SIMPA: A SIP-based Mobile Payment Architecture

Ge Zhang, Feng Cheng, Christoph Meinel
Hasso Plattner Institute, University of Potsdam, 14482, Potsdam, Germany
{ge.zhang, feng.cheng, christoph.meinel}@hpi.uni-potsdam.de

Abstract

In recent years, many Mobile Payment (MP) schemes have been proposed and used in practise. However, a prerequisite for extended acceptance and adoption of MP technologies is to deploy an effective MP system. So far, there is no such a standardised and scalable MP platform. Most current MP schemes are circumscribed by its mobile network infrastructures. Fortunately, the fast advancement of 3G technology equips next generation mobile phone network more benefits. Following this direction, we propose SIMPA -- A SIP-based Mobile Payment Architecture for next generation mobile network, which not only supports P2P payment communications between customers and merchants using Session Initiation Protocol (SIP), but also supports several traditional internet security protocols, to enhance privacy, confidentiality and integrity during the transaction. This paper depicts detailed protocol and system architecture of SIMPA. Some application examples from customers’ view are shown to demonstrate its function and feature.

1. Introduction

MP is an innovative payment method in which one or more components of the transaction are conducted using mobile equipments through mobile network. In the real world, MP is often regarded as an alternative of traditional credit/debit card. In MP scenario, people can simply send messages via their mobile phones to accomplish the transaction. This technical capability could inspire new business models. Currently, MP is widely adopted in several scenarios including TV shopping, online shopping and electronic booking. In its latest report, Juniper Research predicts that MP will achieve a volume of approximately USD 22 billion by 2009 [1]. However, promising as it seems, several drawbacks still exist to prevent the popularity of MP, which have been the critical bottlenecks. Firstly, to realize high-level security protection on MP is not an easy task. Current mobile infrastructures with low bandwidth and limited processing capability are insufficient to achieve most existing security criteria.

Secondly, current mobile phone network is in a closed environment principally configured by Mobile Network Operator (MNO). The architecture is not scalable enough. Adding or removing a purchase services leaves too much works to MNO. Also, most current MP solutions are not compatible with each other. A compatible standard is desired. Thirdly, additional expense has to be invested on MP service integration. For example, users may need to buy special mobile phones which support the MP function.

Fortunately, however, the evolution of mobile network extends new development space for MP. The tendency shows that the success of internet will replicate itself in mobile phone network, particularly as MNO rushes to deploy 3rd Generation Partnership Project (3Gpp) for their customers. According to a research report of In-Stat [2], 3G handsets will continue strong growth over the next five years as second-generation technology wanes. 3G network, with its benefits on bandwidth, is a desirable infrastructure to deploy new MP schemes. Furthermore, as a standard for next generation network, SIP is a potential candidate to be used to carry payment information. Driven by these points, we propose SIMPA --- A SIP-based Mobile Payment Architecture, to address these problems of current MP.

This paper is organized as follows. Section 2 gives some corresponding background. Some drawbacks of current MP solutions are analyzed as well. Section 3 shows the requirement of the new MP architecture and gives motivations to implement SIMPA on SIP. In Section 4, we summarize related works in this field. More detailed design for MP protocol of SIMPA is explained in section 5. Some application examples from customers’ view will be shown in Section 6. Finally, we conclude our research and give a short preview in section 7.

2. Background and Challenges

2.1. SIP-based Instant Message Service

Instant Messaging (IM) has been already widely used in the real world. It is defined as exchange text or media content between two entities in near real time. Now, it is one of the most important services in current mobile network. Therefore, as the signalling protocol of next generation network, SIP also supports IM service. B. Campbell, et al. proposed an SIP extension for IM processing [4]. Shown as Figure 1, the SIP IM message consists of message headers and body. The body of this message can contain MIME type just like E-mail. Generally, IM request have a higher requirement for security than other SIP requests so that end-to-end authentication, body integrity and body confidentiality mechanisms are compulsorily implemented. In our research, we adopt SIP IM services to carry MP information.

![SIP IM message example](image)

**Figure 1. An example of SIP IM message**

### 2.2. Scenarios beyond Current MP Scope

Although the traditional MP solutions have been successfully deployed in many cases, there are still some scenarios where the current MP schemes fail for multiple reasons in techniques, infrastructures, etc. Some of these scenarios will be described as follows.

- **Next Generation Environment:** Because of its benefit on low-cost, VoIP is widely accepted by people as a primary telecommunication alternative these years. However, due to some issues on usability and performance (e.g., bandwidth), current VoIP is seldom achieved in mobile phone. Nevertheless, it is predictive that VoIP will be integrated with mobile phones in the near future. It is a tendency that more and more mobile services are pushed to be down in the new platform. Whereas, many current practical solutions of MP are GSM based, which is infeasible to be transplanted to the new platform directly.

- **Customer and merchant belong to different MNO:** Although some MNO (e.g., Vodafone, T-mobile) have already developed MP services, they are not compatible with each other, that is, a customer of Vodafone probably cannot enjoy the MP services operated by T-Mobile. One solution is that the merchant can provide several independent payment solutions for different MNO. However, it requires additional cost.

- **High requirement of privacy:** Due to the limitation of infrastructures, current MP protocols are designed as concise as possible. It is difficult to realize the protection of privacy. As a result, the sensitive information of both customers and merchants is easily be compromised. For example, the payment gateway may easily collect statistical information of what a customer buys and the market share of merchants.

- **High requirements of security:** So far, the security of MP is its prime bottleneck. Such issues as authentication and trust-management protection are still not perfectly tackled. That is why MP has not been considered as a mainstream payment method. The main problem could be that traditional mobile infrastructures do not have enough capability to allow re-using internet payment protocol with strong authentication and cryptographic algorithm.

- **P2P Payment:** According to a recent survey, many business interviewees perceived current MP solutions as complex and difficult to use [5]. Current MP solutions are not suitable to be employed as a Peer-to-Peer payment platform since they are so complicated that personal sellers are discouraged to take them as a payment alternative. Since it is not scalable, P2P transaction method like Paypal [6] cannot be easily realized.

### 3. Requirements and Proposals

#### 3.1. Requirements for the New MP Solutions

In order to solve the problems mentioned above, several features listed are expected as follows.

- **SIP telephony supporting:** The new framework should be designed to base on internet protocols in favor of surviving in the new environment.

- **Compatibility:** Customers should be allowed to trade with merchants operated by different kinds of MNO. The payment protocol should base on an open protocol in order to be compatible.

- **Privacy:** The sensitive information of customer (e.g., PIN code) shouldn’t be captured by merchants. On the other hand, the purchase information (e.g., what the customer buys) shouldn’t be released to MNO.

- **Enhanced security protection:** Integrity and confidentiality of purchase request should be
protected. The new scheme should support End-to-End authentication. Furthermore, vulnerability of infrastructures should not cause uses’ loss.

- **P2P payment:** Merchants should be easily and autonomic configured. MNO acts as a payment operator, but doesn’t need to be involved in configuration of merchants, which can achieve self-management like ebay.

- **Low cost of payment:** The new MP platform should reuse as much existing infrastructures and methods as possible. Besides, the expense spent on maintaining should be minimized.

### 3.2. SIMPA Solution

The SIMPA solution employs Instant Message (IM) extension of SIP protocol to carry payment information, resulting in a scalable, compatible and secure payment platform.

**Why SIP?** SIP is designed as the signalling standard for the next generation network to provide multimedia services including VoIP and IM. First of all, SIP enable to provide a more security supports for MP services. Many classical internet models of transaction and security can be applied in SIP directly, including HTTP Digest [7], S/MIME [8] and IPSec [9]. Secondly, As a P2P protocol, SIP-based system is more scalable and easy-to-configure. Based on SIP, MNO doesn’t need to spend much time and resources on clients maintaining and this online business model can be easily extended to Customer-to-Customer (C2C) mode, like ebay. Last but not least, low-cost is an indispensable advantage for both customers and MP providers. SIP exploits the existing internet infrastructures and extends new service. All the services are realized on internet. Theoretically, there are not any extra costs for users to take advantage with MP services. Moreover, the P2P architecture of SIP is easy to manage. Therefore, the MP providers can save much budget on operating expenses.

**Why IM method?** First of all, IM method delivers text content between two partners. Text-based, our payment protocol is easy-to-understand. Secondly, according to RFC 3428, several security mechanisms are compulsory for IM. For example, messages must contain a Date header field covered by a signature to prevent replay attack. The message bodies must be encrypted by S/MIME. Finally, IM method is an existing and standardized service of SIP. Reusing IM method is helpful to reduce payment cost.

In sum, requirements of compatibility, security and low cost of payment motivate us to use SIP-based IM as the method to carry payment information.

### 4. Related Works

Previous works on MP mostly focus on business model, security model and its application. J. Ondrus et al., suggest that it is necessary to analyze the MP environment from multi-perspective including market perspective, actors perspective and issues perspective [10]. A. Zmijewska et al., introduce a user-centric classification model for existing MP systems. The dimensions of research derive from the user’s perspective (e.g., payment occurrence, value of payment, etc), which is helpful for developing new successful systems [11]. N. Mallat and V. K. Tuunainen conclude advantages and barriers of MP according to a set of empirical data which are collected from the merchant interviews. The advantages include increasing impulse purchases, promoting company image and offering new services. However, Compatibility, complexity and cost of payment should be tackled at first [5].

S. Karnouskos et al., present a Secure Mobile Payment Service (SEMOPS) which is an innovative solution for delivering a global mobile payment service [12]. SEMOPS has enhanced security, trust and privacy issues. Based on SEMOPS, J. Liu, et al., propose an improve model and protocol [13]. This new model is made to improve the signature validating and privacy issues. Furthermore, C. Yang and M, Qi propose a theoretical application of MP based on 3-D protocol [14]. However, these security schemes are complicated and require additional support.

J. Gao, et al., propose a peer-to-peer wireless payment system based on Bluetooth communications [15]. They design a 2-dimensional transaction protocol integrated several security solutions. I. Mullins et al., propose a MP solution for mobile phone users who play games over Peer to Peer connections. The MP scheme is designed o transfer of credits between game players based on the outcome of the game [16].

### 5. SIMPA Architecture

#### 5.1. Topology of SIMPA

Figure 2 shows the topology of the proposed MP model. There are six separated entities involved in the framework: customer, merchant, Payment Gateway (PG), SIP servers, Lock-Keeper and accounting database.
Customer: It is the participant who pays for goods or services via his/her mobile phone.  
Merchant: It is the participant who provides goods or services and accepts customer’s payment.  
Lock-Keeper[17]: It is a device based on the principle of “physical separation”, which works like a sluice to provide secure data exchange between the physically separated networks. In SIMPA, we deploy Lock-Keeper between SIP servers and PG to countermeasure possible attack towards internal critical infrastructures (PG, accounting database).

PG: It works as a trusted third party and communicates with customer and merchant to accomplish the transaction.

SIP servers: It regularly routes all the SIP messages to or from PG. These messages contain payment information. It also authenticates customers and merchants in case of impersonation.

Accounting Database: It is a database server which records user accounting information. The credits from customer to merchant will be operated here.

5.2. Payment Protocol

The payment protocol is derived from Secure Electronic Transaction (SET) [18], which can achieve privacy protection by separation of Order Information (OI) and Payment Information (PI).

The customers can send the merchant a purchase message, which includes both OI and PI. The OI confirms the purchase of items and the PI contains payment details (e.g., Personal Identification Number (PIN)). Neither the merchant needs to know customers’ PIN included in the PI nor the PG needs to know which item the customer wants to buy. The PI is encrypted in such a way that it should be kept as a cipher to merchant. After receiving the request, the merchant will decrypt the request and forward PI to PG to commit the transaction. Then, PG will ask the customer to confirm his payment request. If the confirm is replied, PG will update accounts of both the customer and merchant to accomplish the transaction.

Also, OI and PI must be linked in a way by which potential conflicts can be solved. Since it is the merchant to pass the PI to PG, the merchant can claim that a forgery OI goes with the PI rather than original OI. The linkage is necessary so that the customer can prove this PI is only intended for a particular order, not for other goods or services. A dual signature (DS) scheme [18] can be employed to protect the integrity of OI and PI.
Figure 4. The working flow of SIMPA

Purchase request: Firstly, the customer inputs a valid ID of the goods with price and his user PIN to purchase something according to a catalog. Then, an encrypted OI and PI with their DS can be automatically generated by the mobile phone of the customer. All the information are encrypted during transaction.

Merchant verification: The merchant can decrypt the OI included in the incoming message. However, only OI is readable to the merchant and the merchant will verify it. If verification is failed, the transaction will be terminated immediately. Otherwise, merchant will forward the encrypted PI, DS with a digest of OI to PG.

PG verification: After decrypting the payment request, PG has three verification tasks. Firstly, it will generate a new DS by PI and the digest of OI in order to compare with original DS. The transaction can continue only if the new and original DS are matched, which prove the linkage of PI and OI is valid. Otherwise, the transaction will be terminated. Secondly, the PG will authenticate customer with user PIN. The user PIN should be correct, otherwise, the payment request will be discarded. Finally, PG will also check whether the customer has enough balance to complete the transaction. If all of these three verifications are successfully passed, a confirmation request contained PI and a transaction identity will be sent to the customer.

Customer confirmation: The customer will first verify the PI, and feed back an acknowledgement to continue the transaction.

Settlement: After receiving the confirmation, the PG will credit the billing account of the customer and debit that of the merchant in favor of settlement. Receipts will be sent to both participates to notify the successful deal before goods delivery.

7. Application Examples

A series of cases of user interface is shown in this section to demonstrate the procedure of a customer conducting a mobile payment on SIMPA. Shown in figure 5, customer purchases goods “ABCD123456” by 2 euro from bob@shop.com on SIMPA.

Step 1: As shown in Figure 5 (a), (b) and (c), the customer fills in the purchase request including merchant, identity of goods and corresponding price with PIN code. And then, the customer sends the request.

Step 2: A confirmation message from PG is received. The customer needs to input PIN again to confirm the payment request (see Figure 5 (d)).

Step 3: A customer notification is received to indicate the transaction is completed (see Figure 5 (e)).
8. Conclusion

It is fairly clear that current MP services are heavily circumscribed by their infrastructures. They are expected to be improved with the next generation platform. In this paper, we present an innovative MP framework called SIMPA, which is based on SIP protocol. SIMPA is especially designed for the next generation mobile network and aims to overcome the drawbacks of current MP schemes. SIMPA provides a more secure platform for MP services. It is possible to implement strong security payment protocols on it. Moreover, it is more scalable and extensible. Compared to existing MP schemes, SIMPA costs less on system management. Detailed working flow and architecture of SIMPA is outlined. We will evaluate the performance and security of it in the future.

9. References