A Payment Scheme using Vouchers

Ernest Foo*
ernest@fit.qut.edu.au
and Colin Boyd
boyd@fit.qut.edu.au

Information Security Research Centre
School of Data Communications
Queensland University of Technology
Brisbane, Australia

Abstract. Electronic payment schemes are traditionally based on the physical model of commerce where customers withdraw cash from bank accounts and spend it at merchants' establishments in return for goods and services. This may not be the most ideal model on which to base electronic payment. A new payment scheme using a different paradigm has been developed. Vouchers are prepared by the bank and the merchant. These are distributed to customers who can redeem them for electronic goods with the help of the bank. This new scheme requires fewer online messages to be transmitted than previous payment schemes involving electronic goods such as NetBill and thus also requires less online processing. The voucher scheme also provides some properties desired by payment schemes based on electronic coins.

1 Introduction

It seems that the future of commercial transactions will be electronic payment over the Internet. For several years now, it has been the expectation of industry that the medium of the Internet will be the future of commercial and private trading. Electronic payment over the Internet has great potential in terms of banking because much of the transaction may be automated. Also many users perceive that the use of the Internet will allow more convenient purchasing. Indeed some believe that electronic payment over the Internet will become an integral part of commercial culture, in the same way that this has happened for automatic teller machines and credit cards. Unfortunately, due to the insecure nature of the Internet, the security of

* Sponsored by Commonwealth Bank and the Australian Research Council

electronic payment is unsure. In general the current public opinion is that transactions over the Internet are extremely risky and until the much awaited SET protocol [13–15] is widely deployed few banking corporations are willing to guarantee the safe transaction of funds over the Internet.

One of the main problems with electronic payment on the Internet is that the transaction occurs remotely. Unlike normal payment there is no physical proof of the transaction occurring. Cryptographic tools are required in payment protocols to provide this proof in the electronic medium. But electronic payment protocols are also different from other secure protocols in that they have two kinds of threat: external threats and internal threats. External threats have been an issue which has been widely addressed by other secure protocols; the processes for dealing with these threats are widely documented [1, 2]. Internal threats are unique to electronic commerce. These are due to entities which legitimately take part in the protocol but attempt in some way to gain unfairly from the transaction. Designers usually develop a series of proofs and commitments to prevent or detect internal threats.

These issues are directly, and sometimes indirectly, addressed by a multitude of payment protocols [4–7, 9, 10, 16–20, 23] each of which provides many different useful properties. The voucher payment scheme described in this paper addresses external threats in much the same manner as other payment schemes but the treatment of the internal threat is unique.

All payment protocols intended for practical use need to take into account their efficiency with regard to processing, communications and storage requirements. Cryptographic processing, particularly with asymmetric algorithms, is computationally expensive, so it is important to minimise the use of cryptography to where it is really required. The SET protocol has been criticised for its intensive use of asymmetric cryptography. Some protocols, particularly those for *micropayments*, are willing to sacrifice some security in return for large gains in efficiency. The voucher protocol proposed in this paper maintains high security, but is more efficient in terms of online messages transmitted and online computer processing required than other protocols with similar aims.

1.1 Related Work

The design of most electronic payment protocols exists within a common framework. This framework is traditionally based on credit card payment models and consists of three entities. The *customer entity* is the user and the entity which wishes to make a purchase of goods or services. The *merchant entity* is the shopkeeper who uses the payment scheme to offer goods and services to the customer entity. The *bank entity* is responsible for transfer of funds between the other entities.

The establishment and distribution of cryptographic keys and other data flows between the different entities in payment protocols exhibit the following common properties.

- A bit string containing certain information is used to convey value. The information varies depending on the type of payment protocol. This bit string is often called a *coin* or *payment commitment* in the literature, and we call it here the *proof of transaction*. Once transmitted it can be used as proof that an entity agrees or commits to the terms of the transaction.
- The proof of transaction is usually digitally signed to indicate who transmitted it or is encrypted in such a way that it is known as to who sent the message.
- This proof of transaction is created by the bank and the customer. During the payment process it is usually sent from the customer to the merchant. The merchant sends it to the bank to verify its authenticity and thus verify the payment transaction.

The integrity of the proof of the transaction is used to prevent or discourage internal threats. The protection of the proof of transaction during transmission is important to defend against both external and internal threats. That is why the proof of transaction is almost always transmitted along authenticated channels.

The voucher scheme employs a proof of transaction but is unique in the way the payment commitment is distributed. Specifically, in comparison with all the known schemes in the literature, the transmission of the proof of transaction is reversed: instead of being transferred from customer to merchant to bank, it is transmitted from merchant to customer to bank. In the voucher scheme the payment

commitment (called a voucher) is created by the merchant with the assistance of the bank. The payment commitment is then distributed to potential customers. The customer has the option to complete the transaction by signing the bit string. The payment commitment is then sent to the bank to verify the validity of the transaction.

The major advantage of the voucher scheme, in comparison to known schemes, is that it allows the merchant to act in a completely passive way. This makes the scheme ideal for use in an Internet environment where merchants already almost universally provide web sites where their customers can download product information. With the voucher scheme merchants can provide goods to be downloaded by customers, but these goods remain encrypted until the customer has committed to payment. As a result the merchant performs no on-line processing. A major benefit of this is that network processing on the merchant side is completely unchanged from the current technology.

It should be made clear that, in comparison with previously proposed schemes, the reduction in merchant processing is accompanied by a consequent shift in processing to the bank. However, overall there is a saving in the online processing required. Moreover, this shift is away from the widely distributed merchants to the central banking facility where it is natural to concentrate processing power, and where processing may be aggregated.

1.2 Outline of Paper

The following section describes the overall idea of the voucher payment scheme and then the detailed protocols are presented. In section 4 a comparison is made with the existing NetBill payment scheme which has many features in common with the voucher scheme.

2 A Voucher Payment Model

In a real world voucher scheme, merchants create vouchers which allow customers to receive discounts for the purchase of goods or even allow the customer to redeem them for the actual goods. This is the basis of the electronic voucher payment scheme. This payment

scheme is ideal for processing of electronic goods in a communications network, such as software or electronic news and information. However, it could be modified to work for physical goods as well by substituting an authorisation message or a release signal for the electronic goods package.

The transaction model has a traditional configuration consisting of merchant, bank and customer. We assume that the bank is trusted by both the merchant and customer entities. In reality the bank entity often represents two separate parties: the acquirer and the issuer. The acquirer is the merchant's bank and the issuer is the customer's bank. If the acquirer and the issuer are separate entities we assume that they share a secure private communications link. This scheme consists of three parts. Each of these parts must have been completed to successfully conduct a transaction.

1. The merchant and the bank work together to create a voucher which contains the important transaction commitment. A major saving of the scheme is that this process is only required once for a particular item. Since electronic items are likely to be purchased many times, this is a significant advantage.
2. The merchant allows the free distribution of the voucher to customers. For electronic goods this would typically mean that the voucher is placed on the merchant's web site. The voucher will be distributed together with the actual electronic goods. However, the goods are encrypted so that during this phase the customer cannot access the goods.
3. The customer and the bank co-operate and enable the customer to decrypt the electronic goods and thus allow the customer to access the goods.

The voucher protocol is designed to achieve the following main objectives. These are common objectives which well-known schemes such as iKP [3] and NetBill [8] payment systems attempt to achieve.

1. The customer and merchant are able to agree on the details of the transaction.
2. The customer can only receive the specified goods if she has paid for them.

3. The customer and merchant have proof that a successful transaction has occurred.
4. The customer is able to protect her identity from the merchant.
5. The transaction cannot be adversely affected by external threats. This means that a malicious party (which is not included as part of the payment model) cannot prevent the transaction from succeeding. This can either be by causing the merchant not to be paid or preventing the customer from receiving the goods.
6. The transaction is efficient in terms of processing and in the number of messages required to complete the protocol.

3 The Voucher Protocol

The protocol description will use the notation $i.\ X \rightarrow Y$ to indicate that the ith message of the protocol is transmitted by entity X to entity Y. The customer entity is represented by C, the merchant entity is represented by M and the bank or notary is represented by B. The basic voucher protocol consists of five steps:

$$
\begin{array}{l}
1.\ M \rightarrow B\ : \text{Request key} \\
2.\ B \rightarrow M\ : \text{Return key} \\
\hline
3.\ M \rightarrow C\ : \text{Distribute voucher} \\
4.\ C \rightarrow B\ : \text{Redeem voucher} \\
5.\ B \rightarrow C\ : \text{Release goods}
\end{array}
$$

The horizontal line after the first two steps separates the protocol part that need be performed only once, in an offline exchange between bank and merchant. The remaining steps may be run repeatedly with different customers at any time. Thus the merchant engages in no online processing.

Objective 1 is achieved in steps 3 and 4 of the protocol. The merchant determines the price for his goods and sets this in the merchant signed voucher. The customer agrees to this price by cashing in the voucher.

The customer can only decrypt the goods by using the correct key. This key is received by the customer after the bank has determined that the transaction should go ahead and the funds have been transferred from the customer's account. Thus Objective 2 is realised.

The goods decryption key received by the customer is her proof that the bank has successfully conducted the transaction. The merchant's proof of transaction is the bank signed product identification code sent in step 5 of the protocol. Objective 3 has been achieved.

The customer's identity is protected from the merchant because the merchant does not transmit any encrypted messages directly to the customer. Also even if the customer does receive a voucher, she is under no obligation to cash in the voucher and decrypt the goods. Thus Objective 4 is attained. Note that anonymity is not obtained because the bank will be able to identify the customer and the goods that she purchases.

Objective 5 is achieved because no messages within the protocol contain data which is either unsigned or unencrypted.

Objective 6 is discussed in later sections. But steps 1 and 2 of the protocol only need to be conducted on a regular basis and do not need to be conducted for every transaction. This decreases the number of messages required for an average transaction. The voucher payment scheme only requires 1 signature from each entity (the merchant does not even need to do this on line) and a one way hash calculation from the bank and the merchant (who also does not need to do this on line).

3.1 Notation

The following notation is used to denote cryptographic operations. X and Y always represent communicating parties. K always represents a cipher key. When describing the following protocols, the sequence of messages is exchanged among three parties: C, the customer, M, the merchant; and B the bank, acquirer or notary entity.

$E_{XY}(Message)$ $Message$, encrypted with the key XY using symmetric key cryptography. It is assumed that the key is known only by X and Y and that only these entities may know the contents of $Message$.

$Sig_X(Message)$ $Message$, digitally signed by X using a suitable signature algorithm, such as RSA [21]. This implies that X's public key is used to ensure that the message was transmitted by X.

$H(Message)$ A cryptographic function which results in a digest and checksum of $Message$, using an algorithm such as the Secure Hash Algorithm (SHA) one-way hash function.

3.2 Voucher Creation Phase

This phase assumes that the merchant and the bank have exchanged RSA public keys so that they are able to verify the authenticity of digital signatures created by the other entity.

1. $M \rightarrow B \ : Sig_M(MID, E_{MB}(MerchantAccountDetails))$

2. $B \ \rightarrow M : Sig_B(E_{MB}(K), Expiry)$

In step 1 the merchant makes a request of the bank for a voucher key. This key will be used to provide the security required by the voucher. The merchant must provide his merchant identification as well as details of his account with the acquiring bank. The acquiring bank stores this information so that any funds which are owed to the merchant by customers may be deposited in that account. It is optional that this message be correctly authenticated with a digital signature. In essence this will allow anyone to sell goods and become a merchant provided that they have a unique merchant identification number. This number may be chosen by the merchant. Merchant account details, like all other account details, must not be allowed to be sent across open networks in the clear.

After it has generated a symmetric key for the merchant the bank encrypts it and sends it to the merchant with an expiry date which indicates when this key is no longer valid. As this key is the only element in the protocol which provides security for the transaction it is essential that it be encrypted so only the merchant and the bank know it. The bank must sign the key and expiry to prevent the merchant from receiving a false key from an external party.

At this point the merchant can create a voucher for each product. The merchant voucher will contain the actual electronic goods which the customer is purchasing. First, the merchant generates the key which will encrypt his goods in the following manner:

$$K_P = H(K, MID, PID, Value)$$

K is the key provided by the bank. This key is only known to the merchant and the bank. MID is the merchant identity which the bank already knows. The product identity (PID) is used to indicate the product which this voucher contains. The merchant can choose to have a different PID for each copy of the product he sells or he can choose to have one product identity for each product or even for a range of products. The PID and MID are used to provide a unique identifier for the voucher which cannot be tampered with. The cost of the product is also included in this key so that customers cannot adjust the value to be paid for the product. It is assumed the the one way hash function is such that the key K cannot be determined, even if multiple valid values for K_P, MID, PID, and $Value$ are known. Now the goods must be encrypted with the key which has been generated by the merchant. The next section will describe the contents of the voucher in more detail.

If the merchant issues one product identity for a number of products or if the merchant has many copies of the same product with the same product identity the customer who has purchased the goods may freely distribute the key K_P to other customers. This would mean that a customer can then obtain certain goods from the merchant and release them using the key she has been given by a friend who has purchased the goods. Unfortunately this protocol cannot prevent this scenario which is in essence the same as software piracy. However, only the legitimate customer has a receipt from the bank which can be used to prove custody of a legal copy. This is the same situation as with purchase of electronic goods on physical media.

This phase of the payment system only has to be conducted once. The merchant can continue to use the key K provided by the bank to prepare vouchers for all of his products indefinitely. In practice it is advisable that the merchant request a new key at regular intervals to maintain the security of the voucher. This is the reason for the inclusion of an expiry date when the key is issued by the bank.

3.3 Voucher Distribution Phase

Vouchers can be freely distributed by the merchant with the associated encrypted goods. The additional data which is included in the voucher is shown below. It is not essential for the security of the

payment scheme that the merchant sign the voucher but as this signature need only be constructed once when the voucher is created it does allow the customer to verify that the voucher and goods she has downloaded originate from the correct source.

$$3.\ M \rightarrow C : Sig_M(E_{K_P}(Goods), MID, PID, Description, Value, Expiry)$$

The voucher package includes the encrypted goods which the voucher will allow the customer to access. The voucher package also includes the merchant and product identities. These are required to uniquely identify the product which the customer is purchasing. Also included is a human readable description of the product so the customer has some indication of the type of product she is purchasing. The value of the product must also be included so the customer can determine whether the cost of the product is worthwhile. The expiry date is also included for the customer as an indicator of how long the voucher will be valid. The customer may download the voucher and decide not to purchase the goods without any loss. Because the voucher is signed by the merchant, the customer can be sure that the goods and the voucher contents have been received correctly providing, of course, that the merchant is not cheating.

3.4 Redeeming Vouchers

Now that the customer has obtained the encrypted goods and the voucher from the merchant and she has decided to purchase the goods, she must request the key from the bank to release the goods. Again it is assumed that the customer is able to establish a secure connection with the bank.

$$4.\ C \rightarrow B : Sig_C(MID, PID, Value, E_{CB}(CustomerAccountDetails), Counter)$$
$$5.\ B \rightarrow C : E_{CB}(K_P)$$

In step 4 of the protocol the customer sends to the bank the merchant and product identity and the value of the product as well as details of her account and a counter value. The merchant and product identity and the value of the goods are obtained from the

voucher the customer has received. The counter is a value which must be maintained by the bank and the customer. The purpose of the counter is to uniquely identify this message and prevent an external entity from replaying the message and thus draining the customer's account of funds. A timestamp could be used instead of a counter provided that problems associated with synchronisation are properly addressed.

It is only when the customer signs this message that the voucher is given value. Up till this stage the customer can abort the transaction. If the customer chooses to accumulate vouchers over a period of time, the customer may concatenate multiple sets of merchant identity, product identity and value bit strings and sign them all once. This will reduce the amount of processing required by the customer.

The bank now makes a decision as to whether the transaction should take place. The bank must consider things like the availability of the customer's funds, and the trustworthiness of both the merchant and the customer and check that the counter value is valid. If the bank decides that the transaction should occur, the bank moves the correct amount of funds from the customer's account to the merchant's account using the details provided by the customer and the merchant during the transaction. At this point the bank may also deduct any transaction, handling or other fees.

As the bank already knows the merchant's key K, the bank uses these additional values to calculate the key K_P. In step 5 of the protocol the bank returns the key K_P to the customer. When the customer obtains the key K_P she is able to decrypt the goods she received with the voucher and complete the transaction.

After the funds transfer has occurred the bank has the option of notifying the merchant that the transaction took place. This notification is only to assist the merchant in updating his inventory and may not be essential for online software goods. When, or if, this notification occurs can be determined by agreement between the bank and merchant. For large value transactions immediate notification may be appropriate; for small values notifications could be batched and sent at the end of each working day. Unfortunately if the merchant chooses not to be notified by the bank he has no indication that a transaction has occurred.

3.5 Disputes

If the merchant or the customer is not satisfied that the transaction has been conducted successfully a dispute has occurred. The voucher payment scheme has a process which is able to deal with most disputes. It is assumed that both the customer and the merchant can trust the bank to be fair in all decisions.

The voucher dispute resolution protocol consists of the following step:

$$1.\ C \rightarrow B : Sig_C(K_P, Sig_M(E_{K_P}(Goods), MID, PID, Description, Value, Expiry))$$

The message consists of the key K_P which the customer received from the bank in step 5 of the payment protocol. The remainder of the message is the merchant signed voucher the customer received in step 3 of the payment protocol. Because the voucher is signed by the merchant the customer is unable to alter the contents of the voucher without detection. The re-transmission of the voucher, including the goods, in the dispute protocol will increase the amount of traffic on the network but it is expected that the dispute protocol will not be required very often.

The resolution of the dispute need not necessarily be referred to the bank. Any trusted third party may be used as a judge, provided that party has access to the transaction key K. The following sections describe how the judge may deal with potential complaints.

Incorrect Key In the case of this dispute, the customer claims that the key that she received from the bank does not correctly decrypt the goods which were received in the voucher.

When the judge receives the message from the dispute protocol he calculates the disputed key K_D using the MID, PID and $Value$ fields from the voucher and the key K which is already known to him.

$$K_D = H(K, MID, PID, Value)$$

The judge then compares K_D and the key K_P received from the customer. If they match then the customer has received a legitimate

key and the transaction should be rolled back. If the keys do not match, either K_P was altered by the customer or the customer has transmitted an incorrect K_P as part of the dispute protocol. In this case the transaction is not altered. It is assumed that the transmission of each message in the protocol occurs successfully and that the contents of each message is not altered by any network interference.

If the customer is not satisfied with this result it is possible that the incorrect goods have been delivered in the voucher.

Incorrect Goods The customer may not be satisfied that the goods that she received are the correct goods that she has purchased. It could be that the merchant has incorrectly constructed the voucher, or that the merchant has encrypted goods which do not match the goods description included in the voucher.

To check the goods, the judge verifies that the merchant has constructed the voucher correctly by calculating the key K_D and checking for the correct key K_P as described in the previous section. The judge then decrypts the goods using K_D. A human arbitrator determines if the decrypted goods match the description provided in the voucher. If the goods cannot be decrypted, the merchant has incorrectly constructed the voucher by providing an incorrect merchant or product identity or key K. In both of these cases the transaction is rolled back and the money returned to the customer.

Incorrect Payment Amounts This type of dispute includes any disagreement on the amount charged for the goods. This includes both the possibility that the customer has been charged too much or the merchant has been paid too little.

In the voucher payment scheme the value that the merchant assigns to the product cannot be maliciously altered by the customer because the value is part of the key which is required to decrypt the electronic goods. Both the customer and the merchant indicate their agreement to the value to be paid for the goods by transmitting the value field correctly. The merchant indicates his requested goods $Value$ within the signed voucher and the customer indicates her agreement to that $Value$ by signing it and sending it to the bank in return for the key K_P.

4 Some Implications of Using Vouchers

By using the concept of vouchers, the resulting payment scheme has several interesting properties. These include greater efficiency than existing payment schemes like *iKP* and *NetBill*, as well as the advantage of requiring no online processing by merchants. The following sections provide a more detailed comparison of payment schemes.

4.1 Comparisons with NetBill

The NetBill protocol [8], like the current proposal, was designed especially for payment of information goods over the Internet. Because of this the NetBill protocol may be used as a benchmark for comparison with the voucher payment protocol. The voucher protocol provides many of the objectives which the NetBill designers required. A brief description of the NetBill protocol is given in Figure 1. Like the voucher protocol the NetBill scheme involves three parties: a customer, a merchant and the NetBill server which is the equivalent to voucher scheme's bank entity. NetBill also involves three phases: price negotiation, goods delivery and payment. During a NetBill transaction, the customer and the merchant interact with each other during the price negotiation and goods delivery phases to exchange the transaction request and encrypted goods. In the payment phase the merchant sends the transaction request to the bank. When the bank is satisfied that the transaction is in order he sends a signed receipt back to the merchant who also signs the receipt and passes it onto the customer along with the decryption key for the goods. The bank is able to handle disputes because he also receives the decryption key with the transaction request.

Table 1 compares the efficiency of the NetBill payment scheme against the voucher payment scheme. The main advantage the voucher payment scheme has over the NetBill payment system is that it requires a smaller number of messages to be transmitted for each transaction. The voucher scheme has only three messages which must be transmitted for a transaction to be successfully completed. The first two messages in the voucher payment protocol which involve the creation of vouchers may be conducted offline prior to the transaction. A new voucher does not need to be created for each purchase. The

Price Negotiation Phase

1. $C \rightarrow M : C, E_{CM}(Product, RequestFlags, TID)$
2. $M \rightarrow C : E_{CM}(ProductID, Price, RequestFlags, TID)$

Goods Delivery Phase

3. $C \rightarrow M : C, \{TID\}_{K_{CM}}$
4. $M \rightarrow C : E_K(Goods), E_{CM}(H(E_K(Goods)), EPOID)$

Payment Phase

5. $C \rightarrow M : C, E_{CM}(Sig_C(EPO))$
6. $M \rightarrow B : M, E_{MB}(Sig_M(Sig_C(EPO), Macct, K))$
7. $B \rightarrow M : E_{MB}(Sig_B(Receipt), E_{CB}(EPOID, Cacct, Bal, Flags))$
8. $M \rightarrow C : E_{CM}(Sig_B(Receipt), E_{CB}(EPOID, Cacct, Bal, Flags))$

Component	Description
$Product$	Bit string representing goods involved in the transaction
$RequestFlags$	Flags which indicates the customers specification for the transaction. Includes delivery instructions
TID	Transaction ID
$ProductID$	Human readable description of the goods
$Price$	Price of the goods
$Goods$	The electronic goods involved in the transaction
EPO	Bit string representing the Electronic Payment Order. Includes the Customer's ID, Product ID, Price, Merchant's ID, Request Flags, Cacct and EPOID data
$EPOID$	Unique ID for EPO
$Macct$	Merchant account number
K	The goods decryption key
$Receipt$	Response from the bank indicating a successful transaction
$Cacct$	Customer account number
Bal	Balance of customer's account
$Flags$	Bit string representing messages from the bank to the customer

Fig. 1. Summary of the NetBill Payment Protocol

NetBill payment scheme requires all eight messages to be transmitted for each successful transaction.

Because the voucher system requires fewer total online messages to be transmitted less online symmetric encryption is required; furthermore, the processing involved is concentrated more at the bank and less at the customer site. In terms of distributed networks centralised processing may not be optimal but it does allow the bank to easily handle dispute situations and allows the owner of the bank server to charge both customers and merchants. The voucher system does move a lot of online processing away from the merchant when

	NetBill	Voucher
Messages for successful payment	8	6
Online Messages	8	3
Offline Messages	0	3
Symmetric Encryptions	11	5
Customer	4	1
Merchant	5	2
Bank	2	2
Hash Calculations	4	2
Customer	3	0
Merchant	1	1
Bank	0	1
Signatures	3	3
Customer	1	1
Merchant	1	1(may be off line)
Bank	1	1

Table 1. A comparison of voucher and NetBill payment protocol processing and message transmission.

compared with the NetBill scheme.The voucher payment system requires the same number of digital signatures as NetBill for purchase of a single item, but one of these is not conducted during run time and may be re-used in subsequent transactions. The merchant need not sign the voucher as the payment protocol is run unlike the NetBill protocol. The voucher system also requires a smaller number of one-way hash functions but the processing for these functions is insignificant when compared to constructing digital signatures.

One of the differences between NetBill and the voucher system, which increases the number of messages required, is that the NetBill scheme distributes a receipt. When NetBill does this, all messages must pass through the merchant. In the voucher system, the bank transmits the proof of transaction directly to the customer. The merchant does not receive a receipt but may optionally request notification from the bank.

One of the advantages of the NetBill system is that it contains a bidding process which allows the merchant to discount the price of goods for groups of customers or individual customers. The voucher payment scheme does not include this facility. Merchants fix the price of goods when the voucher is created. The merchant would most likely advertise the price of the goods or services separately

from the voucher protocol on a web page. If the messages required for downloading the web page are included the total number of messages, both online and offline, for the voucher scheme and NetBill are very similar.

4.2 Comments Regarding Micropayment and Coin Based Payment Protocols

We are unable to fairly compare the voucher payment system with micropayment and coin based payment protocols because these payment systems have different design goals. The main reason for the introduction of electronic coins and the complexity and the large amount of processing associated with them was to enable the complete anonymity of the customer. The anonymity of the customer from the bank was not a design goal of the voucher system. Micropayment protocols such as Payword [22] are specially designed for efficiency. The voucher payment scheme is not as efficient as these schemes but it does include security features which have been dropped from micropayment schemes.

However, it is interesting to note how some design issues which designers of micropayment and coin based payment protocols wrestle with have been addressed or avoided by the voucher payment protocol.

The voucher payment protocol has an advantage over coin based payment protocols. The customer does not commit to the purchase of the goods until the voucher has been signed and received by the bank. No value is given to the voucher until the customer signs the goods. Thus in the situation where the customer's hard drive is accidentally erased, vouchers can be obtained again from the merchant with no loss to the customer. On the other hand if electronic coins are stored on the hard drive their value is lost to the customer. This is especially the case for anonymous cash systems.

The voucher payment scheme also avoids some of the issues, documented in [11], which Payword and other coin based payment schemes must address. One of these issues is divisibility. All of Payword's hash calculations are required to enable the customer to pay out small divisions of her Payword chain. In the voucher system, all goods are paid for without the need to divide the voucher.

Double spending is also not an issue for the voucher system. If a voucher is cashed in more than once to the bank, the correct merchant will always receive the correct value for the goods assuming attackers are unable to substitute their own signature and merchant identity within the voucher.

The property of transferability is also provided by the voucher scheme. Vouchers can be passed from one customer to the next and provided that the customer's acquiring bank has secure communications with the merchant's issuing bank, the voucher can be correctly cashed in. Given the secure communication of funds and keys assumed for transferability, the services of acceptability and scalability will also be provided. It is not unreasonable to assume that this network will be similar to the existing EFTPOS and other electronic funds transfer systems.

References

1. Martin Abadi and Roger Needham. Prudent Engineering Practice for Cryptographic Protocols. *Proceedings of the 1994 IEEE Symposium on Security and Privacy*, pages 122–136, May 1994.
2. Ross Anderson and Roger Needham. Robustness Principles for Public Key Protocols. In *Advances in Cryptology - Proceedings of CRYPTO '95*. Springer-Verlag, 1995.
3. Mihir Bellare, Juan A. Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Micheal Steiner, Gene Tsudik, and Micheal Waidner. iKP – A Family of Secure Electronic Payment Protocols. In *Proceedings of the First Usenix Workshop on Electronic Commerce*, New York, July 1995.
4. Jean-Paul Boly, Antoon Bosselaers, Ronald Cramer, Rolf Michelsen, Stig Mjolsnes, Frank Muller, Torben Pedersen, Birgit Pfitzmann, Peter de Rooij, Berry Schoenmakers, Matthias Schunter, Luc Vallee, and Michael Waidner. The ESPRIT Project CAFE - High Security Digital Payment Systems. In *Computer Security - ESORICS '94*, pages 217–230. Springer-Verlag, 1994.
5. Stefan Brands. Electronic Cash on the Internet. In *Proceedings of the Internet Society 1995 Symposium on Network and Distributed System Security*, pages 64–84, 1995.
6. David Chaum. Online Cash Checks. In *Advances in Cryptology - Proceedings of EUROCRYPT '89*, pages 288–301, 1989.
7. David Chaum, Amos Fiat, and Moni Naor. Untraceable Electronic Cash. In *Advances in Cryptology - Proceedings of CRYPTO '88*, Lecture Notes in Computer Science, pages 319–327. Springer-Verlag, 1990.
8. Benjamin Cox, J. D. Tygar, and Marvin Sirbu. NetBill Security and Transaction Protocol. In *Proceedings of the First Usenix Workshop on Electronic Commerce*, New York, July 1995.

9. Tony Eng and Tatsuaki Okamoto. Single-Term Divisible Electronic Coins. In *Advances in Cryptology - Proceedings of EUROCRYPT '94*, number 950 in Lecture Notes in Computer Science, pages 306–319. Springer-Verlag, 1995.
10. Niels Ferguson. Single Term Off-Line Coins. In *Advances in Cryptology - Proceedings of EUROCRYPT '93*, pages 318–328. Springer-Verlag, 1994.
11. Ernest Foo, Colin Boyd, William Caelli, and Ed Dawson. A Taxonomy of Electronic Cash Schemes. In *Proceedings of IFIP/SEC '97 13th International Information Security Conference*, pages 337–348. Chapman and Hall, 1997.
12. Matthew Franklin and Moti Yung. Secure and Efficient Off-Line Digital Money. In *Proceedings of ICALP '93*, number 700 in Lecture Notes in Computer Science, pages 265–276. Springer-Verlag, 1993.
13. VISA/MasterCard International. Secure Electronic Transaction (SET) Specification Book 1: Business Description. http://www.visa.com/cgi-bin/vee/sf/standard.html.
14. VISA/MasterCard International. Secure Electronic Transaction (SET) Specification Book 2: Programmer's Guide. http://www.visa.com/cgi-bin/vee/sf/standard.html.
15. VISA/MasterCard International. Secure Electronic Transaction (SET) Specification Book 3: Formal Protocol Definition. http://www.visa.com/cgi-bin/vee/sf/standard.html.
16. Markus Jakobsson and Moti Yung. Revokable and Versatile Electronic Money. In *Third ACM Conference on Computer and Communications Security*, pages 76–87. ACM Press, 1996.
17. Wenbo Mao. A Simple Cash Payment Technique for the Internet. In *Computer Security - ESORICS '96*. Springer-Verlag, 1996.
18. Gennady Medvinsky and B. Clifford Neuman. NetCash: A Design for Practical Electronic Currency on the Internet. In *Proceedings of First ACM Conference on Computer and Communications Security*, pages 102–196. ACM Press, 1993.
19. Tatsuaki Okamoto. An Efficient Divisible Electronic Cash Scheme. In *Advances in Cryptology - Proceedings of CRYPTO '95*, pages 438–451. Springer-Verlag, 1995.
20. Tatsuaki Okamoto and Kazuo Ohta. Universal Electronic Cash. In *Advances in Cryptology - Proceedings of CRYPTO '91*, pages 324–337. Springer-Verlag, 1992.
21. A. Shamir R. Rivest and L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM*, pages 120–126, 1978.
22. Ronald L. Rivest and Adi Shamir. PayWord and MicroMint: Two Simple Micropayment Schemes. http://theory.lcs.mit.edu/ rivest/RivestShamir-mpay.ps, January 1996.
23. Yacov Yacobi. Efficient Electronic Money. In *Advances in Cryptology - Proceedings of ASIACRYPT '94*, pages 153–163. Springer-Verlag, 1995.