoing research includes performance and protocol investigation and the implementation of security properties. We believe that the security protocol guarantees that there are no delays or errors in delivery of messages. However, the number of implementation details to be considered in future, for example, error handling.

8. References

[1] Xiangpei Hu, Wenli Li, and Qing Hu, “Are Mobile Payment and Banking the Killer Apps for Mobile Commerce?”, In Proceedings of the 41st Hawaii International Conference on System Sciences, IEEE, pp.84, 2008.

[2] Y.A. Au & R.J. Kauffman, “The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application”, Journal of Electronic Commerce Research and Applications, vol. 7, issue 2, pp.141-164, 2008.

[3] S. Karnouskos & F. Fokus, “Mobile Payment: a journey through existing procedures and standardization initiatives”, IEEE Journal of Communication Surveys and Tutorials, vol.6, no.4, pp.44-66, 2004.

[4] Juniper Research (2004), Global mCommerce Revenue Projections For 2009, URL: http://www.epaynews.com/ statistics/mcommstats.html.

[5] Xiaolin Zheng, Deren Chen, “Study of Mobile Payments System”, In Proceedings of IEEE International Conference on E-Commerce, (CEC’03), pp.24, 2003.

[6] S.Karnouskos, A. Vilmos, P. Hoepner, A. Ramfos, N. Venetakis, “Secure mobile payment: architecture and business model of SEMOPS”, In Proceeding(s) of EURESCOM Summit, Heidelberg, Germany, September 2003.

[7] Ljupco Antovski, Marjan Gusev, "M-Payment", In Proceedings of 25th International Conference on Information Technology Interfaces, 2003.

[8] Jun Liu, Jianxin Liao, Xiaomin Zhu, “A System Model and Protocol for Mobile Payment”, In Proceedings of IEEE International Conference on e-Business Engineering, (ICEBE’05), pp. 638 – 641, 2005.

[9] Natali Delic, Ana Vukasinovic , “Mobile Payment Solution – Symbiosis between banks, application service providers and mobile network operators”, In Proceedings of the Third International Conference on Information Technology: New Generations (ITNG’06), pp.346-350, 2006.

[10] Bellare, Garay, Hauser, Herzberg, Krawczyk, Steiner, Tsudik, Van Herreweghen, and Waidner, “Design, implementation and deployment of the iKP secure electronic payment system”, IEEE Journal on Selected Areas in Communications, vol.18, no.4, pp.611-627, 2000.

[11] Hall, Kilbank, Barbeau, and Kranakis, “WPP: A secure payment protocol for supporting credit and debit card transactions over wireless network”, In Proceeding(s) of IEEE International Conference on Telecommunications (ICT01), 2001.

[12] Lei, Chen, and Jiang, “Generating digital signatures on mobile devices”, In Proceeding(s) of International Conference on Advanced Information Networking and Applications (AINA), Vol.1, pp.532-537, 2004.

[13] Wang and Eranakis, “Secure wireless payments system”, In Proceeding(s) of International Conference on Electronic Commerce, pp.24-29, 2003.

[14] Kungpisdan, Bala Srinivasan, and Phu Dung Le, “A Secure Account-Based Mobile Payment Protocol”, In Proceeding(s) of IEEE International Conference on Information Technology: Coding and Computing (ITCC’04), vol.2, pp.35, 2004.

[15] Jesus Tellez Isaac and Jose Sierra Camara, “An Anonymous Account-Based Mobile Payment Protocol for a Restricted Connectivity Scenario”, In Proceeding(s) of IEEE 18th International Workshop on Database and Expert Systems Applications (DEXA’07), pp.688-692, 2007.