PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ^{6} :
G06F 17/60, H04L 9/32

A1

(11) International Publication Number: **WO 98/25220**

(43) International Publication Date: 11 June 1998 (11.06.98)

(21) International Application Number: PCT/SG97/00065

(22) International Filing Date: 3 December 1997 (03.12.97)

(30) Priority Data:
9611524–1 4 December 1996 (04.12.96) SG

(71) Applicant *(for all designated States except US)*: INSTITUTE OF SYSTEMS SCIENCE [SG/SG]; National University of Singapore, Heng Mui Keng Terrace, Kent Ridge, Singapore 119597 (SG).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: DENG, Huijie [SG/SG]; 57 West Coast Road, Singapore 127787 (SG). NGAIR, Teow–Hin [SG/SG]; Block 334, Kang Ching Road #13–254, Singapore 610334 (SG).

(74) Agent: HO, Lawrence, Y., D.; Thongsia Building, 30 Bideford Road #07–02/03, Singapore 229922 (SG).

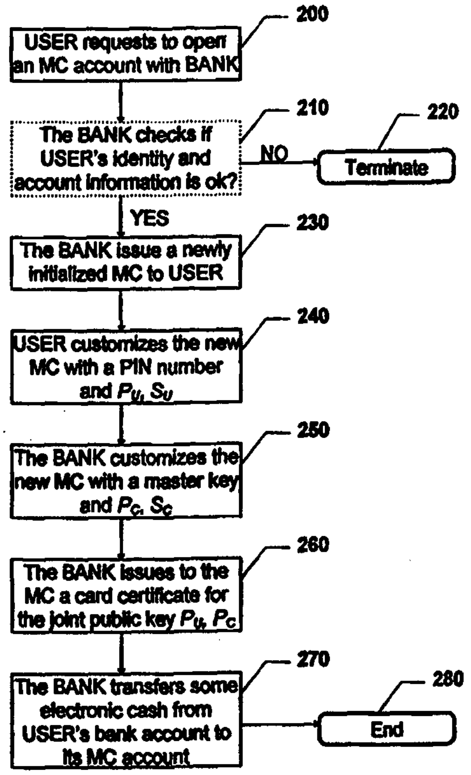
(81) Designated States: AU, CN, JP, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: MICROPROCESSOR CARD PAYMENT SYSTEM

(57) Abstract

The present invention is a system for implementing electronic payment with a tamper resistant microprocessor card (230). The microprocessor card (230) generates joint signatures under a joint digital signature scheme which derives its secret signature key from secret values (240, 250) contributes by different parties such as user, bank and service provider of electronic commerce. The joint signature is used to certify (260) the payment among other information. It follows that no one party has complete knowledge of the secret signature keys (240, 250) of the other parties; therefore, the use of joint digital signature in conjuction with microprocessor card (230) provides unprecedented security. The present invention also defines a protocol including payment, deposit, withdrawal and account opening (200) in providing added protection against potential security attacks. Above all, the protocol also supports off–line payment transactions, thus allowing transaction to be conducted scalably and economically over various forms of electronic networks, including unsecured ones.


200
USER requests to open an MC account with BANK
210
The BANK checks if USER's identity and account information is ok?
NO
220
Terminate
YES
230
The BANK issue a newly initialized MC to USER
240
USER customizes the new MC with a PIN number and P_U, S_U
250
The BANK customizes the new MC with a master key and P_C, S_C
260
The BANK issues to the MC a card certificate for the joint public key P_U, P_C
270
The BANK transfers some electronic cash from USER's bank account to its MC account
280
End

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

MICROPROCESSOR CARD PAYMENT SYSTEM

FIELD OF THE INVENTION

The present invention relates to the field to a system for making payment electronically. In particular, the present invention pertains to a system for conducting electronic commerce efficiently and securely using a temper resistant microprocessor card.

BACKGROUND OF THE INVENTION

It is well known in commerce to settle payment for goods and services with cash, cheques, credit cards and debit cards. With the advent of digital technology and increasing popularity of digital communications, there is an increasing need for new and secure means of electronic payment systems. Security is the overriding concern in electronic payment because it relies exclusively on transmission of digital information - a form which is easily duplicated or forged than its physical counterpart.

Many prior art methods meeting the security requirement of electronic payment are on-line payment systems. Examples are S. Dukach, "SNPP: a simple network payment protocol", Proceeding of the Computer Security Applications Conference, pp. 173-179, San Antonio, TX., Nov. 1992; Mastercard and Visa, "Secure Electronic Transaction", Feb. 1996; G. Medvinsky and B.C. Neuman, "NetCash: A design for practical electronic currency on the Internet", Proceedings of the ACM Conference on Computer and Communications Security, Nov. 1994; and K.R. O'Toole, "The Internet billing server transaction protocol alternatives", Carnegie Mellon University Information Networking Institute, INI TR 1994-1, Apr. 1994). Online financial clearing process is not only expensive, but also bandwidth limiting as it prevents the system from scaling up to handle large number of payment transactions. Such methods are also prone to total system failure because of server breakdown.

A few off-line electronic payment systems were also proposed. Exemplary of such systems are D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash", Advances in Cryptology -- Proceedings of Crypto '88, pp. 319-327, LNCS 403, Springer-Verlag, 1988; and S.A. Brands, "Off-line cash transfer by smart cards", CWI Technical Report CS-R9455, 1994. In general, the proposed off-line prior art systems introduced significant implementation complexity to address the issue of payment privacy.

OBJECT OF THE INVENTION

It is an object of the present invention to implement a system of electronic payment securely and efficiently.

It is another object of the present invention to implement a system of electronic payment scalably without experiencing bottleneck and technical difficulty under prior art systems.

It is yet another object of the present invention to implement a system of electronic payment over a wide range of payment modes.

SUMMARY OF THE INVENTION

The present invention is a system for implementing electronic payment with a tamper resistant microprocessor card. The microprocessor card generates joint digital signatures under a joint digital signature scheme which derives its secret signature key from secret values contributed by different parties such as user, bank and card manufacturer. The joint signature is used to certify the payment among other information. It follows that no one party has complete knowledge of the secret signature keys of the other parties; therefore, the use of joint digital signature in conjunction with a microprocessor card provides unprecedented security. The present invention also defines a protocol including payment, deposit, withdrawal and account opening in providing added protection against potential security attacks. Above all, the protocol also supports off-line payment transactions, thus allowing transaction to be conducted scalably and economically over various forms of electronic networks, including unsecured ones.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 illustrates three basic transactions in an electronic payment system.

FIG. 2 depicts an account opening transaction between a bank and a user.

FIG. 3 depicts an account opening transaction between a bank and a service provider (denoted by SP).

FIG. 4 shows a flowchart of the interaction between the user and the bank under the microprocessor card (denoted by MC) account opening protocol of the present invention.

FIG. 5 shows a set of possible data entries in the bank's database representing a microprocessor card account with the bank after the bank issues the new card to the user.

FIG. 6 illustrates a set of possible entry records in a user's microprocessor card after the user initialises it.

FIG. 7 is a protocol for a microprocessor card to generate a PAYMENT-CERT using the joint digital signature scheme of the present invention.

FIG. 8 shows a flowchart of the interaction between the user and the service provider under the payment protocol of the present invention.

FIG. 9 shows a flowchart of the interaction between the service provider and the bank under the deposit protocol of the present invention.

FIG. 10 shows the flowchart of the interaction between the user and the bank under the withdrawal protocol of the present invention.

DESCRIPTION OF THE EMBODIMENT OF THE INVENTION

A system for conducting electronic payment using a tamper resistant microprocessor card is described herein. In the following description, numerous specific details are set forth such as logical structures of digital information and program steps, etc. in order to provide a thorough understanding of the present invention. It will be obvious to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known parts such as those involved with the generation of public key and private key, and generation and verification of digital signature are not shown in order not to obscure the present invention.

Notation and Nomenclature

The detailed description with respect to conducting electronic payment using a tamper resistant microprocessor card is presented partially in terms of algorithm and symbolic representation upon operation on data bits with the computer or microprocessor card memory. These algorithmic descriptions and representations are the means used by those skilled in the art of electronic payment to most effectively convey the substance of their works to others skilled in the art.

An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. These steps are those require physical manipulation of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, and otherwise manipulated. In this case, the physical quantities are voltage or current signals which correspond to the digital objects/information being distributed. It proves convenient at times, principally for reason of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers or the like. It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities.

Furthermore, the manipulations performed are often referred to in terms such as adding or comparing, which are commonly associated with the mental operations performed by a human operator. No such capability of a human operator is necessary, or desirable. In most cases, in any of the operations described herein which form part of the present invention; the operations are machine operations. Useful machines for performing the operations of the present invention include general purpose digital computers or similar devices such as digital signal processors. In all cases, it should be borne in mind that there is a distinction between the method operation in operating a computer and the method of computation itself. The present invention relates to method steps for conducting electronic payment with a tamper resistant microprocessor card.

The present invention also relates to an apparatus for performing these operations. This apparatus may be specially constructed for the required purpose or it may comprise a general purpose computer as selectively activated or reconfigured by a computer program stores in the computer. The algorithms presented herein are not inherently related to any particular computer or other apparatus. In particular, various general purpose machines may be used with programs written in accordance with the teachings herein, or it may prove more convenient to construct specialised apparatus such as Smart Card terminal to perform the required method steps.

The required structure for a variety of these machines would appear from the description given below.

GENERAL SYSTEM CONFIGURATION

FIG. 1 shows a general model of an electronic payment system. Here, there are at least three different parties that are involved in various possible transactions with each other. A bank 10 refers to an agent responsible for issuing microprocessor card for electronic payment. The bank 10 may also be at least one clearing house which acts on behalf of a plurality of banks in clearing electronic payments. A user 20 using the microprocessor card issued by the bank 10 represents a payer who engages in electronic payment with a service provider 30 or a payee. A transaction 40 between the user 20 and the service provider 30 for payment involves, but not limited to, a microprocessor card and a card reader with a link to a terminal used by the service provider 30. The card reader can either be the property of the service provider 30 or the user 20. The link can be a dedicated physical cable, a telephone line, a wireless link, or through other electronic networks like the internet. A transaction 50 between the service provider 30 and the bank 10 for deposit involves, but not limited to, a terminal used by the service provider with a link to computer used by the bank. Similarly, this link can be any type of electronic connection. The transaction 60 between the bank 10 and the user 20 for withdrawal involves, but not limited to, a microprocessor card and a card reader linked to the bank computer. The card reader can be attached to a bank terminal or it can belong to some third party or the user. Similarly, the link between the card reader and the bank computer can be any type of electronic connection. In actual transactions, it should be understood by one skilled in the art that the bank 10 or the service provider 30 is usually represented by, but not limited to, a fully automated machine, a computer process, or a terminal. Furthermore, a user 20 can be any type of purchasing agent like a computer system routine or an organisation representing many people.

Before a payment transaction occurs, the user 20 obtains a microprocessor card from the bank 10. FIG. 2 shows symbolically a transaction 70 for opening an electronic payment account. Transaction 70 involves, but not limited to, a new microprocessor card and a trusted bank terminal with at least one card reader. It is unnecessary for the user 20 to be present and his role is taken by a proxy who can be a trusted third party or the bank 20 itself. Here, the microprocessor card is transferred or sold to the user 20 after transaction 70.

It also follows that before the bank 10 accepts deposit of payments by the microprocessor card, the service provider 30 opens an electronic deposit account with the bank 10. FIG. 3 illustrates symbolically a transaction 80 for opening an electronic deposit account. The transaction 80 involves, but not limited to, a new microprocessor card and a trusted bank terminal with a card reader.

The microprocessor card referred to above can be any form of secure microprocessor devices including but not limited to Smart Card, PCMCIA card, or specialised computing devices. Likewise, the card reader mentioned briefly before can be any form of devices including but not limited to Smart Card reader and PCMCIA card reader. The link between the microprocessor card and the card reader can be any type of digital signal transmission link including but not limited to physical electrical contacts, wireless communication, and infra-red link. It should be understood by one skilled in the art that the insertion of a microprocessor card into the card reader may therefore be any form of linkage between a card and a card reader including but not limited to physical insertion of card and position the card close to the card reader. Similarly, a PIN-number for a microprocessor card can be a short number, a number computed from an end-user's biometrics information, or any other numbers. The activation can also be substituted by any other means of enabling or unlocking the access to the microprocessor card.

This invention describes methods of executing electronic payment using a tamper resistant microprocessor card. By tamper resistant microprocessor card, the present invention refers to a microprocessor card which repels most but not all forms of security attack. Tamper resistant microprocessor card contrasts with its tamper proof counterpart. As shall be disclosed further below, the unique combination of public keys and digital signature achieves enhanced security without relying on tamper proof microprocessor card. This is one of the key features of the present invention.

With respect to the implementation of a tamper resistant microprocessor card, some of these steps are realised as special purpose software running on general purpose computers. It should be understood by one skilled in the art that each of the service provider, bank and user can simultaneously engage in multiple transactions with other parties. It is also clear that there may be multiple banks, multiple microprocessor cards, and multiple different transaction protocols that serve different electronic payment requirements. For the rest of the presentation of the embodiment of this invention, the description will elaborate on a simplified model of one bank, one service provider, and one user.

PREFERRED EMBODIMENT OF THE PRESENT INVENTION

Referring again to FIG. 1, the transactions 40, 50, and 60 between the parties of electronic commerce are transmission of electronic information protected by digital identification. In the preferred embodiment of the present invention, identification is implemented by using a combination of hash function, digital signature and public key certificate. For further references on hash function, digital signature and public key certificate, please refer to W. Stallings, "Network and Internetwork Security -- Principles and Practice", IEEE Press, Prentice Hall, Englewood Cliffs, New Jersey, 1995; and C. Kaufman, R. Perlman, and M. Spencier, "Network Security -- Private Communication in a Public World", PTR Prentice Hall, Englewood Cliffs, New Jersey, 1995.

In the present invention, a public key certificate CARD-CERT is embedded in each microprocessor card to certify its authenticity. The details of how the CARD-CERT is generated and its data structure are elaborated further below in connection with the process flow as illustrated in FIGS. 4 - 6. Each time the user 20 uses the microprocessor card to conduct a transaction, a different payment transaction certificate PAYMENT-CERT is issued by the microprocessor card. The CARD-CERT and PAYMENT-CERT are not necessarily generated with the same digital signature scheme nor with the same security strength.

More importantly, PAYMENT-CERT incorporates a notion called joint digital signature. A joint digital signature is created by a signature scheme that derives its joint public and private keys from multiple (in this embodiment two) public and private key pairs. In the preferred embodiment of the present invention, the different key pairs are contributed by the bank 10 and the user 20. The purpose of using joint digital signature in conjunction with a microprocessor card is to prevent any single party in electronic commerce except the microprocessor card itself from knowing the private key of the joint digital signature scheme. As such, any party receiving the PAYMENT-CERT is assured that the payment is generated by the microprocessor card on behalf of the user. Besides generating the PAYMENT-CERT, the present invention also allows the service provider 30 to identify and authenticate itself. As shall be elaborated further below, the overall security of electronic payment is enhanced by having a microprocessor card generate joint digital signature.

SETUP PROCEDURE

Opening a user account

Prior to engaging in any electronic payment, the user 20 registers itself with the bank 10 to obtain a microprocessor card as depicted in FIG. 2. FIG. 4 illustrates the account opening process. In step 200, the user 20 requests from the bank 10 for a microprocessor card by, for example, supplying its identification information, a bank account from where cash or electronic equivalent thereof can be transferred to a new microprocessor card account, and the initial cash value of the microprocessor card. The bank 10 verifies user's information in step 210 and issues the user 20 a new microprocessor card in step 230. The bank 10 may optionally provide the user 20 with the hardware and software necessary for the user to perform some of the electronic payment transactions over various electronics networks.

Referring again to FIG. 4, the user 20 in step 240 selects its PIN-number and a public/private key pair denoted by P_U and S_U. The private key S_U should only be known to the microprocessor card and possibly the user. Some methods in which the secrecy of key S_U can be maintained are: 1) using a trusted bank terminal, a list of appropriate random keys is presented to the user for selection. After storing the user's selected private key into the microprocessor card, the bank terminal discards the values permanently; 2) the microprocessor card comes with a random private key generation routine, and the bank's terminal relies on this routine to create the key S_U and the corresponding public key P_U; 3) since the user needs not know the value of key S_U, a random private key can be stored in the card during the card's manufacturing process.

Following the user's customisation process in step 240, the bank 10 in step 250 selects a different public/private key pair denoted by P_C and S_C and an optional master key for the microprocessor card. Next, in step 260 the bank 10 then uses its own private key S_B to create a public key certificate of the joint public key of P_C, P_U and some other information denoted by *cert*$_B$ *(inter, info, P_C, P_U)*. A public key certificate in the present invention contains a digital signature of the data items it certified. The certificate is hereafter referred to as the CARD-CERT. The CARD-CERT contains a data item *inter* that indicates the validity interval of the certificate. Another information data item *info* that identifies the bank and the microprocessor card. The *info* also contains other relevant information like the currency unit of the microprocessor card and any constraint placed on the use of the certificate, for example, that the CARD-CERT can be used only to make telephone calls. Note that the identity of the bank is useful for electronic payment when there are multiple electronic payment systems provided by different banks or even by one single bank.

In step 270 of FIG. 4 the bank transfers an appropriate amount of electronic cash from the user's bank account to the user's new microprocessor card account. The new microprocessor card account is represented by a database record with the bank and illustrated in FIG. 5. The *C_balance* entry of the database record is initialised accordingly. Finally, in step 280, the bank signals the completion of the user's microprocessor card account opening process and prompts the user to collect the new microprocessor card.

FIG. 6 shows a possible set of data entries which are stored in the microprocessor card after the bank and the user initialise and customise it. Referring again to both FIGS. 5 and 6, the *card#* represents a number unique for each microprocessor card; the bank identifies the microprocessor card with this entry. The *user record* entry in FIG. 5 identifies the user and its bank account from where electronic cash can be transferred to its microprocessor card account. In this same entry the bank records other important information about the user.

Again in FIGS. 5 and 6 the initial value of the entry *C_balance* is identical. This entry in the user's microprocessor card account as shown in FIG. 5 is adjusted by an appropriate value (plus any optional service fee) when the bank 10 approves an electronic payment or withdrawal. FIG. 5 illustrates a possible entry record in a user's microprocessor card account after the bank and the user initialise it. While only record 1 is explicitly shown, a microprocessor card can have multiple CARD-CERT in its lifetime, and new records are added to the microprocessor card account to reflect this change.

In FIGS. 5 and 6 the sequence numbers *seq#* and *ser#* are non-repeating numbers that are used to generate PAYMENT-CERT and permit the user to participate in various other transactions. As will be shown further below, the bank and service provider rely on such sequence numbers to prevent various well-known security attacks on the public key certificate and digital signature scheme, such as the replay attack.

Opening a service provider account

The service provider 30 needs to register itself with the bank 10 before it can process any electronic payment from the user 20. The registration procedure is depicted in FIG. 3 The account opening process is substantially the same as that of the user opening a microprocessor card account with the bank as described in FIG. 4. The only differences are:

1. The account type is designated as a deposit account in step 200 instead of a microprocessor card account;
2. The service provider's bank account information in step 210 will be used for deposit instead of withdrawal;
3. The entry *card#* in FIGS. 5 and 6 is known as *S_id* to allow the service provider to communicate with the user and the bank;
4. The entry *C_balance* has no value and step 270 in FIG. 4 is omitted as service provider's microprocessor card account with the bank is used for authenticating the service provider; and
5. The service provider has the necessary software and hardware to accept from the user electronic payments and to deposit them with the bank.

TRANSACTION PROTOCOL OF THE PRESENT INVENTION

1. The Payment Protocol

FIG. 8 is a flowchart of the interaction between the user and the service provider under the payment protocol of the present invention. After registering with the bank, the user uses its microprocessor card to engage in an electronic payment with a service provider. The service provider is assumed to have registered with the bank so that the service provider has at least the following information: 1) the bank's public key and related signature information; and 2) a unique value *S_id* that identifies the service provider with the user and the bank. For a service provider linked to different electronic payment systems offered by different banks, it will have one distinct set of values for each system.

When the user 10 makes a purchase with its microprocessor card, it approaches a service provider 30, either physically or through an electronic network. The user presents its microprocessor card to either the service provider's terminal or the user's own personal computing device coupled to an electronic network as shown in step 400 in FIG. 8. Next in step 410 the service provider reads the CARD-CERT within the microprocessor card and verifies its validity in step 420. The verification in step 420 includes, but not limited to, checking the bank's signature on the CARD-CERT, possible blacklisting of the CARD-CERT, and the time validity specified in the value *inter*.

Again in FIG. 8 the service provider presents the user in step 440 with a payment specification (denoted by *spec*) to confirm. The specification includes, but not limited to, time, date and amount of the payment, and the identity of the service provider. The amount should be converted to the microprocessor card's currency unit if that is not the default unit. Should the transaction be carried over insecure transmission channel or devices, additional information specifying the full details of the purchase and delivery may also be included and probably in a compressed form. If further security is needed, the service provider will have to digitally sign the payment specification. Receiving the payment specification, the user in step 450 enters its PIN number to approve the payment. In step 470 the approval of the payment is send to the microprocessor card. Next, in step 480, the microprocessor card performs validity checks. If the microprocessor card has been locked due to possible errors including, but not limited to, consecutive entry of incorrect PIN numbers (the microprocessor card adjusts an error counter value whenever an incorrect PIN number is entered as in step 490), then the transaction is terminated in step 500. Otherwise, the microprocessor card checks additionally in step 510 for, but not limited to, cash balance, and any authenticated information. If successful, the microprocessor card generates in step 530 the PAYMENT-CERT using the joint digital signature on the payment specification. After receiving the PAYMENT-CERT from the microprocessor card, the service provider verifies in step 540 the joint digital signature and other possible anomalies such as duplicate PAYMENT-CERT. The service provider confirms the payment in step 570 if the verification is successful.

Optionally, the service provider 30 performs a random on-line electronic clearance with the bank 10 or a clearing house for additional security. Such clearance may be a requirement if the payment *amount* exceeds certain predetermined approved value.

FIG. 7 shows the protocol of a microprocessor card in generating a PAYMENT-CERT. It shows that a PAYMENT-CERT is a joint digital signature generated by the joint private keys represented by S_C, S_U. The information being signed includes the payment specification *spec* and an increasing sequence number *ser#*. The payment specification can incorporate additional information. The *ser#* is a non-repeating number used to distinguish every payment under a specific CARD-CERT or a specific service provider and needs not be an increasing value.

The preferred embodiment of the present invention illustrates a practical implementation of generating the PAYMENT-CERT using a joint digital signature based on the Schnorr signature scheme. For information on the Schnorr signature scheme, please refer to C.P. Schnorr, "Efficient Signature Generation by Smart Card", Journal of Cryptology, pp. 161-174, Vol. 4, No. 3, 1991. The bank chooses two prime numbers Q and P such that Q divides P - 1. The bank also chooses a number g such that g is a generator of order Q. The numbers P, Q, and g are public information and are made known to the public in an authenticated manner. Then the public/private key pair P_U and S_U selected by the user in step 240 of FIG. 4 are such that S_U = a random number less than Q, and $P_U = g^{-S_U} \bmod P$. The public/private key pair P_C and S_C selected by the bank in step 250 of FIG. 4 are S_C = a random number less than Q, and $P_C = g^{-S_C} \bmod P$. Then the joint private key of the user's microprocessor card is $(S_U + S_C) \bmod Q$ and the corresponding joint public key is $(P_U P_C) \bmod P$. The PAYMENT-CERT in FIG. 7 can be created by the microprocessor card as follows:

1. Generate a random number w which is less than Q
2. Compute $a = g^{w} \bmod P$
3. Compute $b = h\ (ser\#, spec, a)$, where h is a one-way hash function
4. Compute $r = (b\,(S_C + S_U) + w) \bmod Q$
5. Create PAYMENT-CERT = $\{ser\#, spec, b, r\}$

To verify the PAYMENT-CERT, all that one has to do is to verify that

$$b = h\,(ser\#, spec, g^{r}\ (P_C P_U \bmod P)^{b} \bmod \mathrm{P}).$$

2. The Deposit Protocol

At the end of a business day or other appropriate interval, the service provider conducts a deposit transaction with the bank as illustrated in FIG. 9. The data item that the service provider sends to the bank is the same information that it received from a microprocessor card - the CARD-CERT and the PAYMENT-CERT. Overall, the service provider makes a deposit with the following steps:

1. Connects to the bank's deposit computer as in step 600;
2. Sends the service provider's identity to the bank as in step 610;
3. Sends all payments (CARD-CERT and PAYMENT-CERT) in one single transfer as in step 640;
4. Receives an optional receipt from the bank in step following step 640; and
5. receives the status and/or error information for each payment deposit in step 710.

In the case of multiple electronic payment systems offered by different banks, the service provider can sort the payments it receives accordingly and contacts different banks appropriately. Where there are multiple PAYMENT-CERTs under the same CARD-CERT, the service provider can combine these payments for efficient transmission. It is also possible for a clearing house to process the service providers' deposits before it re-transmits to various issuing banks. In this way, the clearing house can reduce the total communication costs for deposit. With respect to verification, the clearing house can help the banks by performing the front end tasks of checking the certificates and thus alleviate the computation required of the banks' computers. Therefore, the transaction protocols of the present invention facilitate the set up of multiple clearing houses to scale up the present invention on electronic payment system.

With reference to the service provider's actions described in the preceding two paragraphs, the bank verifies the information it receives from the service provider in step 620 of FIG. 9. As mentioned briefly above, the service provider identifies itself with a bank by using a unique *S_id* value which is incorporated in the service provider's microprocessor card or terminal. If the bank's verification is successful, then the service provider continues to transmit the electronic payments it wishes to deposit with the bank in step 640. At this juncture, the bank transmits optionally a receipt, for example a check sum value, to confirm the transmission is error free.

Again in FIG. 9, an iteration process steps 650 - 700 follows next. For every electronic payment the bank receives, it checks if the associated CARD-CERT is valid in step 660. Such verification comprises checking the CARD-CERT's signature, validity period, and cross referencing against a list of blacklisted CARD-CERTs and the user's microprocessor card account. The bank rejects the electronic payment if any of such checks fails, and take the appropriate action for such failure. Otherwise, it continues in step 670 to check if the associated PAYMENT-CERT is valid. This step involves checking its signature, its data and time validity, its *S_id* information against the current depositing service provider, its embedded sequence number *ser#* against that of the user's or service provider's microprocessor card account with the bank, and the payment amount against *C_balance* in the user's microprocessor card account. Note that a double deposit of PAYMENT-CERT will be detected during the check of *ser#* against that in the user's or service provider's microprocessor card account. If the preceding checks fail, then the particular payment will be rejected and the bank should be alerted of possible security breach, if any, accordingly. Otherwise, the bank proceeds in step 690 to transfer the *amount* specified in the PAYMENT-CERT from the user's microprocessor card account to the service provider's deposit account, It will also update the user's or service provider's microprocessor card account on the new payment to prevent double deposit in the future. In step 700, the iteration process is repeated for the remaining PAYMENT-CERTs. After all payments have been processed by the bank, the bank sends a summary of status of the deposit session to the service provider in step 710 and ends the transaction in step 720. The bank may also transmit a status report and error report to the service provider immediately after the checks in steps 660 and 670 for each payment deposit.

To improve the communication security of the deposit protocol, all messages between the service provider and the bank should be protected by using freshness identifier, such as time stamp and sequence number, and integrity check value, such as digital signature, to protect against active attacks like replay, modification and insertion.

3. The Withdrawal Protocol

When the user 20 tops up the cash value in its microprocessor card, it approaches the bank 10 for a withdrawal transaction. Withdrawal takes one of several forms: 1) through a bank teller by completing a transfer form; 2) via a bank terminal; or 3) from the user's computer with a link to the bank's computer.

FIG. 10 is a flowchart of the withdrawal protocol. Authentication between the bank 10 and the user 20 is realised with digital signature. Alternate means includes secret keyed one-way hash value based on non-repeating contents. The latter can be used because the tamper resistant nature of a microprocessor card resolves many potential disputes. Furthermore, verifying one-way hash value is computationally economical than verifying digital signature. The contents comprise secret values and non-repeating numbers shared between the bank 10 and the user 20.

Again in FIG. 10, the user begins the withdrawal process in step 800 by inserting its microprocessor card into the appropriate bank terminal. It should be understood by one skilled in the art that withdrawal is executable through an electronic network. The bank computer in step 810 reads the microprocessor card's CARD-CERT before verifying its validity in step 820. If successful, the user in step 840 is prompted to enter its PIN number, the withdrawal amount, and request for a withdrawal transaction. The information in step 840 is sent to the microprocessor card and validity of the PIN number checked in step 850. If again successful, the microprocessor card in step 870 computes an authenticated withdrawal request and sends it to the bank. The request contains preferably non-repeating information, i.e., non-repeating value of *seq#* to foil or identify replay attack. The authenticated withdrawal request optionally contains the microprocessor card's *card#* , *C_balance* , and the specified withdrawal amount. As described above, the request contains either a digital signature or a secret keyed hash value for authentication. After receiving the request, the bank in step 880 checks the validity of the request. The check includes verifying the authentication data included in the request, and comparing the respective cash balances in the microprocessor card and the user's microprocessor card account. If successful, the bank in step 900 adjusts the user's microprocessor card account to reflect the transaction and in step 910 sends an authenticated acknowledgment to the microprocessor card. This authentication should be based on different contents to foil possibly replay attack. The microprocessor card checks to confirm that correct transaction has been carried out by the bank. The microprocessor card then adjusts its internal state in step 920 to reflect the successful conclusion of the withdrawal process. The bank proceeds in step 930 to print out a transaction record and ends the withdrawal process in step 940.

In step 910 of FIG. 10, an optional renewal of the CARD-CERT of the microprocessor card may be performed. This is done generally for the purpose of increasing the security of the system as well as helping to optimise various bookkeeping processes in the electronic payment system. Some of the conditions for such renewal may depend on values like the remaining validity period of the current CARD-CERT. As a special case, the user may request for a zero value renewal. This is useful if the user just wants to renew its microprocessor card CARD-CERT.

ALTERNATE EMBODIMENTS OF THE INVENTION

While the preferred embodiment of the present invention above describes an essentially debiting system based on the smart card platform, the setup and protocol of the present invention are suitable for a secured off-line credit card payment system. Below are modifications to the description of the preferred embodiment to accomplish such an extension.

Opening a user account

The opening of a user account is identical to that of the preferred embodiment for an electronic cash payment. The only differences are that *C_balance* is now used as a credit limit that the bank sets for the microprocessor card, and no cash value is transferred to the user's microprocessor card account as shown in step 270 in FIG. 4 during the account opening process.

Opening a service provider account

The opening of a service provider account with respect to a credit card payment is substantially the same as the steps described in the preferred embodiment of the present invention which covers an electronic cash payment system. As one can see, one of the advantages of the present invention is the simple and uniform setup and protocol for the service provider with respect to various forms of electronic payment.

1. The Payment Protocol

The off-line payment protocol for a credit card payment is the same as that for an electronic cash payment described above. However, on-line account checking with the bank or clearing house is recommended as a policy because of the increased risk of credit card payment.

2. The Deposit Protocol

The deposit protocol for off-line credit card payment is substantially the same as that for off-line debit card payment. One major change to the previously described deposit protocol is the manner in the bank's transfer of funds from the user's microprocessor card account. For each valid PAYMENT-CERT, the bank does not transfer the payment *amount* directly from the user's microprocessor card account to the service provider's account as in step 690 of FIG. 9. Instead, the payment *amount* subtracting any appropriate fees is deducted from the bank's own account and such transfer may be delayed according to the on-going credit card clearing policy.

3. The Withdrawal Protocol

The withdrawal protocol of an off-line electronic cash payment is adaptable for a settlement protocol of a credit card payment. This settlement protocol is substantially the same as the withdrawal protocol as shown in FIG. 10. The differences are that the bank's ability to impose a maximum top-up amount in step 840 in line with the bank's credit limit for that user, and that interests are chargeable for each credit transaction and late payment.

One can appreciate that the protocol of the present invention does not conflict with existing credit card payment systems. In fact, the present invention complements existing financial practices. An example is the extension of the withdrawal protocol to accommodate a variety forms of settling credit card payments, whether be it cheques or electronic fund transfer. The bank is able to reconcile such settlements and adjust the value of the entry *C_balance* accordingly. Furthermore, an optional on-line withdrawal protocol can be embedded into the payment protocol where the service provider or its terminal executes transparently if the value of *C-balance* is insufficient to cover payment *amount*. In such instances, no transfer of funds occurs but the bank can update the value *C_balance* in the user's microprocessor card via the service provider or its terminal as soon as the user settles its credit card payment by other means. As such, the user's credit information is updated efficiently without requiring additional hardware and software overhead.

The third embodiment of the present invention describes a secure electronic cheque payment system. Here, the difference between an electronic cash payment and an electronic cheque is akin to the difference between cash and cheque. Description below highlights changes to the setup procedure and protocol relating to the description of the preferred embodiment for electronic cash payment.

Opening a user account

A user opens an electronic cheque account in substantially the same way as the account opening procedure for electronic cash payment. The significant changes are the omission of the *C_balance* entry and the absence of any cash transfer to the user's microprocessor card account in step 270 of FIG. 4. *C_balance* may optionally represent the number of cheques issued.

Opening a service provider account

The step a service provider takes to open an electronic cheque account is substantially the same as that for electronic cash.

1. The Payment Protocol

The off-line payment protocol for electronic cheque is substantially the same as that for electronic cash. The only difference is that no verification of payment *amount* in PAYMENT-CERT with a preset spending limit is necessary but a decrement of the C_balance , if present, limits the number of cheques issuable.

2. The Deposit Protocol

The deposit protocol for executing electronic cheque in this embodiment of the present invention is substantially the same as that for electronic cash in the preferred embodiment. The only difference is that for each valid PAYMENT-CERT the bank transfer the payment *amount* directly from the user's bank account, instead of its microprocessor card account, to the service provider's account. It is possible to have insufficient fund in the user's bank account and therefore electronic cheque may bounce just as any ordinary cheque.

3. The Withdrawal Protocol

The present invention does not envisage the need for a withdrawal protocol for executing electronic cheque in this embodiment of the present invention.

While the present invention has been described particularly with reference to FIGS. 1 to 10 with emphasis on a system for conducting electronic payment using a tamper resistant microprocessor card, it should be understood that the figures are for illustration only and should not be taken as a limitation on the invention. In addition, it is clear that the method and apparatus of the present invention have utility in many applications where secure electronic transmission and verification of information are required. It is contemplated that many changes and modifications may be made by one of ordinary skill in the art without departing from the spirit and the scope of the invention as described.

CLAIMS

1. A method for one party to verify information signed by another party over a communication link, said method comprising the steps of:

(a) selecting for each said parties at least one pair of public and private keys under a first predetermined digital signature scheme;

(b) creating a joint digital signature by combining said pair of public keys and private keys respectively under a second predetermined digital signature scheme; said joint digital signature incorporating at least one joint public key and at least one joint private key;

(c) transmitting information securely by signing the information with said joint private keys; and

(d) verifying the validity of said joint digital signature by verifying the signature with said joint public keys,

whereby information signed with said joint digital signature scheme minimises unauthorised signature generation and modification thereto without knowledge of said joint private keys.

2. The verification method as defined in claim 1 wherein said communication link comprises an interface between a microprocessor card and an interface for reading said card.

3. The verification method as defined in claim 1 wherein said communication link comprises at least one computer network.

4. The verification method as defined in claim 1 wherein said first predetermined digital signature scheme is the same as said second predetermined digital signature scheme.

5. The verification method as defined in claim 1 wherein said first predetermined digital signature scheme is different from said second predetermined digital signature scheme.

6. The verification method as defined in claim 1 wherein said combination of public and private key comprising mathematical operation, the result of said combination further creating a joint public and private key pair.

7. The verification method as defined in claim 1 wherein a third predetermined portion of each said selected key is omitted if such omission is retrievable from the remaining portion of said selected keys.

8. The verification method as defined in claim 6 wherein said combination of public and private keys comprises additional keys selected by said parties.

9. In a system for executing electronic payment with at least one tamper resistant microprocessor card, said system including at least one bank, at least one user, and at least one service provider, a method for creating secure signature for said card comprising the steps of:

(a) selecting for each said bank and said user at least one pair of public and private keys under a first predetermined digital signature scheme;

(b) creating a joint digital signature scheme for said card by combining said pair of public keys and private keys respectively under a second predetermined digital signature scheme; said joint digital signature scheme having at least one joint public key and at least one joint private key;

(c) embedding said pair of private keys in said microprocessor card such that neither bank, service provider nor user knows said pair of private keys;

(d) transmitting payment information with said card by signing payment information with said joint private keys; and

(e) checking the validity of said payment information by verifying said joint digital signature with said joint public keys,

whereby payment information signed with said joint digital signature scheme minimises unauthorised generation and modification thereto without knowledge of said joint private keys.

10. The joint digital signature method as defined in claim 9 wherein said card establishes communication link with either said service provider or said bank, said communication link further comprising an interface between said card and an interface for reading said card.

11. The joint digital signature method as defined in claim 10 wherein said communication link comprises at least one computer network.

12. The joint digital signature method as defined in claim 9 wherein said first predetermined digital signature scheme is the same as said second predetermined digital signature scheme.

13. The joint digital signature method as defined in claim 9 wherein said first predetermined digital signature scheme is different from said second predetermined digital signature scheme.

14. The joint digital signature method as defined in claim 9 wherein said combination of public and private key comprising mathematical operation, the result of said combination further creating a joint public and private key pair.

15. The joint digital signature method as defined in claim 9 wherein a third predetermined portion of each said selected key is omitted if such omission is retrievable from the remaining portion of said selected keys.

16. The joint digital signature method as defined in claim 15 wherein said combination of public and private keys comprises additional keys selected by other parties.

17. The joint digital signature method as defined in claim 9 wherein said pair of public and private keys selected by said user is created in part by said bank.

18. The joint digital signature method as defined in claim 9 wherein said pair of public and private keys selected by said user is created in whole by said bank.

19. The joint digital signature method as defined in claim 9 wherein said pair of public and private keys selected by said user is created in part by said card manufacturer.

20. The joint digital signature method as defined in claim 9 wherein said pair of public and private keys selected by said user is created in whole by said card manufacturer.

21. The joint digital signature method as defined in claim 9 wherein said pair of public and private keys selected by said user is created in part by a random value generator program embedded in said card.

22. The joint digital signature method as defined in claim 9 wherein said pair of public and private keys selected by said user is created in whole by a random value generator program embedded in said card.

23. The joint digital signature method as defined in claim 9 wherein said pair of public and private keys selected by said user is created in part by a trusted third party.

24. The joint digital signature method as defined in claim 9 wherein said pair of public and private keys selected by said user is created in whole by a trusted third party.

25. In a system for executing electronic payment with at least one tamper resistant microprocessor card, said system including at least one bank, at least one user, and at least one service provider, a method for opening a microprocessor card account and securing said microprocessor card comprising the steps of:

(a) selecting by said bank for said microprocessor card at least one pair of public and private key P_C and S_C under a first predetermined digital signature scheme;

(b) selecting by said user for said microprocessor card at least one pair of public and private key P_U and S_U under a second predetermined digital signature scheme;

(c) combing the two said pairs of public and private keys to create a joint signature scheme under a third predetermined digital signature scheme, said joint signature scheme incorporating at least one joint public key and one joint private key.

(d) generating a certificate for said microprocessor card for certifying the validity of said card and the said joint public keys, said card certificate being signed by a digital signature for said card using the bank's private key under a fourth predetermined digital signature scheme;

(e) embedding in said microprocessor card said card certificate such that access thereto is restricted, said microprocessor card having at least one body, said body including identification field for identifying uniquely said microprocessor card, private key fields for storing the said joint private keys, and information field for storing said card certificate;

(f) storing with said bank at least one data entry for each said microprocessor card account, said entry comprising at least one entry body, said entry body including identification field for identifying uniquely each said microprocessor card account, and information field for storing corresponding card certificate;

(g) initialising said microprocessor card account and said microprocessor card with an initial transfer value, said value representing electronic cash; and

(h) issuing to said user said microprocessor card,

whereby verification of electronic payment generated by said microprocessor card is assured with said joint digital signature of said card.

26. In a system for executing electronic payment with at least one tamper resistant microprocessor card, said system including at least one user and at least one service provider, a method for enhancing the security of

each electronic payment generated by said microprocessor card comprising the steps of:

(a) checking the validity of the microprocessor card certificate by verifying the certificate signature;

(b) extracting the joint public keys from the microprocessor card certificate;

(c) agreeing by said service provider and said user to a payment specification grouping, said grouping containing at least said service provider's identity and payment amount;

(d) creating a joint digital signature for said grouping of payment specifications using the joint private keys embedded in the microprocessor card under a predetermined digital signature scheme and resulting in a payment certificate

(e) transmitting payment certificate by said microprocessor card; and

(f) checking the validity of said payment certificate by verifying said joint digital signature with said joint public key,

whereby electronic payment generated by said microprocessor card is secured as long as none of the parties knows the joint private keys embedded in said microprocessor card.

27. The method for enhancing the security of each electronic payment generated by said microprocessor card as in claim 26 wherein said joint digital signature is based on partial grouping of payment specification.

28. In a system for executing electronic payment with at least one tamper resistant microprocessor card, said system including at least one user and at least one service provider, a method adopted for implementing off-line

and secured electronic payment generated by said microprocessor card comprising the steps of:

(a) verifying by said service provider the validity of said microprocessor card;

(b) generating by said microprocessor card a payment certificate, said payment certificate being created as a joint digital signature under a predetermined digital signature scheme for said grouping of payment specifications using the joint private keys embedded in the microprocessor card ; and

(c) grouping said payment specifications, said card certificate and said payment certificate,

whereby electronic payment generated by said microprocessor card is secured and processable in an off-line manner as long as none of the parties knows the joint private keys embedded in said microprocessor card.

29. In a system for executing electronic payment with at least one tamper resistant microprocessor card, said system including at least one user and at least one service provider, a method for implementing off-line and secured electronic payment generated by said microprocessor card comprising the steps of:

(a) verifying by said service provider the validity of said microprocessor card;

(b) agreeing by said service provider and said user to a payment specification;

(c) activating by said user said microprocessor card for payment transaction;

(d) generating by said microprocessor card a payment certificate, said payment certificate being created as a joint digital signature under a predetermined digital signature scheme for said grouping of payment specifications using the joint private keys embedded in the microprocessor card ; and

(e) grouping said payment specifications, said card certificate and said payment certificate,

whereby electronic payment generated by said microprocessor card is secured and processable in an off-line manner as long as none of the parties knows the joint private keys embedded in said microprocessor card.

30. In a system for executing electronic payment with at least one tamper resistant microprocessor card, said system including at least one user and at least one service provider, a method for implementing secure electronic deposit generated by said microprocessor card comprising the steps of:

(a) establishing by said service provider communication link with said bank;

(b) identifying by said service provider with said bank;

(c) collecting grouping of payment specifications and transmitting the same to said bank;

(d) verifying by said bank the validity of each depositing electronic payment, said bank adjusts the accounting information of said user and said service provider within said bank's record ; and

(e) updating said service provider by said bank with accounting and status information,

whereby deposit information generated by said service provider is secured.

31. The method for implementing off-line and secured electronic deposit generated by said microprocessor card as in claim 30 wherein said bank comprises a clearing house for performing part of all of steps (a) to (d) before transmitting said deposit information to said bank.

32. In a system for executing electronic payment with at least one tamper resistant microprocessor card, said system including at least one user and at least one service provider, a method adopted for implementing secured withdrawal information generated by said microprocessor card comprising the steps of:

(a) verifying by said bank of the validity of said microprocessor card;

(b) generating by said microprocessor card a withdrawal request;

(c) verifying by said bank said withdrawal request, said bank further adjusting the account information of said user within said bank's records; and

(d) instructing by said bank corresponding adjustment of said user's account information in said microprocessor card,

whereby withdrawal information generated by said microprocessor card is secured.

33. In a system for executing electronic payment with at least one tamper resistant microprocessor card, said system including at least one user and at least one service provider, a method for implementing secure withdrawal information generated by said microprocessor card comprising the steps of:

(a) verifying by said bank of the validity of said microprocessor card;

(b) activating by said user said microprocessor card for withdrawal transaction;

(c) generating by said microprocessor card a withdrawal request;

(d) verifying by said bank said withdrawal request, said bank further adjusting the account information of said user within said bank's records; and

(e) instructing by said bank corresponding adjustment of said user's account information in said microprocessor card,

whereby withdrawal information generated by said microprocessor card is secured.

34. The method for implementing secured electronic withdrawal generated by said microprocessor card as in claims 32 or 33 wherein said withdrawal request comprises a digital authentication.

35. The method for implementing secured electronic withdrawal generated by said microprocessor card as in claims 32 or 33 wherein said withdrawal request comprises a digital signature.

36. In a system for executing electronic payment with at least one tamper resistant microprocessor card, said system including at least one user, at least one bank and at least one service provider, a method for implementing off-line and secured electronic cash generated by said microprocessor card comprising the steps of:

(a) selecting by said bank for said microprocessor card at least one pair of public and private key P_C and S_C under a first predetermined digital signature scheme;

(b) selecting by said user for said microprocessor card at least one pair of public and private key P_u and S_u under a second predetermined digital signature scheme;

(c) combing the two said pairs of public and private keys to create a joint signature scheme under a third predetermined digital signature scheme, said joint signature scheme having at least one joint public key and one joint private key.

(d) generating a certificate for said microprocessor card for certifying the validity of said card and the said joint public keys, said card certificate being signed by a private key of the said bank under a fourth predetermined digital signature scheme;

(e) embedding in said microprocessor card said card certificate such that access thereto is restricted, said microprocessor card having at least one body, said body including identification field for identifying uniquely said microprocessor card, private key fields for storing the said joint private keys, and information field for storing said card certificate;

(f) storing with said bank at least one data entry for each said microprocessor card account, said entry comprising at least one entry body, said entry body including identification field for identifying uniquely each said microprocessor card account, and information field for storing corresponding card certificate;

(g) initialising said microprocessor card account and said microprocessor card with an initial transfer value, said value representing electronic cash;

(h) issuing to said user said microprocessor card;

(i) verifying by said service provider the validity of said microprocessor card;

(j) agreeing by said service provider and said user to a payment specification;

(k) activating by said user said microprocessor card for payment transaction;

(l) generating by said microprocessor card a payment certificate, said payment certificate being created as a joint digital signature under the third predetermined digital signature scheme for said grouping of payment specifications using the joint private keys embedded in the microprocessor card;

(m) grouping said payment specifications, said card certificate and said payment certificate;

(n) establishing by said service provider communication link with said bank;

(o) identifying by said service provider with said bank;

(p) collecting grouping of payment specifications and payment certificates transmitting the same to said bank;

(q) verifying by said bank the validity of each depositing electronic payment, said bank adjusting the accounting information of said user and said service provider within said bank's record;

(r) updating said service provider by said bank with accounting and status information;

(s) verifying by said bank of the validity of said microprocessor card;

(t) generating by said microprocessor card a withdrawal request;

(u) verifying by said bank said withdrawal request, said bank further adjusting the account information of said user within said bank's records; and

(v) instructing by said bank corresponding adjustment of said user's account information in said microprocessor card, whereby electronic cash payment generated by said microprocessor card is secured and processable in an off-line manner as long as none of the parties knows the joint private keys embedded in said microprocessor card.

37. In a system for executing electronic payment with at least one tamper resistant microprocessor card, said system including at least one user, at least one bank and at least one service provider, a method for implementing off-line and secured electronic credit payment generated by said microprocessor card comprising the steps of:

(a) selecting by said bank for said microprocessor card t at least one pair of public and private key P_C and S_C under a first predetermined digital signature scheme;

(b) selecting by said user for said microprocessor card at least one pair of public and private key P_U and S_U under a second predetermined digital signature scheme;

(c) combing the two said pairs of public and private keys to create a joint signature scheme under a third predetermined digital signature scheme, said joint signature scheme having at least one joint public key and one joint private key.

(d) generating a certificate for said microprocessor card for certifying the validity of said card and the said joint public keys, said card certificate being signed using said bank's private key under a fourth predetermined digital signature scheme;

(e) embedding in said microprocessor card said card certificate such that access thereto is restricted, said microprocessor card having at least one body, said body including identification field for identifying uniquely said microprocessor card, private key fields for storing the said joint private keys , and information field for storing said card certificate;

(f) storing with said bank at least one data entry for each said microprocessor card account, said entry comprising at least one entry body, said entry body including identification field for identifying uniquely each said microprocessor card account, and information field for storing corresponding card certificate;

(g) initialising said microprocessor card account and said microprocessor card with an initial credit value, said value representing electronic credit limit;

(h) issuing to said user said microprocessor card;

(i) verifying by said service provider the validity of said microprocessor card;

(j) agreeing by said service provider and said user to a payment specification;

(k) activating by said user said microprocessor card for payment transaction;

(l) generating by said microprocessor card a payment certificate, said payment certificate being created as a joint digital signature under the third predetermined digital signature scheme for said grouping of payment specifications using the joint private keys embedded in the microprocessor card ;

(m) grouping said payment specifications, said card certificate and said payment certificate;

(n) verifying by said bank the validity of each depositing electronic payment, said bank adjusting the accounting information of said user and said service provider within said bank's record;

(o) updating said service provider by said bank with accounting and status information;

(p) verifying by said bank of the validity of said microprocessor card;

(q) generating by said microprocessor card a withdrawal request;

(r) verifying by said bank said withdrawal request, said bank further adjusting the account information of said user within said bank's records; and

(s) instructing by said bank corresponding adjustment of said user's account information in said microprocessor card,

whereby electronic credit payment generated by said microprocessor card is secured and processable in an off-line manner as long as none of the parties knows the joint private keys embedded in said microprocessor card.

38. In a system for executing electronic payment with at least one tamper resistant microprocessor card, said system including at least one user, at least one bank and at least one service provider, a method for implementing off-line and secured electronic cheque generated by said microprocessor card comprising the steps of:

(a) selecting by said bank for said microprocessor card at least one pair of public and private key P_C and S_C under a first predetermined digital signature scheme;

(b) selecting by said user for said microprocessor card at least one pair of public and private key P_U and S_U under a second predetermined digital signature scheme;

(c) combing the two said pairs of public and private keys to create a joint signature scheme under a third predetermined digital signature scheme, said joint signature scheme having at least one joint public key and one joint private key.

(d) generating a certificate for said microprocessor card for certifying the validity of said card and the said joint public keys, said card certificate being signed using said bank's private key under a fourth predetermined digital signature scheme;

(e) embedding in said microprocessor card said card certificate such that access thereto is restricted, said microprocessor card having at least one body, said body including identification field for identifying uniquely said microprocessor card, private key fields for storing the said joint private keys , and information field for storing said card certificate;

(f) storing with said bank at least one data entry for each said microprocessor card account, said entry comprising at least one entry body, said entry body including identification field for identifying uniquely each said microprocessor card account, and information field for storing corresponding card certificate;

(g) initialising said microprocessor card account and said microprocessor card with an initial counter value, said value representing the number of checks issuable;

(h) issuing to said user said microprocessor card;

(i) verifying by said service provider the validity of said microprocessor card;

(j) agreeing by said service provider and said user to a payment specification;

(k) activating by said user said microprocessor card for payment transaction;

(l) generating by said microprocessor card a payment certificate, said payment certificate being created as a joint digital signature under the third predetermined digital signature scheme for said grouping of payment specifications using the joint private keys embedded in the microprocessor card ;

(m) grouping said payment specifications, said card certificate and said payment certificate;

(n) establishing by said service provider communication link with said bank;

(o) identifying by said service provider with said bank;

(p) collecting grouping of payment specifications and transmitting the same to said bank;

(q) verifying by said bank the validity of each depositing electronic payment, said bank adjusting the accounting information of said user and said service provider within said bank's record; and

(r) updating said service provider by said bank with accounting and status information,

whereby electronic cheque payment generated by said microprocessor card is secured and processable in an off-line manner as long as none of the parties knows the joint private keys embedded in said microprocessor card.

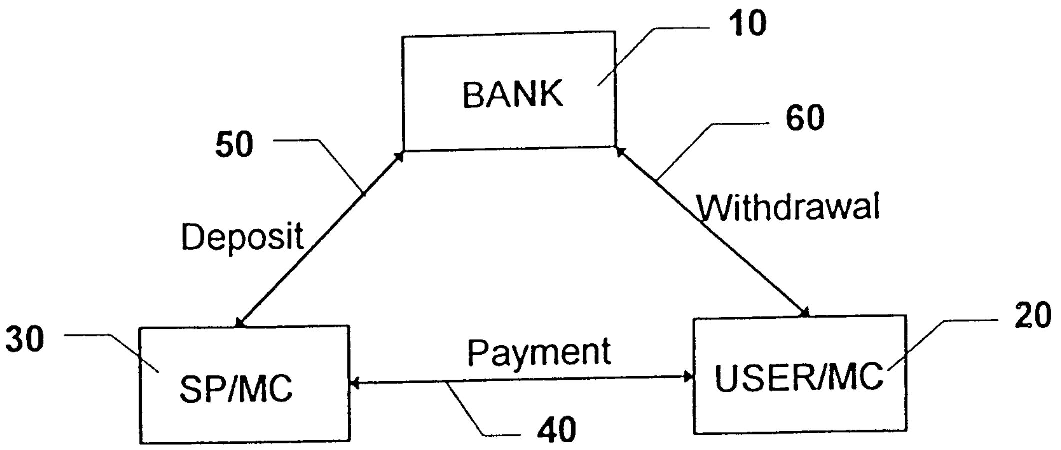


Figure 1

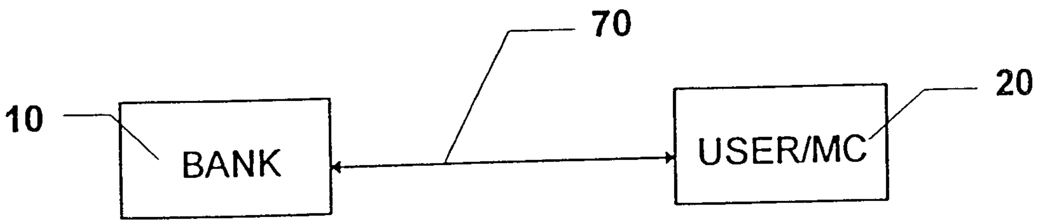


Figure 2

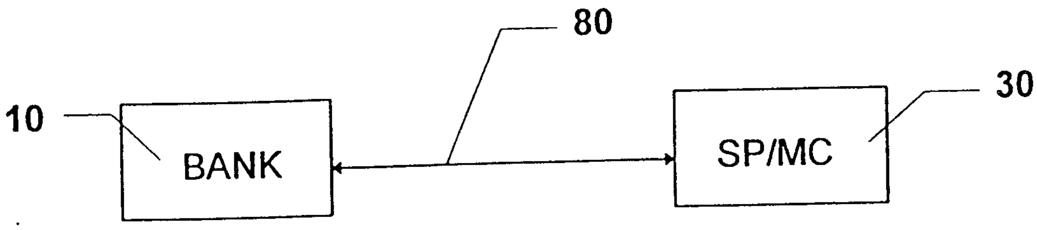


Figure 3

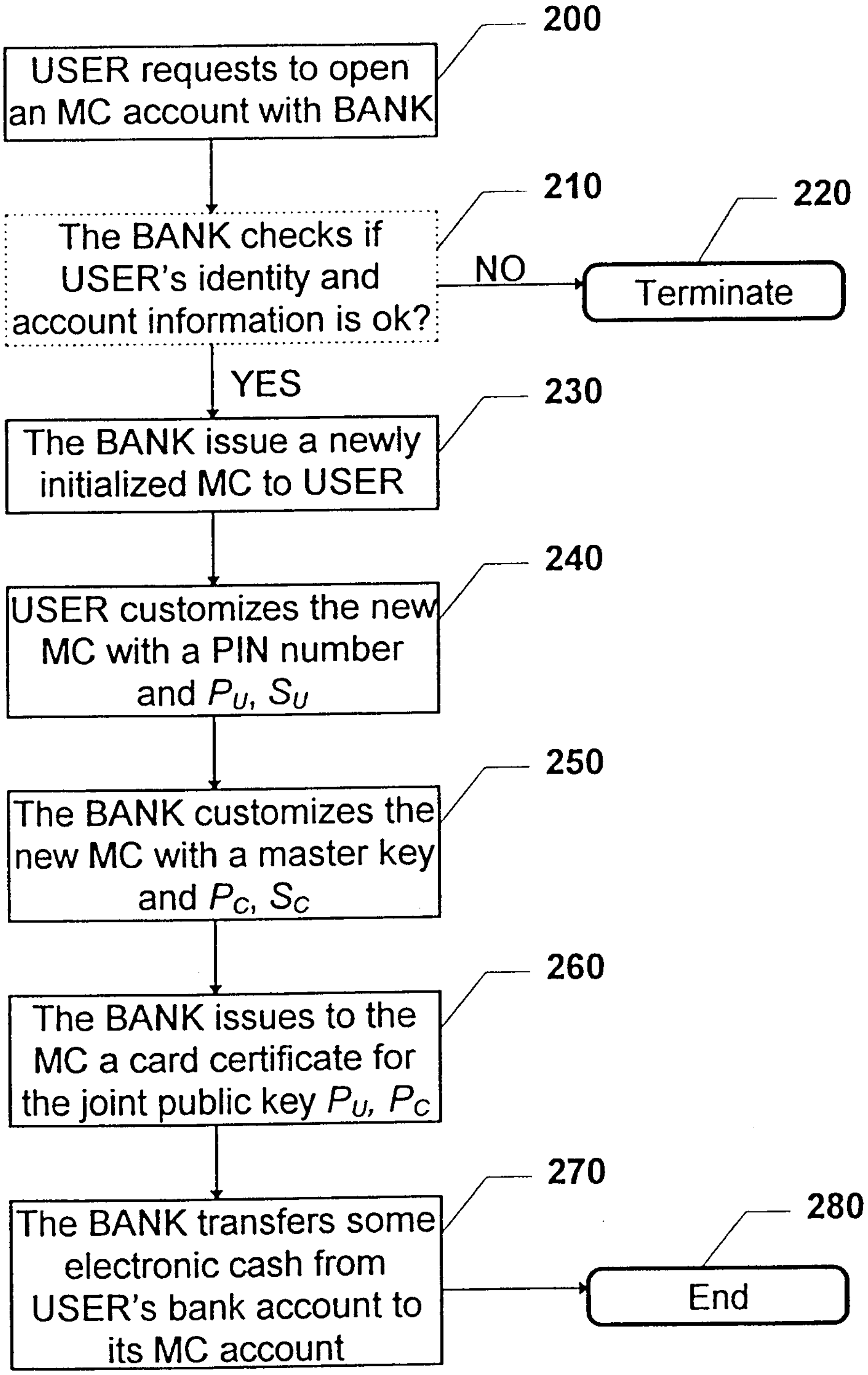

200
USER requests to open an MC account with BANK
210
The BANK checks if USER's identity and account information is ok?
NO
220
Terminate
YES
230
The BANK issue a newly initialized MC to USER
240
USER customizes the new MC with a PIN number and P_U, S_U
250
The BANK customizes the new MC with a master key and P_C, S_C
260
The BANK issues to the MC a card certificate for the joint public key P_U, P_C
270
The BANK transfers some electronic cash from USER's bank account to its MC account
280
End

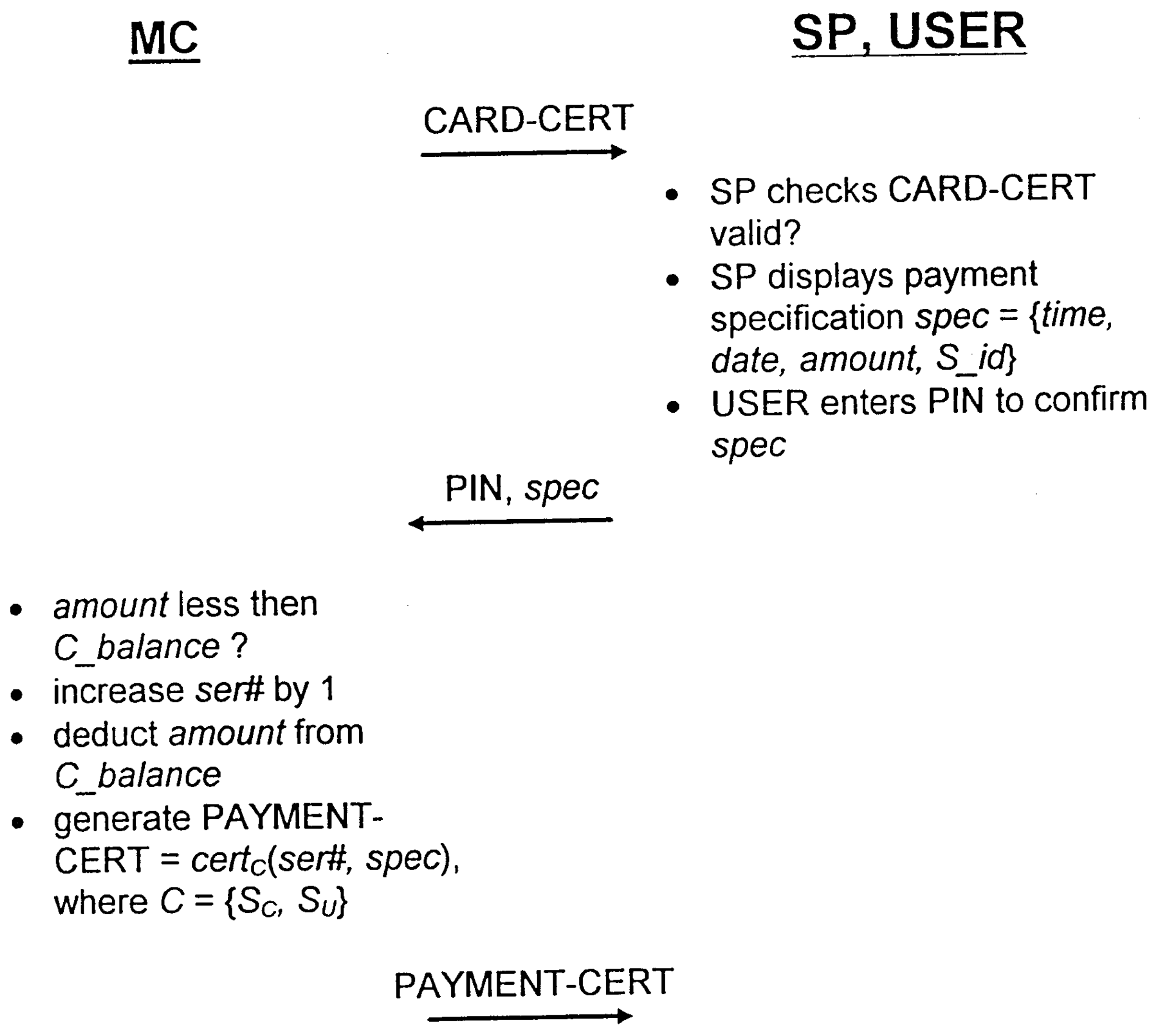
Figure 4

card#	the card number
user record	user's identity and information
Record 1	*cert$_B$(inter, info, P$_C$, P$_U$), C_balance, seq#, ser#*
...	

Figure 5

card#	the card number
master key	the master key used by the bank to access the card
PIN	PIN-number to activate transaction
S$_C$	secret key known by the card and the bank
S$_U$	secret key known by the card and possibly the user
C_balance	the cash balance held by the card
CARD-CERT	the card certificate
seq#	sequence number of withdrawal
ser#	serial number of cash payment for current certificate

Figure 6



MC

SP, USER

CARD-CERT →

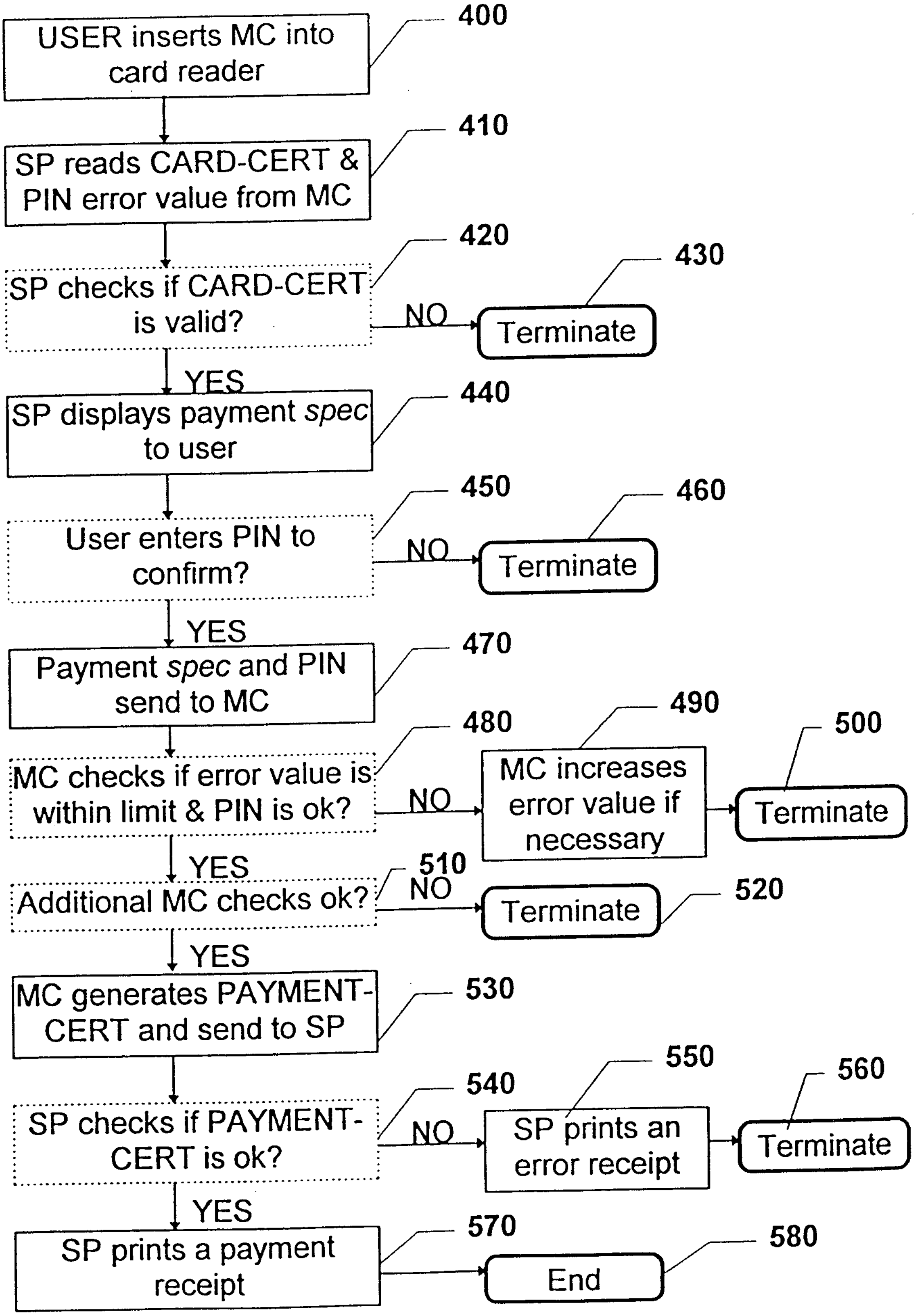
- SP checks CARD-CERT valid?
- SP displays payment specification *spec* = {*time, date, amount, S_id*}
- USER enters PIN to confirm *spec*

← PIN, *spec*

- *amount* less then *C_balance* ?
- increase *ser#* by 1
- deduct *amount* from *C_balance*
- generate PAYMENT-CERT = $cert_C$(*ser#, spec*), where $C = \{S_C, S_U\}$

PAYMENT-CERT →

Figure 7



USER inserts MC into card reader
400
SP reads CARD-CERT & PIN error value from MC
410
SP checks if CARD-CERT is valid?
420
NO
Terminate
430
YES
SP displays payment *spec* to user
440
User enters PIN to confirm?
450
NO
Terminate
460
YES
Payment *spec* and PIN send to MC
470
MC checks if error value is within limit & PIN is ok?
480
NO
MC increases error value if necessary
490
Terminate
500
YES
Additional MC checks ok?
510
NO
Terminate
520
YES
MC generates PAYMENT-CERT and send to SP
530
SP checks if PAYMENT-CERT is ok?
540
NO
SP prints an error receipt
550
Terminate
560
YES
SP prints a payment receipt
570
End
580

Figure 8

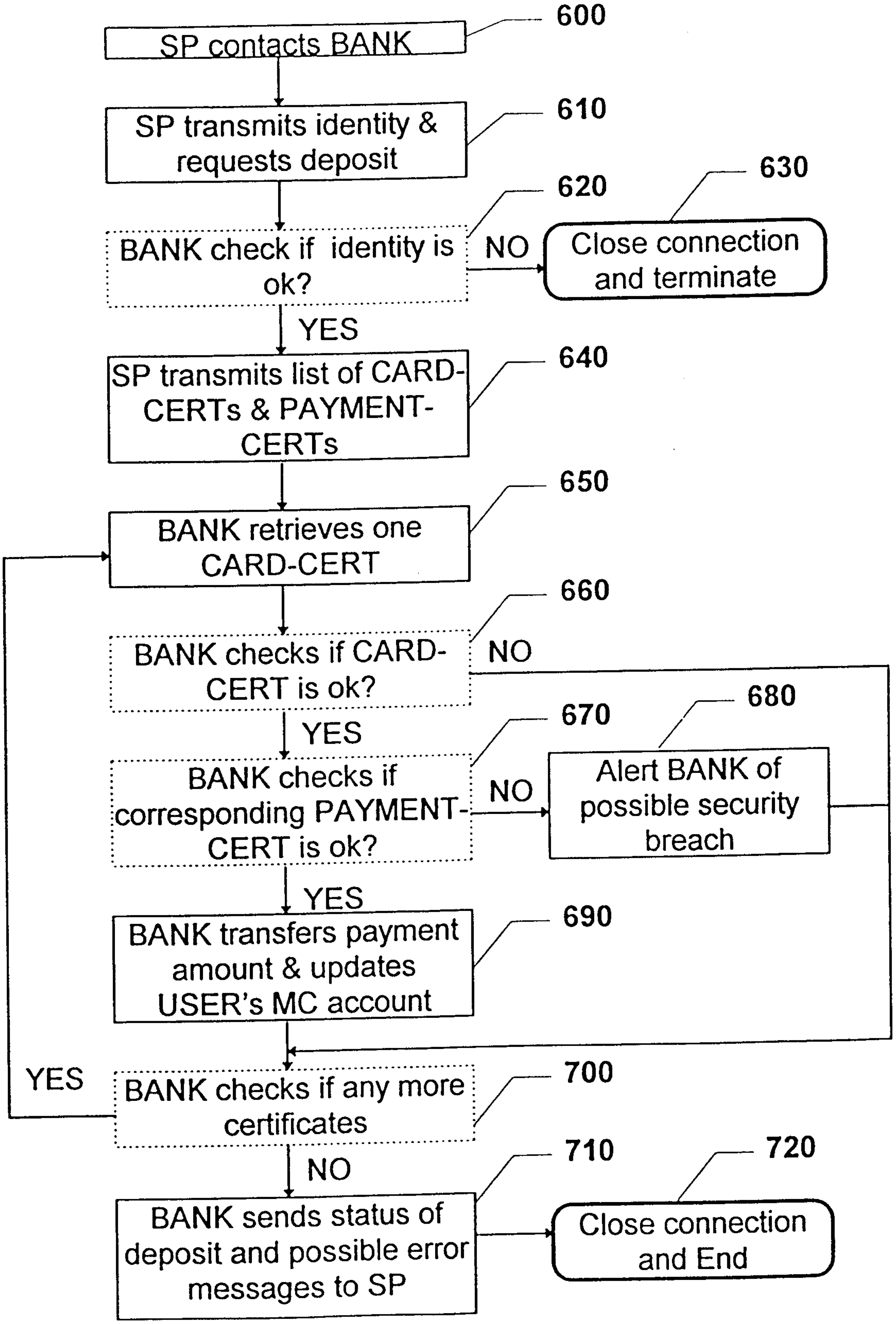

SP contacts BANK
600
SP transmits identity & requests deposit
610
BANK check if identity is ok?
620
NO
Close connection and terminate
630
YES
SP transmits list of CARD-CERTs & PAYMENT-CERTs
640
BANK retrieves one CARD-CERT
650
BANK checks if CARD-CERT is ok?
660
NO
YES
BANK checks if corresponding PAYMENT-CERT is ok?
670
NO
Alert BANK of possible security breach
680
YES
BANK transfers payment amount & updates USER's MC account
690
YES
BANK checks if any more certificates
700
NO
BANK sends status of deposit and possible error messages to SP
710
Close connection and End
720

Figure 9

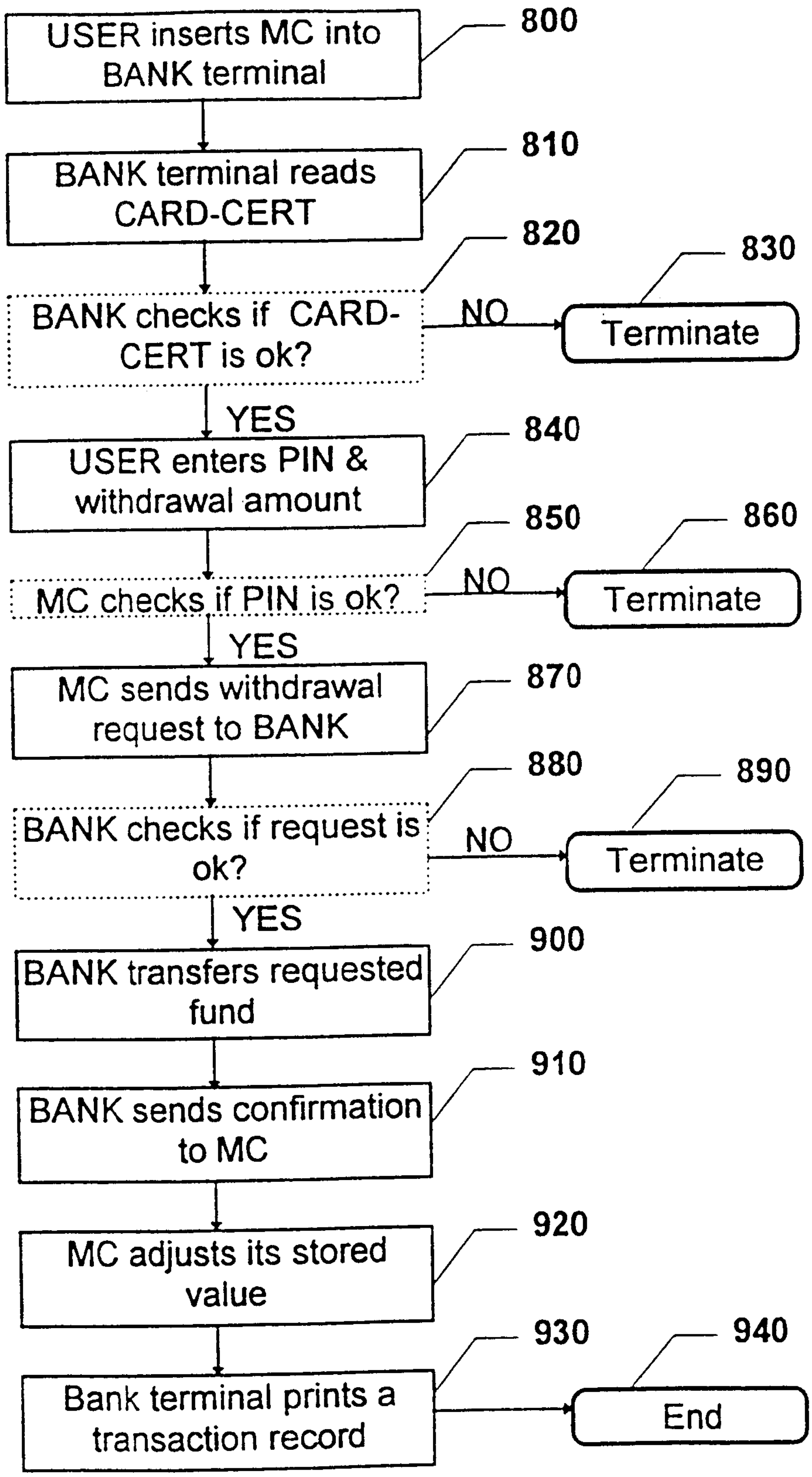

USER inserts MC into BANK terminal
800
BANK terminal reads CARD-CERT
810
BANK checks if CARD-CERT is ok?
820
NO
Terminate
830
YES
USER enters PIN & withdrawal amount
840
MC checks if PIN is ok?
850
NO
Terminate
860
YES
MC sends withdrawal request to BANK
870
BANK checks if request is ok?
880
NO
Terminate
890
YES
BANK transfers requested fund
900
BANK sends confirmation to MC
910
MC adjusts its stored value
920
Bank terminal prints a transaction record
930
End
940

Figure 10

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/SG 97/00065

A.	**CLASSIFICATION OF SUBJECT MATTER**

Int Cl^{6}: G06F 17/60, H04L 9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B.	**FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PUBLIC ( ) KEY, PRIVATE ( ) KEY, DIGITAL ( ) SIGN:

C.	**DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	WO, 97/37461 (HEWLETT-PACKARD COMPANY) 9 October 1997 (see whole document)	1-38
Y	US, 5144665 (TAKARAGI ET AL.) 1 September 1992 (see whole document)	1-38

☒ Further documents are listed in the continuation of Box C

☒ See patent family annex

* Special categories of cited documents:

"A"	document defining the general state of the art which is not considered to be of particular relevance
"E"	earlier document but published on or after the international filing date
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O"	document referring to an oral disclosure, use, exhibition or other means
"P"	document published prior to the international filing date but later than the priority date claimed
"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&"	document member of the same patent family

Date of the actual completion of the international search 30 March 1998	Date of mailing of the international search report 03 APR 1998
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200 WODEN ACT 2606 AUSTRALIA Facsimile No.: (02) 6285 3929	Authorized officer **J.W. THOMSON** Telephone No.: (02) 6283 6283

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/SG 97/00065

C (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0539727 (INTERNATIONAL BUSINESS SCHEMES CORPORATION) 31 October 1991 (see whole document)	1-38
Y	Roy Bright "SMART CARDS" published 1988 by Ellis Horwood Limited see Chapter 6	1-38

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No.
PCT/SG 97/00065

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member							
US	5144665	JP	3243035						
EP	0539727	CA	2071771	JP	5216410	JP	8016827		
		US	5265164						

END OF ANNEX