Int. J. Advanced Networking and Applications
Volume: 02, Issue: 03, Pages: 646-649 (2010)

Mobile Machine for E-payment Scheme

Sattar J Aboud
Information Technology Advisor, Iraqi Council of Representatives, Baghdad-Iraq
Email: sattar_aboud@yahoo.com

ABSTRACT

In this article e-payment scheme by mobile machine is considered. The requirements for a mobile machine in e-payment are presented, particularly when merchant employing accounts for payments and when using advertising. In the proposed scheme we will use the public key infrastructure and certificate for authenticate purchaser and merchant and to secure the communication between them.

Keywords – authentication, certificates, e-payment scheme, mobile machine,

Date of Submission: February 02, 2010 Date of Acceptance: May 20, 2010

1. INTRODUCTION

The attractiveness of mobile e-trade has been growing quickly these today [1]. This is largely due to the exponential increasing of Internet networks in the midst of citizens. In addition, during the past few years the mobile trade has also been growing mostly because of the growth in vending of mobile machine.

Present mobile machine already hold much information since the machine uses daily. The term mobile machine is employed in the mobile e- transactions standard, for a machine that is employed to carry out transaction processes. Porras [2] elaborates the mobile machine for dealing much more than only payment.

In organizations such as university where there are a small community and limited services that require small payments, such as vending machine, the employ of mobile machine for payment sounds attractive. The difficulty in standard coin typed payment is that purchaser has to have sufficient cash so as to make the payment. Credit card corporations charge additional fee from the service providers and generating own coins only for university services, includes another card that has to be hold and can be employed in only one location. Mobile e-transaction defines local payment that solves certain difficulties in the above stated cases [3].

But, mobile-transaction typed on trusted authority for charging, which can build this kind of technique more attracting for small company. However, it is possible to use a mobile machine method in a company without involving the trusted authority.

In this article we will consider the payment scheme for vending machine in local organizations, such as university. The use of mobile machine as a payment tools in this scheme will be considered as well, in addition to the authentication and connection security problems will be discussed. Solution for providing quick and easy purchasing interface in the scheme with secure setting to the scheme is illustrated and a method for this difficulty will be suggested.

2. PAYMENT SCHEME COMPONENT

The proposed payment scheme consists of four major components, purchaser and purchaser mobile machine, in addition to the merchant and merchant scheme. **Error! Reference source not found.** shows the components of the proposed payment scheme.

2.1 Payment Scheme Operation

Operations of a payment scheme can generally be divided to four stages: advertising, purchasing, paying and making the receipt of the commerce. In the proposed scheme vending machine keepers can send out special offers to the payment mobile machine of the purchaser has determined to make a buy, he determines it to the merchant, who makes an invoice according to the buy information. To receive the goods, purchaser has to pay the invoice with his mobile machine. Merchant will end this trade successfully by making a receipt and passing it to the purchaser machine. This receipt can be employed as an evidence of the trade later on.

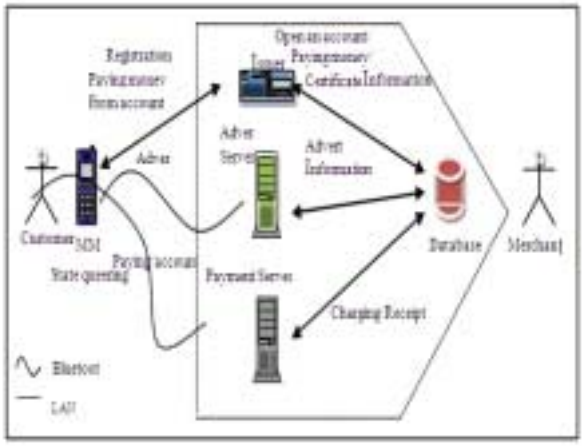

Figure1: participant of the payment scheme

The advertising service can be performed in classical methods, for example flash notes or by employing different methods for example poster [4]. However, this article focuses mainly on the subjects relating to the payment and also to the receipts

Volume: 02, Issue: 03, Pages: 646-649 (2010)

2.2 Payment Methods

The payments can be performed either in advance, at the instant of the trade or later on. Any of these are appropriate for the local milieu payment scheme. The fact how these are implemented is more important. The use of credit cards is an illustration of paying services later. But, we favored to avoid the employ of trusted authority in the proposed scheme, thus all payment cards are beyond the question for this kind of local payment scheme. The employ of mobile phone worker as agent party for billing is also cause dependency of the trusted authority and is not studied.

Employment of tickets for payments is an illustration of paying transaction in advance since purchaser has bounded financial value for the certain service. Tickets are too useful method for paying in a scheme where the amount of goods is restricted. In refectory and vending machines the amount of goods can be very large and that is why the amount of different types of tickets wanted would grow quickly. The employ of true currency is an example of the payment at the instant of buy.

The proposed method that is the employ of accounts is a mix of all these preceding methods. When employing accounts managed by merchant, transactions occur in the instant of buy. But, the accounts can be run in before or after method. If employing the in advance method the payment scheme base on prepaid account of the service provider. When the purchaser makes the buy, the total of credits is decreased from the account. When employing the next method the buys are gathered into the scheme and the purchaser has to pay at accurate intervals. In both cases the purchaser is provided with a receipt from the buyer. While both methods are possible, only the prepaid account is studied at the rest of this article.

2.3 Participants Authentication

The employ of account causes the want for robust authentication actions of purchasers. In addition the merchant has to be dependable authenticated because it takes care of the billing of the purchasers. Because merchant should have certain techniques to check the privileges of the purchaser to employ the account, registration into the scheme is necessary. Purchasers should to have an easy method to pay cash into their credit and to check the situation of account. If mobile machine is employed as payment tools, the authentication of a purchaser is a two-stage process.

1. The mobile machine authenticates its purchaser.
2. The merchant authenticates the mobile machine.

In payment scheme the purchaser authentication has to be fast and the number of operations needed in the authentication process has to be reduced for maintaining the functionality [5]. Classical passwords are the simplest method for authentication. Recently also biometric technique has become more and more common [6]. There are special tools integrated into certain new machines for taking fingerprints. Mobile phone cameras can also be employed to take picture regarding the purchaser for authentication purposes. For simplicity only fixed passwords are employed for that idea in this article.

In the purchaser authentication the restricted functioning of mobile machines has to be taken account. Address typed authentication is generally quite lightweight but connection equipment is dependent. Also, recognition of address does not classify from whom the messages are coming but from where they are coming. This is why address typed authentication is not adequate technique is employed.

Also, disposable password can employ for authentication. For instance, of this is to send an encrypted challenge to participant. This participant can employ the challenge as input in developing a disposable password and the authentication of participant can verify the validity of password. This technique employs generic challenge response method [7].

There is a need for managing the accounts and certificates in order to provide a fine service. With purchaser information such as name, email and company, there is certain machine with specific information involved certificates. For instance an address of payment tools can be built-in an extension field of the certificate. This makes it practical to arrange more than one authentication technique. The certificate can be ended successfully by using a challenge response method. The participants can then altering certificate that is generated by a challenge and then pass it to another participant, by encrypting the challenge method with the public key of that participant but the challenge method cannot be recovered the encrypted message without using the corresponding private key [8].

The size of message encrypted in the payment scheme has to be optimized. However, not every message must be encrypted and certain messages need to be encrypted partly. The challenge response method can also be rearranged in certain payload information and in mutual communication there is at all times possibility to encrypt either by own secret key or by the public key of the other participant. This provides possibilities to optimize the communication security.

3 PAYMENT SCHEME CONSTRUCTION

The employ of public key infrastructure needs specific construction for the payment scheme. The construction of scheme is introduced. The scheme owned by merchant embraces issuer, advertising server, payment server and database. Purchaser employs his mobile machine for joining into the scheme, receiving advertising, paying invoice and making account status. Bluetooth is employed for connections and certificate is employed for authentication and securing communication.

Issuer registers purchasers to the scheme by verifying them and by generating accounts. After registration purchasers can deposit funds in his account. Issuer stores account data and certificate of purchaser in the database.

Advertising is stored in the database and advertising server relays them to the purchasers after some advertising

groups and rules. With the assist of these rules purchasers can define when they want to receive both menus and special offers, either one of them or nothing. Merchant has software, which makes it possible to add advertising to the database.

With payment servers purchasers can pay their purchases and make account status queries. Payment servers store information of payments and their receipts into the database and make charging from the accounts. **Error! Reference source not found.** presents the process of the payment scheme. The process is divided into three elements: connection establishment, goods selection and paying.

3.1 Connection Establishment

The purchaser starts the payment process by defining the server to be employed. Payment servers in the range are queried with the assist of Bluetooth protocol. Information of all payment servers is presented to the purchaser, who can select the right server from the list. Usually there is only one payment server on the range, so selection doesn't cause any harm. Since Bluetooth inquiries take some time, the information of servers can be stored into the mobile machine for faster usage.

Payment process is started by a message, which includes the certificate of purchaser. The server checks the validity of certificate, sends it with certificate and goods list to the purchaser. When the certificate is valid, the goods list will be presented to the purchaser.

3.2 Goods Chosen

Purchaser can select a number of goods from the list and after collection make purchase. When server obtains the buy it will commence the challenge response process. The challenge is an arbitrary number, which is encrypted with the public key of the purchaser. Server calculates a hash of this arbitrary number. Purchaser recovers the challenge response by its secret key and calculates the hash of arbitrary number involved in challenge response. The hash is encrypted by the public key of server and pass to it. The server compares hashes and when they are identical; it makes the invoice and encrypts it by the public key of purchaser.

4 CONCLUSION

Purchasers can perform payments, managing account and receipt information by mobile phone. Whilst the payment scheme needs rapid and secure method for paying services, predefined accounts and public key infrastructure should used in the proposed scheme.

Public key certificate with extension can be employed for managing the privileges of purchasers, such as account numbers and mobile machine in the scheme. These certificates can also be employed for authentication of participants and securing communication between them, in addition to managing validity times of payment tools. The public key infrastructure need for the payment scheme can be prearranged easily without any assist of trusted authority. The proposed payment scheme can be employed in any company by using two servers for payment and advertising.

REFERENCES

[1] Milanovic S. and Mastorakis N., "Building a Strategic m-Commerce Services Platform", 4th WSEAS International Conference on Information Science, Communications and Applications, 2004.

[2] Porras J, Hiirsalmi P and Valtaoja A, "Peer-to-peer communication method for a mobile Environments", 37th Hawaii International Conference on Scheme Science, 2004.

[3] US Patent 7194438 - Electronic payment schemes in a mobile environment for short-range transactions, US Patent Issued on March 20, 2007.

[4] Jäppinen P. and Porras J, "Flash notes over Bluetooth Wireless Technology", International Conference of Wireless LANs and Home networks ICWLHN, 2001.

[5] Ren-Junn Hwang, Sheng-Hua Shiauand Ding-Far Jan, "A new mobile payment scheme for roaming services", Electronic Commerce Research and Applications Volume 6 , Issue 2, 2007, pp. 184-191

[6] Takuji M., Masahito M. and Koichi S, "Quantitative Performance Analysis of Biometrics Identification for Authentication Schemes Design", 4th WSEAS International Conference on Information Science, Communications and Applications, 2004.

[7] Gianluigi Me, Maurizio Adriano Strangio, and Alexander Schuster, "Mobile Local Macro-payments: Security and Prototyping", IEEE Pervasive Computing, volume 5, number 4, 2006, pp. 94-100

[8] Julia Richardson, Mary Mallon, "Mobile Machine for E-payment Scheme", Journal of World Business, Volume 40, Issue 4, November 2005, pp. 409-420

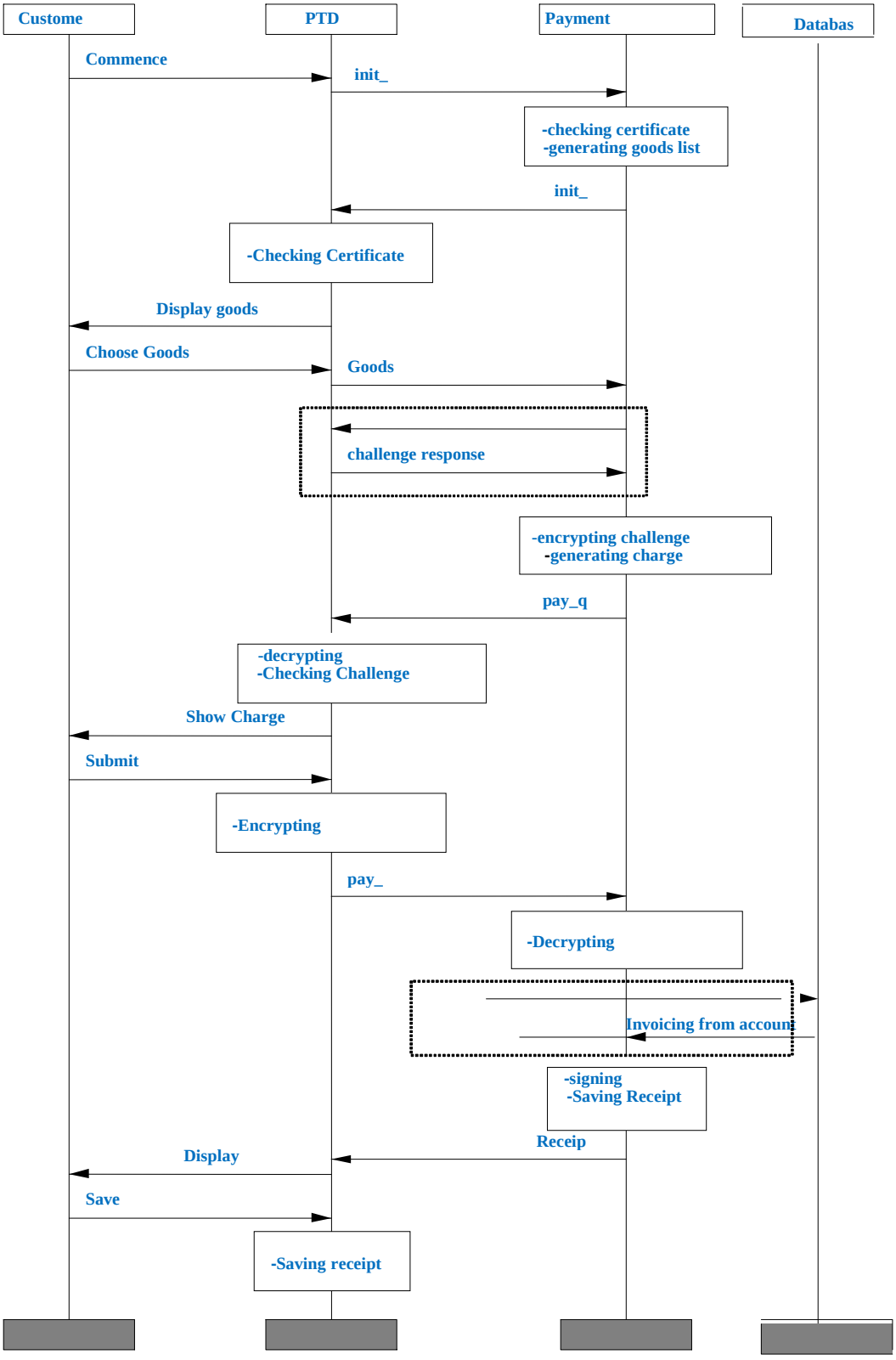

Figure 2: Process of the payment scheme