Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.770 – 778

RESEARCH ARTICLE

Research on Online Transaction Protocols for Supporting Credit/ Debit Card Transaction

[a]Ms. Ritu, [b]Ms. Renu

[a] Student, Lingayas University, Faridabad, India
[b] Student, Lingayas University, Faridabad, India

***Abstract:** The increase of wireless devices, offering connectivity and convenience, continues to exert marvelous demands on merchants to deploy secure wireless applications including electronic commerce. One key element, which would help them in fulfilling this requirement, is a standard protocol for supporting both electronic credit card and debit card transactions over wireless networks. Although the Secure Electronic Transaction (SET) protocol offers end-to-end security for credit card transactions over a wired infrastructure, there are several factors including bandwidth requirements which make it unsuitable for wireless applications. This paper presents the Wireless Payment Protocol (WPP) that supports both credit-card and debit -card transactions using the Wireless Application Protocol's (WAP) Wireless Transport Layer Security (WTLS) and Smart Card technology. In addition, a brief comparison between SET and WPP is done.*

***Keywords:** SET protocol, WAP, WPP, Wireless, SWPP*

Introduction

The unstable growth in the use of mobile devices (428 million mobile users in 1999 [1]) is indicative of the next computational platform, then consumers will soon have the option of accessing web-based applications using personal computers or mobile devices. This wonderful growth fueled by consumers' need for mobile access to information and other services, is serving as a catalyst for the development and deployment of secure wireless applications including electronic commerce. Now, many different payment protocols are used to support electronic payments over the Internet : E-cash for electronic cash [2], e-Check for electronic-cheque [3], Secure Electronic Transaction (SET) for credit card payments [4].While these methods of payment do fulfill the customer's needs, the underlying protocols have been developed in an uncoordinated manner . Whereas an effort to standardize credit card payments through SET has proved beneficial, standards do not necessarily exist for the remaining types of payments. Later, any attempt to migrate these payment protocols from the wired to the wireless environment will more than likely result in a similar excess of protocols. For example, an optimized and wireless-version of SET using mobile software agents has been proposed by [5] to permit credit card transactions over the Internet. This version of SET only focuses on the front-end (client to merchant) of the transaction. Another issue, which has involved a lot of media attention, is credit card scheme perpetrated over the Internet.

What will prove beneficial is a standard payment protocol that supports both credit and debit card payments over wireless networks in a secure and efficient manner.

This paper will introduce the SET, WAP, WPP, SWPP, WPP differs from SET, comparison between WPP and SWPP.

As our objective was to develop a wireless payment protocol which supports credit card payments as well as debit card payments in a secure manner.

A. Secure Electronic Transaction (SET)

The emerging standard for credit-card payments resulted from a call for security standards by MasterCard and Visa in Feb. 1996. The Secure Electronic Transaction is an open encryption and security specification designed to protect credit card transactions on the Internet.

The Secure Electronic Transaction is an open encryption and security specification designed to protect credit card transactions on the Internet. The companies that collaborated in the development of SET include IBM, Microsoft, Netscape, RSA, Terisa and Verisign. It is supported by major corporations such as VISA Inc. and MasterCard. Although SET has been designed to operate in a wired infrastructure its transaction flow and implementation of security are of interest to us since it can also be employed in a wireless scenario.

The SET protocol is an evolution of the existing credit-card based payment system and provides enhanced security for information transfer as well as authentication of transaction participant identities by registration and certification. SET is also an international standard with published protocol specifications. While SET permits customers to make credit-card payment to any merchant offering web-based services, customers also have the option of paying for other types of services using the on-line banking facilities.

Some disadvantages of SET are:

a) SET is designed for wired networks and does not meet all the challenges of wireless network.

b) As the SET protocol was designed to preserve the traditional flow of payment data (CA – MA – Merchant's Bank), an end-to-end security mechanism was required.

c) The third element is the direction of the transaction flow. In SET transactions are carried out between Customer Agent and Merchant. It is vulnerable to attacks like transaction/balance modification by Merchant.

d) The transaction flow is from Customer to Merchant so all the details of the users credit cards/debit cards must flow via the merchant's side. It increases the user's risk, since data can be copied and used later to access a customer account without authorization.

e) There is no notification to the Customer from the customer's Bank after the successful transfer. The user has to check his/her balance after logging on to his/her bank's website again.

f) SET is only for card (credit or debit) based transactions. Account based transactions are not included.

A high-level overview of the SET protocol is illustrated in Fig. 1. Please note that a detailed description of the mechanisms used for enforcing security requirements of the protocol will not be presented in this paper. For additional information, please refer to. In addition, selecting items to be purchased as well as the request for payment and the transfer of funds between merchant and customer at the bank) are considered to be out of scope.

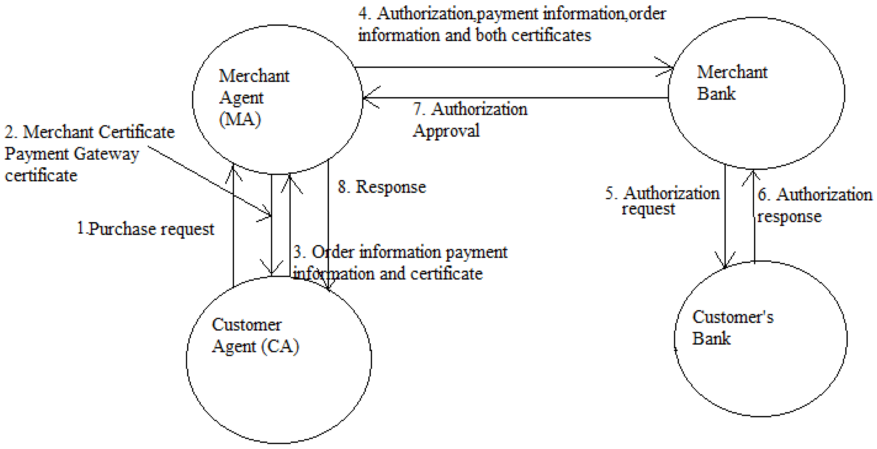

4. Authorization,payment information,order information and both certificates
Merchant Agent (MA)
Merchant Bank
7. Authorization Approval
2. Merchant Certificate Payment Gateway certificate
8. Response
5. Authorization request
6. Authorization response
1.Purchase request
3. Order information payment information and certificate
Customer Agent (CA)
Customer's Bank

Figure 1: SET Protocol

In a typical scenario, the merchant's site will be accessed via the Internet by customers using their personal computers. The payment transaction flow commences once the customer has completed the selection and ordering phase.

1) Customer Agent (CA) sends purchase request to Merchant Agent (MA).
2) MA sends certificates of merchant and payment gateway (bank) and other information to CA.
3) CA creates order information (OI) and payment instructions (PI), encrypts them using the multiple certificates received from the MA, and returns the encrypted PI/OI to the MA.
4) MA requests payment authorization from
Customer's Bank via Merchant's Bank.
5) Merchant's Bank contacts Customer's Bank for authorization.
6) Customer's Bank responds with status of authorization.
7) Merchant's Bank forwards status of authorization to MA.
8) MA prepares a purchase response and sends it to the CA. If this payment transaction flow looks very similar to that of a Point of Sale (POS) transaction, it is not coincidental. One of the key objectives in designing SET was to minimize the impact to existing merchant and banking applications and leverage on existing payment infrastructure. The security and performance aspects of SET will be discussed in the following section when we make a comparison between SET and the Wireless Payment Protocol.

B. Wireless Application Protocol (WAP)

Minimizing the need for application -level security by exploiting the security services offered at the Transport level of the TCP/IP protocol stack was one of our objectives in developing the WPP. To this end, the Wireless Transport Layer Security (WTLS), of the WAP stack was used to address the security requirements of the WPP. However, we could have used any other protocol stack which provided similar security services as the WTLS layer. The WAP represents the de-facto world standard for the presentation and delivery of wireless information and telephone services on mobile phones and wireless terminals. Currently over 90% of the companies providing wireless devices have accepted the WAP protocol [6]. The development of this protocol was intended to make the services of the Internet available to mobile users. Formally released in November 1999 (v 1.2 issued in June 2000), the key elements of the WAP specification which were of particular interest to us is the WAP Programming Model based on the existing WWW Programming Model and the lightweight version of the TCP/IP protocol stack streamlined to minimize bandwidth requirements.

The selection of the Wireless Application Protocol as a framework provides considerable benefits. First, as the protocol is gaining both recognition and widespread acceptance, it will continue to be supported for some time to come [7]. Second, the Wireless Transport Layer Security (WTLS) fulfills most of the key security requirements (data integrity, authentication, encryption and denial of service) of WPP. Third, a number of enhancements to the session, transaction, security and transport layers of the protocol stack have been implemented to optimize the protocol and take into consideration the constraints of wireless networks, namely, low bandwidth and high latency conditions. Finally, the micro browser, proxy technology and compression in the network interface works in concert to reduce the processing load, to reduce power consumption and to extend battery life of mobile devices. The WAP stack is basically divided into five layers including WAE, WSP, WTP, WTLS and WDP. We can take any subset of WAP layers and use them in an already existing framework. WAP encompasses WIM (WAP Identity Module), WML Scrypt, WTLS (Wireless Transport Layer Security) and WPKI (Wireless Public Key Infrastructure), which all apply security at the application, transport and management levels in the wireless environment.

WIM: The WIM is used to store and process information needed for user identification and The WAP stack is basically divided into five layers including WAE, WSP, WTP, WTLS and WDP. We can take any subset of WAP layers and use them in an already existing framework. WAP encompasses WIM (WAP Identity Module), WMLScrypt, WTLS (Wireless Transport Layer Security) and WPKI (Wireless Public Key Infrastructure), which all apply security at the application, transport and management levels in the wireless environment.

WIM: The WIM is used to store and process information needed for user identification and authentication such as certificates and keys. It is also used in performing WTLS and application level security functions. WIMs are most commonly implemented using smart card chips that optionally reside in the WAP device.

WMLSCrypt: The WMLScript Crypto Library Specification provides cryptographic functionality for message signing. The WAP WMLScript signText function provides digital signatures in WAP-compliant customer devices.

WTLS: WTLS is a security protocol originated from TLS/SSL, and takes into account the specific features of the wireless environment.

In order to be used in wireless applications, WTLS has a number of additional characteristics which SSL lacks, such as compact coding, datagram support, optimized handshake, fast encryption and decryption algorithm, etc. There are three levels of security provision at various stages of adoption. WTLS Class 1 provides confidentiality and data integrity between the wireless device and the WAP gateway. Class 2 adds the authentication of the WAP gateway to the security services provided by Class 1. Finally, Class 3 is built on Class 2 by adding support for the authentication of the wireless customer.

The WTLS Handshake is very similar to the SSL handshake. The handshaking protocol is to establish a secure session between a WAP Customer and a WAP gateway. To accommodate the unreliability and unpredictability of connectionless datagram communication, messages are always packed as one Record Protocol packet when sent in one direction, to ensure that they are either received or lost on the other side.

A Digital Certificate is very important for customer authentication and non-repudiation. The X.509 Certificate is the most widely accepted Internet standard. However, X.509 is not supported by the current generation of WAP Customer devices, as they are marked by limited capacity. The WTLS certificate is similar to the X.509 certificate but is coded more compactly, and satisfies the high latencies and low bandwidth of wireless networks, as well as the limited processing resources of WAP Customer devices.

WPKI: Similar to the IETF PKI standards that are most commonly used in wired networks, WPKI standards are the most commonly used in wireless networks. WPKI, an extension of traditional PKI, is used to leverage security features including WIM, WMLS Crypt and WTLS. Like all security and application services within the WAP environment, WPKI must be optimized, using more efficient cryptography and data transport techniques, in order to work with personal wireless devices and the narrow-band wireless networks. WPKI has optimized PKI protocols, certificate format, cryptographic algorithms and keys.[8]

C. WIRELESS PAYMENT PROTOCOL

After having analyzed SET and WAP and having taken into consideration the constraints of the wireless infrastructure, we developed the secure Wireless Payment Protocol (WPP) for supporting credit and debit card transactions over wireless networks. The key elements of the underlying architecture are depicted in Fig. 2. As with the SET protocol, the Merchant Agent (MA) represents a web-based application which executes on the merchant’s server. The application would be made available to the customers through a WAP Gateway (converts HTML to WML and uses the WAP protocol stack to communicate with the wireless/mobile devices of the customer).

The Customer Agent (CA) is an application running on the wireless device. It is used as an interface between the WAP Scripts and the Smart Card (SC). The SC provides a static storage mechanism for personalized data such as encrypted banking information of the customer. As far as the banking institutions are concerned, both the Customer’s Bank and that of the merchant are responsible for issuing digitally signed and encrypted banking profiles (banking information). As with SET, security of the banking infrastructure is assumed to be sufficient and outside the scope of WPP.

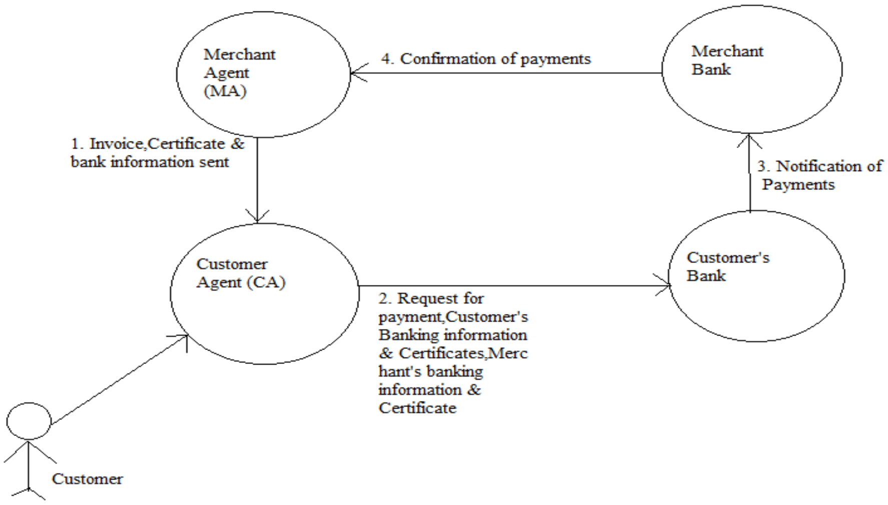

Merchant Agent (MA)
4. Confirmation of payments
Merchant Bank
1. Invoice,Certificate & bank information sent
3. Notification of Payments
Customer Agent (CA)
Customer's Bank
2. Request for payment,Customer's Banking information & Certificates,Merchant's banking information & Certificate
Customer

Figure 2: Wireless Payment Protocol

The protocol commences when the MA sends to the CA an invoice and terminates when the MA receives a confirmation of payment from the Merchant's Bank. Please refer to Fig. 2. As with SET, the ordering and payment/settlement phases as well as resource mechanisms are outside the scope of this protocol. Although, only a brief description and subset of data elements are provided in this paper, details of the protocol are available [9].

The payment transaction flow is as follows.

1) MA prepares invoice and sends the merchant's certificate, encrypted banking information and the invoice to CA.

2) Customer confirms accuracy of the invoice. Once satisfied with the invoice, the customer is prompted to enter the Personal Identification Number (PIN) to authorize access to the SC. Once the PIN has been validated by SC, the CA presents the customer with payment options (i.e. credit-card, debit-card). After a method of payment has been selected by the customer, the CA prepares a payment request. It is digitally signed by SC and is forwarded to the Customer's Bank along with certificates and encrypted banking information of the customer and merchant.

One thing to note is the transfer of certificates from both the merchant and customer to the Customer's Bank. Although the certificates are used by the bank to validate the digital signature of the merchant and customer, it is possible that the bank could make use of a distribution service to obtain these certificates. This will, of course, further reduce the size of data being transmitted and improve the overall performance of the protocol.

Basic characteristics of WPP

The main characteristics of WPP are summarized as follows:

Eliminating fraud source for online transaction:

Credit card fraud is a serious problem on the Internet. WPP eliminates the source of fraud by altering the direction of the transaction flow. The credit card information can only be given to the customer's bank.

WPP is convenient, with the addition of a strong security element.

Dual signature is not required:

Compared with MeT, a dual signature is not required in WPP since customer's payment instructions are sent directly to the Customer's Bank. The merchant's banking information (previously encrypted by the bank) is sent to the customer and then forwarded to the customer's bank.

Using Smart Cards:

In WPP, smart card is used to store encrypted banking information. It can also store Personal Identification Numbers (PINs) so that credit card payments can incorporate other types of payments, such as debit card payments.

End to end security:

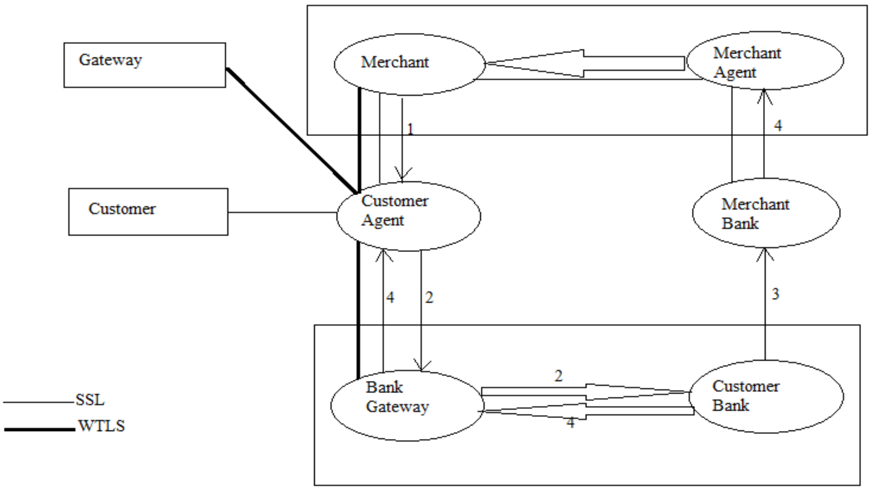
End to end security is guaranteed through a Gateway, which acts as a bridge between the SSL and WTLS protocols. In WPP, security is addressed with the assumption that the WTLS protocol will provide the confidentiality and integrity of all messages exchanged between all participants of the protocol. To put WPP in practical use, WPP must be redesigned to fulfill its security requirements.[10]

D. Secure Wireless Payment Protocol [11]

SWPP is proposed to make up for WPP's security deficiencies. SWPP draws upon WAP, which is designed to make full use of Internet services, for WTLS, WIM, WMLScrypt and WPKI to guarantee the security requirement presented in WPP. SWPP uses proxy technology in conjunction with firewalls to define the boundary for the service domain.

Architecture of SWPP

A generic infrastructure of SWPP and its transaction flow is presented **in Fig 3.**



(1 – acknowledging order 2 – request for payment
3 – Notification of payment 4 – Confirmation of payment)
Figure 3: SWPP architecture

SWPP process commences when the merchant sends an invoice to the customer and terminates when the merchant receives confirmation from its Bank. The gateway in Figure 3 is used to locate the bank gateway or merchant gateway as requested by the customer.

A security channel between the Merchant Agent and the customer is assumed here, as it is quite similar to that between the customer and the customer's bank. In this way, we do not have to take into account a Merchant Gateway between the customer and the Merchant Agent. On the customer side, they can use SWIM to store personalized data such as certificates, keys, PINs and encrypted information.

Secure WTLS session channel

In SWPP, secure WTLS Session Channel is built between the customer and the bank gateway before the message is sent from Customer to Customer Bank. Using the storage and functionality of the WIM, the Customer Agent can now build a secure session with the bank gateway.

End to End Security

End-to-end security between the customer and the customer's Bank cannot be built only based on WTLS. A WAP gateway must be used as a bridge between the different protocols. Not WTLS but SSL is supported when the WAP gateway makes the request to the origin server. As the data is decrypted and again encrypted at the WAP gateway, the gateway introduces a security hole which renders WAP unsuitable for any security-sensitive services. In SWPP, with the strong security required by the banking sector, the gateway is hosted by the content provider and placed behind the content provider's firewall. In Figure 3, the merchant's and the customer's bank have their own gateways in their own network. By placing a WAP gateway in their own network, the connection between the customer and different services (including the merchant service and the bank service) is to be trusted, as the decryption will not take place until the transmission has reached the service provider's own network, and not in the mobile operator's network. To provide the highest security solution, the functionality of the WAP gateway to the origin server can be included. This is the way that is used in our implementation. This set-up obviates both the WAP Gap and the need for SSL between the gateway and the HTTP server. Since both the merchant's and the customer's bank provide WAP services to the customer, they have their own gateway in their own network.

With these two gateways in SWPP, the customer agent needs a mechanism to navigate between them.

In Figure 4 , there are three key components that provide total navigation for the Customer Agent, including: Navigation Document, Master WAPgateway and Subordinate WAP gateway. In SWPP, we focus mainly on the gateway between the customer and the customer's bank. The bank gateway acts as both master gateway and subordinate gateway. A navigation document is unnecessary.

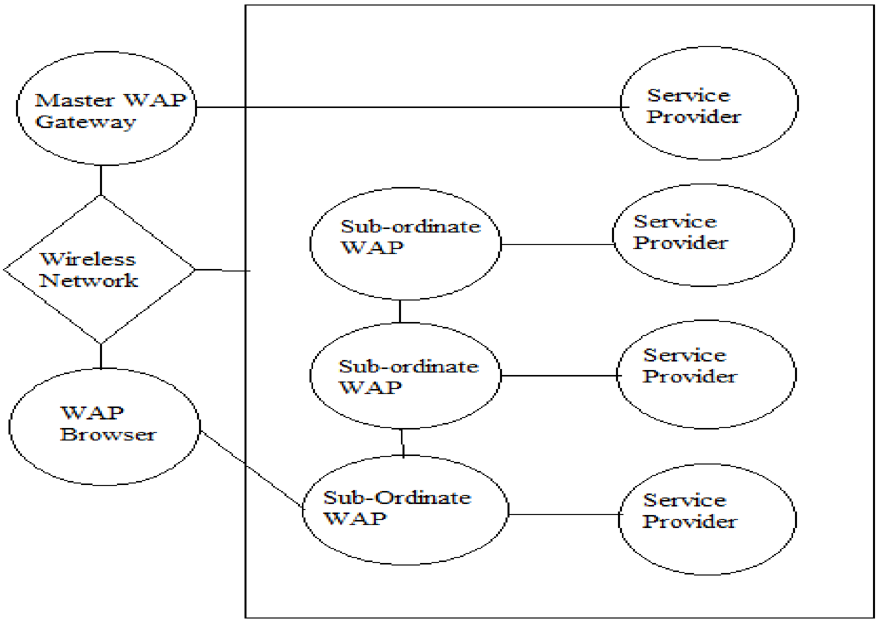


Figure 4: Transport Layer in an end-to-end Security Architecture

Customer Authorization

Customer Authorization in SWPP is implemented using the WMLScript signText function. The following transpires in the signText function:

□ The customer's bank provides a text to be signed and an indication of the required user certificate (as a list of accepted certificate issuers) or key (as a key identifier)

□ The customer confirms the text and certificate being used

□ The customer is prompted to input a signature PIN

□ WIM executes a sign function on the hashed text using a signature key

A. Comparison to SET

This section provides a comparison of the SET and WPP protocols based on selected criteria.

Transaction Flow

In terms of the payment transaction flow, there are two key differences. First, a reduction in the number of messages exchanged between the participating agents of the WPP is expected to reduce the overall processing time of wireless payment transactions and subsequently reduce communication costs for mobile users. In Addition, the data being transmitted will become less weak to various attacks. The second element is the direction of the transaction flow. With WPP, transactions are carried out between the CA and the Customer's Bank (without an intermediary – MA). By altering the traditional flow of transactions, we have addressed consumers' concern of transmitting private information via the merchant.

Security

As the SET protocol was designed to preserve the traditional flow of payment data, an end-to-end security mechanism was required. As a consequence, the provision of security (encryption, data integrity, authentication and non-repudiation) was fulfilled at the application layer.

The use of two certificates per participant (one for encryption/decryption and one for signature) and dual signature for linking and protecting order and payment information (e.g. account number) fulfilled the security requirements.

The biggest problem is the need for clients to acquire/purchase two certificates should they opt to initiate a SET-based transaction. WPP, on the other hand, does not route payment transaction data via the MA. As a result, the implementation of security becomes less onerous. A dual signature is not required since customer's payment instructions are no longer sent to the merchant and thus cannot be altered by the merchant. In fact, in WPP it is the banking information of the merchant (previously encrypted by the bank) which is sent to the CA and then forwarded to the Customer's Bank. In addition, as the WTLS provides most of the security services required, only one certificate is required by the participating entities to sign key data (e.g. purchase request from customer and purchase invoice from merchant) at the application layer. Although customers will be required to obtain a certificate, as with SET, we expect that certificates will be made available (free of charge) in the near future. Finally, the use of SCs for storing encrypted banking information and Personal Identification Number (PIN) permits us to incorporate other types of payments including debit card payments. Since PINs are strictly used for authorizing access to the SCs and are not transmitted over the network, the security of PINs are preserved. If, on the other hand, the encrypted PINs are stored in workstations and transmitted via the Internet, as it could be with the SET protocol, the security of the PINs is questionable. This is one of the main reasons why debit card payments have not been made available via the Internet.

Performance

The issue of performance is equally important to mobile users since improved performance (lower processing time) results in reduced communication costs. The performance of a protocol is dictated by the following key factors: transaction flow, bandwidth requirements (number and size of messages) and computational requirements.

In terms of the transaction flow, it is already clear that WPP is expected to provide a faster processing time per transaction than SET due to the reduced number of messages in the protocol. As far as bandwidth requirements are concerned, the exchange of multiple certificates and data in the SET protocol requires considerably more bandwidth than WPP. By keeping the size of messages to a bare minimum, we were able to lower the requirements for precious bandwidth. Finally, the computational requirement of the protocol is clearly a contributing factor in the area of performance. In terms of SET, the need for dual signature and multiple layers of encryption at the application layer has resulted in a protocol too demanding for mobile computing [12]. WPP, on the other hand, is optimized to operate more efficiently over wireless networks. This includes limited number of security mechanisms (e.g. digital signature) implemented at the application layer as well as the use of SCs to enhance the processing capabilities of the mobile devices.

B. WPP and SWPP

A comparison between WPP and SWPP protocols based on selected criteria is given below:

	WPP	SWPP
Transaction Flow	Customer-Bank-Merchant	
Security Mechanisms	Not actually implemented	Implemented at both the application layer and WTLS class 2/3
Number of certificates Used	None	One
Server Authenticati On	None	Provided by WTLS class 2
Customer Authenticati On	None	Using Plug-in Authentication Module
Data Integrity	Implemented	Message from the merchant is signed using its private key. Message from the customer to the bank gateway is signed based on the definition of WTLS Class 2.
Customer Authorizatio N	None	Uses Access Control provided by Nokia Activ Server and signText function defined in WMLScrypt.
Number of certificates Used	None	Two. One for signature, one for encryption.
User of Gateway	Nokia Server is used to Simulate merchant site	Nokia Activ Server is used as a gateway between customer and merchant. It also acts as a gateway and bank server to the customer.
End to end Security	None	By putting gateway function and bank server together on Nokia Activ Server
User of WIM Cards	None	Yes
Use of Smart Cards	Yes	

CONCLUSION

The WPP represents a non-proprietary solution designed to provide the following benefits: enhanced security, increased performance and support for debit card payments and perhaps other types of payments as well. Enhanced security is achieved by leveraging on the security services of the WTLS layer of the WAP protocol stack and by sending customer's private data directly to the bank. This routing strategy was intended to address customer's greatest concern: transmission of confidential information to the merchant, especially if merchants are using a peer -to-peer protocol such as SSL.

Given that WPP would be implemented over a wireless network marked by limited bandwidth and high latency, every effort was made to reduce the size and number of messages exchanged between all agents participating in the protocol. In addition, the number of cryptographic functions to be carried out on the wireless devices was also kept to a minimum in order to accommodate the processor and battery-constrained devices. Unlike POS purchases and ATM machines which use private networks to support debit -card transactions (transmit the account and PIN numbers), this type of transaction has not been made available over the Internet for a good reason. Storing encrypted PIN numbers on workstations and transmitting them over an open network poses serious security concerns. It is clear that an alternate strategy is required if WPP is to support debit-card transactions as well. By using the PIN number to authorize access to the Smart Card storing confidential banking information, the need to transmit PIN number was eliminated. In fact, the same PIN number will now be required to authorize both credit and debit-card transactions. While a brief comparison to the SET protocol was made to illustrate these benefits, readers are encouraged to consult for additional details. Although results of the implementation suggest the need for greater intelligence on the part of mobile devices (than supported by WAP), we are confident that it is only a matter of time before this issue is addressed.

In the meantime, the use of mobile software agents to further alleviate the resource requirements of mobile devices will be analyzed. Although the use of mobile agents, which carry out their tasks within the operating environment (place) of the merchant, remains controversial with respect to security, the transaction flow of the WPP may minimize the security threats surrounding mobile agents.

REFERENCES

[1] Brokat, Business goes Mobile, Mobile Business Applications, Version 1.2 Business White paper, 1999, Available at www.brokat.com

[2] Ghosh, Anup K. E-Commerce Security Weak Links, Best Defenses, 1998, pp. 137-146

[3] Anderson, Milton M. The Electronic Check Architecture, Financial Services Technology Consortium, Version 1.0.2, September 29, 1998.

[4] VISA & Mastercard, SET Secure Electronic Transaction Specification, 1997.

[5] Romao, Artur and Mira da Silva, Miguel. An Agent-Based Secure Internet Payment System for Mobile Computing. Proceeding of International IFIP/GI Working Conference. Germany, 1998, pp. 80-93.

[6] Website of Bank of Nova Scotia, www.scotiabank.com

[7] WapForum, Wireless Application Protocol (WAP) White Paper, October 1999, Available at www.wapforum.com

[8] J. Hall, S. Killbank, M. Barbeau, E. Kranakis, WPP: A Secure Payment Protocol for Supporting Credit- and Debit-Card Transactions over Wireless Networks. In proceedings of ICT 2001 (International Conference on Telecommunications), Romania, Bucharest, June 4-7, 2001

[9] Hall, Jeyanthi and Kilbank, Susan. WPP: A Wireless Payment Protocol, 2001, Available at www.scs.carleton.ca

[10] Mobile electronic Transactions. (2001). "MeT Account-Based Payment," http://www.mobiletransaction.org/pdf/MeT Account- Based-Payment-20010221.pdf

[11] A. Levi and Ç. K. Koç, "CONSEPP: CONvenient and Secure Electronic Payment Protocol Based on X9.59, " presented at The 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, pp. 286-295, Dec. 10-14, 2001.

[12] Daswani, Neil and Doneh, Dan, Experimenting with Electronic commerce on the PalmPilot, Financial Cryptography : 3rd International Conference, 1999, pp. 1-16