Association for Information Systems

AIS Electronic Library (AISeL)

ICEB 2005 Proceedings

International Conference on Electronic Business (ICEB)

Winter 12-5-2005

Mpdtn: A Novel Mobile Payment Scheme for Secure and Private Transactions

Kuenliang Sue

Chung-Hsien Tsai

Mpdtn: A Novel Mobile Payment Scheme for Secure and Private Transactions

Kuen-Liang Sue, Chung-Hsien Tsai
Department of Information Management, National Central University
Jhongli City, Taoyuan County, Taiwan
Tel.+886-3-4267270
Email:{klsue@mgt.ncu.edu.tw, 93423002@cc.ncu.edu.tw}

Abstract: Mobile commerce is becoming more and more popular which makes it possible to purchase goods and services anywhere and anytime. However, traditional payment schemes do not suffice for our demand as more novel commercial services were provided. Therefore, it's urgent to construct a safer and more convenient payment scheme for the forthcoming mobile era.

A mobile payment scheme is proposed in the paper. The scheme called MPDTN provides an ideal mobile payment with dynamic transaction numbers. Through it, consumers can pay fares by using mobile phones no matter in real store or virtual shop. Besides explaining our payment architecture and processes in detail, evaluation of the MPDTN's security from the aspect of defender and different roles of the attackers is provided in the paper. The investigation shows that, MPDTN can not only satisfy security criteria of confidence, integrity, authentication, and non-repudiation but also provide full transaction privacy to consumers.

Keywords: Security and Privacy, Mobile payment.

I. Introduction

Internet has become an indispensable part of our daily life. Various e-commerce including auction, e-shop, entertainment, etc. grows fast. More and more services can be provided via Internet. At the meanwhile, payment is becoming an important issue of the research about E-commerce.

On the other hand, mobile phones become more and more popular with the developing of mobile devices and telecommunication technologies. For example, each person has at least one mobile phone in Taiwan [1]. Besides, Wireless Application Protocol (WAP) and Wireless Markup Language (WML) makes the dream of surfing the internet through mobile devices come true [2]-[6]. Many commercial applications and services are developed and integrated into cell phones. The convenience of cell phone makes it possible to transact without restriction of time and place. The feature seems to explore the door of mobile commerce and attract consumer's eyes. The convenient and secure payment tool will play an important role during the evolution of m-commerce

Furthermore, the traditional plastic and electronic currencies, such as credit card, smart card, or e-cash, have critical shortcomings that we have to overcome. Hackers or attackers can easily pretend to be the legal users and consume at will if they get the credit card numbers and the expiration date. The existing hole of security causes great losses to merchants, consumers, and banks. Most of important, the untrustworthy feeling restrains the development of novel payment tools and e-commerce.

In order to promote the m-commerce and improve existing payment schemes, the securer and more convenient payment tools are needed urgently. Due to the highly popular mobile phones and the well-developed telecommunication technology, payment via handsets is becoming a visual trend other than a dream. More and more investigations focus on the important issue. People expect that handset can do anything - no wallet and no cards.

A mobile payment scheme by using mobile phone is proposed in the paper. Mobile phones are the main payment media for transactions in the scheme. To reduce the risk of security and provide the user with higher privacy, the scheme called MPDTN provides the idea of "Mobile Payment with Dynamic Transaction Number". The second section introduces some of the existing mobile payment mechanisms. The third part goes into detail about MPDTN mechanism and its architecture. Evaluation of MPDTN's security from different points of view is investigated in section four. Finally, conclusions and possible future research are provided.

II. Related Works

Before introducing our model, we first review some existing mobile payment mechanisms and discuss their advantages and disadvantages.

Considering the transaction cost and the convenience, some mobile payment mechanisms using credit card numbers were proposed. Li used consumer's personal cell phone number as the transaction code instead of credit card number [7]. The author claimed that cell phones should take the place of credit cards when making transaction because of the convenience and the security of cell phone.

Step1: Li's payment process can be depicted as Fig.1. It includes the functions which the participators performed and the information transferred between participators. The process of Fig. 1 is illustrated as follows:

Proceedings of the Fifth International Conference on Electronic Business, Hong Kong, December 5-9, 2005, pp. 496 - 504.

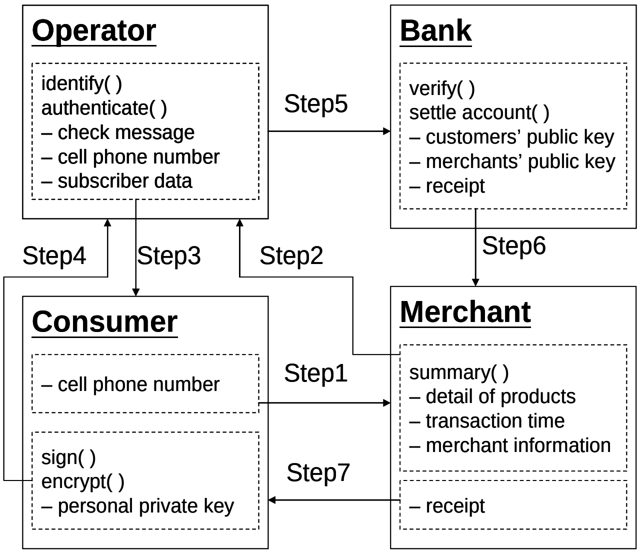

Fig. 1 Process of mobile credit payment

Step2: The consumer can buy products in the real store or the web store, and gives the seller his cell phone number. The merchant summarizes the transaction-related information, such as the product's ID, the transaction date and the customer's cell phone number. This activity is represented by the notation "summary( )". Then, through wired network, he submits these data to the USSD (Unstructured Supplementary Service Data) sever of telecommunication service provider.

Step3: The operator then makes an USSD connection with the consumer through the phone number, and confirms the transaction information with the consumer after authentication.

Step4: After the consumer confirms the transaction information, he will use his personal private key which is stored in the SIM card of the mobile phone to sign the transaction data, and transfer the data back to the operator.

Step5: The operator delivers the signed transaction data to the cooperative bank.

Step6: The bank uses the consumer's public key to verify the consumer's identity and then checks his credit line. The bank also verifies the certificate of the merchant at the same time. After the verification, the bank deals with the transaction and transfers the receipt to the merchant.

Step7: The consumers get the result of the transaction from the merchant.

The advantage of the payment mechanism mentioned above is that we can reduce the consumers' risk even if the phone number is eavesdropped. Usually, it is very risky that consumers provide the credit card number and expiration date when paying with credit card. Besides, the usage of the digital signature in the SIM card can prevent the consumer identity from being forged.

Nowadays, transaction privacy that consumer desired is more and more emphasized. We cannot guarantee the privacy when making transactions by a consumer's phone number. Merchants may gather the consumer's consuming habits or promote their new products by sending messages if they know the phone numbers of the customers. This will bother the consumers to certain extent. Hence, how the payment mechanism provides the transaction privacy cannot be ignored.

Su designed and implemented a mobile payment system with high flexibility [8]. His proposal for mobile payment is similar to the mechanism mentioned before. When the customer transacts, he transferred a fixed "User Identification" to merchant instead of phone number. The merchant summarizes the transaction data and submits it to the operator. Then the operator confirms the transaction to the consumer through the phone number of the corresponding user identification.

Although consumers own their purchasing privacy to some degree by using the "User Identification", the operator still control the private transaction information. Moreover, because the "User Identification" is fixed, the merchants still can collect the consuming habits of certain customer. Therefore, we propose a mobile payment mechanism which not only satisfies the conditions of security, such as confidence, integrity, and non-repudiation, but also provide full transaction privacy by making use of dynamic transaction number. Rubin and Wright proposed a scheme in which a dynamic and limited-lifetime credit card number through symmetric encryption is used [9]. Since the credit card number can just be used a few times, it reduces the security risk. Considering the characteristics of our payment scenario, we adopt the asymmetric encryption protocol to produce a dynamic transaction number, and we believe that it can provide the consumer with the complete privacy during the whole transaction process.

III. Mpdtn Mechanism

The mobile payment mechanism we proposed uses the" dynamic transaction number" to ensure the confidence and privacy. The participators in the transaction process include the merchants, operators, and banks. We have two assumptions in the mechanism:

- ● The operator is trustworthy and will not disclose the sensitive information of the consumers.
- ● The communication network between participators is kept connective.

In the following, we will illustrate the payment mechanism in detail: the architecture of the payment mechanism is described in section one; the interactions between participants are illustrated in section two.

A. Architecture of payment system

The participators in our payment system include:

consumers, merchants, the operator, and banks.

Table 1. Abbreviations of the data used in the proposed mobile payment system

Abbreviation	Description
PhoneNo	The consumer's phone number
BK_R	The bank's private key
BK_U	The bank's public key
OK_R	The operator's private key
OK_U	The operator's public key
$Passwd_{Trans}$	The transaction password which is only known by the consumer and the operator.
$Passwd_{Acct}$	The account password which is only known by the consumer and the bank.
RandNo	A random number.
TransNo	The transaction number only created legally by the consumer.
Price	The total price of the goods.
SerialNo	A serial number generated by the merchant.
Date-Time	The date and time of the transaction.
TransData	The transaction data summarized by the merchant.
Digest	The message digest created by one way hash function. The inputs of the hash function are *TransData* and $Passwd_{Acct}$.
TransRe	The transaction receipt.
$Account_C$	The financial account of the consumer.
$Account_M$	The financial account of the merchant.
$Certificate_M$	The certificate of the merchant.
ID_O	The identity of the operator.
Record	The record of transferring accounts.
PaymentRe	The payment receipt.

- **Consumer:** The consumers can purchase the merchandise with cell phone at a store or website. The operator's public key is stored in the SIM card and used to generate the transaction numbers. The consumers can pay for the purchasing by using the transaction number.
- **Merchant:** The merchants provide goods to consumers. They might be real store or the web store. In the process of transaction, the merchants are responsible for summarizing and transferring the transaction data to the operator.
- **Operator:** The telecommunication operator plays an important role in the payment system. After receiving the transaction data from the merchants, the operator has to confirm this transaction with the consumer using USSD (Unstructured supplementary service data) messages. The operator has asymmetric keys for data encryption, includes the public keys of all cooperative bank. In the proposed payment mechanism, the operator is assumed to be trustworthy. The operator has to check whether if the consumer is a legal subscriber of the payment service.
- **Bank:** The bank is responsible for settlement of accounts and the verification of consumers and merchants. After the settlement, the bank will transfer the receipts to consumer and merchant.

The detail of our payment mechanism is illustrated in next paragraphs, and the abbreviations of the relevant data used in the payment system are shown in Table 1.

B. Interactions between the participators

After the introduction of the participators, we now describe the interactions between the participants of the payment mechanism. There are three phases in our payment scheme: initiation phase, transaction phase, and settlement phase. We demonstrate each phase from the views of the participators.

1) Initiation phase. This phase includes the requirements and the preparations of each participant before the payment mechanism performs. Following, we will illustrate the initiation phase from aspects of each participant.

- **Consumer:** First, the consumer should have the mobile device, such as cell phone or PDA which the telecommunication module is embedded in. The mobile device must have the capability of data storage and cryptographic computing. In addition, the mobile device can also adopt the technology of short-distance wireless transmission to facilitate the procedure of mobile payment. The consumer needs to apply for the mobile payment service and transfer his financial account ($Acct_C$) to the operator. Then, the operator issues a personal transaction password ($Passwd_{Trans}$) and the public key of the operator (OK_U) to the consumer and stores these sensitive data in the SIM card of the cell phone.

In order to reduce the waiting time of payment, the consumer could generate the transaction number (*TransNo*) in advance before going shopping. The transaction number is generated by using the operator's public key to encrypt the consumer's phone number (*PhoneNo*), transaction password, and a random number (*RandNo*). The random number is generated by the cell phone and used to make the transaction number dynamic. After the generation of the transaction number, the customer can start to use the mobile payment service.

- **Merchant:** What ever real or virtual store the merchant is, it must have the capability of summarize the transaction information. The merchant can communicate with the operator or the bank through the Internet. The real store needs a printer to print out the transaction receipt (*TransRe*). The web store can show the transaction receipt on the browser for the consumer to print it out. Besides, the real store can also facilitate the mobile payment by adopting the short-distance wireless transmission device.

For the security concern, the merchant need to apply for a digital certificate and download the certificate of the operator issued by the trusted certificate authority (CA). In the payment process, the merchant uses the public key of the operator to encrypt the transaction data.

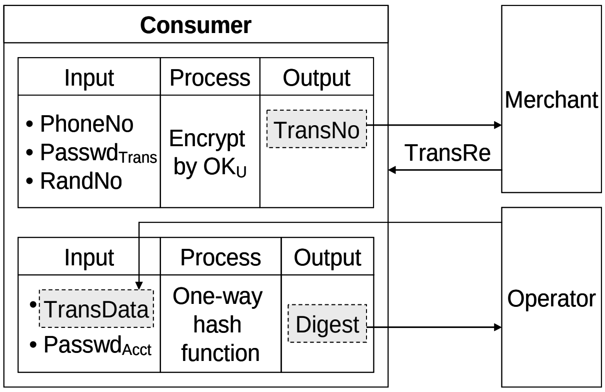

Fig. 2 Transaction phase of the consumer

- ● **Operator:** As for the operator, they have to maintain additional data in the database, such as the transaction passwords and the identities of the consumers' banks. After the customer applies for the mobile payment service, the operator will store the consumer's sensitive data in the secure database. The relation between the sensitive data and the corresponding consumer's phone number are protected by the operator. The operator also applies for its digital certificate and downloads all cooperative banks' certificates from CA.
- ● **Bank:** The bank also has to store additional data in the database, such as the account password (*$Passwd_{Acct}$*) of the consumer which is different from the password of the cash card. Besides, the bank needs to maintain the transaction record for future inquiries. The same with the operator, the bank need to apply for its certificate, too.

2) Transaction phase. This phase describes the data transmission and processing of all participators during the payment process. We focus on the consumer, the merchant, and the operator.

- ● **Consumer:** To make the payment, the consumer transfers the transaction number and the identity of the operator (*ID_O*) to the merchant. The transaction number is a ciphertext encrypted by using the public key of the operator. As mentioned in the initiation phase, several transaction numbers could be generated before the consumer goes shopping. After the merchant summarizes the transaction information, the consumer receives a transaction receipt as an evidence of this transaction from the merchant. The transaction receipt includes all transaction details, such as the product name, unit price of the product, and so on.

Then, the consumer has to wait for the USSD message from the operator to confirm the transaction. If the transaction information is correct, the consumer has to input the account password (*$Passwd_{Acct}$*) as a confirmation of his identification. The cell phone will hash the transaction data and the account password by a hash function while the account password is valid. After the hash function being performed, it will create a message digest (*Digest*). Finally, the consumer transmits the message digest back to the operator to finish the transaction confirmation as shown in Fig. 2.

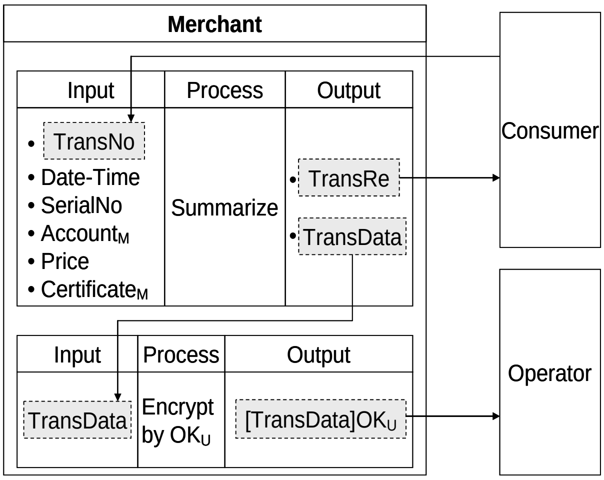

Fig.3 Transaction phase of the merchant**s**

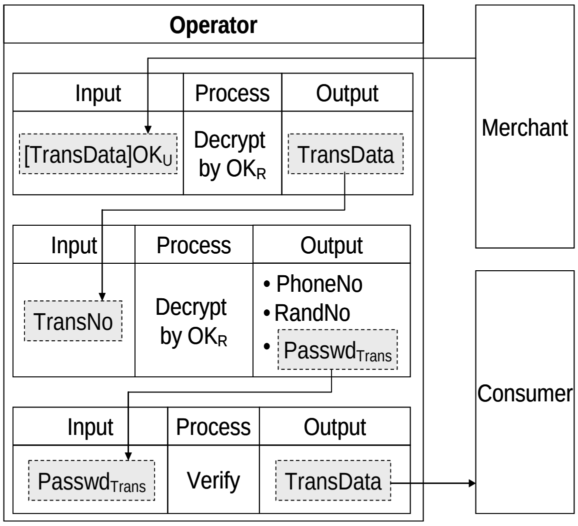
Operator
Input
Process
Output
$\text{[TransData]OK}_{\text{U}}$
Decrypt by OK_{R}
TransData
Merchant
Input
Process
Output
TransNo
Decrypt by OK_{R}
• PhoneNo
• RandNo
• $\text{Passwd}_{\text{Trans}}$
Input
Process
Output
$\text{Passwd}_{\text{Trans}}$
Verify
TransData
Consumer

Fig. 4 Transaction phase of the operator

- **Merchant:** The merchant summarizes the required information into the transaction data (*TransData*), and encrypts the transaction data by using the operator's public key. Then, the merchant prints out the transaction receipt to the consumer as a verification of this transaction. All details about this transaction such as the item name and unit price are included in this receipt. The merchant transmits the transaction data to the operator according to the ID_O of the consumer for further confirmation. As shown in Fig. 3, the transaction data transferred includes the relative information except the details of the goods in order to ensure the transaction privacy of the consumer.
- **Operator:** The operator takes charge of the verification of the consumer and the transaction. After the operator receives the transaction data from the merchant, it decrypts the transaction data with its private key (OK_R) to get the transaction number. The operator further decrypts the transaction number and verifies the consumer's transaction password. If no error occurs in the verification, the operator will transfer the transaction data to the consumer through USSD connection for further check and waits for the consumer's response as depicted in fig. 4.

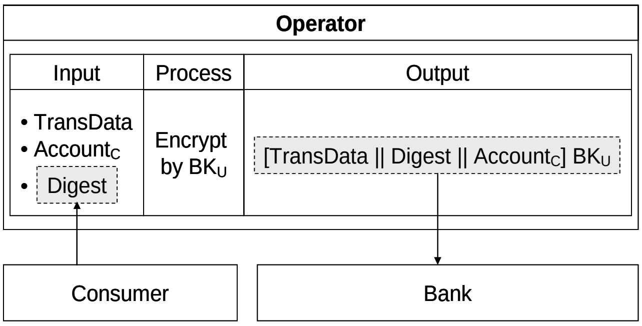

Fig. 5 Transaction phase of the operator (cont.)

Then, the operator will receive the message digest from the consumer if the transaction data is correct. The operator encrypts the transaction data, the message digest, and the consumer's bank account (*$Account_C$*) with the bank's public key (*BK_U*) and transfers these data to the cooperative bank for account settlement as shown in Fig 5.

3) Settlement phase. The settlement phase describes the verification and account settlement performed by the bank. When the bank receives the encrypted data from the operator, it uses its private key (*BK_R*) to decrypt the ciphertext. The bank can find the account password of the consumer by the corresponding financial account. Then the bank calculates the hash function over the concatenation of the transaction data and the account password of the consumer. If the comparison between the output of the hash function and the message digest from the operator is the same, the bank will further check the consumer's credit line and complete account settlement.

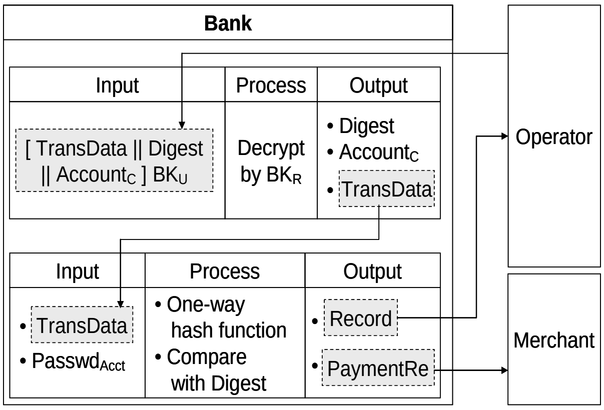

Fig. 6 Settlement phase of the bank

After settling account, the bank sums up the transaction and transfer the payment receipt to the merchant. The bank also needs to transmit the transaction record to the operator for avoiding the possible dispute. Then the merchant prints the payment receipt to the consumer, as shown in Fig. 6. Every transaction has to go through the transaction phase and settlement phase.

C. Overview of the payment process

In this section, we go into detail about the payment process of our scheme. Some notation should be explained at first. X → Y : Z denotes that a sender X sends a message or data Z to the receiver Y, h( ) denotes a one way hash function, M || N denotes a concatenation of data M and N, and [I] J denotes a message I encrypted by key J. In our payment scheme, the payment process includes seven steps. The transaction steps are as follows:

Step 1) Consumer → Merchant : *TransNo*, ID_O
Step 2) Merchant → Consumer : *TransRe*
Merchant → Operator : [*TransData*] OK_U
Step 3) Operator → Consumer : *TransData*
Step 4) Consumer → Operator : *Digest*
Step 5) Operator → Bank :
[*TransData* || *Digest* || $Account_C$] BK_U
Step 6) Bank → Merchant : *PaymentRe*
Bank → Operator : *Record*
Step 7) Merchant → Consumer : *PaymentRe*

In step 1, when the consumer shops at a real store or a web store, he has to transfer the *TransNo* to the merchant. The *TtransNo* is generated as follows:

$$TransNo = [PhoneNo \;||\; Passwd_{Trans} \;||\; RandNo]\; OK_U \quad (1)$$

The consumer can generate several transaction numbers and store them in the cell phone to facilitate the payment.

In step 2, after merchant received the *TransNo*, it summarizes the transaction information into *TransData*.

$$TransData = TransNo \parallel Date\text{-}Time \parallel SerialNo \parallel Account_M \parallel Price \parallel Certificate_M \quad (2)$$

Then, the merchant prints out the transaction receipt to the consumer. The merchant also encrypts the *TransData* with OK_U and transmits it to the operator according to the ID_O received from consumer.

In step 3, the operator decrypts the data received from the merchant and gets the *TransNo*. The operator further decrypts the *TransNo* and gets the $Passwd_{Trans}$ of the consumer. The operator will check if the transaction password is correct. If the $Passwd_{Trans}$ is valid, the operator will transmit the *TransData* to the consumer through USSD connection.

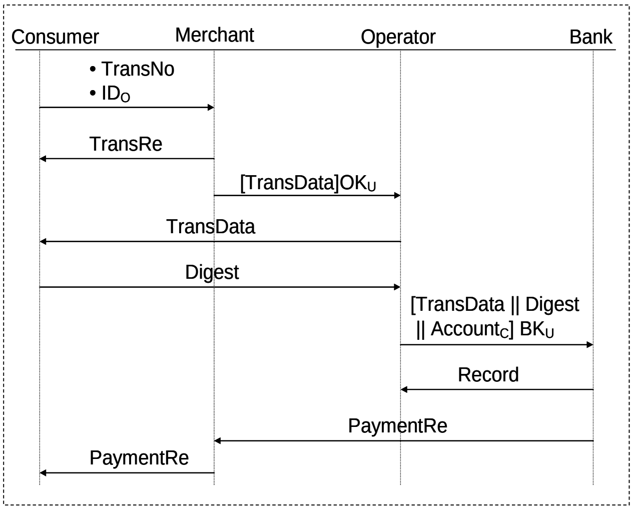

Fig. 7 Data flow of transaction procedure

In step 4, the consumer checks the *TransData* received from the operator. If this transaction is confirmed, the consumer is asked to enter the $Passwd_{Acct}$ for a hash function:

$$Digest = \mathrm{h}\,(TransData \parallel Passwd_{Acct}) \quad (3)$$

The cell phone will create a message digest and send it back to the operator. But if the consumer rejects the payment or enters the wrong $Passwd_{Acct}$ three times, the operator will transfer a message to inform the merchant about the breach of the transaction.

In step 5, the operator summarizes the relative transaction information and encrypts them with the BK_U. The operator transmits the encrypted data to the bank through wired network.

In step 6, the bank decrypts the data received from the operator with its BK_R. The bank will find the corresponding $Passwd_{Acct}$ of the consumer according to the $Account_C$ and check if the $Passwd_{Acct}$ is valid. Then, the bank calculates the same hash function and compares it with the *Digest* as follows:

$$\text{Check if} \quad \mathrm{h}\,(TransData \parallel Passwd_{Acct}) = Digest \quad (4)$$

If the result of the hash function is the same with *Digest*, the bank will settle accounts and transmit the payment receipt to the merchant. At the same time, the bank also transmits the transferring record to the operator and sends the short message to notify the consumer. In step 7, the merchant prints out the payment receipt to the consumer. The web store can show the payment receipt on the web browser, and the consumer can print it by himself.

Above, the payment mechanism has been demonstrated in detail. All data transferred between the participants are shown in Fig. 7. According to the security criteria, we evaluate our payment mechanism from different points of view in section four.

IV. Analysis of Security and Discussion

When we talk about security and related subject, some security requirements should be achieved, as mentioned in [10]-[13]. In this section, we evaluate our payment mechanism from two aspects: the aspect of the security criteria and the aspect of the attacker's role.

A. Evaluate from the aspect of security criteria

1) Confidentiality. We first consider the aspect of data storage; the sensitive data of transaction and the encryption keys are stored in the SIM card which is a tamper-resist device. And if the cell phone was lost or stolen by others, the verification of the PIN and the $Passwd_{Acct}$ prevent the cell phone from misusing by someone else. It is proven that even the SIM of legal user is cloned, the fraudulent usage can be detected quickly [14].

As for data transmission, the data between the merchant and the operator or between the operator and the bank can be transferred through the wired network such as ADSL, which use SSL transaction protocol to ensure the security of data. SSL is also a practical solution for ensuring end-to-end security of wireless Internet transactions even within today's technological constraints [15]. In our payment scheme, the data transferred in the wired network is protected by the public-key based algorithm which can prevent the confidential attack effectively [16]. For example, the RSA public-key encryption algorithm is used for the protection between the bank and the operator, and illustrated as follows:

The Operator has the public key of the bank: $BK_U = \{e, n\}$ and the bank has the corresponding private key: $BK_R = \{d, n\}$ (n is calculated from $p*q$, p *and* q are both prime, e is a selected integer and the greatest common divisor of e and (p-1)(q-1) is 1, d is calculated from $d = e^{-1}\mathrm{mod}((p\text{-}1)(q\text{-}1))$). Let M be the plaintext and C be the cipertext. The operator encrypts the secret transaction information with BK_U :

Operator : $C = M^e \pmod{n}$, $M<n$ (5)

Only one that has corresponding private key can decrypt the ciphertext and gets the secret information (i.e. in the example above, only legal bank that has the privet key BK_R can decrypt the ciphertext).

Bank : $M = C^d \pmod{n} = M^{ed} \pmod{n}$ (6)

It is infeasible to determine d given e and n. Currently, a 1024-bit key size is considered strong enough for virtually all applications. Besides, the secure connection of USSD between the operator and the consumer is provided by the signal protection mechanisms of GSM/UMTS [17].

Table 2. Key sizes for equivalent security levels (bits).

Symmetric	ECC	RSA/DH/DSA
80	163	1024
128	283	3072
192	409	7680
256	571	15,360

2) Privacy. The transaction privacy of the consumer depends on the *TransNo* — it is very difficult for the merchant to get personal information of the consumer because it has no corresponding key to decrypt the *TransNo*. The *TransNo* is protected by the encryption of the asymmetric cryptography which is hard to be broken [18]. Some cryptographic algorithms which are suitable for the wireless communication were proposed, such as Elliptic Curve cryptography (ECC) [19]. A 571-bit ECC is currently equivalent in security to 15,360-bit RSA, as shown in Table 2. The smaller key size for equivalent security levels accounts for the performance advantages to be obtained from substituting ECC for RSA, especially in wireless environment. The Elliptic Curve cryptography is derived from the equation of elliptic curve:

$$y^2 = x^3 + ax + b \qquad (7)$$

where a and b are elements of a finite field with p^n elements, p is a prime greater than 3. The detail about Elliptic Curve cryptography can be found in the reference [20].

Under the proposed mechanism, the merchant is unable to collect the purchasing habits of a consumer because of the secure protections of the asymmetric cryptography suitable for small hardware, such as ECC.

In the aspect of the operator and bank, only total amount of the price is in the transaction data. So, even though the operator and the bank knew well about the real identity of the consumers, they cannot know what merchandise the consumer has purchased (as shown in Fig. 4 and Fig. 6). In our payment mechanism, the consumers have the overall privacy.

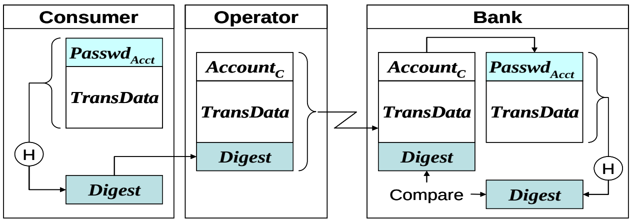

Fig. 8 Authentication using a one-way hash function

3) Authentication. The consumer is authenticated three times in our payment mechanism:

First, the cell phone verifies the PIN of the consumer.

- Second, the operator verifies the $Passwd_{Trans}$ after decrypting the *TransNo*.
- Third, the bank verifies the $Passwd_{Acct}$ of the consumer through message authentication using a one-way hash function depicted in Fig. 8.

With those tree authentications, the risk of counterfeit is reduced to the minimum.

As for the merchant, the bank authenticates the merchant by verifying its certificate. The certificate of the merchant is issued from the trusted third party which could be the governmental institution, so it can retrain the malicious merchant. Sulin proposed a new design of trusted third party which is built on the current models of CAs but has enriched functionality [21]. They proposed a Trusted Third Party System Strategy (TTPSS). TTPSS is a sequential equilibrium strategy of the trusted third party system stage game. The TTP model can be very effective in promoting small business online transactions and consumer-to-consumer transactions. This authentication model could also be adopted in our payment scheme to expend the participators and to ensure the transaction effectiveness.

4) Non-repudiation. After the consumer confirms the transaction, he has to enter the $Passwd_{Acct}$ for the calculation of message digest. Then, the bank authenticates the consumer by verifying the message digest. Only the legal consumer and the bank can calculate the same *Digest* because the $Passwd_{Acct}$ is only known by them. The transaction is confirmed if the *Digest* was correctly verified, and the consumer cannot deny the transaction. The bank transmits the payment receipt to merchant after account settlement, so the merchant can avoid the risk of consumer's bad debit.

5) Integrity. After the merchant summarizes the *TransData*, it prints out the *TransRe* to the consumer. The bank transfers a *PaymentRe* to the merchant after the account settlement (as shown in Fig. 2). Then the merchant print the *PaymentRe* to the consumer. These two receipts can be combined through the *SerialNo* of the transaction. The consumer can ensure the integrity of the transaction by comparing these two receipts.

6) Other Discussion. Besides the security criteria mentioned above, our payment mechanism is also feasible. The main reason is that it will not take great cost to the participator to adopt the payment mechanism into his business model.

The consumer can generate the *TransNo* before go shopping. And the computational load can be reduced in the payment process because only hash function is performed by the cell phone.

B. Evaluation from the aspect of attacker's role

There are four participators in our payment scheme and any of them might be malicious except the operator. The operator is assumed to be trustworthy in our mechanism. We will discuss the possible attacks of the malicious participators and how to prevent them in our payment scheme in this section.

1) Malicious merchant—deny the transaction. In our payment scheme, the merchant need to deliver the goods to the consumer after receiving the *PaymentRe*. The malicious merchant might refuse to deliver the goods and conceal the *PaymentRe* from the bank. But while the bank completes the account settlement, it will not only transfer the *PaymentRe* to the merchant but also send the consumer a short message which is used to notify the consumer of the completion of the payment. The bank also needs to transmit the transaction record to the operator for future inquiry. Therefore, after the consumer received the short message, the truth of the payment can be proved. The consumer can demonstrate the evidence of the payment from the transaction record preserved in the operator and bank.

2) Malicious merchant—steal the *TransNo* from the consumer. The malicious merchant might try to get the legal *TransNo* of the consumer by hook or by crook. If the merchant uses the *TransNo* which is stolen from the consumer to forge a transaction, the consumer will be aware of the misuse of the *TransNo*. In the step 3 of our payment process, when the operator confirms the transaction with the consumer through USSD connection, the consumer can refuse the transaction. Moreover, once the consumer found the misappropriation of the *TransNo*, he (she) can inform the operator to trace the malicious merchant through the digital certificate of the merchant.

3) Malicious consumer—fabricate the *TransNo*. The malicious consumer might try to forge the *TransNo* of another legal consumer to make transaction. They might create a *TransNo* by getting wise to another consumer's *PhoneNo*. But the fake *TransNo* will soon be revealed because the malicious consumer cannot get the exact $Passwd_{Trans}$ of the corresponding *PhoneNo*. Even if the malicious consumer is lucky enough to guess the right $Passwd_{Trans}$, he will not pass the transaction confirmation in the step 3 and the verification of $Passwd_{Acct}$ in the step 4 of our payment scheme. The probability of guessing right the $Passwd_{Trans}$ and the $Passwd_{Acct}$ at the same time is very little.

4) Malicious bank—disclose the $Passwd_{Acct}$. Generally, the bank is trusty. However, the employee of the bank might benefit from disclosing the important consumer information. For example, the employee might eavesdrop to the $Passwd_{Acct}$ of the consumer and sell it to the evildoer. But our payment mechanism is secure enough to against the attack which the $Passwd_{Acct}$ is misused. As for the consumer, the exact $Passwd_{Trans}$ and $Passwd_{Acct}$ are needed in every transaction. The transaction can not be complete without one of these two passwords. Besides, the transaction confirmation by the operator can prevent the transaction relative passwords are misused by malicious consumer. As for the merchant, it delivers the good to the consumer only when the *PaymentRe* is received and no cancel message is received from the operator. The consumer authentication and the transaction confirmation executed by the operator can prevent the consumer and the merchant from losing on illegal transaction.

5) Malicious merchant and bank—tamper the *TransData*. The malicious merchant might collude with the employee of the bank, and devise a way to tamper the *TransData* to make profit illegally. For example, the employee of the bank might tamper the *Price* of the transaction in our payment process. Because the bank knows the $Passwd_{Acct}$ of the consumer, it can forge the original *Digest* and confirm the transaction. The malicious merchant might use the fake *PaymentRe* to take the place of the real one. But while the bank transfers the fake price into the account of malicious merchant, the *Record* transmitted to the operator in the step 6 of the payment process will reveal the illegal activity. The *Record* is generated through the secure mechanism of the bank, and it is not easy to be tampered.

6) Malicious consumer and bank—forge the *PaymentRe*. The malicious consumer may cooperate with the employee of the bank. The malicious consumer might pretend to purchase goods in the merchant and refuse to pay for the transaction actually. Then, the employee of the bank may try to forge a *PaymentRe* according to the confirmation data transmitted from the operator to the consumer. But in our payment mechanism, if the legal consumer rejects the payment, the operator will notify the merchant that the payment is cancelled by the consumer. So, even if the merchant received the fake *PaymentRe*, it will have the sufficient reason to deny the transaction.

After the discussion and evaluation, our payment mechanism can ensure high security for all participators.

7) Malicious consumer and merchant— repudiate the transaction. The malicious consumer might collaborate with malicious merchant to make the transaction inconsistent, and request for the compensation to the bank. But the bank proceeds to transfer account only after the identifications of the consumer and the merchant are authenticated and the transaction is confirmed by the legal consumer. Therefore, the merchant and the consumer cannot deny the transaction and have no reason to ask the bank for compensation.

V. Conclusion

The development of the Internet, handset devices, and telecommunication technologies are changing the way of our life extremely, especially in commerce. Lots of novel business models emerge rapidly. However, the most important and insecure stage in the transaction is payment. Without an appropriate payment mechanism, any business model will be hardly put into practice. Therefore, we have an urgent need for designing a securer and more convenient payment mechanism.

The payment mechanism we proposed adopts the cell phone to be the payment tool. By making use of the transaction number, our payment mechanism provides many advantages:

- **Security**: Our payment scheme meets security criteria which includes confidentiality, authentication, integrity, and non-repudiation during the payment process. Besides, the risk can be minimized when the consumer loses the cell phone or the cell phone is forged because our method provides multiple authentications.
- **Full transaction privacy**: The merchant cannot get the real identification of the consumer because the transaction number is dynamically changed and protected by the asymmetric encryption. Besides, the operator and the bank cannot acquire the detail of the merchandise purchased by the consumer except the total amount of price. Therefore, no one except the consumer can gather the transaction habit.
- **Convenience**: The time of the payment can be shortened because the time-consuming operation of the encrypt algorithm can be done in the initiation phase. In other words, the transaction number can be generated and stored in the cell phone before the consumer goes shopping.
- **Low computational load of the mobile phone:** The operation of the consumer in the transaction phase can be only a one-way hash function. The speed of one-way hash function is approximately 100 times faster than that of the encryption/decryption of the secret-key system and the speed of the encryption/decryption of the secret-key system is about 100 times faster than that of the signature/verification of the public key system [13].
- **Feasibility:** In addition, the participators can adopt our payment scheme into their business model without additional cost of hardware. And it is implemented based on the existing network environment.

Besides the advantages mentioned above, we also evaluate the payment scheme from the aspect of security criteria and the attacker's role in detail. Our payment scheme has been proved that it can effectively prevent any participator's malicious attack.

Our payment mechanism is very suitable for the payment from medium to large amounts of money because it has overall protection of security and full transaction privacy. And it can be more flexible if we integrate it with other payment systems, such as micro-payment system, e-cash and so on. Our mobile payment scheme has made great progress toward a more omnibus and secure payment scheme for the new era.

References

[1] Wei-Han Hsu, "Analysis of Mobile Payment Systems", *Master Theses, Department of Information Management, National Taiwan University*, September 2003.

[2] David McKitterick, and Jim Dowling," State of the Art Review of Mobile Payment Technology", *TCD Computer Science Technical Reports*, 2003, TCD-CS-2003-24.

[3] Cheng-Huang Yen, *Mobile and wireless communications*, Key Hold Information INC, 2003.

[4] WAP Forum, "Wireless Application protocol WAP 2.0 Technical white paper", *Wireless Application Protocol Forum Ltd*., 2002.

[5] Samir Omar, Cecilia Chong, Wei Zhang, "New Java mobile handset browser to support both WML and HTML", *IEEE, Control, Communications and Signal Processing, First International Symposium on*, 2004, 103-106.

[6] Varshney, U., "Mobile payments", *IEEE Journal, Computer,* 2002, 35(12), 120-121.

[7] Chia-En Lee, "A Secure and Convenient Mobile Credit Payment Scheme Using Public Personal Information", *Master Theses, Department of Information Engineering and Computer Science, Feng Chia University*, 2003.

[8] Wen Hung Su, "Adaptive Payment System for Mobile Environment", *Master Theses, Department of Electrical Engineering, National Taiwan University***,** 2002.

[9] Aviel D. Rubin, and Rebecca N. Wright, "Off-line generation of limited-use credit card numbers", *Financial Cryptography Conference*, 2001, 196-209.

[10] Mobile Payment Forum, "Mobile payment forum white paper", 2002.

[11] Neuman, B.C., "Security, payment, and privacy for network commerce", *IEEE Journal, Communications*, 1995, 13(8), 1523-1531.

[12] Yuanjun Dai, Lihe Zhang, "A security payment scheme of mobile e-commerce", *Communication Technology Proceedings, 2003. ICCT 2003. International Conference on*, 2003, 2, 949-952.

[13] Wei-Bin Lee, Chang-Kuo Yeh, "A New Delegation-Based Authentication Protocol for Use in Portable Communication Systems", *IEEE Transactions on Wireless Communications*, 2005, 4(1), 57-64.

[14] Yi-Bing Lin, Ming-Feng Chen, Rao, H.C.-H., "Potential fraudulent usage in mobile telecommunications networks", *Mobile Computing, IEEE Transactions on* , 2002, 1(2), 123-131.

[15] Gupta, V., Gupta, S., "Experiments in wireless Internet security", *Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE*, 2002, 2, 860-864.

[16] William Stallings, *Network Security Essentials*, Prentice Hall, 2000.

[17] S. Schwiderski Grosche and H. Knospe, "Secure mobile commerce", *Electronics & Communication Engineering Journal*, 2002, 228-238.

[18] David Pointcheval, "Asymmetric cryptography and practical security", *Journal of Telecommunications and Information Technology*, 2002, 41-56.

[19] Lauter, K., "The advantages of elliptic curve cryptography for wireless security", *Wireless Communications, IEEE*, Feb 2004, 11(1), 62-67.

[20] Masaaki Shirase and Yasushi Hibino, "An architecture for elliptic curve cryptograph computation", *ACM SIGARCH Computer Architecture News*, 2005, 33(1), 124-133.

[21] Sulin Ba, Andrew B. Whinston, Hang Zhang, "Building trust in the electronic market through an economic incentive mechanism", *Proceeding of the 20th international conference on Information Systems*, 1999, 208-213.