An Alternate E-Payment Method for B2C E-Commerce Transactions to Increase E-Commerce Penetration in Sri Lanka

C.N. Weerakoon1, G. Nuwan Kodagoda2
Sri Lanka Institute of Information Technology, Metropolitan Campus, Sri Lanka
cnweera@yahoo.co.uk 1, nuwank@sliit.lk2

Abstract: One of the most important factors in e-business is the ability of the customer to buy goods & services online, using electronic payment methods. Due to non-availability of alternate electronic payment methods, the Credit Card has become the most widely used online payment method available for B2C e-commerce transactions in Sri Lanka. But the statistics show that less than 4% of the population in Sri Lanka has a credit card. This is a limiting factor in encouraging the business to take their operations online. Even among those who have credit cards, some are reluctant to buy online due to privacy and security concerns, over disclosing credit card information online. Compared to the credit card penetration, Sri Lanka has a tremendous growth in mobile phone market, where penetration level is over 15%. This paper will try to exploit that situation by focusing on developing an alternate e-payment method using the mobile phone as a payment device.

Keywords: E-commerce, Electronic Payment, Mobile Payment.

1. Introduction

Electronic payments have become a vital part of e-commerce and the emerging realm of e-business. However, in Sri Lanka very few web sites / Merchants accept payments online. The only online payment method available for Sri Lankan e-commerce merchants is that of accepting credit cards. The problem in this is that not everyone owns a credit card in Sri Lanka (less than 4% of the total population) [1] and there is also a serious antipathy towards using credit cards online because of mistrust and potential fraud.

Financial institutions and merchants are increasingly interested in automated electronic forms of payment. The reasons for this are simple; the more the payment process is made electronic, the lower the costs for both the technology to process conventional money and the actual manual processing of payments. The main reason people want to use credit cards is focused on the convenience they provided. Despite the inviting advantage, the more convenient these credit cards can be used for daily deals also makes them more desirable to thieves or evildoers.

A survey conducted by The Sri Lanka Business Development Centre in June 2002 has identified the payment method as a bottleneck [2] in purchasing goods over the Internet. And this is also interpreted as a key reason for the low e-commerce penetration in the country.

This paper will specify and propose a system that enables users to perform secure payment transactions using mobile phones. System will use the GSM infrastructure for establishing a convenient, secure and usable e-payment scheme.

2. Proposed Mobile Payment Model

In the proposed payment model would use the existing GSM security mechanisms and the communication between the mobile phone and the MSP (Mobile Service Provider) will be conducted in the ciphering mode [3], which would enable the transmitted data to be encrypted. The use of existing GSM security mechanisms will enable the service provider to use the existing SIM cards without any modifications in the payment model and this would eliminate the cost of replacing SIM cards.

The communication between the bank & the MSP and the merchant & the MSP will be conducted using the existing telecommunication infrastructure. In the proposed payment system the MSP will be responsible for receiving, processing and verifying the payment request from the merchant, establishing user authentication and authorization, and giving the bank the instructions necessary for the payment settlement between the user and merchant. The MSP will also communicate the transaction confirmation, received from the bank, to the merchant and the user.

Message Flow

1. Shopping Phase: The customer goes to an online store and adds items to his shopping cart. Then the customer will select the method of payment as the MOBILE and will enter his Mobile Phone number and the alias at merchant’s web site.

2. Payment Request Submission Phase: The merchant submits the purchasing information, along with the customer’s mobile number; alias signed using the
The transaction dialogue between the Mobile and the MSP will be conducted in Ciphering Mode to ensure that no one but the intended MS (Mobile Station / Mobile Phone) could decrypt the message. In ciphering mode the data transmission from and to the MS will be encrypted using the A5 algorithm and the individual subscriber authentication key, which uniquely identify the subscriber [3]. The message from the MS will also be encrypted to ensure that only the MSP could decrypt the message. In ciphering mode the data transmission from and to the MS will be encrypted using the A5 algorithm and the individual subscriber authentication key, which uniquely identify the subscriber [3]. The message from the MS will also be encrypted to ensure that only the MSP could decrypt the message. In ciphering mode the data transmission from and to the MS will be encrypted using the A5 algorithm and the individual subscriber authentication key, which uniquely identify the subscriber [3]. The message from the MS will also be encrypted to ensure that only the MSP could decrypt the message. In ciphering mode the data transmission from and to the MS will be encrypted using the A5 algorithm and the individual subscriber authentication key, which uniquely identify the subscriber [3]. The message from the MS will also be encrypted to ensure that only the MSP could decrypt the message.

The transaction procedure of the proposed system has some similarities to the traditional credit card payment system. The primary difference is that the customer would use his mobile phone number and the alias instead of the credit card number to carry out the transaction. Then the MSP will prompt the customer via his mobile phone to verify the transaction. This will ensure additional security because ultimately only the mobile user, via his mobile phone, could authorize the transaction. Even stealing the mobile phone will not help as the payment authorization will require the knowledge of the PIN, which is only known by the customer (mobile user), whereas a stolen credit card could be used for offline transactions (over the counter payments) without much complication because only the customer’s signature (signature is present at the back of the credit card) is required, and anyone with practice could duplicate the signature.

3. Mobile Payment System – Service Preparation & Transaction Flow

In order to register for the mobile payment system user should have to fulfill the following criteria.

1. Own a mobile phone registered with an authorized MSP, under user’s own name.
2. A bank account in user’s name in an authorized bank.

The users who want to register with this service should get approval from the bank to integrate the bank account with this service. Bank will issue the user with an ‘Account Activation Code’, which the user will have to submit with the bank account details in the registration phase. The Mobile Payment Service Provider will submit the bank account information along with the account activation code to the financial institute, which will verify the details and will integrate the bank account with the service.

In order to use the payment system users will be required to have an alias phone number (which will be issued by the MSP), which will only be known to the mobile user. Alias phone number will guarantee that only the authorized user will be able to use the system.

User would be billed at a fixed rate per transaction and bill will be sent along with the ‘Mobile Phone Bill’ and merchants will be charged a percentage of the total transaction amount just like credit card payments, which could be agreed upon by the merchant and the MSP.

Transaction flow of the proposed payment model is illustrated in figure 2.

Transaction flow:

1. Mobile User selects the products and adds them to his shopping cart. Then the user will select the method of payment as the MOBILE and will enter his Mobile Phone No. and the Alias Phone No., at merchant’s web site, instead of his credit card number.
2. Merchant forwards the Transaction Details plus the Mobile & Alias numbers of the customer to the MSP.
3. Upon receiving the payment request, the MSP validates the combination of Mobile No. & Alias and if accurate then the MSP prompts the Mobile Phone to verify the Transaction. (User will be shown the merchant’s name, e.g. “ABC Store”, and the amount, e.g. “LKR 1,500.00”).
4. User verifies the transaction by entering the PIN number, in the mobile phone, provided by the MSP.
5. MSP, after verifying the PIN, requests the bank to process the transaction.
6. Bank will authorize the transaction and sends MSP the confirmation code.
7. MSP confirms the transaction to both the Mobile Phone and the Merchant.
8. Merchant will display confirmation details to Mobile User over the web.

In the proposed system, if the customers mobile number/alias is acquired by a third party, it couldn’t be used to make a payment due to the fact that a payment request could only be approved by the customer via his/her mobile phone using the PIN number, which is only known to the customer. However, the knowledge of the customer’s mobile number & alias could be used by a third party to flood the customers’ mobile phone with bogus payment request messages. This could create a problem, as there could be complications as to who would be responsible for the payment of network usage, for the failed transactions (bogus payment requests).

In the online scenario customer is required to enter both the Mobile Phone No. as well as the Alias Phone No. in order to make a payment, which will ensure that only the authorized customer will be able to enter both numbers correctly (Phone number may be known by everyone but the alias will only be known to the authorized customer) and thereby avoid unauthorized usage which could be used flood customers phone with messages.

In the offline scenario when the customer uses the payment system to pay for over the counter purchases, the customer is required to key in the alias phone number in the mobile payment processing terminal at the store. The alias is only known by the authorized customer and only he/she will be able to enter the number correctly. Customers, by directly entering the alias in the terminal will ensure the numbers are not available to the merchant or a third party (eavesdropper) and thereby avoid unauthorized usage.

By using the alias, which is only known to the authorized customer along with the mobile phone number, the system will ensure that customer could not deny using the system for a payment. This is especially important in this system due to the fact that even a failed transaction uses the GSM network and someone has to take responsibility for the failed transaction (Cost to the MSP).

In the online and offline scenarios, because it requires the knowledge of the alias to use the payment system, the users will be protected from a third party which could use the knowledge of the users mobile phone number to make bogus purchase requests and flood the customers mobile phone with messages.

4. Advantages of Proposed Payment Model

The main concern for the majority of e-commerce customers who use World Wide Web is the security of the payment information (credit card details, bank account details) and it has become a stumbling block for e-commerce development. The lack of a proper electronic payment mechanism, which has a decent market penetration, is identified as a major barrier for the development of e-commerce in the Sri Lankan.

The proposed scheme is aimed at solving the above concerns of both the customers and the merchants, who wants to market their goods over the web. In the proposed scheme the mobile phone number/alias is used instead of the credit card/account information thereby hiding the sensitive information such as the credit card numbers. And by using the mobile phone as a payment device, the system can achieve a market penetration level, which is five times that of credit cards in Sri Lanka.

The advantages of the proposed scheme could be listed as follows.

Advantages to the customer
1. The customer does not need to declare private information such as name, or credit number through the Internet. Only the mobile phone number and the alias phone number, are required for the online transaction and thereby the proposed scheme protects the customer from revealing sensitive information over the Internet.
2. In case the SIM card got lost or stolen, anyone other than the user could not use it to make payments because it requires the knowledge of the PIN number to authorize the transaction. This requirement of having to have the SIM as well as the knowledge of the PIN number makes the payment method safer than average credit cards.
3. In the offline/over the counter payment scenario the payment method could be used by another person to pay on behalf of the original customer, because ultimately only the original customer could authorize the payment via his/her mobile using the PIN. This method could be used as an alternative to supplementary credit card cards and could give distinctive advantages to the original customer as he would be able to monitor the transactions as well as control them, whereas with supplementary cards the main card holder gets the transaction details and the bill at end of the month.

Advantages to the Service Provider (MSP)
1. Proposed system uses USSD, which supports sessions and works on almost all-existing GSM mobile phones [4], for transaction dialogue. Because of this reason SIM replacement or phone upgrade is not necessary.
2. USSD is an ideal cost-effective channel for operators as it uses the signalling channels of a GSM network to transmit information, whereas an IVR (Interactive Voice Response) system utilizes expensive voice channels [5].

3. At the back end of the payment system, bank settles transactions using traditional account transfers, therefore the problem with customers’ defaulting payments does not arise. (Customer should have sufficient funds in the bank account in order to bank to confirm transaction)

4. Customer could be billed for the mobile transactions (for the session time or at a fixed rate per transaction) using the mobile phone bill. To use the system to pay for an online transaction, it would require the knowledge of both the mobile phone number as well as the alias phone number, which is known only to the customer. Therefore, third party could not enter both the mobile and alias number combination correctly. This ensures that even in case of a failed transaction, customers cannot deny using the system to make a payment.

5. Even the prepaid card mobile phones could be easily incorporated into the system because the transaction is carried out using the funds in the customer’s bank account.

Advantages to the Merchant

1. The system uses two-factor authentication and offers strong protection against customer transaction repudiation. The customer cannot deny the transaction due to the fact that he has authorized the transaction using the mobile phone and the PIN (which is only known by the customer).

Advantages to the Bank

1. Transaction costs will be minimal to the bank as the bank does not get directly involved in the transaction, but only confirms the transaction by verifying the funds in the bank accounts and performs direct credit/debit the funds between customer and merchant accounts using traditional banking methods.

All the parties involved in the mobile payment system rely heavily on the service provider to handle the transaction. The MSP in the proposed system will,

- Authenticate the customer,
- Informs the bank to pay the merchant, using the funds from the customers account and
- Confirms the transaction to both customer and the merchant.

Therefore the system to work the merchant, the customer and the bank has to trust the MSP.

5. Further Improvements

The system could be further developed, where the user’s mobile phone could be used to send and receive money to and from another mobile user. This would allow account-to-account money transfer using a mobile. This could be an ideal low-tech solution for a third world developing country like Sri Lanka to develop e-commerce aspect in small and medium industries (handloom, handy crafts etc) in the country. A small-scale industry may not have the investment capability to buy a computer, but they may have the capability to buy a mobile phone, and use the mobile phone as a virtual POS by using it to receive money from the customers.

6. Conclusion

The Government of Sri Lanka is in the process of preparing an E-Commerce Legislation [6], which is aimed at providing a legal regime to facilitate the conduct of commercial transactions electronically. It will give much-needed legal and regulatory framework for the development of e-commerce in Sri Lanka.

The identification of the mobile phone as a payment media has given the much-needed level of market penetration, which is over 15%. The proposed Mobile Payment System, by utilizing customer’s mobile phone number and an alias, as opposed to the customer name and the credit card number in credit card payment method, provides much needed privacy for the customers. In the proposed MPS (Mobile Payment System), ultimately only the customer can authorize the payment via his/her mobile phone by entering the PIN number and it offers better protection due to the fact that even if the mobile is stolen or lost, an unauthorized person could not use it without the knowledge of the PIN, which is only known to the customer.

Further, the mobile phone as a payment media offers superior balance of security and convenience, whereas the consumers’ mobile phone could be utilized as both communication and a payment device.

7. References


