Journal of Universal Computer Science, vol. 14, no. 14 (2008), 2309-2328
submitted: 30/9/07, accepted: 30/4/08, appeared: 28/7/08 © *J.UCS*

Non-repudiation Mechanism of Agent-based Mobile Payment Systems: Perspectives on Wireless PKI

Chung-Ming Ou
(Department of Information Management, Kainan University, Taiwan
cou077@mail.knu.edu.tw)

Chung-Ren Ou
(Department of Electrical Engineering, Hsiuping Institute of Technology
Taiwan
crou@mail.hit.edu.tw)

Abstract: Non-repudiation of a mobile payment transaction ensures that when a buyer (B) sends some messages to a seller (S), neither B nor S can deny having participated in this transaction. An evidence of a transaction is generated by wireless PKI (WPKI) mechanism such that B and S cannot repudiate sending and receiving the purchase order respectively. Broker generates a mobile agent for B which carries encrypted purchase order to S. A trusted third party (TTP) acts as a lightweight notary for evidence generations. One advantage of this agent-based non-repudiation protocol is to reduce inconvenience for mobile clients such as connection time and search for suitable merchant servers, etc.; it provides necessary security mechanisms for fair mobile payment transactions.
Key Words: non-repudiation, mobile agent, WPKI, trusted third party, security
Category: E.3, K.6.5, D.4.6

1 Introduction

Mobile agents are believed to play an important role in future electronic commerce and mobile commerce. This is due to their flexibility for information gathering on prices and goods available from varied merchant servers, in addition to aspects of the electronic transactions from price settlement to paying and delivery of the purchased goods [Das and Gongxuan 2001]. For three basic stages of mobile payment systems, namely, information gathering, negotiation and payment & delivery, mobile agents may play active role in every stage according to the involvement of these agents. In particular, for payment & delivery, mobile agents can be used to pay for purchased goods and help collect an evidence of payment transaction. For the latter, security issue has been concerned for mobile payment for a long time. For example, dispute of a transaction is a common problem that could jeopardize the mobile commerce [Zhou et al. 1999].

In many applications, one essential security requirement is that all participant parties reach their goals of fairness. Undeniability of exchange data for commercial transaction is also essential. The purpose of non-repudiation is to collect, maintain, make available and validate irrefutable evidence concerning a claimed event or action in order to resolve disputes on the occurrence or non-occurrence of the event or action [ITU-T 1996][Li and Luo 2004]. However, in the real world situation, lots of mobile stock brokerage services and mobile banks have already been promoted but without any non-repudiation mechanism.

Non-repudiation mechanisms rely on operations of digital signatures, which are provided by the public key infrastructure (PKI). The phrase wireless public key infrastructure (WPKI) is a loose definition as adopting PKI in wireless (or mobile) environment, such as WAP (Wireless Application Protocol) proposed by the WAP Forum (now called the OpenMobile Alliance). PKI utilizes digital signature along with other cryptographic techniques to reach confidentiality, integrity, authentication and non-repudiation for information systems. Basically, mobile clients can utilize PKI-enabled services through his/her mobile devices with secure PKI components embedded.

There are several electronic invoice systems promoted by the Ministry of Economic Affair (MOEA) in Taiwan since 2004. One purpose of these systems is to reduce the cost of generating paper-based receipts and invoices. According to MOEA, electronic invoice systems based on PKI are the most successful PKI-enabled applications in Taiwan which greatly reduce the cost of purchasing system. However, these PKI-based systems do not adopt any non-repudiation mechanism between buyers and sellers. Another motivation for this research is the mobile TAIWAN project (mTAIWAN). Since 2005, mTAIWAN is one major nation-wide project of establishing seamless and ubiquitous wireless infrastructure. This next generation communication network combines mobile communication systems such as 2G (GSM), 2.5G (GPRS), 3G (UMTS), wireless network systems such as WiFi and WiMAX technologies. One major goal for mTAIWAN project is to promote the ubiquitous mobile applications using varied mobile devices such as mobile phone, PDA, laptop PC, etc. Combining these motivations, we propose an agent-based architecture and protocol to implement non-repudiation mechanism over the mobile payment systems; this will improve security mechanisms of those existing electronic invoice systems.

Non-repudiation services must ensure that when buyer B sends a message to seller S over a network, neither B nor S can deny having participated in a part or the whole of this transaction. The basic idea is the following: an evidence of origin (EOO) is generated for buyer B and an evidence of receipt (EOR) is generated for seller S. Evidences are generated by PKI-based digital signatures. Disputes may arise over the origin or the receipt of messages. For the case of origin dispute, B denies sending a message while S claims having received it, or vice versa for the receipt dispute. Buyer is at risks that seller repudiate receiving this purchase order. Our mobile payment system is as follows. First buyer sends out encrypted purchase order to Broker, which is a entity trusted by buyer. Then this Broker generates a mobile agent which carries this encrypted purchase order to seller, which decrypts this order. The deployment of Broker between wired and wireless networks can ease the access to web information from the mobile devices, and it can also alleviate some of these security constraints [Esparza et al. 2006]. Mobile payment systems need time information included in evidences for dispute resolutions.

Mobile agents are considered to be an alternative to client-server systems, in particular for mobile commerce where mobile devices and communications have limited computing resource. A mobile agent of the host is a set of code and data which can execute the code with the data as parameter in some trusted processing environment (TPE). However, there are several issues related to security and trust while considering mobile agent-based electronic commerce [Pagnia et al. 2000][Wilhelm et al. 1998][Esparza et al. 2003] such as non-repudiation. We need to consider coordinations between Broker and TPE in our mobile payment systems to meet the commerce requirements of both efficiency and security. The advantage of adopting this mobile agent architecture to non-repudiation protocol is the following: the buyer needs only to send the purchase order while its device connects to the mobile base station; once such order is sent to the Broker, mobile devices may be disconnected from this base station. Once the transaction is complete, this mobile agent can carry the message of payment and transaction completion and returns to its host (buyer). This is an ideal transaction model for mobile commerce.

The arrangement of this paper is as follows. In section 2, we introduce preliminary knowledge for WPKI and mobile agents. In section 3, we propose an agent-based non-repudiation protocol suitable for mobile payment systems; we also analyze the security mechanisms of agent-based non-repudiation protocols, namely, dispute resolutions. In section 4, some evaluations of this protocol, such as performance efficiency and other security mechanisms, are given.

2 Preliminary Knowledge for WPKI and Mobile Agents

Before designing an agent-based non-repudiation protocol for mobile payment systems, we introduce necessary knowledge such as mobile agents and WPKI in more retails.

2.1 Mobile Agent Security

A mobile agent is a set of code of data generated by its host or some trusted broker. The code is executable with reference to these carried data. A mobile agent consists of the following components: agent owner, identifier, goal/result, life time and states. There are several security issues related to mobile agents such as repudiation; an agent threatens another agent [Jansen and Karygiannis 1999];

an agent may deny having exchanged message with other host, and so on. On the other hand, an agent may be modified by some malicious agents or hosts while transferring to some merchant servers. A general guideline for protecting these mobile agents utilizing WPKI is as follows.

– Broker obtains the certified public key of the merchant server.

– Broker encrypts this mobile agent using merchant server's public key and sends it to the merchant server.

Each agent carries the item which is intended to be exchanged. These items may include purchase orders with payment information (e.g. bank account number, credit card number, or micro-payment account number, etc). When the buyer's agent enters into TPE of some merchant server, Broker must ensure that they play fair. Furthermore, none of these agents is allowed to communicate with any other entity except its host (buyer) or transacted seller.

Some opponents of mobile agents cite lots of mobile security problems as reasons not to use them. According to [Ma and Tsai 2006], we should adapt mobile agent systems to some application environment where risk of security can be mitigated to an acceptable level. For example, we will adapt mobile agents to mobile payment systems to see whether the risk of such systems can be reduced.

Many security protocols are basically assumed direct connection among entities; these protocols do not consider agent-based transactions at all. Once agent delegations are considered by adopting these security protocols, some new security threats appear. These threats also influence the security of these originally non agent-based non-repudiation protocols. These security issues can be divided into two parts, one is the mobile agent protection issue, the other is the TPE protection issue. We outline these security issues as follows. For more details, see [Jansen and Karygiannis 1999][Ma and Tsai 2006].

2.1.1 Mobile agent protections

A mobile agent has to expose its information to TPE to which it is migrated and its carried codes are executed. One challenge for agent-based systems is the threat from malicious hosts. One way to protect mobile agents is by the Host Revocation List (HRL) mechanisms to passively prevent mobile agent from being sent to malicious hosts; the other active measure is to make mobile agent act intelligently, namely, mobile agents are capable of doing cryptographic operations. In details, rather that adapting proxy certificates as in [Ou and Ou 2008], the privilege to access agent's data and code is granted if hash values are computationally coincident by both agent and TPE.

In our agent-based protocol, we adapt the first passive preventing mechanisms. While the second one will be the future research interest.

2.1.2 TPE protections

A TPE in a mobile agent system similar to a server in the traditional client-server environment; many conventional security mechanisms for client-server environment, such as SSL (Secure Socket Layer), firewall, IDS/IPS(Intrusion Detection/Prevension System) and application gateway, etc., are suitable for countermeasures to protect TPEs. According to [Ma and Tsai 2006], a safe environment must be provided for execution of any alien program, these include software-based fault isolation and safe-code interpretation. Also the check of safety property of any alien code is necessary before being execution on TPE. We won't discuss details of this issues and readers may refer to [Ma and Tsai 2006].

2.2 WPKI

WPKI is the core cryptographic mechanism for non-repudiation protocol; it consists of two parts, one is the operation; the other is the entity. WPKI entities must contain at least two public-private key pairs for encryption/decryption and signature generation/verification, respectively. For more stringent security consideration, it may impose two public-private key pairs for digital signature parts, one is for authentication, the other is for non-repudiation. These key pairs are generated by some certification authority (CA) whose major task is to bind public key, private key and entity together.

There are two major WPKI operations in our non-repudiation protocol, one is the PKI encryption and decryption, the other is the digital signature-based evidence generation and verification. WPKI entities for non-repudiation service include CAs and certificate subjects. There are two types of certificate subjects within this WPKI, one is mobile clients, the other is the servers such as TPEs and banks.

2.2.1 Certificate authority (CA)

There are three CAs in this WPKI. The root CA (RCA) issues certificates to subscriber CA (SCA) and Home Revocation Authority (HoRA). SCA issues certificates to mobile clients and server certificates to TTPs and Broker. HoRA issues certificates to TPEs of merchant servers. These entities can authenticate each other by verifying digital signatures and transmit encrypted information if necessary.

A CA needs to provide certificate management service to ensure the validity of certificates. There is a repository which stores certificates and updated certificate revocation list (CRL). For WPKI-based application services such as mobile payment system, CAs may also provide On-line Certificate Status Protocol (OCSP) service to these WPKI entities for checking certificates validity.

These entities would continue WPKI operations if and only if related certificates are valid.

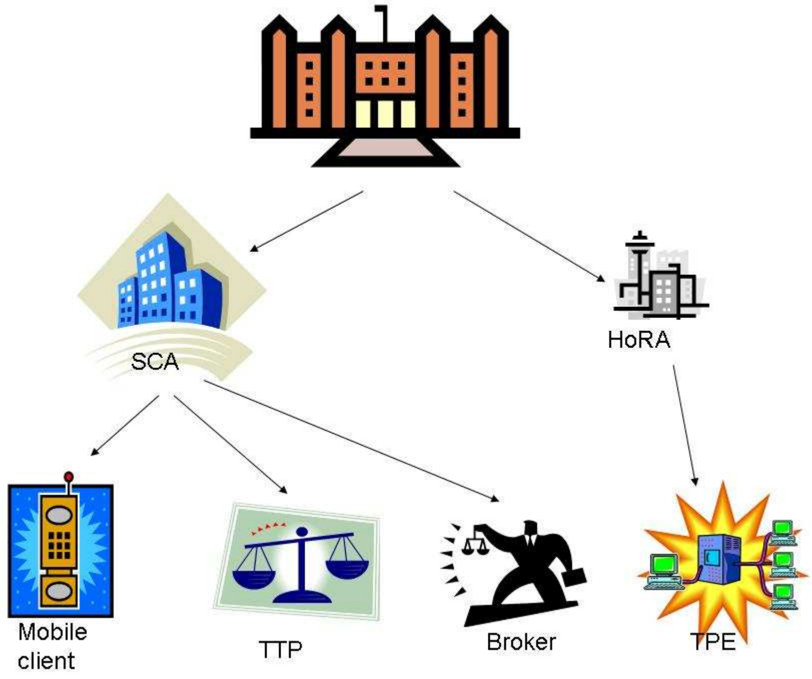

Figure 1: The WPKI architecture

In this paper, SCA is simply playing the role of certificate management. Mobile clients will be issued his/her WPKI certificate by SCA and the corresponding private key will be installed within the USIMs (universal Subscriber Identity Module). The security of this private key is crucial and in general, CA's certificate Policy Statement (CPS) will emphasis the necessity of preserving private key within USIMs. There are several agent-based fair exchange protocols rely on delegating mobile client's private key to its mobile agent. In this paper, we avoid such a concept and do not let agent perform signature generation for his host.

2.2.2 Mobile client

We suggest that a mobile client be a USIM-based 3G mobile equipment for efficient signature generation and verification. USIM-based mobile devices share cryptographically equivalent security with smart cards, which is the most secure tokens for agent-based E-commerce, see [Lopez 2007] for more details. A USIM stores only necessary WPKI components due to possible limitation of USIM resources affordable to PKI operations. In our non-repudiation protocol described in the following section, the USIM stores the TTP's server certificate and subscriber's two private keys. These public-key certificates are all issued by SCA within this WPKI. Private keys should be generated within USIMs and contained in them afterwards.

2.2.3 Host revocation authority (HoRA)

HoRA issues host certificates (HC) to merchant servers which are in charge of their own TPEs; these certificates bind mobile agent execution capability to the merchant host identity. When a merchant server acts maliciously, HoRA only needs to revoke this server's HC to prevent the broker from sending agents to it. Even though some the TPE of this merchant server is still secure, HoRA adopts highest security measure to revoke this HC, thus broker will prevent sending agents to any TPE belonging to this merchant server. The functionality of HoRA to detect the status of merchant servers can be referred to [Esparza et al. 2006].

The connection of HoRA and broker is as follows. HoRA issues the host revocation List (HRL), which is a digital-signed list of revoked HCs. Once the update of HRL is released by HoRA, broker's side of HRL will be updated simultaneously.

2.3 Trusted Third Party (TTP)

The trusted third party here is a notary server which simply generates necessary evidences for buyers and sellers. TTP needs to perform WPKI operations according to the non-repudiation protocol described in the next section. Therefore TTP needs to access CA's repository to retrieve necessary certificates of buyers' (or HCs of sellers') and verify digital signatures. TTP needs to store the broker's public-key certificates and plays a role as the time stamp authority if necessary. For those generated evidences, TTP will store these information in its public directory from which buyers and sellers may fetch evidences.

TTPs may be online, inline, offline according to the non-repudiation protocols. There are lots of research related to this issue such as [Du et al. 2006] [Kremer et al. 2002]. Our protocol provides online TTP which is suitable for mobile payment, where peer-to-peer(P2P) architecture is hard to be accepted by service providers. It lacks confidences for P2P-based payment systems these days, while fully trusted TTP by both seller and buyer is a feasible way for service providers. Some discussions of this issue, such as the concept of limited trusts and multiple mediators, can be referred to [Ito et al. 2002].

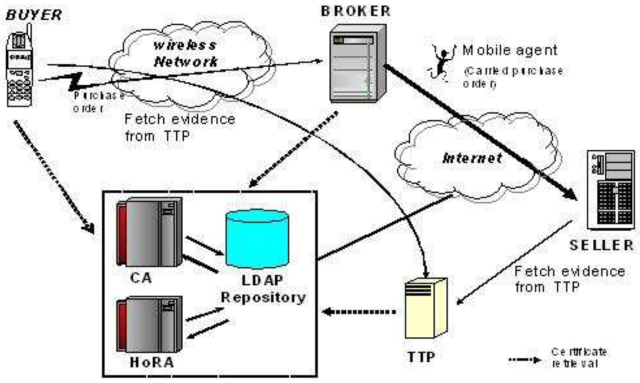

Figure 2: The architecture of agent-based non-repudiation protocol

TTP acts as a lightweight notary in our agent-based non-repudiation protocol that only notarizes purchase order by requests. TTP also provides directory services accessible to the public. For the non-repudiation protocol introduced in the next section, TTP only deal with “keys” rather than purchase order, that is, TTP does not know any information of this order. Therefore the communication overheads between parties and TTP are reduced, and the buyer’s purchasing privacy is also guaranteed.

2.4 Broker

Mobile clients want to pay sellers according to purchase orders. Broker acts as a mediator between mobile clients in the wireless network and merchant servers in the Internet, see Figure 2. Broker must distinguish malicious servers from the honest ones according to the HRL in order to avoid sending agents to them. It is possible that honest server become malicious before the HRL is updated. [Esparza et al. 2006] provides some solutions to solve this mobile agent security problem. HoRA will issue an updated HRL to Broker if a merchant server is detected to be malicious. Broker needs to authenticate TTPs on behalf of mobile clients before the non-repudiation protocol runs.

Before sending an agent of a mobile client to a merchant server, Broker must check the status of all servers on the agent's itinerary to see if any server is on the HRL. Broker determines itineraries by considering transaction efficiency. Within time constrains, Broker may find different itineraries for this transactions. If all the checks are positive, Broker will stop sending this agent to the merchant server and informs buyer the risk of sending this purchase order; this mobile payment transaction is terminated. In order to maintain the itinerary security, Broker needs to update HRL periodically, for more detains, see [Borrell et al.1999].

2.5 Trusted Processing Environment (TPE)

TPE is a mobile agent platform maintained by its merchant. Mobile agents are sent by Broker to a TPE to perform conversation and negotiation on behalf on mobile clients with the corresponding seller. TPE is a secure platform not only to protect agents but also protect itself from attacks by malicious codes. To reach this goal, TPE has to follow the access control policy specified by its merchant server. In general, mobile service provider will provide such security management to sellers for promoting mobile commerce. According to this access control policy, TPE cannot access confidential data or access-limited code of mobile agents; against this policy, HoRA will revoke merchant server's HC. On the other hand, TPE will define its access privilege to mobile agents in order to confine normal activities of such agents. More access control issues of both TPE and mobile agents, please refer to [Ma and Tsai 2006] [Roth and Jalali-Sohi 1998] [Bierman and Cloete 2002].

3 Fair Non-repudiation Protocol of Agent-based Mobile Payment Transactions

There are two security issues of non-repudiation protocol for mobile payments. The first issue is the following: WPKI architecture suitable for non-repudiation mechanism relies not only on its entities, but also some TTPs which may generate final evidences for purchase orders between buyers and sellers. The other issue is the secure environment of performing non-repudiation protocols. Lopes et al. [Lopez 2007] proposed a fair non-repudiation protocol based on smart cards. Here, rather than utilizing smart cards, we propose similar security mechanisms of USIM, which has similar cryptographic hardware module as smart card. The latter is regarded as the most secure PKI implemented token.

In this section, we focus on evidence generations of purchase orders between a mobile client and a merchant server through some brokers. As mentioned in previous section, these brokers improve the efficiencies of mobile transactions and security, if only brokers themselves are trustworthy and well-protected. It is reasonable to assume these two basic factors in mobile transaction maintained majorally by mobile service providers and telecommunication companies. There are several researches related to mobile agent-based P2P transaction which does not rely on any online TTP or brokers, see, for example, [Ou and Ou 2008] [Gurgens et al. 2005] [Braun and Rossak 2005]. However, P2P mobile transaction involved with monetary still under restriction by governments due to the taxation issues; it is still impractical to discuss this issue so far.

Non-repudiation evidences are extremely important to mobile payment systems. Once buyer and seller own their evidences respectively, seller can request its bank for fund transferring according to this purchase order without worrying about being cheated by buyers; non-repudiation evidences can protect such privilege. Seller needs to guarantee the amount of transferred fund be coincident with that on the purchase order. Otherwise TTP can point it out to the arbitrator that this seller is cheating. Therefore, it is sufficient for us to concentrate on the evidence generation of the purchase order rather than that of billing. This approach is also similar to that in [Esparza et al. 2006].

3.1 Basic Structure for Secure 3G Mobile Payment Services

Mobile payment becomes a crucial issue for mobile commerce. It is still very inconvenient for mobile subscribers to pay online due to the mobile device characteristics (touch pad, small screen, etc.). On the other hand, mobile clients still hesitate to pay online due to the security issues; there is no solid evidence to protect these mobile clients against potential security threats. According to the investigation by Tak et al. [Tak et al. 2003], SSL (Secure Socket Layer), which is the most popular secure transaction mechanism, is a bilateral agreement without any TTP to mediate, nor did its counterpart in mobile transaction, namely, WTLS (Wireless Transport Layer Security). Therefore, a reliable non-repudiation security service does not exist neither in SSL nor in WTLS. On the other hand, SET (Secure Electronic Transaction) did deploy a TTP called "payment gateway" to protect customer's payment information from merchants. However, it simply concerns whether the payment by the customer is complete or not.

According to the above discussion of mobile payment systems, we have motivations to propose non-repudiation protocols for mobile payment systems. It is known that one major message in mobile payment system is the purchase order with sensitive payment information which include buyer's information, bank account number or credit card number, etc. This information needs to be securely protected from unauthorized entities. Now, the architecture for mobile payment system is composed of the following entities: a buyer represented by some mobile equipment (ME), WPKI, a seller (merchant server), a bank and a Broker, see

Figure 3. For simplicity, we assume that both buyer and seller have the same bank for fund transfer. These entities are also issued certificates by some CA within this WPKI. ME utilizes the USIM to store mobile client's information such as IMSI (International Mobile Subscriber Identity) and WPKI components. ME is capable of efficiently verifying digital signatures to authenticate other entities, if necessary.

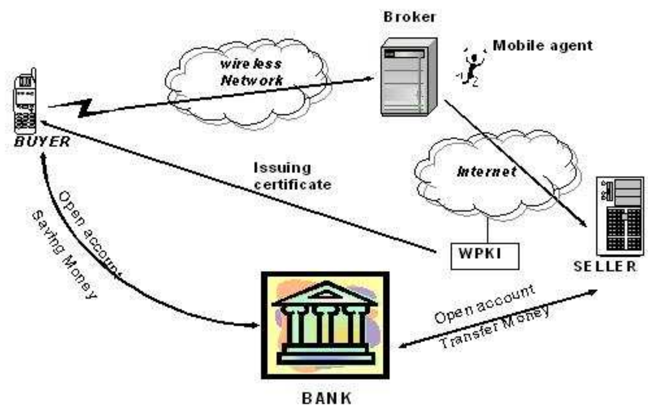

Figure 3: The architecture of an agent-based mobile payment system

3.2 Design of Agent-based Non-repudiation Protocol

Besides two security requirements for agent-based system mentioned in the beginning of this section, the non-repudiation protocol needs more trusted entities to achieve fairness and dispute resolutions. For our agent-based non-repudiation protocol, buyer's agents are generated by Broker then sent to some TPEs according to the agent itinerary, which is also authorized by this Broker. TPEs are maintained by some merchant servers which provide secure transacting platforms to mitigate the risk of threats from malicious hosts and agents. For simplicity, we consider situations that Broker generates buyer's mobile agent which is roaming among TPEs for mobile payment transactions. The question now is how to protect this mobile agent from malicious hosts while transmitting non-repudiation evidences. One situation is that a malicious host is sending some fake message to lure mobile agents to hand-in important messages. Therefore agent-based non-repudiation protocol, besides original security consideration which including fairness and timeliness, needs to prevents security threats from other agents or hosts.

An efficient and fair non-repudiation protocol was proposed by Zhou and Gollmann (we name it ZGP) where TTP acts as a lightweight notary, see [Zhou and Gollmann 1996] for more details. This protocol is suitable for 3G communication by analyzing the capability of implementing cryptographic operations such as digital signature, symmetric key encryption(decryption), hash function and random number generations [Ou 2004][1]. Although this TTP is a lightweight notary, namely, its involvement in the ZGP is greatly reduced; however, this TTP is crucial and it has to be online through the ZGP. Moreover, for designing agent-based non-repudiation protocol, we realize that ZGP greatly reduced the step number of message transmissions, also see [Ou and Ou 2008]. According to these investigations, we adapt ZGP to agent-based non-repudiation protocol suitable for mobile payment systems.

3.3 Fair Agent-based Non-repudiation Protocol with Timeliness

Time information of sending and receiving purchase orders are crucial in mobile payment system. It can be achieved by appending some time stamps to evidences generated by no -repudiation protocols. The ZGP did not consider time information; Li and Luo improved ZGP by considering the time span for evidence preservation [Li and Luo 2004]. This improvement needs only TTP plays the role of time stamping authority while buyers and sellers just define their intended time spans.

For non-repudiation protocol, it is essential that no transacted party can gain advantage over the other. Otherwise, either buyer or seller may find some opportunity to cheat. We define such advantages in details. A non-repudiation protocol is *fair* if it can ensure that at the end of a protocol execution, none or both of the two entities, the sender and the receiver, can retrieve all the evidences it expects [Li and Luo 2004]. Therefore fairness guarantees that neither sender nor receiver can gain advantage over the other. Although it is easy to define such fairness, it is more difficult to design fair non-repudiation protocol. For example, Ou and Ou [Ou and Ou 2008] proposed a fair non-repudiation protocol by adapting proxy certificates rather than relying on brokers. Buyers need to generate mobile agents themselves and issue certificates to agents.

Now we design a fair non-repudiation protocol suitable for agent-based mobile payment systems; this protocol relies on the trust of Broker. Trust is more a social

[1] The original ZGP did not design particularly for mobile transactions. The author has discussed with Chunghwa Telecom Lab in Taiwan for RSA digital signature implementation in mobile environment. The capability of USIM cryptographic module is reasonable for WPKI operations.

issue than a technical one. We may assume reasonably that mobile operators or some mobile service providers provide Brokers which are completely trusted by mobile clients. The purpose of this non-repudiation protocol is to transmit encrypted purchase order M and obtain non-repudiation evidences for buyer B and seller S. Purchase order M contains two parts, one is a commitment C, and the other is a key K. Notations are as follows.

- M: purchase order being sent from B to S.
- K: key generated by B.
- C=e_K(M): commitment for purchase order M (e_K represents encryption by key K).
- sS_B(M): signature of message M signed by B's private key.
- L=H(M,K): a label linking C and K (H represents a hash function).
- f_i: flag indicating the purpose of a signed message.
- e_S(.): encryption by S's public key
- EOO_C: evidence of origin of C, which is equal to sS_B(f_{EOO}, S, L, C).
- EOR_C: evidence of receipt of C, which is equal to sS_S(f_{EOR}, B, L, t_S, C).
- sub_K: authenticator of receipt of C, which is equal to sS_B(f_{SUB}, S, L, t_B, K, EOO_C).
- con_K: evidence of confirmation of K issued by the TTP with time stamp T, which is equal to sS_{TTP}(f_{CON}, B, S, L, T, t_B, t_S, K, EOO_C, EOR_C).

We include time information in this protocols; t_B is a time span defined by buyer B indicating that sub_K will be kept in TTP's private directory for t_B time units; t_S is a time span defined by seller S indicating that TTP will keep EOR_C in its private directory for t_S time units. T is the time stamp indicating the actual time TTP generate key confirmation con_K and make it public. This non-repudiation protocol which relies on two different mobile agents {A1}, {A2} generated by the broker is as follows.

1. B$\longrightarrow$Broker$\longrightarrow_{\{A1\}}$S: f_{EOO}, S, L, e_S(C), EOO_C
2. B$\longrightarrow$Broker$\longrightarrow_{\{A2\}}$TTP: f_{SUB}, S, L, t_B, K, EOO_C, sub_K
3. S$\longrightarrow$TTP: f_{EOR}, B, L, t_S, EOO_C, EOR_C
4. TTP$\longleftarrow$B : f_{CON}, B, S, L, T, t_B, t_S, K, EOR_C, con_K

5. TTP$\longleftarrow$S : f_{CON}, B, S, L, T, t_B, t_S, K, EOR_C, con_K

"B$\longrightarrow$ Broker$\longrightarrow_{\{A\}}$ S: M" means B sends message M to broker, then broker will generate an agent {A} for B; message M will be carried by this agent {A} to S;"TTP $\longleftarrow$ B"means B fetches messages from TTP. The basic idea is that buyer B is able to send K, sub_K to TTP in exchange for con_K; on the other hand, seller S sends EOO_C, EOR_C and t_S to TTP. We describe details of each step as follows.

- In step 1, B sends f_{EOO}, S, L, e_S(C), EOO_C to Broker which generates mobile agent {A1}. This agent carries these information to S. S needs to verify the validity of EOO_C by retrieving B's (signature) public key from the SCA's repository. If EOO_C is valid, then it is saved as an evidence of origin for S. Broker also helps B authenticate TPE such that attackers cannot impersonate this seller.
- In step 2, after receiving these information,TTP keeps sub_K in its private directory and delete it after t_B time units or until con_K (in step 4) is generated and published.
- In step 3, after receiving EOO_C, EOR_C and t_S from S, TTP needs to verify EOR_C using S's (signature) public key and compare this EOO_C with the one sent by {A2}in step 2. If either one is not true, TTP concludes that at least one party is cheating and it will not generate con_K. TTP also checks if labels L from step 2 and 3 are coincident. If not, buyer B and seller S must be disagreed with this purchase order M. TTP will stop this protocol.
- In step 4, if steps 1-3 are shown positive results, TTP starts to generate con_K with time stamp T attached. We call {f_{CON}, B, S, L, T, t_B, t_S, K, EOR_C, con_K } the evidence of this purchase order M. Buyer B fetches evidence of purchase order M from TTP.
- In step 5, seller S fetches evidence of purchase order from TTP to prove that encryption key K is available for S.

3.4 Security of Agent-based Non-repudiation Protocol

The most important security issue of a non-repudiation protocol is the dispute resolution. We analyze both the generated evidences of step 4 in the above agent-based non-repudiation protocol, and dispute resolution mechanisms of buyer and seller to see whether non-repudiation can be reached. A trusted arbitrator will help solve the dispute according to submitted evidences.

3.4.1 Security of the purchase order

The purchase order is well-protected by encryption key K and not revealed to other entities including TTP and Broker. Moreover, buyer and seller can reach secure communications, i.e. end-to-end security, for further transactions by sharing common session keys which is not known by other parties.

3.4.2 Validity of evidence

Non-repudiation protocols will fail if bogus evidence is accepted or no evidence is received by either buyer or seller. Validity of non-repudiation evidence depends on the security of cryptographic keys used for generating evidences. These keys need to be revoked if they are at the risk of being compromised according to WPKI certificate policy practice.

According to WPKI, buyer B, seller S and TTP could retrieve certificates of each other's from CA's repository to verify digital signatures as in step 1 and 2 in this protocol. By the nature of hash functions, it is computationally hard to find two different key K and K' (with reasonable key length) with the same labels, namely L= H(M, K)= H(M, K')= L' and M= dK(C)= dK'(C)= M', where dK(.) represents message decryption by key K. Therefore, TTP can investigate the validity of evidences by checking these labels.

3.4.3 Dispute of origin

When buyer B denies having sent purchase order M to seller S, S may present EOO_C, EOR_C and con_K to the arbitrator in the following way:

S $\longrightarrow$ arbitrator : EOO_C, EOR_C, con_K, sS_S(EOO_C, EOR_C, con_K), L, K, M, C

The arbitrator first verifies the signature of S, sS_S(EOO_C, EOR_C, con_K); if the verification is positive, the arbitrator checks the following five steps:

- step 1: if EOO_C is equal to $sS_B(f_{EOO}$, S, L, C).
- step 2: if EOR_C is equal to $sS_S(f_{EOR}$, B, L, t_S, C).
- step 3: if con_K is equal to $sS_{TTP}(f_{CON}$, B, S, L, T, t_B, t_S, K, EOO_C, EOR_C).
- step 4: if L is equal to H(M,K).
- step 5: if M is equal to dK(C).

If step 1 is checked positive, this arbitrator concludes that buyer B has sent seller S the encrypted purchase order C. If step 2 is checked positive, arbitrator concludes that S has sent all the correct information to TTP in (step 3 in protocol). For all 5 steps being checked positive, this arbitrator finally concludes that B has sent S the purchase order M, which is encrypted by K and presented to be commitment C.

3.4.4 Dispute of receipt

When seller S denies receiving the purchase order M from buyer B, buyer may present EOO_C, EOR_C, con_K to the arbitrator in the following way:

B $\longrightarrow$ arbitrator : EOO_C, EOR_C, con_K, sS$_B$(EOO_C, EOR_C, con_K), L, K, M, C

The arbitrator first verifies the signature of buyer B, sS$_B$(EOO_C, EOR_C, con_K); if the verification is positive, the arbitrator checks all five steps same as those in the dispute of origin. For all five steps being checked positive, arbitrator concludes that seller S has received M, which is encrypted by K and presented to be C.

3.4.5 Dispute of fund transfer

If buyer B realizes the amount of transferred fund is different from that on the purchase order M, he may ask this arbitrator to check. Arbitrator will check M presented by buyer B and M' by seller S. Arbitrator also fetches K and L from TTP. If H(M,K) is not equal to L, the arbitrator concludes that buyer B is cheating. On the other hand, if H(M',K) is not equal to L, the arbitrator concludes that seller S is cheating.

4 Protocol Evaluation

In this section, other than dispute resolutions, we analyze performance efficiency and security mechanisms of this agent-based non-repudiation protocol introduced in the previous section.

4.1 Analysis of Performance Efficiency

It has been a frequently-asked question about the implementation of digital signature on mobile devices. M'Raihi and Yung have pointed out that recent smart cards are equipped with impressive mechanisms to support PKI applications [M'Raihi and Yung 2001] in reasonable performance and with high-level functionality. According to [www.st.com 2004], such performance is greatly improved by the on-the-shelf USIM cards within compatible handsets.

The Table 1 is a step-by-step performance analysis of this protocol. **CryptOp** represents cryptographic operations; **SigGen** represents digital signature generation; **SigVer** represents digital signature verification. AES (Advanced Encryption Standard) is the well-known encryption algorithm.

Table 1: Performance efficiency for agent-based non-repudiation protocol

CryptOp	SigGen	SigVer	AES	Hash
Step 1	1(B)	1(S)	1(B)	1(B)
Step 2	1(B)	1(TTP)	0	1(B)
Step 3	1(S)	1(TTP)	0	1(S)
Step 4	1(TTP)	1(B)	0	1(TTP)
Step 5	0	1(S)	1(S)	0
Total numbers	4	5	1	5
Times(s)	4×0.3227	5×0.00056	small	small

Table 2: Information revealment to entities

Info. reveal.	buyer	Broker	seller	TTP	Bank
con_K	YES	NO	YES	YES	NO
M	YES	NO	YES	NO	NO
C	YES	NO	YES	NO	NO
EOO_C	YES	NO	YES	YES	NO
EOR_C	YES	YES	YES	YES	NO
K	YES	YES	YES	YES	NO

4.2 Security Analysis

In previous section, we have analyzed the dispute resolution for this agent-based non-repudiation protocol. Now we analyze varied information revealment to protocol participating entities, see Table 2. Table 3 is a trust analysis of these third parties other than buyer and seller.

Table 3: Trust relationship between buyer and other entities

	trust	authentication	secure channel
TTP	YES	optional (by Broker)	NO
Broker	YES	NO	YES
TPE	NO	YES (by Broker)	NO
CA	YES	NO	NO

Table 4: WPKI contributions to agent-based non-repudiation Protocol

	encryption	digital sig.	Hash func.	cert. magn.
evidence generation	YES	YES	YES	NO
itinerary protection	YES	NO	NO	YES
TPE Protection	NO	YES	YES	NO
malicious host prevention	NO	YES	YES	YES
TTP authentication	NO	YES	YES	YES
BROKER protection	YES	YES	YES	optional
Banks authentication	YES	YES	YES	YES
TPE authentication	NO	YES	YES	YES
mobile client verification	NO	YES	YES	YES
purchase order protection	YES	NO	NO	NO

4.3 WPKI Contributions to Agent-based Non-repudiation Protocol

Deploying a WPKI is a complicated task for security infrastructure which can be successful only by the support of mobile service provider and telecommunication company. In Table 4, we list the contributions of WPKI to non-repudiation protocol and entity protections from WPKI operations and certificate managements.

5 Conclusions

We propose a fair non-repudiation protocol based on wireless PKI and mobile agents. An evidence of mobile payment transaction is generated by WPKI mechanism such that buyer and seller cannot repudiate sending and receiving purchase orders respectively. One challenge of non-repudiation protocols is to avoid any entity to cheat and gain advantage over the other. On the other hand, mobile payment transactions need time information included in evidences for dispute resolutions. Broker generates a mobile agent for buyer which carries this encrypted purchase order to the seller. The advantage of this agent-based protocol is to provide a convenient way for mobile clients to reach non-repudiation for mobile payment transactions. This protocol is feasible for mobile telecommunication service providers and gains the confidence of their mobile clients.

The future research of this paper is to establish and simulate mobile agent-based electronic invoice systems for mobile payments. The author and his research team will continue this work with close connections to MOEA and mTaiwan project. On the other hand, it is a more complicated situation for practical mobile payment systems when merchant servers and mobile clients belong to different WPKI domains; this is related to interoperability issues of different WPKI. The author will discuss this scenario in the future.

References

[Bierman and Cloete 2002] Bierman, E. and Cloete, E.: "Classification of Malicious Host Threats in Mobile Agent Computing", Proceedings of SAICSIT, 2002, pp.141-148.

[Borrell et al.1999] Borrell, J., Robles, S., Serra, J. and Riera A.: "Securing the Itinerary of Mobile Agents through a Non-repudiation Protocol", IEEE 33rd annual international Carnahan conference on security, 1999.

[Braun and Rossak 2005] Braun P., Rossak W.: Mobile Agents, Elsevier, 2005

[Das and Gongxuan 2001] Das, A. and Gongxuan, Y.: "A Secure Payment Protocol using Mobile Agents in an Untrusted Host Environment", LNCS, No.2040, pp.33-41, 2001.

[Du et al. 2006] Du, H., Li, Y. and Zhang, J.: "An Optimistic Fair Non-repudiation Protocol with Semi-Trusted Third Party", J. Graduate School of the Chinese Academy of Sciences, 2006, 23(3), pp.377-381.

[Esparza et al. 2006] Esparza O., Munoz J., Soriano M., Forne J.: "Secure Brokerage Mechanisms for Mobile Electronic Commerce", Computer Communications, 29 (2006), pp.2308-2321.

[Esparza et al. 2003] Esparza O., Munoz J., Soriano M., Forne J.: "Host Revocation Authority: A Way of Protecting Mobile Agents from Malicious Hosts", LNCS No.2722, pp.289-292, 2003.

[Gurgens et al. 2005] Gurgens S., Rudolph C., Vogt H.: "On the Security of Fair Non-repudiation Protocols", International Journal of Information Security, Vol.4, Issue 4, 2005, pp.253-262.

[Ito et al. 2002] Ito, C., Iwaihra, M. and Kambayashi, K.: "Fair Exchange under Limited Trust", LNCS No.2444, pp.161-169, 2002.

[ITU-T 1996] ITU-T, Recommendation: "X.813: Information Technology-Open Systems Interconnection- Security Frameworks in Open Systems. Non-repudiation Framework",1996.

[Jansen and Karygiannis 1999] Jansen W., Karygiannis T.: "Mobile Agent Security", NIST Special Publication, 800-19,1999.

[Kremer et al. 2002] Kremer, S., Markowitch, O. and Zhou, J.: "An Intensive Survey of Fair Non-repudiation Protocols", Computer Communications, 25, pp.1606-1621, 2002.

[Li and Luo 2004] Li B., Luo J.: "On Timeliness of a Fair Non-repudiation Protocol", InfoSecu'04, Nov 14-16, 2004, pp.99-106.

[Lopez 2007] Lopez, A., "Smart card-based agents for fair non-repudiation," *Comput. Netw,* (2007), doi:10.1016/j.comnet.2007.01.014.

[Ma and Tsai 2006] Ma L.,Tsai J.: "Security Modeling and Analysis of Mobile Agent Systems", Imperial College Press, 2006.

[M'Raihi and Yung 2001] M'Raihi, D., Yung M.: "E-commerce Applications of Smart Cards", Computer Network, 36, pp. 453-472, 2001.

[Ou 2004] Ou, C.: "WPKI Implementation, Initial stage, Testing and Experiments", Chunghwa Telecom Lab, 2004, Taiwan.

[Ou and Ou 2008] Ou, C.-M, Ou, C.-R: "Adaptation of Proxy Certificates to Non-repudiation Protocol of Agent-based Mobile Payment Systems", Applied Intelligence, DOI 10.1007/s10489-007-0089-4.

[Pagnia et al. 2000] Pagnia H., Vogt H., Gartner F., Wilhelm U.: "Solving Fair Exchange with Mobile Agents", LNCS No.1882, pp.57-72, 2000.

[Roth and Jalali-Sohi 1998] Roth, V. and Jalali-Sohi, M.: "Access Control and Key Management for Mobile Agents", Comput. & Graphics, Vol. 22, No.4, pp.457-461, 1998.

[Tak et al. 2003] Tak S., Du, Lee Y., Li Y., Park E.: "A Software Framework for Non-repudiation Service in Electronic Commerce Based on the Internet", Microprocessors and Microsystems, 2003, 27, PP.265-276.

[Wilhelm et al. 1998] Wilhelm U., Staamann S., Buttyan L.: "On the Problem of Trust in Mobile Agent Systems", In Symposium on Network and Distributed System Security, pp.114-124, Internet Society, Mar. 1998.

[www.st.com 2004] Data brief, "Smartcard 32-bit RISC MCU with 72kbute EEPROM Javacard HW execution & cryptographic library", www.st.com, April 2004, Rev 2.

[Zhou et al. 1999] Zhou J., Deng R., Bao F.: "Evolution of Fair Non-repudiation with TTP", LNCS No.1587, pp. 258-269, 1999.

[Zhou and Gollmann 1996] Zhou, J. and Gollmann, D.: "A Fair Non-repudiation Protocol", Proceedings of 1996 IEEE Symposium on Security and Privacy, pp.55-61, Oakland, California, May 1996.