Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 1 – 11

This paper is Available online at
www.jtaer.com

Anonymous Payment in a Kiosk Centric Model using Digital signature scheme with message recovery and Low Computational Power Devices

Jesús Téllez Isaac[1] and José Sierra Camara[2],
Antonio Izquierdo Manzanares[2] and Joaquín Torres Márquez[2]

[1] Universidad de Carabobo, Computer Science Department (Facyt)
Av. Universidad, Sector Bárbula, Valencia, Venezuela.
jtellez@uc.edu.ve
[2] Universidad Carlos III de Madrid, Computer Science Department,
Avda. de la Universidad, 30, 28911, Leganés (Madrid), Spain.
{sierra,aizquier,jtmarque}@inf.uc3m.es

Received 26 May 2006; accepted 28 July 2006

Abstract

In this paper we present an anonymous protocol for a mobile payment system based on a Kiosk Centric Case Mobile Scenario where the customer cannot communicate with the issuer due to absence of Internet access with her mobile device and the costs of implementing other mechanism of communication between both of them are high. Our protocol protects the real identity of the clients during the purchase and employs a digital signature scheme with message recovery using self-certified public keys that reduces the public space and the communication cost in comparison with the certificate-based signature schemes. Moreover, our proposed protocol requires low computational power that makes it suitable for mobile devices. As a result, our proposal illustrates how a portable device equipped with a short range link (such Bluetooth, Infrared or Wi-Fi) and low computational power should be enough to interact with a vendor machine in order to buy goods or services in a secure way.

Key words: Anonymous Protocol, Mobile Payment System, Kiosk Centric Model, Digital Signature with message recovery, Self-certifi ed public keys

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 1 – 11

This paper is Available online at
www.jtaer.com

1 Introduction

M-commerce refers to any electronic transaction or information conducted using a mobile device and mobile networks. Its popularity has increased in the last years thanks to advances in the portable devices and the rapid development of the mobile communication technologies that have allowed people to use mobile telephones or Personal Digital Assistant (PDA) to access Internet (to read email, browse web pages or purchase goods) anywhere and anytime.

Advances in the portable devices make m-commerce more profi table and promising, nevertheless there is still a widespread skepticism about buying and paying for them on-line, due to the vulnerability of sensitive information when transmitted through communication channels. Therefore, it is necessary to develop mobile payment systems capable of providing safe and trustworthy communications between the customer and on-line mobile services providers. Moreover, these payment systems should overcome the common limitations existing in mobile devices currently available, which prevent that these devices execute, in an effi cient way, operations that require a lot of computing resources. The common limitations are: 1) poor computational capabilities, 2) limited storage and 3) short battery life.

Different mobile payment systems have emerged in the last years which allow the payment of services/goods from mobile devices, but the one developed by [16] (called 3-D Secure) has become a standard due to its benefi ts regarding security and flexibility in the authentication methods. This scheme allows the authentication of the payer (customer) when she makes an on-line payment using a debit or credit card.

Despite of the flexibility that 3-D Secure provides to the issuer to choose the authentication method (password, symmetric and asymmetric signature, and biometric techniques), the relationship between payer and issuer is quite strict (although required for Visa's 3D-Secure scheme) and does not allow the use of schemes in which the communication among these parties is not possible due to: 1) the impossibility of the client to connect to Internet from the mobile device and 2) the high costs and / or inconveniences of using the infrastructure necessary to implement other mechanisms of communication between the client and the issuer (such SMS, phone call, etc).

Most of the mobile payment systems proposed up until now assume the consumer has Internet connectivity through her mobile device, so the restrictions mentioned previously do not represent an important issue. However, it is quite common that the client meets situations in which it is not possible to connect to Internet so it becomes necessary to develop mobile payment systems where the user could use her mobile device as a shopping means, even thought she may not have Internet access.

Digital Signature can be represented as a secure base in electronic payment system because it provides authentication, data integrity and non-reputation cryptography services [10]. However, the traditional digital signature schemes are based on asymmetric techniques which make the signature computation very expensive and not suitable for mobile devices. Moreover, these schemes suffer from the well-know authentication problem[1] which requires the usage of certifi cate to avoid it. The public-key certifi cate must be verifi ed by a Certifi cate Authority (CA), and that verifi cation causes an additional information exchange during a transaction.

According to our operational model, the above schemes are not suitable because clients interact only with a vendor during a purchase and communication with other party (like CA to verify a certifi cate) is not possible. Therefore, usage of a non-traditional digital signature scheme is required in order to satisfy our requirements. Digital signature with message recovery using self-certifi ed public keys [3],[15] provides an authenticated encryption scheme that integrates the mechanisms of signature and encryption, which enable only the specifi ed receiver to verify and recover the original message. The authentication of the public key can implicitly be accomplished with the signature verifi cation.

Contributions: In this paper, we present an anonymous protocol (that supports both credit-card and debit-card transactions) for a mobile payment system based on a Kiosk Centric Model (proposed by [4]) which overcomes the limitations mentioned before and is suitable for mobiles devices with low computational power. Our protocol protects the real identity of the clients during the purchase and employs a digital signature scheme with message recovery using self-certifi ed public keys that reduces the public space and the communication cost in comparison with the certifi cate-based signature schemes [17]. As a result, our proposal represents an alternative to other mobile payment systems with restrictions regarding a mandatory connection between the client and the issuer, like Visa's 3D Secure.

[1] An imposter may impersonate any innocent user with a valid cryptographic but incorrect public key (because it does not belong to the innocent user).

Outline of this paper: We begin by presenting the motivation for this work (section 2), followed by the related work that include a description of some known results associated to our research. We then present a brief review of some preliminaries (section 4). More precisely, we give a comparison between symmetric and asymmetric cryptography for mobile payment transactions and an overview of digital signature and self-certifi ed public key. Following this, we present our approach which includes a complete list of notations used in our scheme, the operational model, the initial assumptions and the proposed protocol. In section 6, a security analysis of the proposed protocol is presented. We end this paper with the conclusions in section 7.

2 Motivation

In this research, we can distinguish the following objectives: a) eliminate the restriction of those mobile payment systems (including Visa's 3-D Secure) about the direct communication between client and issuer for authentication purposes and b) provide anonymity of data origin to prevent the merchant from associating the client with the messages sent from her. This anonymity implies the protection of relevant information by third parties but not unrestrained anonymity [1].

Our fi rst objective is greatly inspired by the Kiosk Centric Case mobile Scenario proposed by [4]. This scenario is very representative of mobile application frameworks where the client device interacts directly with the kiosk, which in turn connects to the infrastructure. Note that the client's device never communicates with the infrastructure in a direct way but has a feasible connection with the vendor (using a short range link such bluetooth, infrared or wi-fi).

In order to solve the problem of buy and payment of goods/services in the aforementioned scenario, in section 5, we construct a protocol that allows clients to send from their mobile device a message to the issuer through the vendor (who will not be able to decrypt this message). The proposed protocol (divided in 2 sub–protocols) employs the authentication encryption scheme proposed by [17] that allows only specifi ed receivers to verify and recover the message, so any other receiver will not be able to access the information.

According to our second objective, we make sure not to reveal the real identity of the client to a merchant during the purchase process. In order to achieve this goal, a nickname instead of client's real identity is used when she communicates with the merchant. While a client registers to the issuer, several nicknames are assigned to the client and those nicknames are known only to the client and the issuer. Since the merchant does not know the mapping the nickname and the true identity of a client, the client's privacy is protected [8].

3 Related Work

The widespread of m-commerce in recent years has created new security and privacy challenges because of new technology, novel applications, and increased pervasiveness [4]. Several studies have been conducted to improve the security of mobile payment systems. Meanwhile, efforts have also been dedicated to unify concepts and scenarios into frameworks that will be useful to develop new electronic payment systems and to analyze security issues.

Research conducted by [4] is one of those studies that unifi es many proposed m–commerce usages into a single framework. This research intended to revise the possible range of mobility scenarios, identifying the security issues for each connectivity scenario. As a result, fi ve scenarios were identifi ed and analyzed: Disconnected Interaction, Server Centric Case, Client Centric Case, Full Connectivity and Kiosk Centric Case. The latest has been considered as the starting point in the design of our proposal.

The Full Connectivity scenario (where all the entities are directly connected to one another) has been widely used in most of the mobile payment systems proposed up until now [11],[7],[16] because it allows protocol's designers to simplify the protocols and obtain stronger security guarantees than similar applications in the others models.

Most of the protocols proposed in recent years for the Full Connectivity scenario are based on public-key infrastructure (PKI) [2],[7],[10] whereas the remaining employ symmetric-key operations which is more suitable for wireless networks [9]. Unfortunately, usage of those protocols within the Kiosk Centric Case mobile scenario is not possible, as it restricts the communication which allows only interaction between the client and the merchant. However, some protocols could be reformulated to overcome this restriction, achieving the same security and performance but in a different scenario.

For example, Téllez *et al*. [14] reformulate the mobile payment protocol proposed by [9] to satisfy the requirements of their proposal (based on Kiosk Centric Model).

Many signature schemes with message recovery have been proposed in recent years [3],[15],[17]. These schemes allow a signer's public key to be simultaneously authenticated in verifying the signature. As the public keys does not need to be included in a certifi cate to be authenticated by verifi ers (as happens in protocols based on public-key infrastructure), communication with a Certifi cate Authority during a transaction to verify the validity of a certifi cate is not necessary. Therefore, digital signature schemes with message recovery are suitable for mobile payment systems based on a kiosk centric model like the one being suggested in this work.

In order to provide limited but practical anonymity by using limited disclosure of information, some proposals have been suggested in the past [1],[8]. While the cryptography techniques and operational models used in those works are different from ours, we follow the approach of using nicknames usage instead of the real identity, implemented in [8] to prevent a merchant from knowing the customer's identity.

As the payment software (also called wallet software, and that from now on we will assume that is programmed using the Java language due to the multiplatform capabilities of this language) must be sent to the customer by the issuer through the vendor, it becomes necessary the usage of techniques to protect the software against reverse engineering and/or software tampering. To achieve this, we employ the three techniques for obfuscation of program design proposed by [13]: 1) The *class coalescing obfuscation* replaces several classes with a single class, 2) In the *class splitting obfuscation*, a single class is replaced with multiple classes, each responsible for a part of the functionality of the original class, and 3) The *type hiding obfuscation* uses the mechanism of interfaces in java to obscure the type of objects manipulated by the program.

The experimental results (applying the techniques mentioned before to a medium-size java program) show that the run-time overhead, in the worst of possible scenario (class splitting obfuscation), is less than 10% of the total running time of the program.

4 Background

In this section, preliminaries necessary for the remainder of this paper will be introduced.

4.1 Comparison of Symmetric and Asymmetric Cryptography for Mobile Payment Transactions

Symmetric and asymmetric cryptography have been widely used for secure communications among engaging parties. In Symmetric cryptography, a secret is shared between two parties (called sender and receiver) that want to communicate safely without revealing details of the message. This technique provides message confi dentiality, message integrity and party authentication.

On the other hand, asymmetric cryptography employs a pair of cryptographic keys (public/private key) to allow users to communicate securely without having previous access to a shared secret key. This technique provides all the security properties that the symmetric cryptography does (confi dentiality, message integrity and party authentication),and also provides non-repudiation, which symmetric cryptographic could not provide and is very important for fi nancial transactions that are relevant to fund transfer and good ordering. Normally, it can be achieved by using digital signatures but in symmetric-key based protocols, there is no possibility to prove the originator of an encrypted message because the secret key is shared between two parties [9].

Symmetric-key operations are more suitable for wireless networks than asymmetric ones due to the time required to be processed and their lower computational requirements. However, key management is complex since shared secret key must be agreed upon by both parties and any participant has to maintain n number of secret keys, one for each party she is communicating with. Moreover, authenticity of origin or receipt cannot be proved because the secret key is shared.

4.2 Digital Signature and Self-certified public key

Public-key cryptography, introduced in 1976 by Diffi e-Hellman to solve the problem of key management, is a class of cryptography which allows users to communicate securely without having prior access to a shared secret key. In asymmetric cryptosystems, each user has two keys: the private key that is kept secret by the user and could be used to produce a signature for a message and the public key which is made public to all users in a public directory maintained by a system authority (SA) [17]. These systems suffer from well-known authentication problems, being the most important one that an imposter may impersonate any innocent user with a valid cryptographic but incorrect public key (because it does not belong to the innocent user). To deal with the problem, the usage of certifi ed for every public key is applied but this approach puts a high burden on users since they should connect themselves to the SA in order to verify the certifi cate before using the corresponding public key [3].

In 1984, an ID-based public key cryptosystem was proposed by [12], where the public key of a user is computed from her identity(e.g. an email address, and IP address or a complete name). Unfortunately, this approach relies too much on system authority because the user's private key is not chosen by the user, but the SA. To deal with both the problem of verifi cation of public keys without the usage of certifi cates and the drawbacks on the identity-based cryptography, the notion of self-certifi ed public keys cryptosystem was fi rst introduced by [5] where each user chooses her private key, and the user's public key is derived from the signature of the user's private key (signed by the system authority using the system's secret key) and the user's identity. The authentication of the public key can implicitly be accomplished with the signature verifi cation.

5 Our Approach

5.1 Parties and Notations

All the entities involved in our protocol are called parties and communicate through wireless and wired network.

The symbols C, M, PG, I, A are used to denote the names of the parties Client, Merchant, Payment Gateway, Issuer and Acquirer respectively. The following symbols are used to represent other messages and protocols:

- ID_P : the identity of party P that contains the contact information of P.
- NID_C : Client's nickname, temporary identity.
- K_P : party's K public key.
- K_S : party's K private key.
- $E_{P-P'}(X)$: message X signed and encrypted by the user ID_P to a specifi ed receiver $ID_{P'}$.
- TID: Identity of transaction that includes time and date of the transaction.
- OI: Order information (OI = $\{$TID, OD, h(OD, Price)$\}$) where OD and Price are order descriptions and its amount.
- TC: The type of card used in the purchase process (TC=Credit, Debit).
- Stt: The status of transaction (Stt = $\{$Accepted, Rejected$\}$).
- TIDReq : The request fot TID.
- MIDReq : The resquest for ID_M.
- XMReq : The request for x_M.
- h(M) : the one-way hash function of the message M.

5.2 Operational Model

Generally, operational models for m-commerce found in literature involve transaction between two or more entities. Our operational model is composed of fi ve entities:

1. *Client*: a user who wants to buy goods or services from the merchant. Particulary, in our proposal, the user has a mobile device with the following features: a) low computational power (e.g mobile phone, PDA, etc.), b) equipped with a built-in display, an input method and short range link (such Infrared, Wi-Fi or Bluetooth), c) capability to execute a java program, and d) not able to access Internet.
2. *Merchant*: a computational entity that has products or services to offer/sell to the client and with which the user participates in a transaction. This entity could be a normal web server or an intelligent vending machine which the user can connect to using a short range link. Moreover, this entity connects with the Payment Gateway through a secure wired channel allowing the client to communicate with the issuer using this connection. A formal defi nition of the merchant may be found in [4].
3. *Acquirer*: is the merchant's fi nancial institution. It verifi es the validity of the deposited payment instrument and manages the merchant's account including fund transfer.
4. *Issuer*: is the client's fi nancial institution. It provides electronic payment instruments to the client to use in a payment and manage the client's account including fund transfer.
5. *Payment Gateway*: an additional entity that acts as a medium between acquirer/issuer at banking private network side and client/merchant at the Internet side for clearing purpose [9].

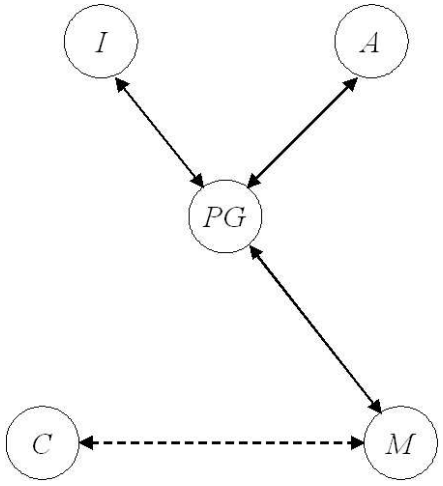

Figure 1: Operational Model.

In fi gure 1, we specify the links among the fi ve entities of our scheme. Note that there is no direct connection involving the client and the issuer. Moreover, the connection between the customer and the vendor (denoted as the dotted arrow) is set up through a wireless channel.

On the other hand, interaction among the vendor and the payment gateway (depicted as solid arrow in the scheme) should be reliable and secure against passive and active attacks. Therefore, the connection is supposed to be established through a secure wired channel by using the well-know security protocol like SSL/TLS [6]. Note that the issuer, acquirer and payment gateway operates under the banking private network, so the security of the messages exchanged among them is out of the scope of this paper.

5.3 Initial Assumptions

The initial assumptions for our proposed protocol can be stated as follows:

1. Client registers herself to an issuer before making payments. The registration can be done either personally at the issuer's premises or via the issuer's website.
2. The Client shares her credit- and/or debit-card information (CDCI) with her issuer (who will not reveal it to any merchant). q, p' and q' secret and publishes N, g and a collision-resistant hash function $h(\cdot)$ to all users
3. The trusted system authority (SA) is responsible for generation system parameters in the system initialization phase (by the procedure described in [17][15]).
4. Every party of the system P_i (whose identity is ID_{P_i}) choose a number K_{S_i} as her secret key and computes x_i = $g^{K_{S_i}}$ mod N. Then, P_i sends (x_i, ID_{P_i}) to SA. After receiving (x_i, ID_{P_i}), the trusted system authority computes and publishes the public key of P_i as K_{P_i}=$(x_i - ID_{P_i})^{h^{-1}(ID_{P_i})}$ mod N [17]. As the client uses a nickname instead the real identity to protect her privacy, one K_{P_i} must be generated and published for every nickname assigned to the client.
5. When a client registers to a issuer, several nicknames are assigned to the client and those nicknames are known only by the client and the issuer [8]. Furthermore, with the assistance of issuer, the client sends her nicknames and x_C to SA and receives all system parameters from the system authority.
6. The client holds C_S, ID_I, x_I and system parameters in her mobile device.
7. The Price and description of the goods and services have been decided by client and merchant.

5.4 Signature with Message Recovery Techniques

In order to a sender P_i (with identity ID_{P_i}) sign and encrypt a message W to a specifi ed receiver P_j (with identity ID_{P_j}), we follow the generation procedure of signature proposed by [17]. First, P_i chooses a random number y and computes r_1, r_2 and s. Afterwards, P_i sends the triple (r_1,r_2,s) as the signature of message W (from now on, $E_{P_i-P_j}$) to the verifi er P_j. After receiving (r_1,r_2,s), the verifi er P_j recovers message W and verifi es that the signature is valid using the same procedure described in [17].

5.5 Detailed Protocols

Our protocol consists of two sub–protocols. In the *Registration Protocol*, a client requests the values ID_M and x_M from the merchant. Then, if the client does not have the wallet software, M sends a request for the software to the issuer, and it will be delivered to the client through the merchant. After the client receives x_M and the wallet software is available in client's mobile device, the client can start the *Payment Protocol*. The main functions of both protocols are shown as follow:

Merchant Registration Protocol

C $\rightarrow$ **M:** $\{NID_C, n, MIDReq, XMReq\}_w$
M $\rightarrow$ **C:** $\{ID_M, x_M, h(n, x_M)\}_w$
C $\rightarrow$ **M:** $h(ID_M, n, x_M)$

Due the absence of connection between the client and the trusted system authority during a payment, the client can not access the public value x_M used in the signature process. As a consequence, the merchant needs to send this value to client. First, C sends to M her nickname NID_C, a nonce n for challenge-response, MIDReq and XMReq (the request for x_M), encrypted with a session key w generated by running AKE protocol [2] with C. Then, M confi rms C's

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 1 – 11

This paper is Available online at
www.jtaer.com

registration by sending the value X_M, merchant's identity (ID_M) and $h(n, x_M)$, encrypted with the session key w. Finally, C sends $h(ID_M, n, x_M)$ to M as a confi rmation to have received x_M.

Afterwards, the merchant will detect if the wallet software is available or not in the mobile device. If not, M sends a software request to PG, which will forward the request to I. The issuer intends to protect the software against various types of attacks carried away at any moment, preparing the software following these steps:

- Choose one of the obfuscation methods proposed by [13] and apply it to the java code.
- Then, the software is signed using the Authenticated encryption scheme with message linkages proposed by [3],[17].

Once the software has been prepared, the issuer will forward it to the PG, which will send it to C (through the merchant) who will install the software after receiving it.

Payment Protocol

1) C → M: $NID_C, TIDReq$
M → C: $E_{M-C}(TID, ID_M)$

2) C → M: $E_{C-M}(OI, Price, NID_C, ID_I, VSRequest, h(OI, NID_C, ID_I))$
$VSRequest = E_{C-I}(Price, h(OI), TC, ID_M)$

3) M → PG: $E_{M-PG}(VCRequest, ID_M)$
$VCRequest = (VSRequest, h(OI), TID, Price, NID_C, ID_I)$

4) Under banking private network,
4.1) PG → I: $VSRequest, h(OI), TID, Price, NID_C, ID_M$
4.2) PG → A: $Price, ID_M$
4.3) I,A → PG: $VSResponse, Stt, h(Stt, h(OI))$
$VSResponse = E_{I-C}(Stt, h(OI))$

5) PG → M: $VCResponse$
$VCResponse = E_{PG-M}(Stt, VSResponse, h(Stt, h(OI)))$

6) M → C: $PResponse$
$PResponse = E_{M-C}(VSResponse)$

Step 1: The Client **C** and merchant **M** exchange the information necessary to start the protocol.

Step 2: **C** creates a *Payment Request* (referred to the General Payment Model described in [11],[9]) including C's nickname, M's and I's identity, *Price*, *OI* and *Value-Subtraction Request* (called *VSRequest*, which is encrypted to be recovered only by an issuer **I**). *OI* is used to inform **M** about the goods and prices requested and *Payment Request* is encrypted by **C** to the specifi c receiver **M**. Once the *Payment Request* has been prepared, **C** sends it to **M**. Note that some important fi elds, such as *OI*, *Price*, NID_C, ID_I, are hashed in order to check if they are modifi ed or replaced with others while in transit.

Step 3: **M** decrypts the message received from **C** to retrieve *OI*. The Merchant **M** prepares the *Value-Claim Request* (called *VCRequest*) and then sends it with the merchant's identity to *PG*, encrypted to be recovered only by her in order to ensure that only the payment gateway is the intended recipient of the message. The *Value-Claim Request* contains the forwarded *Value-Substraction Request*, C's nickname, I's identity, order's amount, identity of transaction and the hash of the order information.

Step 4: **PG** decrypts the message received from **M** to retrieve *VSRequest* and the others fi elds included in *VCRequest*. Then, **PG** forwards *VSRequest* and other important information, namely: *h(OI)*, *TID*, *Price*, NID_C, ID_I to **I** who will

Journal of Theoretical and Applied Electronic Commerce Research
ISSN 0718–1876 Electronic Version
VOL 1 / ISSUE 2 / AUGUST 2006 / 1 – 11

This paper is Available online at
www.jtaer.com

process it to approve or reject the transaction. Also, **PG** sends ID_M and the requested price (*Price*) to claim to acquirer **A** that she is the party whom the requested amount *Price* will be transferred to. After checking the validity of the client's account, the total amount of *OI* is transferred to the merchant's account, the issuer **I** prepares *Value-Substraction Response* (called *VSResponse*) and sends it to **PG** with the approval result (*Stt*). Note that *VSResponse* is encrypted to be recovered only by an issuer **C**.

Step 5: PG sends *Value-Claim Response* (called *VCResponse*) encrypted to be recovered only by **M**. *VCResponse* includes *VSResponse* which will be forwarded to **C**. As **M** has her own *OI*, she can compare this fi eld with the received *h(OI)* to check whether or not the message is the response of her request. If they are not matched, **M** sends a message to the PG pointing the problem. The PG may now start a recovery procedure or resend the message.

Step 6: M encrypts *Value-Subtraction Response* to be recovered only by **C**. Then, **M** sends it to **C** as *Payment Response* (called *PResponse*). Once **C** receives the message, decrypts it to retrieve the result of her request.

Once the purchase has been completed, the client does not have to run *Merchant Registration Protocol* again unless she wants to perform transaction with a new merchant. Note that, after clients fi nish all purchases with a merchant, she will remove the values ID_M and x_M from her mobile device due to its limited amount of storage.

6 Analysis and Discussions

6.1 Security issues

After each run of the proposed protocol, the achievement of the following goals will ensure the security of the payment in our mobile payment system.

- **Goal 1**: Authentication between the client and the issuer

  The operational model used in this proposal has a communication restriction: client can not communicate directly with the issuer. Therefore, in order to allow that issuer authenticates a client, *C* has to send a message to *I* (through the merchant) with the following features: 1) resistant to attacks while in transit, 2) recoverable only by the issuer, and 3) able to assure that it has been created and sent by *C*.

  Since the authenticated encryption scheme used in our protocol integrates the mechanisms of signature and encryption, the message *VSRequest* sent by *C* to *I*, satisfi es all the requirements mentioned above and can be used by the issuer to authenticate the client.

- **Goal 2**: Anonymity

  In order to prevent a merchant from knowing the identity of her clients, usage of client's nickname (NID_C) instead of her real identity is required during a communication from *C* to *M*. Since the C's nickname is known only by the client and the issuer, merchant cannot map the nickname and C's true identity. Thus, client's privacy is protected and untraceable.

- **Goal 3**: Confi dentiality

  The authentication encryption scheme used in our protocol ensures the encryption of important data of per transaction while in transit. Moreover, since this scheme allows that only the specifi ed receiver can verify and recover the message, any other receiver is unable to do it. For example, the *VSRequest* is created by *C* and encrypted to be recovered only by *I*. Any other party couldn't decrypt the message because requires the issuer's private key which is known only by *I*.

- **Goal 4**: Integrity

  It is important to protect data from being modifi ed or/and replaced while in transit. To achieve that, usage of message digest algorithms and/or digital signature are required. In our protocol, the integrity is mainly ensured by the digital signature with message recover technique. Also, we use a hash function of some information (e.g, *Order Information*, *Client's nickname*, etc), padded into some message in order to ensure the integrity where the digital signature is not used (e.g under banking private network).

using hash value of some important information (e.g, *Order Information*, *Client's nickname*, etc), padded into some messages.

- **Goal 5**: Non-repudiation of Origin (NRO)

  The Non-repudiation of Origin is ensured since the signature of a message is generated by the signer U using her private key U_S (known only by U). Therefore, the signer should not be able to repudiate his signature creation later.

- **Goal 6**: Trust Relationships

  Generally, in any transaction, a party should not trust others unless they can provide a proof of trustworthiness [9]. However, as in our protocol the issuer issues a credit- and/or debit-card to the client and she will not reveal it to any part, we state the trust relationship between the client and the issuer.

7 Conclusions and Further work

This paper proposes a protocol for secure payments in a mobile payment system where direct communication between client and issuer does not exist. Our protocol uses a digital signature scheme with message recovery using self-certifi ed public keys. Furthermore, it allows clients to make purchases without disclosing private information and takes advantage of the infrastructure of the *merchant* and *payment gateway* to communicate with the issuer. With this protocol the client is able to purchase securely from her mobile device in a similar way to that of traditional mobile payment systems.

Our proposal represents an alternative to all mobile payment systems based on the Full Connectivity scenario (including Visa's 3-D Secure scheme) where communication between the client and issuer is mandatory. Moreover, we state that a portable device with a short range link (such Bluetooth, Infrared or Wi-Fi) and low computational capabilities is enough for interacting with a merchant in order to buy goods or services in a secure way.

As a result, we assert that our proposed protocol allows mobile users to have effi cient and secure payment systems even if the communication with the issuer is not possible.

In the future, as the proposed protocol includes only non-repudiation of origin, it will be valuable to incorporate more non-repudiation services (such as non-repudiation of receipt, non-repudiation of submission and non-repudiation of delivery) in order to prevent entities from denying that they have sent or received certain messages.

Acknowledgements

This work was supported in part by ASPECTS-M Project (Reference Models for Secure Architectures in Mobile Electronic Payments), CICYT-2004, however it represents the view of the authors.

References

[1] N. Asokan, Anonymity in a Mobile Computing Environment, in Proceedings of IEEE Workshop on Mobile Computing Systems and Applications. IEEE, 1994, pp. 200–204.

[2] M. Bellare, J. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, E. V. Herreweghen, and M. Waidner, Design, implementation, and deployment of the iKP secure electronic payment system, IEEE Journal on Selected Areas in Communications, vol. 18, no. 4, pp. 611–627, 2000.

[3] Y. Chang, C. Chang, and H. Huang, Digital signature with message recovery using self-certifi ed public keys without trustworthy system authority, Journal of Applied Mathematics and Computation, vol. 161, no. 1, pp. 211–227, 2005.

[4] S. Chari, P. Kermani, S. Smith, and L. Tassiulas, Security Issues in M-Commerce: A Usage-Based Taxonomy, in Proceedings of E-Commerce Agents, 2001, pp. 264–282.

[5] M. Girault,Self-Certifi ed Public Keys, in Proceedings of EUROCRYPT, 1991, pp. 490–497.

[6] W. Ham, H. Choi, Y. Xie, M. Lee, and K. Kim, Secure One-way Mobile Payment System Keeping Low Computation in Mobile Devices, in Proceedings of WISA'02, 2002, pp. 287–301.

[7] J. Hall, S. Kilbank, M. Barbeau, and E. Kranakis, WPP: A Secure Payment Protocol for Supporting Credit- and Debit-Card Transactions over Wireless Networks, in Proceedings of International Conference on Telecommunications (ICT 2001). IEEE, 2001.

[8] Z. Hu, Y. Liu, X. Hu, and J. Li, Anonymous Micropayments Authentication(AMA) in Mobile Data Network, in Proceedings of INFOCOM, 2004.

[9] S. Kungpisdan, B. Srinivasan, and P. D. Le, A Secure Account-Based Mobile Payment Protocol, in Proceedings of ITCC (1), 2004, pp. 35–39.

[10] Y. Lei, D. Chen, and Z. Jiang, Generating Digital Signatures on Mobile Devices, in Proceedings of AINA (2), 2004, pp. 532–535.

[11] J. L. A. Peiro, N. Asokan, M. Steiner, and M. Waidner, Designing a generic payment service, IBM Syst. J., vol. 34, no. 1, pp.72–80, 1997.

[12] A. Shamir, Identity-Based Cryptosystems and Signature Schemes, in Proceedings of CRYPTO, 1984, pp. 47–53.

[13] M. Sosonkin, G. Naumovich, and N. D. Memon, Obfuscation of design intent in object-oriented applications, in Proceedings of Digital Rights Management Workshop, 2003, pp. 142–153.

[14] J. Téllez, J. Sierra, A. Izquierdo, and M. Carbonell, Payment in a Kiosk Centric Model with Mobile and Low Computational Power Devices, in Proceedings of ICCSA (5), 2006, pp. 798–807.

[15] Y. Tseng, J. Jan, and H. Chien, Digital signature with message recovery using self-certifi ed public keys and its variants, Journal of Applied Mathematics and Computation, vol. 136, no. 2–3, 2003.

[16] Visa International, (2002). 3-d secure mobile authentication scenarios version 1.0. [Online], Available: http://partnernetwork.visa.com/pf/3dsec/specifi cations.jsp

[17] J. Zhang, W. Zou, D. Chen, and Y. Wang, On the Security of a Digital Signature with Message Recovery using Self-certifi ed Public Key, Soft Computing in Multimedia Processing Special Issue of the Informatica Journal, vol. 29, no. 3, pp. 343–346, 2005.