2009 First International Workshop on Education Technology and Computer Science

# B2B Electronic Payment Protocol Based on iKP

Hong Wang
Department of Computer Science and Application
Shenyang Normal University
Software College
Shenyang, China
horoscope_leo@126.com

XiaofenZhang
Department of Computer Science and Application
Shenyang Normal University
Software College
Shenyang, China
xiaofen_zh2003@163.com

JingSun
Department of Computer Science and Application
Shenyang Normal University
Software College
Shenyang, China
sunjing431@tom.com

***Abstract*—with the increasing development of the Internet and electronic commerce, electronic payment systems have gradually become an important issue nowadays. Business-to-business E-commerce model involves a complex process with large transaction size, so that B2B payment is the next focus of the popular research topics on electronic commerce. Though there are many existing e-payment protocols designed for transactions of low-to-medium volumes and medium-to-high value, these schemes only suit for B2C and C2C E-commerce model. iKP is one of the most popular macro payment schemes using in B2C model. Considering that B2B payment is evolution of B2C payment, through analyzing the similarity and difference between B2B and B2C payment, as well as pointing out the virtues and drawbacks of iKP, this paper describes an improved iKP protocol based on B2B. The proposed protocol not only preserves the security properties of iKP but also achieves the needs of B2B payment. The future work will concentrate on satisfying different payment conditions of B2B e-payment.**

***Keywords-E-payment; B2B; iKP; macro payment; fairness;micro-payment***

## I. INTRODUCTION

With the rapid growth of the E-commerce, secure electronic payment systems become one of bottle-necks in the future developing process of E-commerce. In this paper, we mainly discuss a family of secure electronic payment protocols-iKP (i-Key-Protocol, i=1,2,3). These protocols implement credit card based transaction between the customer and the merchant while using the existing financial network for clearing an authorization [1]. They can be able to extend to other payment models, such as debit cards and electronic checks, but it mainly are applied to commercial model of B2C.

Considering the difference between B2B and B2C model, this paper proposes an improved iKP protocol to realize electronic payment process in the B2B model.

The rest of this paper is organized as followed: Section2 gives a comparison between B2C and B2B commercial model. In Section3, it provides a brief summary of the history of iKP. The improved iKP is described and analyzed in Section4. Then, the last part gives the conclusion.

## II. COMPARISON BETWEEN B2C AND B2B MODEL

The paper puts emphasis on the E-payment protocol, so that the comparison starts from this aspect, that is, focus on the characteristics related with E-payment activities.

### *A. E-payment tools*

In recent years, China's e-payment has developed rather rapidly, featuring a continuous emergence of new types of e-payment tools as well as rise of trading volume via e-payment. E-payment B2C business model refers to various business users provides payment services to consumers through E-payment service providers' platforms.

The below table Ⅰ gives respectively the main used e-payment tools in B2B and B2C model. It shows that the number of E-payment tool's type adopted in B2B is relatively little than B2C model.

### *B. Micro Payment vs. Macro Payment*

In fact, B2B transactions account for about 95% of e-commerce transaction in China, while 90% of B2B deals are sealed offline.

According to [3] and [4] classified e-payment systems as follows:

- Micro Payment (<$10) that is mainly conducted in C2C and B2C transactions.
- Consumer Payment is also called macro payment which has a value between $10 and $500. It is conducted mainly in B2C transactions.
- Business Payment that has value more than $500. It is conducted mainly in B2B transactions.

It indicates that the amount of B2B transactions is large. For macro-payment in B2C model, the payment process is completed by single payment, while in the process of B2B payment it needs multi-payment. The normal way to B2B offline payment is to prepay in certain proportion, after accept the goods, the remainder payment is finished. Our model will handle multi-payment B2B transactions.

In B2B transactions, there are many other payment requirements with the changes of conditions and environments. Recently, a lot of researches on macro and micro payment have been present，see[5],[6]. However, these schemes are not practical for B2B payment.

978-0-7695-3557-9/09 $25.00 © 2009 IEEE
DOI 10.1109/ETCS.2009.230

TABLE I. E-PAYMENT TOOLS

| Commercial model | E-payment Tools |
|---|---|
| B2B | E-Bank, E-Draft |
| B2C | Bank Card<br>(debit card, credit card ,membership card, deposit account)<br>E-cash,E-check, E-Bank |

## III. iKP HISTORY AND RELATED WORK

iKP (Internet Keyed Payment Protocols) was developed by IBM Research Labs Zurich and Watson Research Centre in 1995 and became an open industry standard. One important difference between iKP and most of other proposals which were proposed from 1994 to 1996 is that iKP is not just a paper design: The "Zurick iKP Prototype (Zip)" is a fully operational prototype of 2KP and 3KP[2].

### A. The iKP Payment Model

The payment system involves three parties: the Customer, the Merchant, and the Acquirer gateway, see Fig1. The Customer is the party to conduct the payment while the Merchant is the party to accept the payment. The Acquirer is simply a front-end to the current unchanged infrastructure for credit card clearing and authorization. It is assumed that credit cards are issued to buyers from banks which are called issuers. BIN stands for Bank Identification Number, and each bank has an only BIN as part of credit card numbers. It is also assumed that each customer receives a credit card from an issuer and also maintains a PIN that stands for Personal Identification Number.

### B. iKP Protocol Flow

The followe is a simple description of iKP protocol flow, see Fig2.

- C constructs Initiate message and notifies M to start this protocol;
- M responds with an Invoice message;
- C confirms the information of the transaction and sends the Payment flow to M;
- M requests payment authorization from A by sending Auth-Req message;
- A obtains payment commands from C and constructs Auth-Resp message to response the payment request.
- In the final flow, M verifies A's signature and forwards both response flow and signature of A to C.
- M finishes the shipment of goods and the service provision.

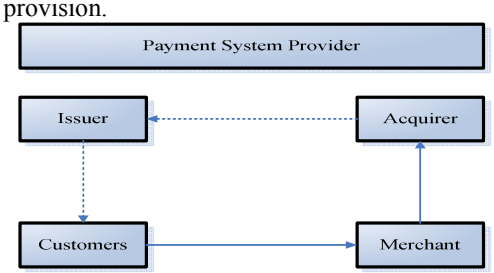


Figure 1. iKP Payment System Model

TABLE II. INITIAL INFORMATION OF NEW PROTOCOL

| Communication party | Initial information |
|---|---|
| Purchaser（P） | DESC, $PK_{CA}$, $SK_P$, $CERT_P$ |
| Supplier（S） | DESC, $PK_{CA}$, $SK_S$, $CERT_S$,$CERT_A$ |
| Acquirer (A) | $PK_{CA}$, $SK_A$, $CERT_A$ |

### C. iKP Protocol Analysis

iKP solves security problems in e-payment from many aspects:

- All iKP protocols are based on public-key cryptograph, but they vary in the number of parties. This number is indicated by the name of the individual protocols（1,2,3）KP. In this paper, we focus on 3KP.
- iKP guarantees information isolation of each party. The merchant can not obtain account number of the client while the acquirer can not obtain shopping list of the client.
- iKP provides multiple parties identification authentication.

The limits of the iKP are:

- iKP provides micro-payment as well macro-payment in single time. We need multiple times payment in B2B model.
- iKP only provides identification authentication in payment step, but does not provide authentication in shipment step.
- The issuer does not provide evidence that indicates the customer has received the good.

## IV. THE PROPOSED PAYMENT PROTOCOL

In this new protocol also involves three parties: the supplier(S), the purchaser (P), and the acquirer (A). The table Ⅱ shows the initial information of each party.

### A. Components of the Protocol

Some of the following symbols will be used to represent the parameters for our scheme. The others following notation are used to denote cryptographic operations.

Keys: $PK_X$, $SK_X$, $CERT_X$

$PK_X$, $SK_X$:Public and secret key of Party X

$CERT_X$: Public key certificate of Party X issued by CA.

PRICE: The total price of the order

Percentage: proportion of prepayment

IDp,IDs:Acccount number of purchaser and supplier.

DESC: The description of the order.

Common: PRICE, PERCENTAGE, $ID_s$,$TID_s$, DATE, $ID_p$, H(DESC, $SALT_p$), H(C)

Clear: $ID_s$, $ID_p$, $TID_s$, DATE, H(C), H(Common)

H(): Secure hash function

Ex(): Public-key encryption using PKx

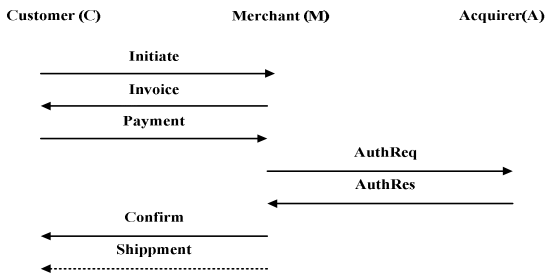


Figure 2. iKP Protocol Flow

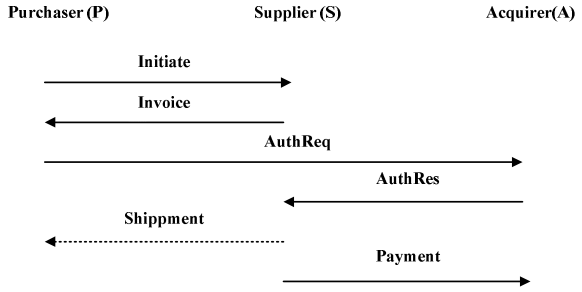


Figure 3. Improved iKP Protocol Flow

### B. *New Protocol Flow*

The proposed protocol is designed by improving iKP and using its basic idea. To make the structure clear, we will describe them in Fig3. The protocol is shown as follows:

*1) Initiate P→S:* SALTp, CERTp, H(DESC,SALTc) , H(np)

*2) Invoice S→P:*Clear, $Sig_S$

*3) AuthReq P→A:* $E_A$(Price,Percentage,$ID_p$,$Sig_p$), Clear

*4) AuthRes A→S:* TID,AuthTime,RespCode and $Sig_p$

*5) Shipment:*

*a)* S→P: $n_p$

*b)* S→P: Goods and Services

*c)* P→S: $n_s$

*6) Remainder payment S→A：* $n_s$, RespCode, TID, AuthTime

### C. *New Protocol Flow Description*

The purchaser and the supplier conforms to consistence through security channel about the order information (DESC), price (PRICE) and propotation of prepayment (PERCENTAGE) of the order.

*1) Initiation*

*a)* Purchaser computers $H(n_p)$ by generating random number $n_p$. Then, $n_p$ should be keep secret by purchaser. In shipment step, supplier needs $n_p$ to confirm identification of the purchaser.

*b)* Purchaser saves $H(n_p)$.

*c)* Purchaser generates another enough long random number $SALT_p$ to be used for "salting" the hashing of merchandise description (DESC) in subsequent flows, which can make sure that acquirer can not get the information of the order.

*d)* Sends Initiate flow including $SALT_p$, $CERT_p$, $H(DESC,SALT_p)$ , $H(n_p)$.

*2) Invoicement*

*a)* Supplier retrieves $SALT_p$ from Initiate. He already has order information (DESC) and computes $H'(DESC,SALT_p)$ and checks that this matches the $H(DESC,SALT_p)$ in Initiate.

*b)* Supplier generates random number $n_s$ and computers $H(n_s)$. Note: $n_s$ needs be kept secret, it will be used later by purchaser to identify receipt of the goods. The hash value of $H(n_s)$ is declared.

*c)* Supplier chooses a transaction id TID which uniquely identifies the context and obtains DATE-this is a time stamp.

*d)* Forms Clear as defined above.

*e)* The combination of Clear, Price and PERCENTAGE is used to form Common. Computes H(Common).

*f)* Supplier gives the signature of H(Common) and forms $Sig_s$.

*g)* Clear, which consists of $ID_s$, $ID_p$, $TID_s$, DATE, H(C) and H(Common), is then transmitted to P as Invoice. $Sig_s$ can be sent with this message to P later.

*3) Payment Authentication Requirement*

*a)* Purchaser retrieves and checks Clear from Invoice .

*b)* Puchaser retrieves $ID_s$, $ID_p$, $TID_s$, DATE and H(C). He already has PRICE and PERCENTAGE, so that he can now form Common. He computers new H'(Common) and checks that this matches the value in Clear. The intergrity of PRICE, PERCENTAGE can be guaranteed.

*c)* Puchaser gives the signature of H(Common) and forms $Sig_p$.

*d)* The Price, Percentage, $ID_p$and $Sig_p$ are now encrpted under the acquirer public key and get $E_A$(Price, Percentage, $ID_p$, $Sig_p$）.

*e)* Saves Common, $Sig_p$, $Sig_s$ and sends Clear with $E_A$(Price, Percentage, $ID_p$, $Sig_p$) to payment gateway Acquirer.

*4) Payment authentication Response*

*a)* The Acquirer gateway extracts AuthRes and decryptes $E_A$(Price, Percentage, $ID_p$, $Sig_p$) using public key of P.

*b)* If the decrption fails, then the altertion of $E_A$(Price, Percentage, $ID_p$, $Sig_p$) is detected and the transaction is invalid. If not, A extracts PRICE and PERCENTAGE.

*c)* It checks H'(Common)= H(Common).

*d)* Generates AuthTime.

*e)* Acquirer verifies $CERT_P$ and $CERT_S$ through CA, it is ensured that P and A are authorized parties.

*f)* It uses the existing clearing and authorization system to on-line authorize the payment and generates RespCode.

*g)* Purchaser pays prepayment to S. Upon receipt of a response Y/N from S' issuer, P's issuer sends RespCode and PaymentID to A and gives the signature of those message. S's issuer verifies the receipt of the prepayment and sends RespCode and ConfirmID to A and gives the signatures.

*h)* Forms $Sig_p$ combining with the signature of H(Common), AuthTime and Y/N.

*i)* Saves H(Common)，AuthTime，Y/N.

*j)* Sends TID, AuthtTime, RespCode, $H(Sig_P)$, $H(Sig_S)$ and $Sig_A$ to M.

*5) shipment*

*a)* S retrieves the AuthRes from A, that is, the supplier has receipt the advance payment. Then, sends good or provides services to P. P needs to show $n_p$ to confirm his identity.

*b)* S provides $n_s$ to confirm this transaction.

*c)* Finishes the shipment and saves $n_p$.

*6) remainder payment*

*a)* S provides $n_s$ to A, A finishes the payment of remainder of the order.

### *D. Security Analysis*

*1) Confidentiality of transaction information*

No one except S and P knows DESC, PRICE and PERCENTAGE. On payment step, A only gets PRICE and PERCENTAGE.

*2) Intergrity of transaction information*

Using hash function and digital signature keeps the information of transaction from tempering.

*3) Identification authentication of participants*

Each party in this scheme holds public key pairs and public key certificates.

*4) Non-repudiation*

In transaction process, each party can not deny his message with signatures. $n_s$ and $n_p$ individually provide evidences of payment and receipt of good .

## V. CONCLUSION

In this paper, we present a new protocol with improvement of iKP for B2B e-payment. The protocol changes the original flow to provide twice payment in single B2B transaction. In future, we will discuss the realization of other payment conditions in B2B payment process.

## REFERENCES


[1] Mihir Bellare, Juan A. Garay. "IKP- a family of secure electronic payment protocols ", Proceedings of the 1st conference on USENIX Workshop on Electronic Commerce – Volume1, July 1995, pp.89-106

[2] Bellare, M., Garay, J., Hauser, R., Herzberg, A., Steiner, M., Tsudik, G.,Van Herreweghen, E., and Waidner, M, "Design,Implementation, and deployment of the iKP secure electronic payment system", IEEE Journal of Selected Areas in Communications, 2000, pp. 611-627. 10.1109/49.839936

[3] Abrazhevich-Dennis, "Classification and characteristics of electronic payment systems", Lecture Notes in Computer Science 2115, 2001,pp. 81-90. 10.1007/3-540-44700-8_8

[4] Fadi abdulhamid, EzZ hattab, "A model for person-to-person electronic payment system", unpublished.

[5] Liu Jingwei, Sun Rong, Kou weidong, "Fair e-payment protocol based on simple partially blind signature scheme", Wuhan University Journty of Natural Sciences, Volume 12, Number 1,2007,pp181-184, 10.1007/s11859-006-0287-7

[6] Xiaoling Dai Grundy, J. Lo, B.W.N, "Comparing and contrasting micro-payment models for e-commerce systems", International Conferences of Info-tech and Info-net(ICII),China,2001pp.35-41 10.1109/ICII.2001.983001