Electronic Commerce

4. Payment Schemes

V Rajaraman

V Rajaraman is with the Jawaharlal Nehru Centre for Advanced Scientific Research and the Indian Institute of Science, Bangalore. Several generations of scientists and engineers in India have learnt computer science using his lucidly written textbooks on programming and computer fundamentals.

Part 1. What is E-Commerce?, *Resonance*, Vol.5, No.10, 13-23, 2000.
Part 2. E-Commerce System Architecture, *Resonance*, Vol.5, No.11, 26-36, 2000.
Part 3. Secure messaging, *Resonance*, Vol.6, No.1, 8-17, 2001.

In this part, we will describe payments using credit cards and cheques in e-commerce.

Payment is an important component in e-commerce. In day-to-day commercial dealings there are many modes of payment, each with its own advantages and disadvantages. The most common payment, especially for low value purchases, is by cash. Credit cards are preferred by customers for higher value purchases (though not all merchants!). If a customer is a trusted party, merchants normally accept cheques. Payment for services such as telephone bills, electricity bills, etc. and settlement of bills between businesses is normally by cheque. In e-commerce also we need systems, which are equivalent to these three modes of payment. Of these three modes cash transaction is the one which is most difficult to mimic. Large electronic cash transactions are discouraged by most governments. It is thus still in a fluid state. In this article we will discuss payments made using credit cards or cheques.

Payment Using Credit Cards

We will first review how credit card payments are made in day-to-day shopping. There are four parties involved in these transactions. They are: the customer who owns a credit card, merchants who accept credit cards (typically a merchant would accept credit cards of several companies such as VISA, MASTERCARD, etc.), a bank which issues credit cards to customers, guarantees payments to merchants and collects payments from its customers and lastly an acquirer which is a financial institution that establishes an account with a merchant and validates card information presented by a merchant and authorizes sale based on customer's credit status. The acquirer

accepts cards of several bankcard associations, takes the responsibility of electronically transferring payment to merchants' account and is in turn reimbursed by the issuing bank. Credit card transactions are carried out as follows:

1. A customer presents a credit card to a merchant after purchasing goods.
2. The merchant reads information contained in the credit card's magnetic strip using a terminal and enters the transaction amount.
3. The information goes to the acquirer via a private telephone line. The acquirer's computer checks the validity of the card, credit available to the customer and sends an OK authorizing transaction, provided card and credit are OK.
4. The merchant takes the signature of the customer on the authorization slip, compares the signature with that in the card and delivers the goods.
5. The acquirer pays the merchant and collects the money from the appropriate issuing bank.
6. The bank sends a monthly statement to the customer and collects the outstanding amount.

Observe that the card transaction is validated using the physical card and customer's signature on the card. In e-commerce there is no physical contact between the merchant and the customer making it impossible to verify a physical signature. Also it is necessary for the merchant to verify the genuineness of the customer and for the customer to be assured that he is not dealing with a fake merchant. Thus a customer would be reluctant to reveal his credit card number and details using the internet as the merchant may be a fake or the number may be stolen by eavesdroppers on the internet. Further, if the merchant is careless, a hacker may access the merchant's database and steal credit card numbers. There have been cases reported in the press of credit card numbers being stolen by hackers as well as by disgruntled employees of merchants. Thus a protocol is required in which the credit card number is not revealed to

In e-commerce there is no physical contact between the merchant and the customer making it impossible to verify a physical signature.

A customer would be reluctant to reveal his credit card number and details using the internet as the merchant may be a fake or the number may be stolen by eavesdroppers on the internet.

A protocol called Secure Electronic Transaction (SET) protocol has been standardised for credit card payments by major credit card companies.

a merchant but only to the acquirer who authorises sale based on the credit card validity and available credit. In addition to this, the acquirer and the bank need not know what was bought by a customer (to protect the privacy of customers). They need to know only how much is the bill amount.

Secure Electronic Transaction (SET) protocol.

A protocol called Secure Electronic Transaction (SET) protocol has been standardised for credit card payments by major credit card companies such as VISA and MASTERCARD in USA. To use the SET protocol for credit card transactions it is assumed that:

1. A public key encryption system (such as RSA) is used by both customers and merchants. (For details on RSA system please see [1]). Thus each of the parties involved in e-commerce transactions have a pair of keys – a private and a public key.
2. All parties have their public keys certified by a certification authority and these certificates accompany requests for service sent by them. This is to assure both customers and merchants that they are dealing with genuine parties.
3. A standard hashing algorithm is used to create message digests for digitally signing purchase order. (See Part 3 of this series to understand digital signature).

The main features of this protocol are:

SET protocol ensures that a customer's credit card number is not revealed to a merchant. It is revealed only to the acquirer who authorizes payment.

1. It ensures that a customer's credit card number is not revealed to a merchant. It is revealed only to the acquirer who authorizes payment.
2. Purchase invoice details are not revealed to the acquirer. Only the credit card number and total amount is revealed to the acquirer.
3. Purchase invoice coupled with the credit card number is digitally signed by the customer so that an arbitrator can settle disputes, if any, on purchase invoice and cost.

The complete protocol is given in detail (and runs to 262 pages!)

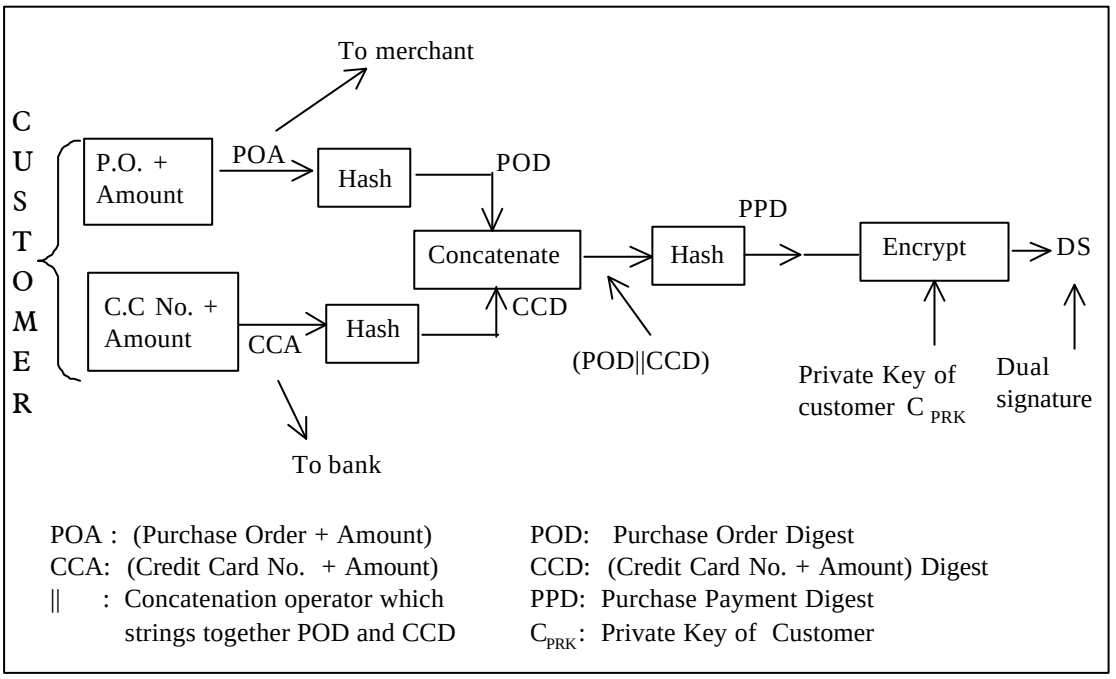
in a formal SET protocol definition. We will present simplified essentials of the protocol in what follows. Readers interested in learning about the detailed protocol are referred to [2] and [4]

Dual Signature Scheme

SET protocol depends on an innovation called dual signature whose main purpose is to give to a merchant the purchase order and amount only (without revealing the credit card number) and give the credit card number and the amount to be paid (without revealing the purchase order details) to the acquirer. It will also ensure that the payment is for the actual purchase made. The essentials of the idea are explained here (see *Figure* 1). A customer's purchase information consists of a purchase order (PO) accompanied by credit card number (CCN) and amount to be paid. This is divided into two parts (PO + Amount) and (CCN + Amount). The two parts are separately hashed using a standard one-way hash algorithm (such as MD5 explained in Part 3 of this series). Let us call these POD and CCD, respectively. The two are concatenated (i.e. stringed

Purchase invoice coupled with the credit card number is digitally signed by the customer so that an arbitrator can settle disputes, if any, on purchase invoice and cost.

Figure 1. Dual signature system.



together) and hashed again giving PPD (see *Figure* 1). PPD is encrypted using customer's private key C_{PRK}. This is the customer's digitally signed copy of purchase order + credit card number. Let us call it DS. The formula to get DS is given as (1).

$$DS = C_{PRK}\{H(POD \,||\, CCD)\}. \quad (1)$$

The purchase order and amount, namely POA is separately encrypted using the *merchant's public key* and sent to the merchant. He can decrypt it using his private key to obtain POA. CCD and DS are also sent to him separately. Remember that given CCD he cannot find CCA, as hashing is a one-way function. Thus credit card number is not available to the merchant. The merchant can compute

$$H(H(POA)\,||\,CCD) = H(POD \,||\, CCD). \quad (2)$$

The signature DS received by the merchant can be decrypted by him using the *public key of the customer* to obtain

$$C_{PUK}(DS), \quad (3)$$

where C_{PUK} is the certified public key of the customer, which is sent to the merchant by the customer along with his purchase order. If (2) equals (3), then the merchant has verified the customer's signature. If payment is authorized by the acquirer he can ship the order.

As far as the bank is concerned it will receive CCA encrypted by the customer with bank's public key forwarded by the acquirer. It can decrypt it using its private key and obtain CCA. The bank will also receive POD and DS. Remember that POA cannot be found from POD as it is obtained by hashing POA with a one-way hash function. The bank will not thus know the purchase details. It can however compute

$$H(POD \,||\, H(CCA)) = H(POD \,||\, CCD) \quad (4)$$

and $C_{PUK}(DS)$. If (4) equals $C_{PUK}(DS)$, the signature of the customer is verified by the bank. If the customer's balance in

credit card account is sufficient the bank can authorise the merchant to honour the purchase order.

Observe that the customer cannot repudiate his purchase order as it has been signed by him and deposited with the bank. The merchant also cannot substitute a customer's purchase order with some other purchase order as the signature contains a unique digest of the customer's purchase order deposited with the bank.

The customer cannot repudiate his purchase order as it has been signed by him and deposited with the bank.

We summarise the procedure below:

Step 1: Customer fills purchase order, amount payable and credit card number in his PC. A software in the PC strips it into two parts; purchase order with amount and credit card number with amount. Let us call them POA and CCA.

POA is encrypted using merchant's public key and CCA with the bank's public key. Both are sent to the merchant along with CCD and dual signature (DS). Merchant verifies signature and proceeds further if signature is OK.

Step 2: Merchant forwards encrypted CCA, POD and DS to acquirer who forwards it to the customer's bank.

Step 3: The bank decrypts CCA with its private key, checks the validity of the credit card and available balance in the credit card account. If it is OK and the customer's digital signature is OK, it authorises the acquirer to proceed with the transaction.

Step 4: The acquirer in turn OKs transaction to the merchant and credits his account.

Step 5: The merchant accepts the customer's purchase order and informs him about delivery details.

Step 6: At the end of the month the bank issuing the credit card sends a consolidated bill to the customer.

It should be remembered that all of the operations are carried out by software stored in the respective computers and effected by clicks of a mouse button!

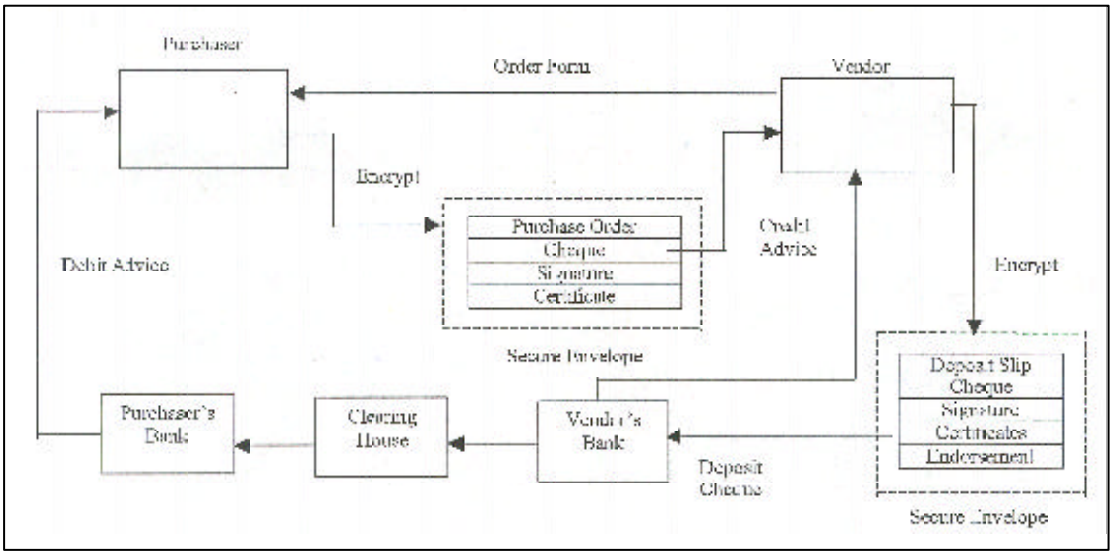
It should be remembered that all of the operations are carried out by software stored in the respective computers and effected by clicks of a mouse button.

Electronic Cheque Payment

We will now describe an electronic cheque clearance system developed by a company called Financial Services Technology Consortium Inc. (FSTC) which is supported by a number of American banks. Most of the cheque-based transactions will be between businesses and therefore this mode of payment is relevant in B2B e-commerce. It is assumed that businesses will be willing to invest in special hardware (normally an electronic circuit attached to a PC) to sign payments. Hardware encryption of signatures is secure as it will be difficult for hackers to steal keys stored by hardware. The system is shown in *Figure* 2. This system assumes that all organizations participating in the system will use public key encryption scheme such as RSA and have their public keys certified by certification agencies. It is also assumed that banks have trusted relationship among them and the clearing house which settles cheque payments (in India, Reserve Bank of India is the clearing house and all scheduled banks use RBI's services and a private secure network). The transaction proceeds as follows:

Figure 2. Clearing cheque payment electronically.

Step 1 Purchaser fills a purchase order form, attaches a payment advice (electronic cheque), signs it with his private key



(using his signature hardware), attaches his public key certificate, encrypts it using the vendor's public key and sends it to the vendor.

Step 2 The vendor decrypts the information using his private key, checks purchaser's certificates, signature and cheque, attaches his deposit slip, and endorses the deposit attaching his public key certificates. This is encrypted and sent to his bank.

Step 3 The vendor's bank checks the signatures and certificates and sends the cheque for clearance. The banks and clearing house normally have a private secure data network.

Step 4 When the cheque is cleared the amount is credited to the vendor's account and a credit advice is sent to him.

Step 5 The purchaser gets a consolidated debit advice periodically.

We have not described the signing process in detail as it has been described already.

In this part we have described credit card and cheque payments only. In the next part, we will describe how cash payments are made in e-commerce.

Suggested Reading

[1] Palash Sarkar, *Resonance*, Vol. 5, No. 9, p. 22, 2000.

[2] William Stallings, *Cryptography and Network Security – Principles and Practices*, Second Edition, Prentice Hall, NJ, USA, 1999.

[3] D E Denning, *Information Warfare and Security*, Addison Wesley Longman, Reading, MA, USA, 1999.

[4] http://www.ibm.com/redbook/SG244978 gives details of SET protocol

Address for Correspondence
V Rajaraman
IBM Professor of Information Technology
JNCASR
Bangalore 560 064, India.
Email:rajaram@serc.iisc.ernet.in

O Diamond! Diamond!
Thou little knowest the
mischief done!

Newton