A Fully Anonymous Electronic Payment Scheme for B2B[*]

Josep Lluís Ferrer-Gomila, Magdalena Payeras-Capellà, and Ll. Huguet-Rotger

Universitat de les Illes Balears
Carretera de Valldemossa km. 7.5, Palma de Mallorca, 07122, Spain
{dijjfg, mpayeras, dmilhr0}@clust.uib.es

Abstract. In this paper we present a fully anonymous (for payer and payee) electronic payment scheme for B2B transactions involving high amounts, without using tamper resistant devices, without pseudonyms, and preventing double spending. Schemes with detection of double spending at deposit are not well suited for high amount transactions (merchants and banks don't want to assume potential high losses). Our scheme allows anonymity revocation in case of illegal activities (using prevention techniques).

1 Introduction

B2B transactions demand a specific electronic payment scheme, because amounts can be high (more than 1000 dollars). It should be "impossible" to counterfeit money. It should not be based on tamper resistant devices [1, 4] (an attack could be very attractive). Nobody wants to assume possible double spending (with high amounts). So, it is not useful to detect double spending a posteriori, and we can not use transferable [5, 9] and/or off-line [2, 3, 7, 8] schemes. The anonymity should be absolute (as in paper-based transactions, e.g., for undeclared earnings). Otherwise, merchants will continue using paper money. We have to achieve the untraceabilty property (not achieved in [1, 6]). We don't want to use pseudonyms because it is not a real anonymity. The behavior of the bank has to be verifiable. Merchants and the bank have the necessary communications infrastructure to carry out on-line transactions. Finally, anonymity should be revocable if the appropriate authorities order it. In fact, some of the previous requirements were listed in [9]. But we have to keep in mind that this electronic payment scheme is specific for B2B and for high amounts.

Here we present a scheme that avoids counterfeiting, forgery and double spending, without using tamper resistant devices (nobody assumes undesirable risks). Untraceability and anonymity are guaranteed without using pseudonyms. Finally, our scheme allows the anonymity revocation in case of illegal activities (using prevention techniques when the illegal activity is suspected).

[*] This work has been partially supported by the Balearic Islands Government under project PRDIB-2002GC3-18.

J.M. Cueva Lovelle et al. (Eds.): ICWE 2003, LNCS 2722, pp. 76–79, 2003.

2 Fully Anonymous Electronic Payment Scheme

The presented scheme includes *withdrawal, transfer* and *deposit* sub-protocols. We use the term *e-note* to refer to the electronic bank notes. In the description of the protocol *A* is a merchant acting as a payer, *B* is the payee and *F* is the bank. Other notation and elements are as follows:

ID_X	identity of actor *X*
Q_i	amount to be withdrawn, transferred or deposited
Y, Z	concatenation of two messages (or tokens) *Y* and *Z*
$Sign_i(Y)$	digital signature of principal *i* on message *Y*
$i \rightarrow j$: Y	principal *i* sends message (or token) *Y* to principal *j*
$E_K(M)$	symmetric encryption of message *M* with key *K*
$PU_F(K)$	key *K* enciphered with the public key of the bank
$SN_i=H(SP_i)$	serial number (SN_i) of an *e-note*, hash of a random secret proof (SP_i)
$M_i= Sign_{Fx}(SN_i)$	signature on SN_i with a private key indicating value *x*

2.1 Withdrawal Sub-protocol

In the *withdrawal* sub-protocol, a merchant, *A*, requests an *e-note* to *F*. *F* creates an *e-note* and debits *A*'s account:

1. $A \rightarrow F$: $ID_A, Q_1, SN_1, Sign_A(Q_1, SN_1)$
2. $F \rightarrow A$: Q_1, SN_1, M_1

A generates a random number SP_1 (the secret proof to validate the *e-note*), and it must be kept secret. SN_1 (the serial number of the future *e-note*) is a hashing of SP_1. *A* proves ownership of his account signing the serial number and the amount, Q_1. *F*'s signature on SN_1, and SP_1, is the *e-note*. SN_1 will be used to prevent double spending of the *e-note*. *A* can prove the ownership with the knowledge of SP_1 and M_1.

To redeem an *e-note*, the owner must show the knowledge of the *e-note* secret proof (SP_1), but he is not forced to reveal his identity. If *F* saves all available information about the *e-note*, it could recognise that *e-note* at deposit, but thanks to the use of the *transfer* sub-protocol (see section 2.2), the bank (or the collusion of the bank and the merchant depositing the *e-note*) cannot reveal where *A* spent it. So payments will be anonymous and untraceables. And the scheme is secure against money forging.

2.2 Transfer Sub-protocol

When *A* wants to pay to *B*, *A* executes the following sub-protocol:

1. $A \rightarrow B$: Purchase_order
2. $B \rightarrow A$: $Q_i, SN_i, Sign_B(Q_i, SN_i)$
3. $A \rightarrow F$: $PU_F(K), E_K(SN_j, M_j, SP_j, Q_i, SN_i, SN_r)$
4. $F \rightarrow A$: M_i, M_r
5. $A \rightarrow B$: SN_i, M_i

B sends to *A* a serial number (SN_i), the price of the item (Q_i) and the digital signature of the previous information, as a response to the *Purchase_order*, without revealing the secret proof (SP_i). *A* will request to *F* an *e-note* to pay *B*, with the serial number given by *B* (SN_i). *A* sends her *e-note* M_j to the bank, with the associated secret proof (SP_j). The request is encrypted with a session key (*K*), so nobody can intercept SP_j. *A* indicates the amount (Q_i) of the *e-note* M_j to be converted in the new *e-note* using SN_i. The remaining fraction Q_r (if $Q_i < Q_j$) will be used to create another *e-note* with serial number SN_r. *F* cannot find out the identities of the merchants.

If SN_j is found in the list of spent *e-notes*, *F* has detected a double spending attempt, and will abort the operation. If the *e-note* (SP_j, M_j) is valid, *F* creates the new *e-notes* M_i and M_r, and sends them to *A*. *A* knows the *e-note* M_i and SN_i, but *A* doesn't know SP_i. *A* stores the information related to the payment during an established period. This information can be requested in case of anonymity revocation. The scheme is anonymous for *A*, because *B* doesn't know the identity of *A*.

B checks the validity of the *e-note* M_i (verifying the signature of *F*). Only *B* knows SP_i and he is the only one that can spend that *e-note*. He doesn't need to contact *F*. Now, *B* has an *e-note* with the same properties that a withdrawn one. *B* can deposit it identifying his account. Also, *B* can use the *e-note* for a new payment, but a collusion between *A* and *F* will be able to trace *B*. To solve this problem *B* has to use the auto-transfer sub-protocol.

Transfer Sub-protocol Applied to Auto-transfer. *A* knows SN_i and *B*'s identity. So, payments with that *e-note* could be traced by the collusion of *A* and *F*. The solution is the auto-transfer operation:

1. B → F: $PU_F(K), E_K(SN_i, M_i, SP_i, Q_s, SN_s, SN_t)$
2. F → B: M_s, M_t

B calculates SN_s and SN_t from the random secret proofs SP_s and SP_t, respectively. *B* requests *F* that a specific *e-note* is going to be transferred. *B* sends SP_i encrypted with a session key (and other information analogous to the previous case).

If the *e-note* is valid (e.g., not double spent), *F* creates two new *e-notes* with the new serial numbers and the required values, and SP_i is appended to the list of spent *e-notes*. *F* doesn't know who is the user auto-transferring the *e-note*. Furthermore, *F* cannot distinguish if the user is auto-transferring the total amount of the *e-note*, or if he is preparing a payment with a fraction of the *e-note* and auto-transferring the remaining part, or if he is preparing two payments.

2.3 Deposit Sub-protocol

In the *deposit* sub-protocol, it is necessary an identification of the merchant's account:

1. B → F: $PU_F(K), E_K(ID_B, SN_i, M_i, SP_i, Q_i), Sign_B(ID_B, SN_i, M_i, SP_i, Q_i)$

B sends the secret proof SP_i, and some identifying information (to deposit money in the right account), all encrypted with a session key *K*. *F* checks the validity of the *e-note*, and if it is correct then credits *B*'s account.

3 Conclusion: Fraud Protection and Privacy

We have achieved security requirements: *e-notes* cannot be counterfeited (thanks to the use of the bank private keys), overspending and double spending are avoided (*e-notes* are created after a debit in an user account, and the bank saves the list of redeemed serial numbers, deposited and transferred, with their secret proofs), and stolen *e-notes* cannot be redeemed (it is necessary the secret proof, and it is encrypted when is transmitted). On the other hand, our scheme provides anonymity and untraceability to payers and payees, thanks to the *auto-transfer* subprotocol. *E-notes* can be transferred multiple times without depositing and without any identification. Payments between the same pair of merchants are unlinkable. There isn't any relationship between them: new serial numbers are used in each payment.

Our scheme prevents illegal activities (as blackmailing, money laundering and illegal purchases/sales). For example, if blackmailing is suspected or reported, the appropriate authority will allow to the bank to demand the identity of the user who will try to *transfer* or *deposit* the suspicious serial number (*SN*). We don't use blind signatures to achieve anonymity, and so a blackmailed user always knows the serial number of the money given to the blackmailer. If money laundering is suspected, the authority will allow to the bank to demand user identification when this user is going to transfer the money.

We want to remark that we don't use tamper resistant devices, nor pseudonyms. The possibility of anonymous payment and redemption, the double spending prevention and other security properties, makes this scheme suitable for anonymous payments of high amounts in B2B transactions.

References

[1] Anderson, R., et alter: "NetCard - a practical electronic cash system", 4th Security Protocols International Workshop, LNCS 1189, pages 49-57, Springer Verlag, 1996.

[2] Brands, S.: "Untraceable off-line cash in wallet with observers", Crypto'93, LNCS 773, pages 302-318, Springer Verlag, 1993.

[3] Chaum, D., et alter: "Untraceable electronic cash", Crypto'88, LNCS 403, pages 319–327, Springer Verlag, 1988.

[4] Chaum, D. and Pedersen, T.: "Wallet databases with observers", Crypto'92, LNCS 740, pages 89–105, Springer Verlag, 1992.

[5] Eng, T. and Okamoto, T.: "Single-term divisible electronic coins", Eurocrypt'94, LNCS 576, pages 306–319, Springer Verlag, 1994.

[6] Medvinsky, G. and Neuman, B.C.: "Netcash: A design for practical electronic currency on the internet", 1st ACM Conference on Computer and Communication Security, pages 102–106, 1993.

[7] Mu, Y., et alter: "A Fair Electronic Cash Scheme", ISEC 2001, LNCS 2040, pages 20–32, Springer Verlag, 2001.

[8] Nakanishi, T. and Sugiyama, Y.: "Unlinkable Divisible Electronic Cash", ISW 2000, LNCS 1975, pages 121–134, Springer Verlag, 2000.

[9] Okamoto, T. and Otha, K.: "Universal electronic cash", Crypto'91, LNCS 576, pages 324–337, Springer Verlag, 1991.