The Security of Information in Financial Transactions via Mobile: Algorithms

ASSIS. PROF. DR. ELHAM FARIBORZI†, ENG. HODA ANVARI KAZEMABAD‡

† Faculty member, Department of Educational Studies, Islamic Azad University-Mashhad Branch, Mashhad, Iran
‡ Islamic Azad University-Mashhad Branch, Mashhad, Iran

E-mail: †elhamfariborzi@gmail.com, ‡hodaanvari@yahoo.com

*Corresponding author

ABSTRACT

Today, mobile commerce or m-commerce has been considered by many companies, business, and organizations. In mobile commerce, information security of financial transactions is very important. It is due to account information which exchanged including account number, password, credit accounts, etc. and the disclosure of this information will cause a lot of financial and moral losses. For this reason, it should be used algorithms for them to make and increase secure transactions. Among these algorithms, WAP, J2ME, Toolkit SIM applications are identified and described in this article based on a systematic review. In addition, there are some recommendations regarding to suit different situations to implement a particular algorithm for this issue. More results are subsequently explained in this paper.

Keywords: Algorithms, security, mobile, mobile device.

1 INTRODUCTION

In today's world, m-commerce has been discussed as one of the most important issues in business organizations and companies; Mobile Commerce is any transaction in which a financial exchange done via mobile communications networks [1]. According to this definition, m-commerce represents a subset of all e-commerce including both business-to-consumer and business-to-business. M-Commerce uses the internet for purchasing goods and services as well as sending and receiving messages using hand-held wireless devices. M-commerce can be defined such as: any electronic transaction or information interaction conducted using a mobile device and mobile networks which leads to transfer real or perceived value in exchange for information, services, or goods [2]. M-commerce offers consumers convenience and flexibility of mobile services anytime and anyplace; mobile commerce is known as mobile e-commerce or wireless e-commerce [1]. Some people conceive m-commerce as an extension of e-commerce to mobile phones; some people think it is another new channel after the Internet. In addition, mobile payment is defined as the process of two parties exchanging financial value using a mobile device in return for goods or services [2, 3].

Computers connect to a wired or wireless network. Wireless communication is more difficult and dangerous than wired communication for many reasons including signal routes and interacts with its surroundings, sounds and possible illegal wiretapping due to the use of radio waves. These problems lead to less bandwidth, higher error rate and repeat fault (without user intervention), so the wireless link quality is lower than a wired connection. Hence, many companies and organizations are not willing to use mobile commerce [1, 2, 3, 4, 5].

Another issue in Mobile Commerce is personalization; on the one hand, it is a powerful feature for business organizations and companies in order to identify the specific needs of the users, and on the other hand, provides good control of
personal mobile devices. Any person has different reasons to want to keep the information confidential; perhaps the most important reason is terrorism and its various attacks in different parts of life and obtain the information to sabotage. One of the potential threat in today's world is terrorism who leaves negative and destructive effects in various sectors of life, including transport services, information, energy, chemical and nuclear weapons, etc., it is fitting that we harness the nation's exceptional scientific and technological capabilities to counter terrorist threats because of terrorists seek to exploit these vulnerabilities [1, 2, 6].

In this paper, the researchers' aim is to identify and describe algorithms including WEB, J2ME, SIM Application Toolkit, so as to suit different requirements and features, chose the best algorithms for secure transactions by mobile phone.

This study was a systematic review on this issue. A systematic review is literature review focused on a single question that tries to identify, appraise, select and synthesize all high quality research evidence relevant to that question [7].

2 SOLUTIONS TO PREVENT SECURITY PROBLEMS IN MOBILE NETWORKS

M-commerce uses mobile devices; the mobile device is a wireless communication device, including cell phones, handheld computer, wireless tablets and mobile computers. Security problems in networks such as wireless networks include hears, manipulating messages (change), generate fake messages and timeout (bar association); so four properties have always been essential for secure transaction, including [2, 3, 5]: Authentication is concerned about verifying the identities of parties in a communication and confirming that they are who they claim to be. Confidentiality is about ensuring that only the sender and intended recipient of a message can read its content and information will be kept away of access of unauthorized and alien users. Integrity is concerned about ensuring the content of the messages and transactions not being altered, whether accidentally or maliciously. Non-repudiation is about providing mechanisms to guarantee that a party involved in a transaction cannot falsely claim later that she did not participate in that transaction [1, 2].

3 ALGORITHMS FOR Secure Transactions IN MOBILE NETWORKS

3.1 Public Key Infrastructure (PKI)

Any person requires authentication of organization to conduct financial transactions. Authentication of individuals and organizations can be with exchange their public keys; a way to exchange public keys is using a reputable organization that is agreed by all. Individuals and organizations register our public key for communication in the organization, and for communication receive the other party's public key from this organization, and to this end, it should be always online, and if it is in trouble problems (for instance log-out), all communication is impossible or unsafe; another problem is that it will become a bottleneck and being exposed to malicious attacks; as a result, PKI is proposed for cellular phones using public key certificates in 1999. PKI is an issuer of digital certificates or in other words, is confirming the registration, which provides a secure mobile commerce with solutions. The theory of PKI is presented as follows [1, 2, 3]:

This organization known as CA stipulates the name of key holder with his public key, then the digital certificate and signature block CA (String Hash certificate with private key CA encrypted as below Figure) are sent to the applicant, therefore, it does not need to be always online.

![Fig. 1. An example of a certificate and signed Hash string [5].](image)
3.2 Public Key Cryptography

Public key infrastructures are based on public key cryptography which uses two keys: a private key that is kept a secret, and a public key that can be divulged publicly. An interesting property of this pair of keys is that to decrypt messages encrypted with one, the other is needed. The keys are said to be asymmetric. The most popular algorithm for public key cryptography is RSA. Elliptic curve cryptography algorithms are starting to gain acceptance into mobile devices. They rely on different mathematical properties that allow for shorter keys which enable faster computations, lower power consumption, less memory and bandwidth requirements and hence, are quite appealing for mobile devices.

3.3 Digital signature

Digital signatures can ensure the authenticity of transaction parties, integrity, and non-repudiation of transmissions. A digital signature is created when the document to be transmitted is enciphered using a private key. The process of enciphering the document using the private key authenticates the document, since the document could only have been enciphered using the private key of the owner. The recipients can verify the signature by deciphering using the public key. In real world, documents are not completely encrypted to save time. In such cases one-way hash functions are used. A hash uses a one-way mathematical function to transform data into fixed length digest called a hash which is subsequently enciphered. The verification of the signature involves reproducing the hash generated from the received message and comparing it with the deciphered original hash.

3.4 Digital Certificate

Digital signatures are not sufficient means for automatic verification since even if a signature can be verified, there is no guarantee of the fact that the person who made the signature is who he claims to be. Public key certificates are a powerful means of establishing trust in public key cryptography. A certificate is someone’s public key, signed and packaged for use in a public key infrastructure. In general, a certificate contains the following three pieces of information: 1) the name of the subject for whom the certificate has been issued, 2) the public key associated with the subject, and 3) a digital signature signed by the issuer of the certificate. The digital signature will verify the information of the certificate, and if the verification succeeds, it is assured that the public key in the certificate does in fact belong to the entity the certificate claim. Being only one organization that certifies persons’ public key is not possible for the following reasons: All people disagree with one organization, some conceive that it is worthy of government and the other vice versa; meaning: in this context, there is no government interference.

Assuming the existence of such an organization, if the organization is in trouble, all communications disrupted and the organization has become a bottleneck and many attacks will expose the organization to the public keys [3, 6, 8].

![Hierarchical structure of PKI](image)

Fig. 2. (a) Hierarchical structure of PKI. (B) A chain of certificates [5].

Therefore, it was decided that be several organizations instead of one organization in hierarchical form which become high and low in practice. Based on the above figure, PKI is composed of several components, including users, CA (The Certification Authority), certificates, etc.

Root is the highest level and confirms RA or the level 2 certification centers which covers a specific geographical area such as a city or country. Level 2 Certification Centers warrant and confirm CA identity centers in order to issue X.509 digital certificates established for organization and individuals; when root confirms its subset RA, issued an X.509 certificate for the center in which is inserted and has been signed, the public key and the identity of the center. By the same method when RA confirms new CA center, this center be able to issue digital certificates for individuals and organizations that contain their public keys.
There are many "roots" and one of them has many CAs and RAs for own, by default, the public key is included in more than one hundred roots in new browsers that will prevent focus on a global unit. This set of public keys is known as "moments of confidence". However, users should take rational decisions and review moments of trust in your browser and then confirm them. Each user can personally maintain his certificate; this is a safe way to store certificates because there is no way for other users to be able to manipulate his signed certificate without detect it, but this method is not very convenient. Another way is to use the DNS server as the Certificate List [1, 2, 3, 5, 9].

The following protocols and technologies make easy transferring data payment from/to mobile devices in mobile payment transactions. Currently, WAP and GSM are two well-known technologies in wireless world.

### 3.5 Wireless application protocol (WAP)

The functional areas related to security in WAP considered include Wireless Transport Layer Security (WTLS), Wireless Identity Module, WAP Public Key Infrastructure, WML Script sign-Text, and End-to-End Transport Layer Security. The WTLS (Wireless Transport Layer Security) protocol is a PKI-enabled security protocol, designed for securing communications and transactions over wireless networks. WTLS protocol like SSL is one way to secure WAP connection; it is used with the WAP transport protocols to provide security on the transport layer between the WAP client in the mobile device and the WAP server in the WAP gateway.

The security services that are provided by the WTLS protocol are authentication, confidentiality and integrity. WTLS provides functionality similar to the Internet transport layer security systems TLS (Transport Layer Security) and SSL (Secure Sockets Layer), and has been largely based on TLS, but has been optimized for narrow-band communications and incorporates datagram support. The main difference between WTLS and SSL is that WTLS has been completed to ensure be suitable in an environment with wide bandwidth, memory and processing constraints. WTLS is implemented in most major micro-browsers and WAP servers. WAP 1.x series use the WTLS protocol to protect messages in the wireless network part and some way into the wired network that is between the wireless device and WAP Gateway. The WAP gateway transforms the WAP 1.x stack to/from the wired TCP/IP stack, relays the data between the wireless and wired network, and communicates with the Web Server that the mobile device is accessing. Wireless Identity Module (WIM) is used in performing functions related to WTLS and application level security by storing and processing information like secret keys and certificates needed for authentication and non-repudiation. To enable tamper resistance, WIM is implemented as software on a microprocessor-based smart card. Sign-Text function allows a wireless user to sign a transaction digitally in a way that can be verified by a content server. This provides end-to-end authentication of the client, together with integrity and non-repudiation of the transaction. WPKI is an optimized extension of a traditional PKI for the wireless environment. WPKI requires the same components as a traditional PKI: an End-Entity Application (EE), a Registration Authority (RA), a Certification Authority (CA) and a PKI Repository. In WPKI, the end entities (EE) and the registration authority (RA) are implemented differently and a new entity, referred to as the PKI Portal, is introduced. The EE in WPKI runs on the WAP device. It is responsible for the same functions as the EE in a traditional PKI. The PKI Portal like a WAP gateway can be a dual-networked system. It functions as the RA and is responsible for translating requests of WAP clients to the RA and interacts with CA over wired network. The RA validates the EE’s credentials to approve or reject the request to receive a digital certificate.

The WAP PKI defines three levels of transport layer session security, WTLS classes 1, 2 and 3, and a sign-Text (WML-Script functionality for digital signatures). WTLS Class 1 provides encryption; WTLS Class 2 provides encryption and gateway authentication; WTLS Class 3 provides encryption and two-way authentication. The WML-Script sign-Text is a functionality that the user interface can utilize for creating digital signatures. The sign-Text uses the underlying security element WIM (Wireless Identity Module) that actually performs the cryptographic procedures and stores the secret keys securely. Basically, WPKI is concerned with the requirements on a PKI imposed by WTLS and the sign Text function.

The merchant server authenticates itself by sending its digital certificate (SSL certificate) to the WAP gateway which will have the root certificate of the CA that issued the merchant servers digital certificate. Similarly the WAP gateway will authenticate itself to the mobile client by passing its digital certificate to the mobile client. The mobile client in turn will have the root certificate of the CA that issues the gateway’s certificate. For
security the mobile client should also be able to check whether the WAP gateway certificate has been revoked. For mobile client authentication, two methods can be applied: I) using WTLS class 3 between the client and the gateway, II) using WML-Script digital signatures between the mobile client and the merchant’s server. These methods require a private key and a digital certificate to be stored in a WIM. For client authentication, the client should have an URL pointer to the location of the complete SSL certificate which is too large to store in a mobile phone. All the members involved in a mobile payment system can access the full version of the SSL certificates [2, 3, 4, 5, 9].

3.6 Security WAP 2.0

For the most part, developers’ WAP use standard protocols, and widely in all layers in WAP 2.0, due to the non-standard WAP 1.0 protocol stack. Since WAP is based on IP, at the network layer, is supported entirely IP-sec and the transport layer protects of a TCP connection using TLS. In the upper layer, supports HTTP authentication method. There is a library system at the application layer for encryption, is placed adequate facilities for accurate control and undeniable message to the developers of WAP. Since WAP 2.0 is based on recognized standards, there is a great chance that its security services be better and safer than 802.11 and Bluetooth, especially for authentication services, survey data, being undeniable and confidentiality of messages [2, 4, 5].

3.7 Application Toolkit (SAT)

The GSM (Global System for Mobile Communications) Subscriber Identity Module (SIM) which stores personal subscriber data can be implemented in the form of a smart card called SIM card. SIM toolkit is a specification of SIM and terminal functionalities that allow the SIM to take control of the mobile terminal for certain functions. SIM application toolkit (SAT) is used to create Short Message Service (SMS) based mobile payment applications. In SIM Application toolkit based systems, the communication between the mobile client and the payment server occur using SMS. The SMS is used to initiate and authorize payments. The user is identified and authenticated by GSM authentication service and hence, the GSM mobile network operator acts as an intermediary between the mobile client, the payment server and the merchant.

Authentication is provided by strong authentication algorithms which can be chosen by the payment provider. Data integrity is realized using message digest like SHA and MDS 5. Other than not providing support for prevention of non-repudiation, the SAT also has another flaw caused by its usage of the mobile clients PIN code. PIN codes are usually 4 digit-numbers which can be guessed and entered into stolen or lost mobile phones, and undo the security provided by encryption algorithms or large keys. Security requirements of SIM Toolkit cover the transport layer security issues, such as peer authentication, message integrity, replay detection and sequence integrity, proof of receipt, and message confidentiality. Each payment application message is divided into packets that are individually secured by protecting the payload and adding security headers.

Proof of execution is required as well to assure the sending application (e.g., a bank application) that the receiving application (e.g., the home banking application on a SIM card) has performed an action initiated by the sending application. This proof should be provided at the application layer, so no mechanism for it is defined in the GSM specifications.

Advantages and Disadvantages: SAT provides confidentiality, authentication, integrity protection and replication message (message replay protection), but it does not provide denial of service or undeniable. As a result, lack of support undeniable is a major disruptive factor to accept SAT m-commerce applications. SAT is built to support data encryption standards such as triple DES. Service provider places the encryption key before SIM is sent to the client. This will ensure that the private key never leave the immediate area [2, 5, 8].

3.8 J2ME

3.8.1 Advantages and Disadvantages

The use of this platform is a Sun product to meet the demand for information about the versatility of the Java application environment. Its main advantages are the ability to provide dynamic content and information security, in addition, is capable, powerful object oriented programming language with a large developer base. Information devices and other portable devices are integrated with audio, multimedia, connectivity and services available on a single platform. A growing and dynamic computing power on these devices will
enable developers of high-value-added services. For example, local information services allowing passengers to connect to the Internet using mobile and access to needed information, including the location of the nearest hotel, table plans and schedules. One of the applications of m-commerce is using mobile payments at the gas pump by driver. The successes of these applications require a high level of reliability and security. Mobile devices contain a digital ID; because of this, there must be a way to authenticate users and ensure system reliability. To provide secure data access is absolutely critical in a mobile network and decreases the rate of fraud in mobile payment systems.

Current practices in Platform J2ME rely on the services provided in secure smart card or similar device in order to build trust and confidence that has been done safely store keys and cryptographic operations and calculations. To complete a secure transaction requires the seller to verify that wireless subscribers, the transaction are authorized or not. After that the seller must send a receipt to the subscriber.

The use of digital signatures is the best method for user authentication. SATSA provides a service of digital notation which allows J2ME application to generate a digital signature in accordance with the CSM. User authentication is usually with the public key which is confirmed by the certificate public key. SATSA is related to certificate management functions which will give device, authority device manager from user. Using Application Interface SATSAT, system can produce request a certificate of registration which can be sent to the issuer of the certificate. Power management and user permissions, add/remove, the license it to/from the repository license.

3.8.2 Safe and reliable Service Application Program Interface for J2ME Platform

A lot of data is managed in modern wireless networks. Most of these data are included personal communication and information which should be handled in a secure encrypted form. To create this functionality, SATSAT has a common cryptographic library which provides a subset of J2SE platform encryption of API. J2SE supports basic cryptographic functions such as identification and authentication signature, encryption and decryption which allow the application J2ME provide secure data communications, data protection and management details. Digital signature generation and user authorization management rely on a security element to store sensitive data (e.g. private keys, public key certificates and other personal information). Security element does data integrity and reliability, computation and cryptographic operations to support payment protocols. This feature is designed for smart cards. Smart cards provide a secure programming environment and J2ME applications can use these services for the use of many value-added services including mobile commerce, banking, business and commercial capital (Stock trading) and game. SATSA provides a standard method to produce secure services in Java applications. It increase productivity and reduce programming (coding), debugging and maintenance costs. SATSA sets reliable and secure service available for all applications on compliant platform [2, 5, 10].

4 CONCLUSIONS

By According to advantages and disadvantages of the introduced algorithms and the research done in this field, it is concluded that what algorithms are used in mobile-Iranian banks: J2ME platform would be more appropriate for the following reasons: Performed with a mobile exchange, there are problems including hears, manipulating message, generate fake messages and interruption, and as mentioned earlier, so to avoid these problems, the following procedures are necessary: authentication, confidentiality, monitoring accuracy and unquestionable; any way would be appropriate which provide these four solutions and also be applicable in Java programs (because mobile devices generally use the Java programs) due to advances in technology and the importance of keeping information confidential.

PKI provides these four-ways using digital certificates and HASH function, the only problem is applicable on mobile phones that would be appropriate if the problem is resolved.

WAP provides these four-ways too and like PKI is difficult to apply in mobile phones, like SAT provides authentication, confidentiality and integrity of data but cannot provide safely undeniable because of using 4-digit PIN code (this feature is essential for transactions conducted by mobile); as a result, it would not be appropriate.

In total, J2ME platform use to meet the demand of information systems according to java software environment (one of the most suitable for the
chosen), as explained earlier, it provides these four-ways, and another advantage is that these services, they can constantly be updated with new or improved applications installed on a smart card.

Perhaps due to these advantages, Iran Melli-bank also use this method for own mobile bank [11]. It is recommended that other researchers do case studies about the issue to realize the weaknesses of the current system in Iran about it and to suggest the one might be better practically.

5 REFERENCES