PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ^{6} :
G06F 17/60, G06K 5/00

A1

(11) International Publication Number: **WO 97/10560**

(43) International Publication Date: 20 March 1997 (20.03.97)

(21) International Application Number: PCT/US96/14414

(22) International Filing Date: 12 September 1996 (12.09.96)

(30) Priority Data:
08/528,307 14 September 1995 (14.09.95) US

(71) Applicant: CYBERMARK, L.L.C. [US/US]; 4171 Arlinggate Plaza, Columbus, OH 43228 (US).

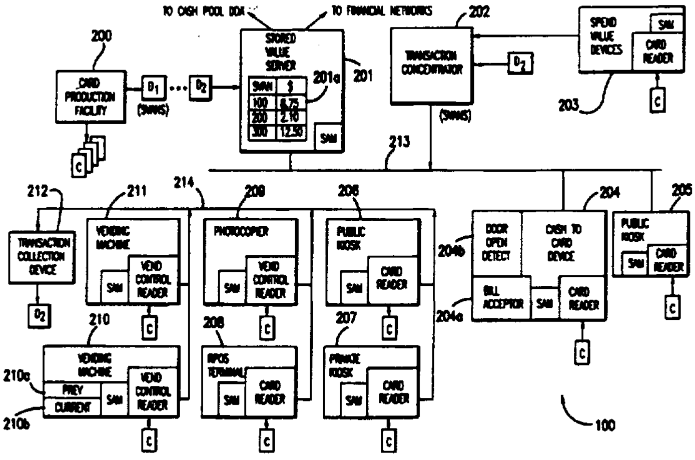
(72) Inventors: RENNER, G., Fred; 4882 Donegal Cliffs Drive, Dublin, OH 43017 (US). GARON, Gilles; 175 Yorkview Drive, Willowdale, Ontario M2R 1K2 (CA).

(74) Agents: WRIGHT, Bradley, C. et al.; Banner & Witcoff, Ltd., Suite 1100, 1001 G Street, N.W., Washington, DC 20001 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: STORED VALUE TRANSACTION SYSTEM AND METHOD USING ANONYMOUS ACCOUNT NUMBERS



(57) Abstract

A stored value transaction system includes a computer having a database of stored value accounts identified by an anonymous account number (i.e. not correlated with any particular cardholder). Using an on-line transaction with the computer database, cash equivalent value can be added to smart cards (C) onto which corresponding anonymous account numbers have been written. Properly valued cards can then be used in off-line transactions at various types of spend value devices such as vending machines, photocopiers and the like. The off-line transactions from the spend value devices (206, 207, 208, 209, 210, 211, 212) are collected and settled with the account numbers in the anonymous database, thus ensuring system integrity in an off-line system. The settled transactions are sorted by merchant and payment is made to the merchants based on accumulated transactions. The system also includes an efficient transaction collection approach.

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.

AM	Armenia
AT	Austria
AU	Australia
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
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
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
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

STORED VALUE TRANSACTION SYSTEM AND METHOD USING ANONYMOUS ACCOUNT NUMBERS

This application is a continuation-in-part of U.S. application serial number 08/414,495, filed on March 31, 1995, which is incorporated by reference herein.

BACKGROUND OF THE INVENTION

1. Technical Field

This invention relates generally to so-called "stored value" systems which use smart cards (i.e., cards having an embedded microprocessor) to replace cash. More particularly, the invention provides a system in which smart cards can be used to perform financial transactions wherein individual transactions can be settled against a cardholder's account balance while preventing the cardholder's account number or balance from being traced to the cardholder.

2. Related Information

The use of smart cards to perform cashless transactions in systems is well known. These systems typically provide a way for a cardholder to install a fixed amount of cash equivalent value onto a smart card and to spend the value on the card by inserting the card into any of various types of devices, such as vending machines. After the value on a card is exhausted, the cardholder may "revalue" the card by inserting it into a cash-to-card machine and then inserting cash, a debit card, or a credit card to transfer additional funds to the smart card.

Smart cards which electronically hold a cash equivalent value are hereinafter referred to as "stored value" cards. One example of such a card is the Gemplus MPCOS card, made by Gemplus Card International. Devices which install or increase value on stored value cards, such as a cash-to-card machine, are hereinafter referred to as "revalue devices". Devices which accept stored value cards and dispense a product or service in exchange for decrementing the value on the card are hereinafter referred to as "spend value" devices.

The term "debit card" as used herein will be understood to refer to a card which is used to transfer funds directly from a cardholder's identifiable bank account, usually via an on-line transaction from an ATM or other suitable terminal. In contrast, the term "stored value card" as used herein will be understood to refer to cards in which a certain predetermined value is installed directly on the card itself and which can be expended by the cardholder without requiring an on-line transaction.

Stored value systems can be generally classified into one of three types: (1) on-line systems; (2) off-line systems; and (3) hybrid systems. In an entirely on-line system, each time a card is used to make a purchase in a spend value device, an on-line transaction occurs between the spend value device and a central computer. The central computer is thus able to verify prior to authorizing the transaction that the inserted card has been properly valued, and that the proposed transaction can proceed. A major drawback of such systems is the overhead of on-line communications, including cost of the equipment and communication delays. It would thus be extremely expensive, for example, to provide a communication link between a central computer and every vending machine which accepts stored value cards.

An off-line stored value system allows purchases to be made without an on-line authorization. In an entirely off-line system, when a stored value card is used to make a purchase, the spend value device (e.g., a vending machine) decrements a value directly on the card in exchange for a product or service. As long as a card which appears to be properly valued is inserted into the machine, a successful transaction occurs, even if the value on the card was fraudulently installed or increased.

A major drawback of conventional off-line systems is the lack of security and a resulting potential for fraudulent transactions. It may be possible to mitigate this lack of security in certain circumstances by providing security features intrinsic to the stored value card itself and security features in revalue devices used to install value on the cards. However, to the extent that a crook is able to defeat a single revalue device (such as a cash-to-card machine) and cause it to produce newly revalued cards, or is able to persuade a crooked clerical employee to fraudulently add value to cards without requiring a corresponding payment, the entire system can still be defeated. For example, if a crook steals a cash-to-card machine and cracks it open, it may be possible to insert a single $20 bill repeatedly to "revalue" many valid stored value cards. Thus, even if a crook is unable to defeat the data security scheme used to install value on the card or crack cryptographic data stored on the card, cards can still be fraudulently revalued. Accordingly, off-line systems are considerably more vulnerable to theft.

The present invention contemplates a "hybrid" system in which revalue transactions are performed on-line with a central computer server, but in which spend value transactions are performed in an off-line manner. Records of the off-line transactions are stored and transmitted back to the central computer server for later off-line settlement with accounts which track the on-line valuations. Such a scheme maximizes security by (1) ensuring that stored value cards cannot be fraudulently valued, (2) ensuring that all spend value transactions are eventually "settled" with accounts maintained in a central computer, and (3) providing auditable information which allows suspicious trends to be followed and security breaches detected.

One major problem in implementing a so-called hybrid system is the need to avoid becoming a "bank". The United States government imposes strict regulations which require that entities which provide banking services to individuals must provide monthly statements and receipts for transactions, and must cover certain losses. Therefore, if each cardholder in a stored value system is provided with an identifiable account number which is credited with value in a central computer and later debited in the central computer when a transaction takes place, the arrangement appears to be similar in many respects to a bank (i.e., spend value transactions become very similar to writing checks which are later settled with the cardholder's bank account).

Under regulations such as a regulation "E" promulgated by the Treasury Department, providers of services which are deemed to be "banking" services must comply with a litany of costly rules and restrictions. Accordingly, a major drawback of implementing a hybrid system as described above is that the system provider may be considered to be a bank, thus imposing onerous requirements and significantly driving up cost. For example, the system provider may need to provide deposit insurance to cover losses from cardholder accounts.

In addition to the above problems, conventional stored value transaction systems do not provide an efficient method of collecting off-line transaction information from a variety of different types of spend value devices for settlement with different merchants. For example, a first merchant may provide a variety of vending machines which accept stored value cards; a second merchant may provide a group of photocopiers which accept stored value cards; and a third merchant may provide retail point-of-sale (RPOS) terminals which accept stored value cards in addition to credit and debit cards. In order to collect off-line transactions from each of the different merchants, a common collection scheme is needed to facilitate settlement with the vendors' accounts.

Unfortunately, large investments must be made to modify the machines according to a common scheme, or else new machines adapted to a common scheme must be used. Additionally, security mechanisms must be provided to ensure that crooked merchants cannot fraudulently obtain credits for goods or services which were never provided. Consequently, there is a high cost associated with providing merchants with the ability to accept stored value cards in their devices.

SUMMARY OF THE INVENTION

The present invention solves the aforementioned problems by providing a stored value system in which revalue transactions are performed in an on-line manner, but in which spend value transactions are performed off-line. Records of the off-line transactions are later collected, consolidated, and settled against individual accounts in a manner which prevents any individual account from being traced to a particular cardholder, thus assuring cardholder anonymity and avoiding onerous banking regulations. Such a "closed loop" approach overcomes problems associated with entirely off-line systems without compromising cardholder privacy.

The system of the present invention may include so-called "intelligent card readers" as described and disclosed in copending parent application serial number 08/414,495, filed on March 31, 1995, entitled "Intelligent Card Reader Having Emulation Features", which is incorporated by reference herein. The use of such intelligent card readers allows the card-based devices herein to accept a variety of different types of smart cards. Details of various types of vending machine card readers, public and private kiosk card readers, multimachine controllers and the like are described in more detail in the aforementioned copending application and are not repeated here.

In various embodiments of the invention, a stored value account number is created as a function of a unique smart card identifier, and a corresponding account having a balance is established in a stored value server. Each account is thus associated with a specific smart card, but the account is not directly traceable to any particular cardholder. A single cash pool is maintained at a financial institution which corresponds to the sum of all the balances of the anonymous account numbers.

When a cardholder installs value on a card at a revalue device, an on-line transaction occurs between the revalue device, a stored value server and, in certain cases, the cardholder's personal bank account. Cash inserted into the revalue device or transferred from the cardholder's bank account is installed on the stored value card and a corresponding balance is established in the stored value server under the anonymous stored value account number.

As the cardholder spends value on the card in various types of devices (such as vending machines) using off-line transactions, records of the transactions are transmitted back to the stored value server for settlement with the stored value account. Batches of such transactions are sorted by merchant, and corresponding funds transfers are initiated from the cash pool account to each merchant's account. Additionally, the off-line transactions are posted to the cardholder's stored value account. If a merchant transmits "spend value" transactions for a particular stored value account in an amount which exceeds the available balance in the central computer, such fraudulent transactions can be easily detected. Additional security provisions to prevent theft and fraud are explained in more detail herein.

Off-line transactions may be collected from vending machines and the like through one or more transaction collection devices which batch together multiple transactions for later transmission to a transaction concentrator, which in turn provides the transactions to the stored value server. By using a double buffering scheme to clear out old transactions only when verification of a previous transfer has occurred, the possibility of losing a batch of transactions is significantly reduced.

The system may be employed on a college campus or at a company-wide location with devices coupled through a local area network or wide area network as suited to the particular geography. Various other objects and advantages of the present invention will become apparent through the following detailed description, figures, and the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1A shows in simplified form various principles of the invention relating to the transfer of funds from individual cardholder bank accounts to merchant bank accounts.

FIG. 1B shows in simplified form steps which may be performed to carry out various principles of the invention.

FIG. 2 depicts in more detail one possible implementation of a stored value system corresponding to element 100 of FIG. 1A.

FIG. 3 shows relevant portions of one possible file structure for storing data on each stored value card.

FIG. 4 shows various steps of a method which may be carried out to add value to a card.

FIG. 5 shows various steps of a method which may be carried out to spend value on a card which has been previously valued.

FIG. 6 shows various steps of a method which may be carried out to download and settle off-line transactions.

FIG. 7 shows one possible arrangement for implementing computer processes on a stored value server to carry out the principles of the invention.

FIG. 8 illustrates one possible approach for creating a stored value account number (SVAN).

FIG. 9 shows one possible configuration for a revalue device such as a public kiosk.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

1. SYSTEM OVERVIEW AND GENERAL PRINCIPLES

FIG. 1A shows in simplified form a system employing various principles of the invention. A stored value system 100 (shown in more detail in FIG. 2) is coupled to a cash pool account 101 at Bank A, which may comprise a commercial checking account owned by the stored value system provider. The stored value system 100 is also coupled to one or more financial networks 102 through which various financial transactions such as debit or credit transactions may be initiated. Transactions in such a network may be effected by using financial service providers such as Gensar (one regional financial service provider) who provide such services.

Each cardholder may optionally maintain a regular bank account 103 which is coupled to one of the financial networks 102 in order to transfer funds from the cardholder's account to the cash pool 101. It is not necessary for a cardholder to maintain such a bank account if the cardholder always uses "hard" currency to revalue a stored value card.

Cash pool account 101 may also be coupled to an Automated Clearing House (ACH) network 105 to facilitate transfers of funds from the cash pool account 101 to merchant accounts 104 maintained at other banks. In general, stored value system 100 generates requests to transfer funds from cardholder accounts 103 to cash pool account 101 as part of a revalue transaction. Off-line spend value transactions using cardholders' stored value cards are batched and sorted according to specific merchants, and corresponding fund transfers are initiated from stored value system 100 to effect fund transfers from cash pool 101 to individual merchant accounts 104 maintained at other banks. The bank at which cash pool account 101 is maintained may also transmit account activity and balance reports back to stored value system 100. Stored value system 100 includes a stored value server 201 (shown in FIG. 2) which authorizes on-line revalue operations and settles off-line spend value transactions.

Variations on the basic architecture shown in FIG. 1A are of course possible; a primary objective is the ability to transfer funds from a common cash pool account to various merchant accounts according to posted transactions, and optionally to transfer funds from a cardholder's bank account to the common cash pool account under the control of stored value system 100.

FIG. 1B shows in simplified form various steps which may be carried out in accordance with the system shown in FIG. 1A. Beginning in step 120, an anonymous stored value account number is created, preferably using a cryptographic function based on a unique card identifier such as a serial number (details of these steps are described in more detail herein). The term "stored value account number", referring to this anonymous identifier, is hereinafter abbreviated SVAN.

In step 121, the SVAN is written to a stored value card, and an account having a zero or a predetermined balance is created in a database in stored value server 201. The step of creating many different SVANs may be carried out at a card production facility long before the cards themselves are to be used: the SVANs may be transferred to the stored value server in bulk via floppy disk or the like. The end result of performing steps 120 and 121 is that SVANs are installed on stored value cards and corresponding accounts are created in stored value server 201 with zero or predetermined balances. The total value of all balances in the stored value accounts maintained in stored value server 201 should equal the account balance in cash pool 101.

Of primary importance in the system is the non-association (in stored value server 201 or in cash pool 101) of the SVAN with any information which could identify the cardholder. In other words, the stored value server does not maintain a record of the cardholder's identity (such as name, address, social security number, or the like) in connection with the SVAN; the expenditure of funds in each stored value account is uniquely associated with the SVAN and not any particular cardholder. Thus, for example, if the cardholder loses his stored value card, a person who finds the card could spend the value on the card. In this respect, the stored value card is nearly as vulnerable as carrying cash. The latter problem can be mitigated somewhat by requiring the entry of a PIN prior to performing certain high-value spend value transactions.

After step 121, one of steps 122, 123, or 124 is performed at a revalue device in system 100. In step 122, a cardholder inserts a stored value card into a revalue device and inserts hard currency into a bill acceptor. Alternatively, in step 123 the cardholder may perform a debit transaction using his bank debit card to transfer funds from his bank account. Rather than using a separate debit card, the cardholder's regular bank account number may be pre-stored on a magnetic stripe on the back of the stored value smart card itself. This allows a single card to be used to transfer funds from a bank account to the stored value account.

Instead of steps 122 or 123, a credit transaction may be performed in step 124 in which the customer's credit card account is used to transfer funds on margin. As with step 123, rather than requiring a separate credit card, the cardholder's credit card information may be stored on a magnetic stripe on the stored value card itself, or it may be programmed in the stored value card.

Regardless of how funds are obtained (i.e., by inserting cash into a revalue device, performing a debit transaction, or performing a credit transaction), an on-line transaction occurs in step 125 to credit the SVAN account in the stored value server corresponding to the stored value card which was inserted. In other words, even if the cardholder inserts hard currency into a stored value machine, no value will be added to the stored value card until after an on-line communication between the revalue device and the stored value server takes place. During this communication, the SVAN is verified and then credited (at the stored value server) with the amount of funds provided by the cardholder. In step 126, the credited value is also written to the stored value card using an electronic purse function which is well known in the art. After value has been added to the card and a corresponding credit added to the SVAN at the server computer, the card is ejected and the cardholder is free to spend the value on the card.

In step 127, the cardholder may spend value on the card in any of a variety of spend value devices using off-line transactions as described in more detail herein. For example, the cardholder may use the card in vending machines, photocopiers, or RPOS terminals equipped to handle the cards. These transactions result in the value stored on the card being decremented, but no on-line communication with the stored value server takes place. It is, however, within the scope of this invention to also allow on-line spend value transactions, such that the system can support a mixture of off-line and on-line transactions. For on-line spend value transactions, steps relating to the collection of off-line transactions can be omitted. For example, there would be no need to store in a vending machine a record of an on-line transaction.

In step 128, each spend value device accumulates off-line spend transactions over a period of time, such as a day or a week. The accumulated transactions are transferred to the stored value server using devices such as those shown in FIG. 2, or using store-and-forward techniques. Finally, in step 129, settlement occurs both with the stored value accounts in the server and with merchant's accounts which may be at the same or other banks. This settlement step includes decrementing value of the SVANs in the stored value server by the amount of spend value transactions which have been accumulated in various devices, and also sorting out credits to be applied to the various merchants whose spend value devices were used. For example, the value of all transactions conducted at a particular merchant's vending machines is accumulated and then credited to the merchant's bank account (see FIG. 1A).

FIG. 2 shows in more detail one possible embodiment for the stored value system 100 depicted in FIG. 1A. Card production facility 200 initializes a plurality of stored value cards and creates a unique SVAN for each card. One possible method of generating a SVAN is to use a cryptographic function based on the serial number of each card. For example, a triple DES (Data Encryption Standard) operation may be performed using a privacy key to generate a unique anonymous SVAN for each card based on the card's serial number. The SVAN is written to the card and also to a medium such as disk D1, preferably in batches. Issued cards thus have an SVAN installed on them, and the SVANs are transmitted to stored value server 201 as shown in FIG. 2.

Stored value server 201 receives the SVANs and stores them in a database 201a, such as a relational database. Each SVAN has an associated balance as illustrated in 201a. Balances may be initially set to zero and then increased when revaluing a corresponding card; alternatively, each card may be provided with an initial balance. Stored value server 201 thus maintains a record of balances for each SVAN in an anonymous manner.

Stored value server 201 may be coupled to a cash pool and to financial networks as illustrated in FIG. 1A. Additionally, stored value server 201 is preferably connected to a network 213 which may comprise a LAN or WAN. A transaction concentrator 202, also coupled to network 213, collects off-line transactions from various spend value devices and transmits the transactions to stored value server 201, preferably over network 213. Transaction concentrator 202 may collect off-line spend value transactions from media such as disk D2, or through direct connection from various spend value devices 203. Spend value device 203, which represents any of a variety of devices such as vending machines and the like, includes a card reader which accepts stored value cards previously initialized by card production facility 200.

The various types of spend value devices will now be described. Vending machines 210 and 211 include a vending control reader which may be of a type described in copending parent application serial number 08/414,495, incorporated by reference herein. Such readers can accept smart cards of various types and operate vending machines such as those conforming to the MC 5000, MC 5800, or multidrop standards, the particular control lines being selected to suit the specific vending machine type. In various embodiments, these readers comprise a microcontroller which executes a "spend value" process which is described in more detail herein.

Alternatively, the vending control readers may be any type of smart card reader which controls the vending machine in response to insertion of a stored value card and maintains a log of all transactions. Generally speaking, each vending control reader verifies that an inserted card is authentic, dispenses a product or service in response to a cardholder's selection, and decrements the value on the stored value card by a corresponding amount. Additionally, a transaction record containing the SVAN is created in the machine for later off-line settlement.

Each vending machine may also include a Secure Application Module (SAM) which performs card authentication and other security features associated with an inserted card. Additionally, each SAM contains a unique number which is stored in each transaction record and which allows the transaction to be later associated with a particular merchant. For example, a merchant who owns a group of 5 vending machines can be provided with 5 SAMs to install in the machines. Each of the SAMs may contain a unique identifier which, when stored into a transaction record, allows the transaction to be traced back to the merchant when the transaction is settled in stored value server 201.

Photocopier 209 also includes a vending control reader which operates the photocopier in response to the insertion of a stored value card. Other types of spend value devices, such as washing machines and the like, are of course possible.

A Retail Point of Sale (RPOS) terminal 208 is provided with a card reader and (optionally) a SAM, and operates in a manner similar to the vending machines. The terminal may include a cash register type of device which calculates a total amount to be purchased and a card reader which accepts a cardholder's stored value card. In response to insertion of the card, RPOS terminal 208 causes the value on the card to be decremented by the amount of the purchase and creates a transaction log record for later off-line settlement.

Public kiosk 206 may comprise a terminal located in a public location which includes a card reader and (optionally) a SAM. This public kiosk may provide services such as the sale of information or the installation of various applications such as a meal plan on the card. Additionally, a cardholder may order goods and services such as a pizza or the like using his stored value card at the kiosk. The kiosk generally allows the cardholder to select various goods or services, and generates a receipt.

Private kiosk 207 may comprise a home computer which is equipped to accept stored value cards, and may provide a limited set of services which differs from those offered at public kiosk 206.

Transaction collection device 212 may be coupled to all of the above described spend value devices through one or more links 214 such as RS-232, RS-485, a LAN, or the like. Generally speaking, transactions which are stored in each spend value device may be transmitted over link 214 to transaction collection device at predetermined intervals, such as daily. Transactions which have been downloaded into collection device 212 may be offloaded to a disk D2 and subsequently transferred to transaction concentrator 202. In this manner, efficient collection of transaction information may be achieved. Note that instead of transmitting transaction information across link 214, each spend value device may be provided with a disk unit to individually offload stored transactions. Other variations are of course possible. For example, spend value devices may be directly connected to network 213, or to one or more transaction concentrators 202 such as illustrated in FIG. 2.

Cash to card device 204 includes a bill acceptor 204a which allows a cardholder to add value to a stored value card by inserting hard currency. However, in accordance with various principles of the invention, when cash is used to add value to a card, an on-line transaction with stored value server 201 occurs to ensure that the SVAN on the card is valid, and to store a corresponding balance amount in database 201a in the stored value server. Cash-to-card device 204 also preferably includes a door open detector 204b which transmits a message to stored value server 201 when the device is opened. This message may be time stamped and used to coordinate door openings with maintenance operations in order to prevent fraud. For example, revalue operations which occur while the door is open, or after the door has been opened during a non-maintenance period, can be identified as suspicious and an appropriate alert can be generated to prevent further on-line card valuations from that device.

Public kiosk 205 may be physically the same type of unit as public kiosk 206, but configured to include the ability to revalue a stored value card. For example, it may include the ability to read a magnetic stripe from a debit card or credit card in order to add value to a stored value card. Alternatively, it may include a hybrid card reader which uses a magnetic stripe on the stored value card itself to extract bank account information in order to perform a revalue operation.

In various embodiments, the devices coupled to network 213 may use a DCE/Encina client-server protocol to perform transactions over the network.

It will be recognized that while the system shown in FIG. 2 may preferably be employed at a single company-wide or campus-wide location, two or more systems such as that shown in FIG. 2 may be connected to handle transactions across multiple locations. For example, network 213 may be connected to another network (not shown) of another such system through a gateway, such that transactions can be processed across systems. This would allow, for example, a student who purchases a stored value account card for use at one campus to use the card at a second campus at a second geographic location and still provide for settlement of transactions.

2. CARD INITIALIZATION AND DATA FILES

This section describes generally how cards may be initialized in the system, and various data structures which may be used to hold information on the cards.

As noted above, one type of card which may be used to implement stored value features in accordance with the invention is the MPCOS card produced by Gemplus. The MPCOS card uses encryption keys and secret codes for security purposes. These security features may be used to provide message and data security for storage and transfer. Other types of cards may of course be used.

The stored value card preferably provides an intrinsic stored value function (electronic purse) which is protected using encryption/decryption techniques based on keys which may be derived from a unique issuer serial number or from the SVAN. Payment security functions preferably include secure messaging and cryptographic certificate verification based on cryptographic payment keys. Electronic purse transactions are preferably protected by payment keys stored on each card which are unique to the card. A certificate verification derivation key is preferably known to all SAMs. In various embodiments, cryptographic keys are not directly stored in revalue or spend value devices, but instead are protected within each SAM associated with the devices. All purse transactions that result in a change to the purse balance preferably use a cryptographic key for secure messaging.

The stored value account number (SVAN) generated and stored on each card may be generated using a cryptographically derived number which is unique on every card. In various embodiments, this number may be generated by performing a "triple DES" function on the card's serial number using a protected privacy key. The resulting number (SVAN) is then stored onto the card and also transmitted to the stored value server, preferably in batches on media such as a floppy disk.

In accordance with the principles of the present invention, a cardholder's identity is not maintained in connection to a SVAN; however, it may be generally desirable to maintain a cardholder's identity in connection with an issuer serial number associated with a particular card. Because the SVAN may be generated from the issuer serial number using an encipherment process, the SVAN can, in various embodiments, be linked to the last four bytes of the issuer serial number when using a cryptographic key for SVAN calculation. In case of fraud or illegal activity, this association could be used to help trace a card back to a particular card serial number (e.g., if supplied with the key used to generate the original SVAN, a reverse operation could be performed to restore the last 4 bytes of the issuer serial number, which could help trace the number to a particular card). However, as explained herein, there is no direct correlation between a cardholder's identity and the SVAN used to revalue and devalue credits stored on his card.

A data structure is preferably defined on the card to maintain the 10 most recent financial transactions. For security reasons, it may be desirable to require that the cardholder enter a PIN before certain information on the card is allowed to be read by a device (for example, the transaction log). This provides some measure of protection for lost or stolen cards.

FIG. 3 shows relevant portions of a file structure 301 for storing information relating to the stored value application on the cards. The file structure includes, in relevant part, a group of stored value files 302 and one or more bank files 303. It will be recognized that this structure is exemplary only and various different structures are of course possible. The following describes in more detail data which may be stored in these files.

KCT (304): a control key file which contains a stored value control key used to create files, download cryptographic keys, passwords, and the like.

KAD (305): authentication, certification, and debit key file which contains an authentication key, a certification key used for off-line debit, and an on-line debit key.

KCR (306): stores a key used for enabling a purse credit function and for computing a credit cryptogram.

PUR (307): a purse file, which may be supplied by the smart card vendor, used to store the card's monetary value. The purse file can be loaded either from a cash-to-card process or from an on-line debit from a cardholder's financial institution such as a bank identified in bank files 315. Various smart card vendors, such as Gemplus, may allow only indirect access to purse files on the card.

TXL (308): a transaction log file used to store the 10 most recent transactions of the card's stored value file. Each transaction entry may include for example the following information:

1. amount of the transaction
2. type of transaction

3. terminal/vendor ID
4. date
5. time
6. transaction certificate (includes SVAN)

DFC (309): cardholder data file which is used to store the stored value account number (SVAN).

Bank Files (303): contains cardholder banking information such as checking account number, credit card numbers, etc. (This information may also be stored on a magnetic stripe on the smart card itself).

Although not shown explicitly in FIG. 3, each card may also contain a transaction counter which is incremented for each transaction.

Stored value cards may be initialized at a first level by the card manufacturer, such as Gemplus. For example, the card manufacturer can initialize the card so that secure messaging is required to create files, and to write and update the files created. Additionally, the manufacturer can install a card serial number and issuer reference number.

Stored value cards may be initialized at a second level by the card issuer, such as the entity that installs and operates the stored value system. This second-level initialization can be protected through the use of secure procedures which require that a card be authenticated before certain information is installed on the card. During second-level initialization, personalized information can be installed, as well as the creation of other files such as those shown in FIG. 3 preferably using secure techniques to prevent fraudulent card creation. Provisions may also be made for de-activating a previously initialized card.

3. ADDING VALUE TO A CARD

As shown by steps 122 to 124 in FIG. 1B, value may be generally added to a stored value card in one of three ways: (1) inserting cash into a cash-to-card machine; (2) performing a debit transaction between the cardholder's personal bank account and the cash pool maintained by the stored value provider, or (3) performing a credit transaction between the cardholder's credit account at his bank and the cash pool maintained by the stored value provider. This section describes in more detail how value may be added to a card using the SVAN in a manner which prevents the cardholder's account from being associated with individual purchases traceable to the cardholder.

Regardless of whether cash, an on-line debit transaction, or an on-line credit transaction is used, certain principles are generally followed to ensure that value is not fraudulently installed on a card. These principles can take two different forms, depending on whether or not the device being used to revalue the card includes a Secure Application Module (SAM).

Although both the cash-to-card device 204 and the public kiosk 205 shown in FIG. 2 preferably include such a SAM for providing security features, it will be appreciated that cards can be revalued without the use of such a SAM. Accordingly, two different methods are described herein; the first method assumes that the revalue device includes a SAM, while the second method assumes that the revalue device does not include such a SAM. Each SAM may be implemented either in hardware or in software, and generally provides certain cryptographic services to support the device into which it is installed. A detailed description of each revalue process (with SAM and without SAM) appears separately below.

FIG. 7 shows one possible context in which card revaluation may be performed. Generally speaking, FIG. 7 shows various databases and computer processes which may reside on stored value server 201 (see FIG. 2). A revalue control process 701, financial network access process 702, and SVAN account database 703 (identical to database 201a of FIG. 2) may be implemented to carry out the process described in more detail below. In summary, stored value account numbers may be received from a disk into a maintenance process 713, which creates entries in SVAN account database 703. Messages from revalue devices can be processed by revalue control process 701, which, in cooperation with financial network access process 702, performs the necessary bank transfers to transfer funds from a cardholder's private bank account to the cash pool account 101 (see FIG. 1) and thereafter credits the corresponding SVAN in database 703. Further details of FIG. 7 are explained below with respect to spending value from the cards and transaction settlement.

A. Revalue Method Using a Secure Application Module (SAM)

FIG. 4 shows various steps which can be performed at a revalue device (such as cash-to-card device 204 or public kiosk 205) to add value to a stored value card in the case where the revalue device includes a SAM. Beginning in step 401, the stored value card is activated. For card readers which can support different types of smart cards (see parent application serial no. 08/414,495, incorporated by reference herein), this step could include the step of determining what type of card was inserted, and initializing software pointers in the card reader to support the specific type of card inserted.

Step 401 includes steps of checking the answer-to-reset data supplied by the card, selecting the stored value file (DFC in FIG. 3) and reading the SVAN from this file, and requesting that the SAM derive the correct key from the issuer serial number or SVAN for the particular card. Using the SAM, the revalue device can authenticate the smart card and communicate encrypted data with the smart card.

In order to increase the level of security, it is preferable to use different keys for authenticating a stored value card, performing an on-line revalue operation, performing an off-line spend value operation, and calculating various certificates. Additional keys may be used to encrypt data transmitted between various types of devices and the stored value server. Rather than explicitly identifying keys, implicit key identifiers (e.g., a file name identifying where a key may be found) may instead be used to prevent the misuse of cryptographic keys and to save storage space in off-line transaction logs, while explicit key identification may be used for on-line transactions.

Continuing with FIG. 4, in step 402 the stored value card is authenticated through the use of the SAM. This step generally includes requesting a random number from the SAM, sending the random number to the card, having the card encipher the random number and requesting that the SAM also encipher the random number, then requesting that the SAM compare the enciphered number returned from the card with that enciphered in the SAM. If the results match (i.e., the comparison is favorable), the card is deemed to have been authenticated. Such authentication techniques are well known.

Next, in step 403, the cardholder specifies a revalue amount through the use of a suitable input device such as a keyboard or touch-panel display, and, if the cardholder is using the cardholder's own bank account to transfer funds, the cardholder enters his PIN to be used with his normal bank account (this is not to be confused with a PIN or password which can be stored on the card itself). If the cardholder is using a credit card or cash to transfer funds, no PIN need be provided, although it is within the scope of the invention to also require a PIN for credit transactions. If either the cardholder's debit account or credit card account are used, the appropriate bank information can be read from the appropriate bank file (see FIG. 3) or from a magnetic stripe on the smart card itself. If the cardholder inserts hard currency into the machine, the machine itself can determine the revalue amount.

Step 404 includes steps of reading the purse value from the card, verifying that the amount requested plus the current purse value on the card does not exceed a maximum balance for the card, and aborting the transaction if the maximum purse value would be exceeded. Additionally, a card transaction counter and card balance certificate is obtained from the card in order to ensure non-repudiation (i.e., it allows the system to prove that the transaction came from that particular card and prevents unauthorized changes to the card balance amount; the card transaction counter also ensures that transactions such as loading value on a card cannot be replayed). In various embodiments, the card balance certificate may be provided as a function by the smart card vendor (e.g., Gemplus).

In step 405, a request message to validate the funds transfer operation is created, authenticated, encrypted, and transmitted on-line to the stored value server (element 201 in FIG. 2). This generally includes steps of encrypting the SVAN, card balance certificate, and PIN (if required), and transmitting the encrypted message to the stored value server over a network with a message authentication code (MAC) provided by the SAM. The network may include DCE/Encina client/server protocols to perform these transactions. The stored value server decrypts the request, verifies the MAC, verifies the balance certificate, and verifies that the SVAN from the card exists in database 201a and that the accumulated balance is not less than zero (if so, an unauthorized revalue might have taken place and appropriate reporting may be initiated).

If the funds transfer was an on-line debit or on-line credit transaction, the stored value server initiates a funds transfer request through a financial network 102 or ACH as illustrated in FIG. 1A. If the funds transfer was a hard currency operation at the revalue device, there is no need to perform such a transaction. After receiving a verification that the funds transfer has occurred (i.e., a successful debit operation or credit transaction from the cardholder's bank account), the stored value server prepares a credit certificate for the card, and authenticates and encrypts the response message to the revalue device. Note that stored value server 201 may include a SAM to perform the security-related features.

Step 407 includes steps of decrypting the response message in the revalue device, extracting and verifying the MAC, transmitting a credit certificate to the stored value card, verifying in the stored value card that the credit certificate is valid, and, if valid, updating the current balance (i.e., updating the purse file), and obtaining a transaction certificate in the card. The generation and verification of credit certificates is well known in the art (the MPCOS card provides proprietary functions for performing these operations which differ in some respects from corresponding ISO standards), and a detailed explanation of that portion of the operation is omitted.

In step 408, a record is written to the transaction log on the card (including the transaction certificate), and the card is ejected from the revalue device.

Finally, in step 409, a completion message is generated in the revalue device and encrypted for transmission back to the stored value server. This step includes steps of calculating a MAC, inserting a certificate obtained-from the card which confirms that the card has been revalued, authenticating the message, encrypting the message, and transmitting the encrypted message to the stored value server over a network.

B. Revalue Method Without a Secure Application Module (SAM)

A revalue device (such as cash-to-card device 204 or public kiosk 205) can also be used to add value to a stored value card in the case where the revalue device does not include a SAM. Instead of using a SAM, keys maintained in the stored value server and on the card may be used to encrypt data between the two, with the revalue device merely "passing through" the encrypted data.

4. SPENDING VALUE ON A CARD

FIG. 5 illustrates steps which may be performed to spend value on a previously valued card. In various embodiments, it is assumed that a SAM is provided in each spend value device to assist in certain security functions, and the explanation below assumes that such a SAM is provided. However, the use of a SAM may not be required, and the steps below can be performed as explained above to omit a SAM.

Beginning in step 501, a stored value card inserted into a spend value device is activated in a manner similar to step 401 of FIG. 4.

In step 502, the inserted card is authenticated to ensure that the card can be initially trusted. This step is similar to step 402 of FIG. 4. Additionally, the available balance on the card may be displayed on the spend value device.

In step 503, the purchase amount is determined. For a vending machine or menu type display at a kiosk, the cardholder may make a selection which generates a signal indicating the amount of the selected item. For an RPOS terminal, a cash register may generate a total indicating the accumulated value of a purchase. For a photocopier, a signal may be generated indicating a standard cost (e.g., 10 cents) for each dispensed copy. Other variations are of course possible.

In step 504, the purchase amount is compared with the available balance on the card. Optionally, if the purchase amount exceeds a predetermined threshold, the cardholder may be required to enter a password (PIN) which is compared to the pre-stored PIN on the stored value card. If the purchase amount exceeds the available balance, the transaction is aborted and the card returned to the cardholder.

In step 505, the purse on the card is debited. This may include steps of decrementing the purse by the purchase amount, obtaining a debit certificate from the card (this can be done using intrinsic MPCOS card functions, supplied by Gemplus), verifying the debit certificate in the spend value device (such as using a Gemplus-supplied method), and aborting the transaction if it is not legitimate.

In step 506, a card transaction record is created containing fields such as those described with reference to FIG. 3 and stored into the transaction log on the card (TXL file). This log may be viewed by the cardholder when the card is inserted into a machine.

In step 507, a transaction record is created and stored in a transaction log in the spend value device itself. This may include steps of calculating a message authentication code (MAC), encrypting the transaction data, and storing the encrypted record in the spend value device. The transaction record stored in the spend value device may, in various embodiments, include more information than that stored on the card itself. For example, the following information may be included in the device's transaction log:

1. serial number of the SAM used in the transaction (used to trace merchant)
2. stored value account number (SVAN)
3. card transaction certificate for the transaction
4. card transaction counter (a one-up counter)
5. terminal identifier
6. actual debit amount
7. terminal transaction counter (a one-up counter)
8. time stamp
9. MAC for the transaction record

In various embodiments, storing the SAM serial number of the spend value device allows a transaction to be credited to the merchant who owns or operates the device. Preferably, the stored value system provider provides SAMs to merchants to control the generation of encrypted transaction records in order to prevent unscrupulous merchants from fraudulently generating spend value transactions. However, other types of identifiers such as a merchant code or machine identifier may be used.

Storage of transaction records may be done using a "double buffering" method in each spend value device. In this regard, each spend value device maintains a "current transactions" buffer 210b (see FIG. 2) which records transactions which have occurred since the last download operation from the device was performed, and a "previous transactions" buffer 210a (see FIG. 2) which retains the previous batch of transactions which were downloaded. After the "current transactions" buffer is downloaded from the spend value device and successfully stored in the stored value server, a verification is preferably generated for the spend value device which indicates that the previous transactions were actually received and stored in the stored value server and that the corresponding "previous transactions" buffer can be deleted. This principle is explained in more detail in the next section.

In step 508, the product or service selected by the cardholder is dispensed or otherwise provided to the cardholder. It will be recognized that this step need not be performed at this particular stage in the process; it could occur before step 507 or earlier, for example.

5. TRANSACTION COLLECTION AND SETTLEMENT

Reference will now be made to FIG. 6, which shows various steps which may be carried out to collect and settle transactions. Reference will also be made to FIG. 2, which shows a system containing devices for implementing these steps, and FIG. 7, which illustrates various computer processes which may be implemented for carrying out these steps.

Referring first to FIG. 2, each spend value device (elements 207 through 211) may be coupled via a communication link to a transaction collection device 212 such as a PC-compatible computer. Periodically, the spend value devices may download a current buffer of transactions to the transaction collection device. This may be done on an hourly, daily, weekly basis or the like, or upon demand. Transaction collection device 212 may collect multiple batches from different devices and store the combined batches on a medium such as disk D2. Thereafter, the medium may be inserted into a transaction concentrator 202 which can accept disks from many different transaction collection devices and further download the transactions into stored value server 201 over a network 213.

Alternatively, spend value devices such as device 203 may directly download transactions into transaction concentrator 202 as shown in FIG. 2. Yet another variation is for transaction collection device 212 to be connected directly to network 213 to download batches of transactions into stored value server 201. Regardless of the particular arrangement used, the net result is that batches of transactions previously logged off line in the spend value devices are loaded into stored value server 201 for settlement.

Referring now to FIG. 6, step 601 indicates that batches of transaction logs from the spend value devices are transferred to a collection device such as 212 or 202 as explained above. In step 602, each spend value device which has downloaded its current transaction log switches over its transaction log buffer to a second "current" buffer, and designates the downloaded buffer as "previous transactions". In other words, each spend value device preferably maintains a copy of the old transactions in the event that they are not successfully loaded into stored value server 201.

Next, in step 603, batches of transaction logs which have been received from transaction concentrator 202 (or transaction collector device 212) are transferred to the stored value server 201. Referring to FIG. 7, a transaction batch receiver process 704 in stored value server 201 receives batches of transactions, decrypts each transaction and verifies the MAC for each, and stores them into a database 705.

In step 604, each transaction extracted from database 705 is posted against the stored value account corresponding to the transaction. In other words, the SVAN for each transaction is extracted from the transaction record, and the balance of the corresponding account in SVAN account database 703 is decremented by the amount of the transaction. Other steps of verifying the authenticity of each transaction (e.g., verifying the transaction certificate) are also included but not explicitly shown in FIG. 6.

In various embodiments, it may be preferably to include two types of transaction certificates: and off-line certificate, and an on-line certificate. An off-line certificate can be generated by the card during a card decrementing operation, and the certificate verified by a SAM in the spend value device. After verifying this off-line certificate, the spend value device can request that the card generate an on-line certificate using a key which is not known to the SAM, but which is known to the computer server which will eventually settle the transaction in an on-line process. This prevents can help prevent fraudulent generation of transaction certificates by someone who steals a SAM.

In step 605, transactions which have been newly posted in the database are sorted by merchant in process 706, preferably based on the SAM serial number extracted from each transaction record. The correlation between SAM serial number and merchant identifier can be stored in a merchant information database 712. The result of this step is that all newly posted transactions are sorted by merchant and accumulated in value (i.e., the value of all transactions attributable to a particular merchant are added together).

In step 606, each merchant can be paid using a merchant repayment process 709 which extracts merchant bank account information from database 712 and initiates a funds transfer using ACH process 708. This step may also include a human review of the payments before authorizing the bank funds transfer.

In step 607, reports may be optionally generated to send to the merchants showing a detailed breakdown of sales per device and the like. An accounting package 710 may be used to generate statistical analyses and the like as desired.

Finally, in step 608, a "buffer verified" indication is generated either by storing a flag on a disk D2 used for later collection, by transmitting a message over network 213, or the like, to indicate to each spend value device that the "previous transactions" buffer may be discarded. This indication may be conveniently combined with the next round of transaction collections, such that the step of transaction collection begins with a verification that the previously downloaded transactions have been properly posted.

The above described procedure provides a convenient and reliable method of collecting and settling off-line transactions in a system. Other variations are of course possible.

When each transaction record is verified, a failure of verification may result in aborting the current batch of transactions and returning them to the merchant for further action. It is apparent that the information in the transaction records can be combined, sorted and analyzed for various purposes such as detecting fraud and tracing suspicious activity to a particular machine or merchant.

6. GENERATING STORED VALUE ACCOUNT NUMBERS

In various embodiments, an anonymous stored value account number (SVAN) may comprise 12 bytes that uniquely identify a stored value card. It is apparent, however, that fewer or more than 12 bytes may be used. FIG. 8 illustrates one possible method for deriving a SVAN in the manner described below. The first two bytes may be set to zero, and the last eight bytes can be derived by enciphering the issuer serial number using a double length privacy key as follows:

SVAN (8) = ede*KEY(issuer serial number)

where ede = encipher/decipher/encipher

KEY = a double length key

issuer serial number = constructed and stored on the card.

The issuer serial number may be constructed as follows:

first 4 bytes = the last 4 bytes of the SAM serial number of a SAM used in the card production process

fifth byte = not used (zero)

last 3 bytes = a unique sequence number (one-up counter) generated by the card preparation system SAM.

The SAM serial number may be an 8 byte number that uniquely identifies a SAM, and may be constructed as follows:

first 4 bytes = same as the issuer reference

last 4 bytes = a number sequentially assigned which uniquely identifies the SAM.

The issuer reference number may be used to identify the geographic location of the system, such as a campus identifier or a company location identifier. A card preparation SAM may be used to prepare cards, including deriving various types of keys.

7. REVALUE DEVICE DESIGN

One possible configuration for a revalue device such as public kiosk 205 is shown in FIG. 9. The revalue device 901 generally includes a processor 902 and memory 903 for storing control programs and information needed to execute various steps described elsewhere in this specification. SAM 910 is coupled to processor 902 and generally provides security functions such as key storage and derivation, authentication, certification, and encryption/decryption functions. A hybrid card acceptor 906 accepts microprocessor-equipped smart cards which may also have a magnetic stripe. This allows certain bank information to be stored on the magnetic stripe in a manner compatible with existing debit cards, and this information may be used to perform an on-line debit operation in the revalue device.

Control circuit 905 generally performs card reader-related functions, augmented slightly to handle the magnetic stripe information from cards so equipped. An encrypted PIN pad 907 may be used to enter a PIN for cardholder verification. A receipt printer 908 generates receipts for products or services purchased by the cardholder. An input device 909 may comprise a keyboard or the like, or alteratively display 904 may comprise a touch-panel display which performs these functions. Processor 902 may be coupled to a network such as network 213 shown in FIG. 2.

It is apparent that many modifications and variations of the present invention are possible, and references to specific values are by example only. The method steps of the invention may be practiced in a different ordered sequence from that illustrated without departing from the scope of the invention. It is, therefore, to be understood that within the scope of the appended claims the invention may be practiced otherwise than as specifically described.

CLAIMS

1. A stored value transaction system for carrying out transactions using a plurality of smart cards, comprising:

a computer comprising a database which maintains a balance for each of a plurality of stored value accounts, wherein each of the stored value accounts has an identifying number which is stored on one of the plurality of smart cards and which is not correlated in the computer to any particular cardholder; and

a spend value device which conducts an off-line transaction with one of the plurality of smart cards by decrementing value stored on the one smart card and storing a record of the off-line transaction including the identifying number stored on the one smart card;

wherein the computer decreases the balance of one of the stored value accounts corresponding to the identifying number of the one smart card in response to receiving at a later time a copy of the stored record of the off-line transaction.

2. The system of claim 1, wherein the record of the off-line transaction is stored in encrypted form in the revalue device.

3. The system of claim 2, wherein the computer receives a plurality of encrypted off-line transaction records and separately decrypts each record prior to decreasing the balance of a corresponding stored value account.

4. The system of claim 1, further comprising:

a revalue device which adds value to the one smart card by performing an on-line transaction with the computer, wherein the computer verifies the authenticity of the identifying number stored on the one smart card by checking the database prior to authorizing the addition of value to the one smart card.

5. The system of claim 4, wherein the revalue device comprises a currency acceptor which accepts hard currency, wherein the on-line transaction is conducted in an amount equal to the amount of hard currency accepted in the currency acceptor.

6. The system of claim 5, wherein the revalue device comprises a secure application module (SAM) which is used to authenticate the one smart card prior to adding value to the one smart card.

7. The system of claim 4, wherein the on-line transaction comprises an on-line debit operation using a cardholder-entered PIN.

8. The system of claim 7, wherein the on-line debit operation is performed between a cardholder's private bank account and a cash pool account maintained at a separate bank.

9. The system of claim 7, wherein the on-line debit operation is performed on the basis of data read from a magnetic stripe on the smart card.

10. The system of claim 4, wherein the on-line transaction comprises an on-line credit operation using cardholder-provided credit card information.

11. The system of claim 10, wherein the credit card information is read from a magnetic stripe on the smart card.

12. The system of claim 1, wherein the identifying number is derived by performing an encryption operation on another number.

13. The system of claim 12, wherein the encryption operation is performed on a number provided by a secure application module in a card preparation device.

14. The system of claim 1, further comprising a transaction collection device, coupled to the spend value device, for collecting batches of transactions stored in the spend value device and providing them to the computer.

15. The system of claim 14, wherein the spend value device maintains a current transaction storage area used to store ongoing transactions and a previous transaction storage area used to retain transactions which were previously collected by the transaction collection device but not yet stored in the computer.

16. The system of claim 1, wherein the spend value device comprises a vending machine having a secure application module (SAM) used for encrypting transaction records.

17. The system of claim 16, wherein the vending machine accumulates a plurality of off-line transactions and downloads the accumulated transactions to a transaction collection device.

18. The system of claim 1, wherein the spend value device comprises a retail point of sale (RPOS) terminal which accumulates a total sale amount as the value to be decremented on the one smart card.

19. The system of claim 1, wherein the spend value device comprises a photocopy machine.

20. The system of claim 1, wherein the spend value device comprises a kiosk having a display and means for selecting a product or service from the display.

21. The system of claim 1, wherein the spend value device further stores transaction information on the one smart card.

22. The system of claim 1, wherein the spend value device accepts a plurality of different types of smart cards.

23. A system comprising:

a plurality of different types of spend value devices each of which decrements, using an off-line transaction, value from a smart card and retains an encrypted record of each off-line transaction, wherein each transaction includes an anonymous account number used for settling the transaction against an anonymous account maintained in a computer; and

a transaction collection device, coupled to the plurality of different types of spend value devices, for collecting a plurality of encrypted transactions stored in the plurality of spend value devices and downloading the collected transactions to the computer in which the anonymous accounts are maintained.

24. The system of claim 23, wherein each of the plurality of spend value devices comprises a card reader which can read a plurality of different types of smart cards.

25. The system of claim 23, wherein each of the plurality of spend value devices maintains a current transaction storage area for storing ongoing transactions and a previous transaction storage area for storing transactions which were previously collected by the transaction collection device but not yet stored in the computer.

26. The system of claim 23, further comprising a transaction concentrator which accepts off-line transaction records collected by the transaction collection device and downloads them to the computer.

27. A system for conducting transactions with smart cards, the system comprising:

a computer comprising a database which maintains a balance for each of a plurality of stored value accounts, each of the stored value accounts being identified by an anonymous account number which is not associated with any particular cardholder;

a plurality of smart cards each having one of the anonymous account numbers stored thereon;

a plurality of spend value devices each of which decrements value from one of the smart cards using an off-line transaction and retains a record of each transaction including the anonymous account number of the smart card used in the transaction; and

means for settling each of the retained transaction records with the stored value accounts in the database.

28. The system of claim 27, further comprising means for generating the plurality of anonymous account numbers using an encryption function.

29. The system of claim 27, further comprising a transaction collection device, coupled to the plurality of different types of spend value devices, for collecting a plurality of transactions stored in the plurality of spend value devices and downloading the collected transactions to the computer in which the anonymous accounts are maintained.

30. The system of claim 29, wherein the transaction collection device uses a disk for collecting the plurality of transactions.

31. The system of claim 29, further comprising a transaction concentrator, coupled to the computer, for concentrating transactions from one or more transaction collection devices.

32. The system of claim 27, further comprising means for sorting and accumulating transactions by merchant and authorizing a funds transfer to merchants for the accumulated amounts.

33. The system of claim 32, wherein each of the spend value devices comprises a secure application module having a unique number which is included in each of the off-line transactions, and wherein the sorting and accumulating means uses the unique number to sort transactions by merchant.

34. The system of claim 27, wherein the system controls transfers from a bank cash pool account having a value corresponding to the accumulated value of the stored value accounts.

35. The system of claim 27, wherein the system is coupled to a financial network and issues funds transfer requests to the financial network in order to increase the value of one of the stored value accounts.

36. The system of claim 27, further comprising a revalue device, coupled to the computer, which accepts one of the smart cards and increases value on the one smart card after communicating with the computer, wherein the revalue device comprises a door open detector which transmits a message to the computer upon detecting that a door on the revalue device has been opened.

37. A method for tracking expenditures in a system which uses smart cards, comprising the steps of:

(1) inserting a smart card into a revalue device in communication with a computer having a plurality of stored value accounts, wherein the smart card contains an anonymous account number which corresponds to one of the stored value accounts in the computer but which is not directly traceable to any

particular cardholder; and

(2) adding value directly to the smart card only after communicating with the computer to verify that the stored value account number on the inserted smart card corresponds to one of the anonymous account numbers stored in the computer.

38. The method of claim 37, wherein step (2) comprises the step of transferring, under the control of the computer, funds from a cardholder's private bank account to a cash pool account corresponding to the total value of all the stored value accounts in the computer.

39. The method of claim 37, further comprising the step of increasing a balance of one of the stored value accounts in the computer corresponding to the stored value account number contained on the smart card inserted in step (1).

40. The method of claim 37, further comprising the steps of:

(3) inserting the smart card into an off-line spend value device which decrements value on the smart card without communicating with the computer and which stores a record of the value decrementing transaction; and

(4) downloading at a later time the record of the transaction to the computer and settling the transaction with one of the stored value accounts.

41. The method of claim 40, further comprising the step of accumulating a plurality of value decrementing transactions in a transaction collection device and downloading the accumulated plurality of transactions to the computer for settlement.

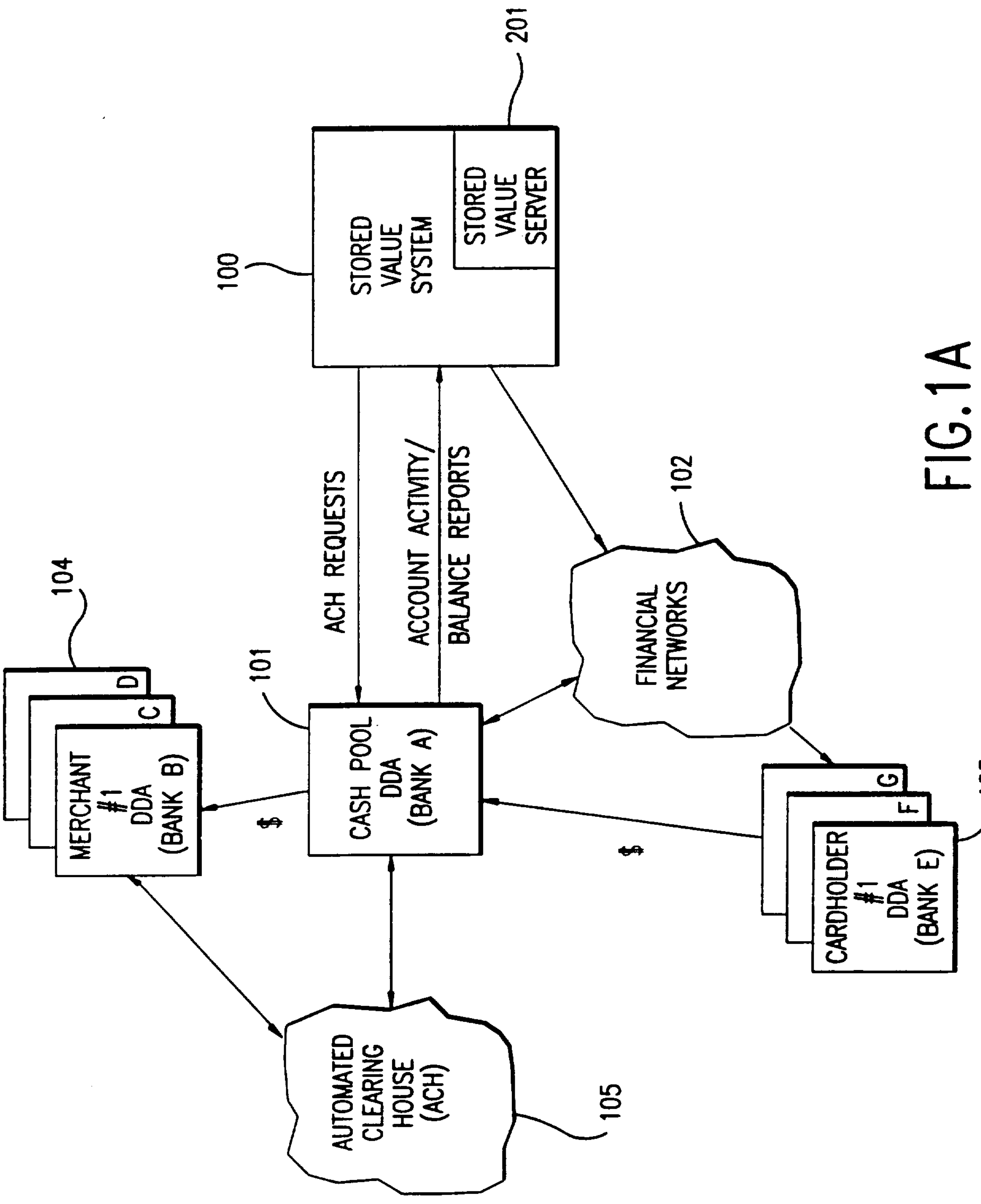

201
100
STORED VALUE SYSTEM
STORED VALUE SERVER
ACH REQUESTS
ACCOUNT ACTIVITY/ BALANCE REPORTS
102
FINANCIAL NETWORKS
104
D
C
MERCHANT #1 DDA (BANK B)
101
CASH POOL DDA (BANK A)
$
$
G
F
CARDHOLDER #1 DDA (BANK E)
103
AUTOMATED CLEARING HOUSE (ACH)
105

FIG.1A

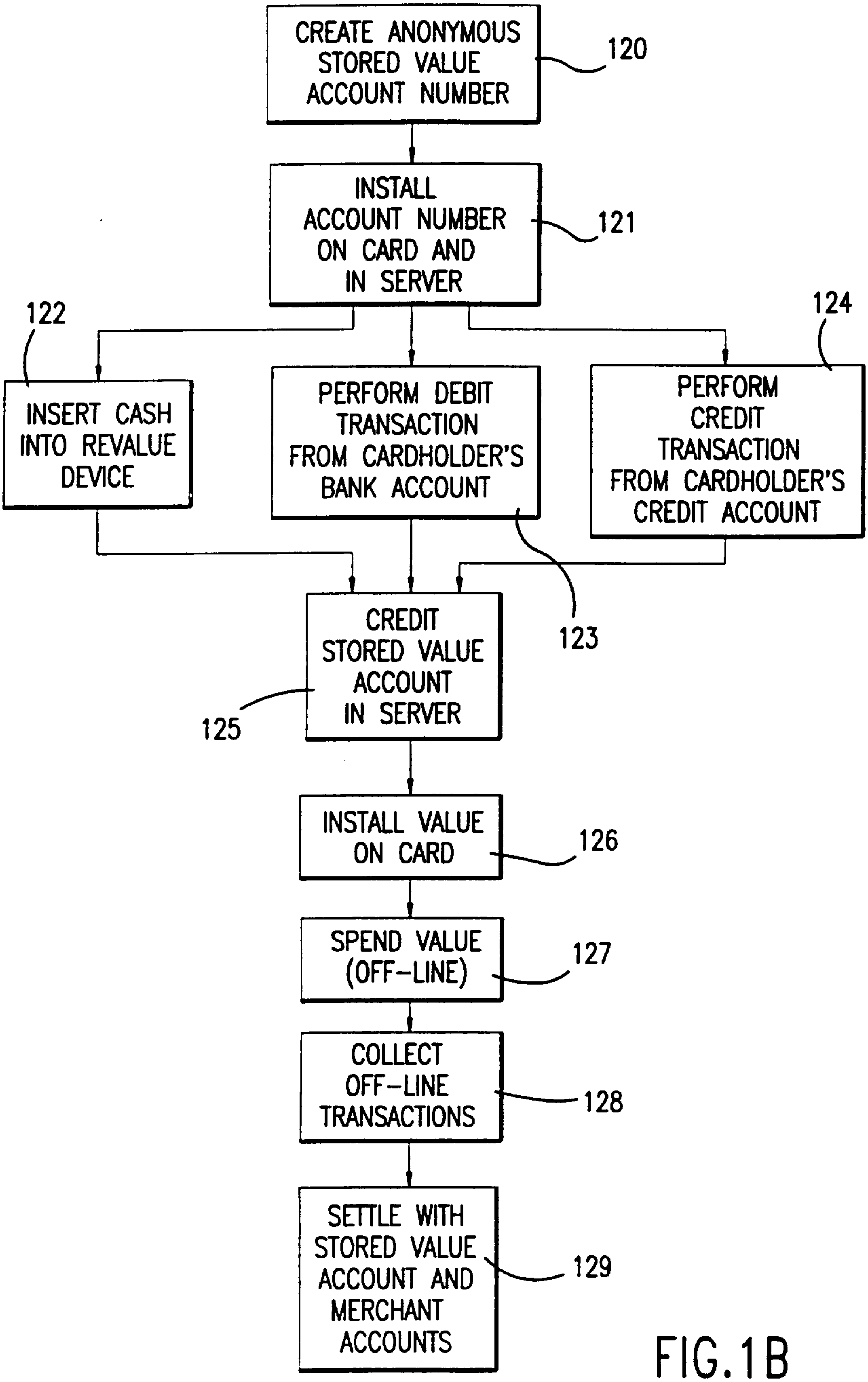
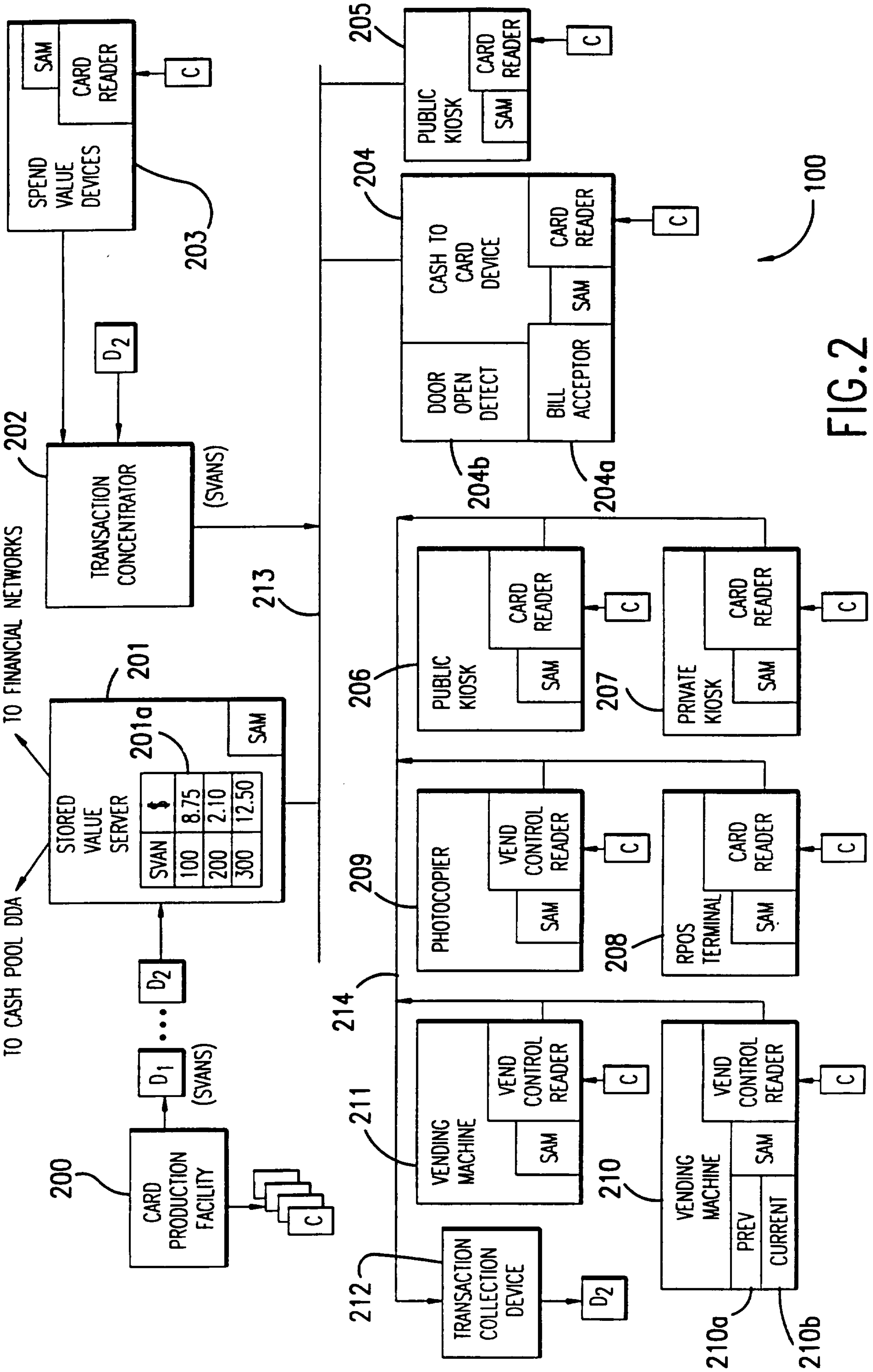

CREATE ANONYMOUS STORED VALUE ACCOUNT NUMBER
120
INSTALL ACCOUNT NUMBER ON CARD AND IN SERVER
121
122
124
INSERT CASH INTO REVALUE DEVICE
PERFORM DEBIT TRANSACTION FROM CARDHOLDER'S BANK ACCOUNT
PERFORM CREDIT TRANSACTION FROM CARDHOLDER'S CREDIT ACCOUNT
CREDIT STORED VALUE ACCOUNT IN SERVER
123
125
INSTALL VALUE ON CARD
126
SPEND VALUE (OFF-LINE)
127
COLLECT OFF-LINE TRANSACTIONS
128
SETTLE WITH STORED VALUE ACCOUNT AND MERCHANT ACCOUNTS
129

FIG.1B



SPEND VALUE DEVICES
SAM
CARD READER
C
203
D2
202
TRANSACTION CONCENTRATOR
(SVANS)
TO FINANCIAL NETWORKS
TO CASH POOL DDA
201
STORED VALUE SERVER
201a
SVAN
$
100
8.75
200
2.10
300
12.50
SAM
D2
D1
(SVANS)
200
CARD PRODUCTION FACILITY
C
213
205
PUBLIC KIOSK
CARD READER
SAM
C
204
CASH TO CARD DEVICE
CARD READER
SAM
C
DOOR OPEN DETECT
BILL ACCEPTOR
204b
204a
100
206
PUBLIC KIOSK
CARD READER
SAM
C
207
PRIVATE KIOSK
CARD READER
SAM
C
209
PHOTOCOPIER
VEND CONTROL READER
SAM
C
208
RPOS TERMINAL
CARD READER
SAM
C
214
211
VENDING MACHINE
VEND CONTROL READER
SAM
C
210
VENDING MACHINE
VEND CONTROL READER
SAM
PREV
CURRENT
C
210a
210b
212
TRANSACTION COLLECTION DEVICE
D2

FIG.2

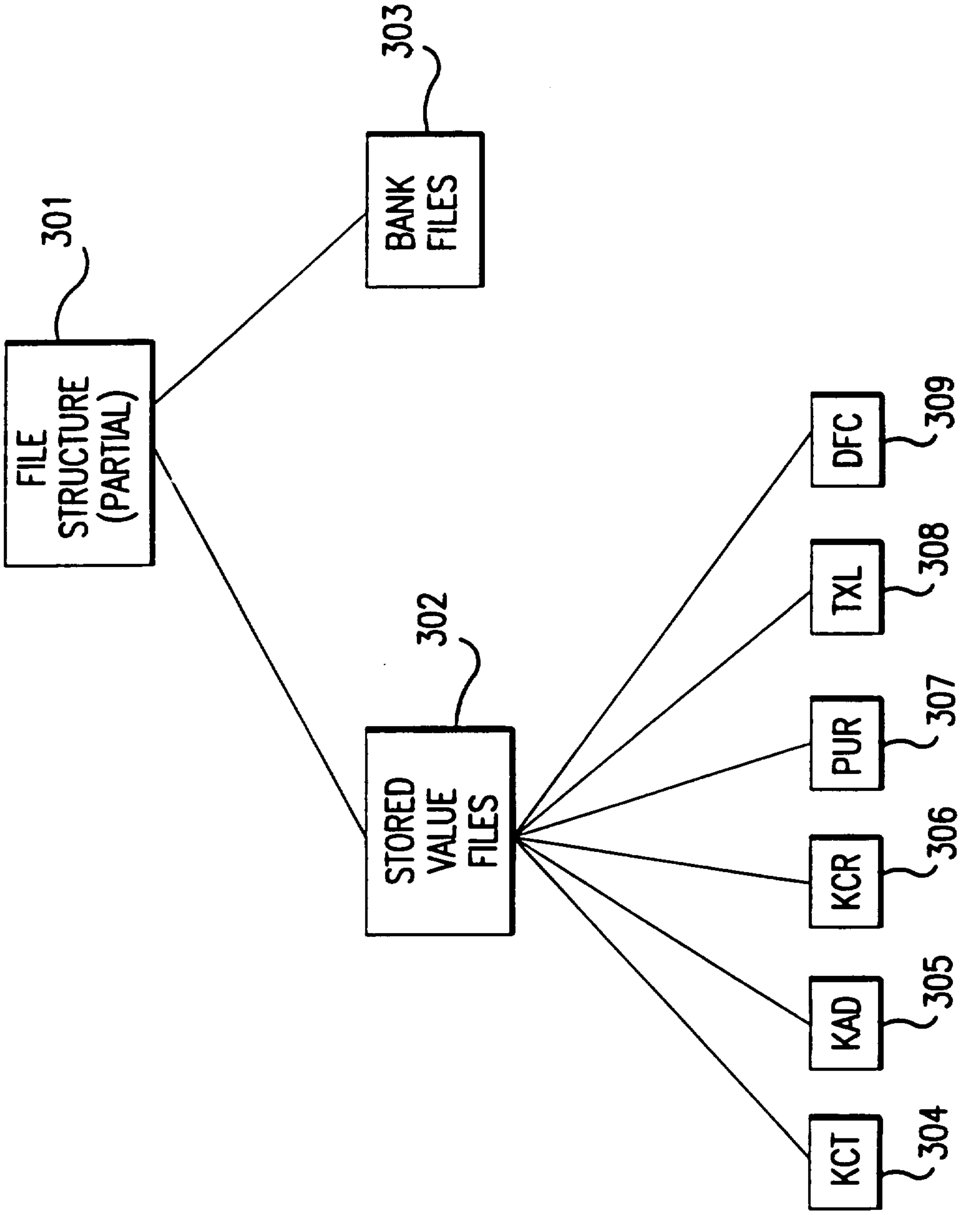

FILE
STRUCTURE
(PARTIAL)
301
BANK
FILES
303
STORED
VALUE
FILES
302
KCT
304
KAD
305
KCR
306
PUR
307
TXL
308
DFC
309

FIG.3

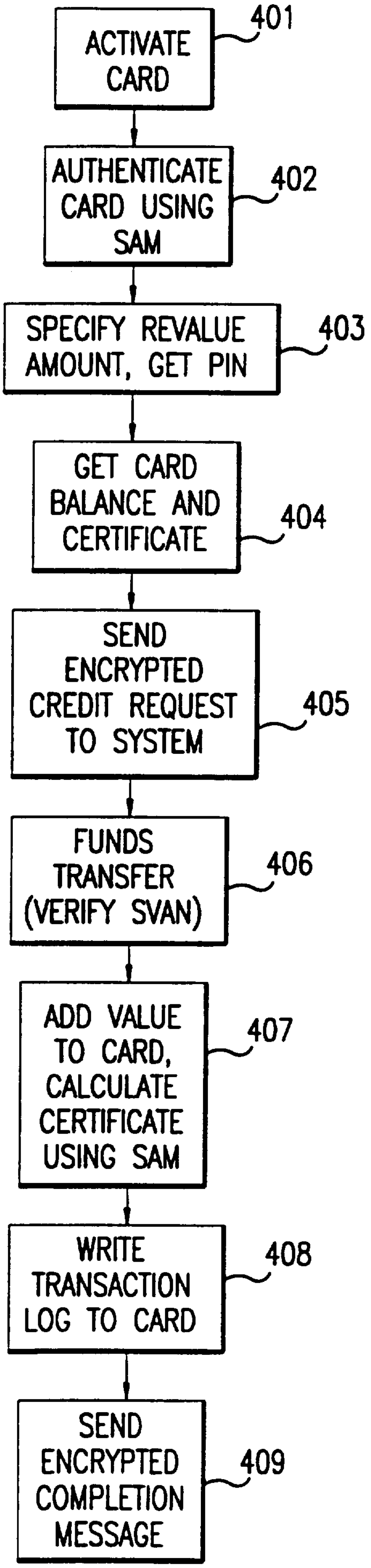

ACTIVATE CARD
401
AUTHENTICATE CARD USING SAM
402
SPECIFY REVALUE AMOUNT, GET PIN
403
GET CARD BALANCE AND CERTIFICATE
404
SEND ENCRYPTED CREDIT REQUEST TO SYSTEM
405
FUNDS TRANSFER (VERIFY SVAN)
406
ADD VALUE TO CARD, CALCULATE CERTIFICATE USING SAM
407
WRITE TRANSACTION LOG TO CARD
408
SEND ENCRYPTED COMPLETION MESSAGE
409

FIG.4

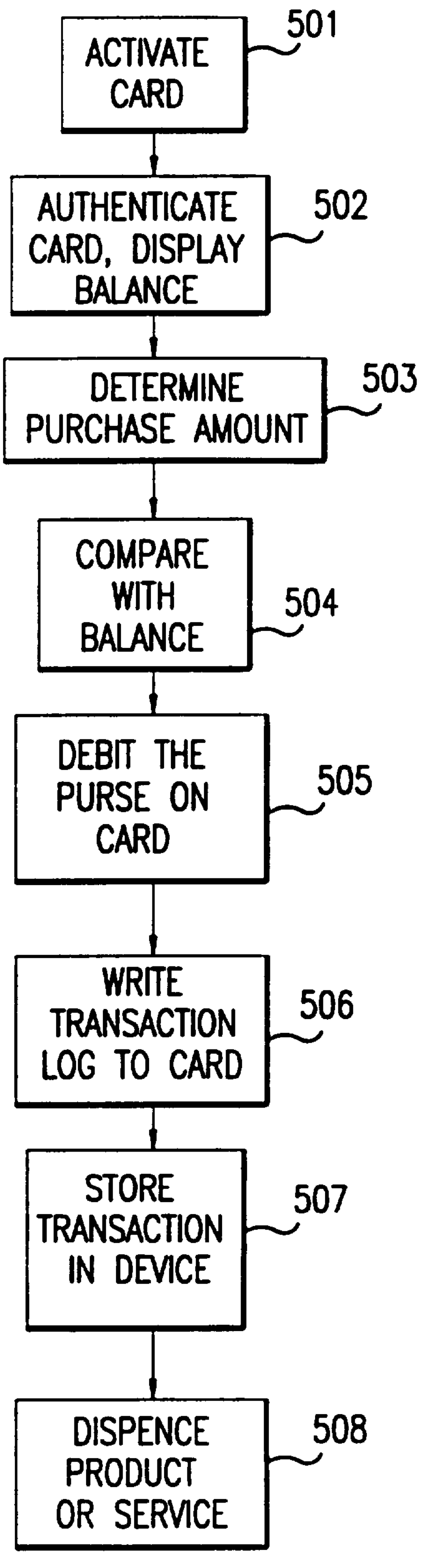

ACTIVATE CARD
501
AUTHENTICATE CARD, DISPLAY BALANCE
502
DETERMINE PURCHASE AMOUNT
503
COMPARE WITH BALANCE
504
DEBIT THE PURSE ON CARD
505
WRITE TRANSACTION LOG TO CARD
506
STORE TRANSACTION IN DEVICE
507
DISPENCE PRODUCT OR SERVICE
508

FIG.5

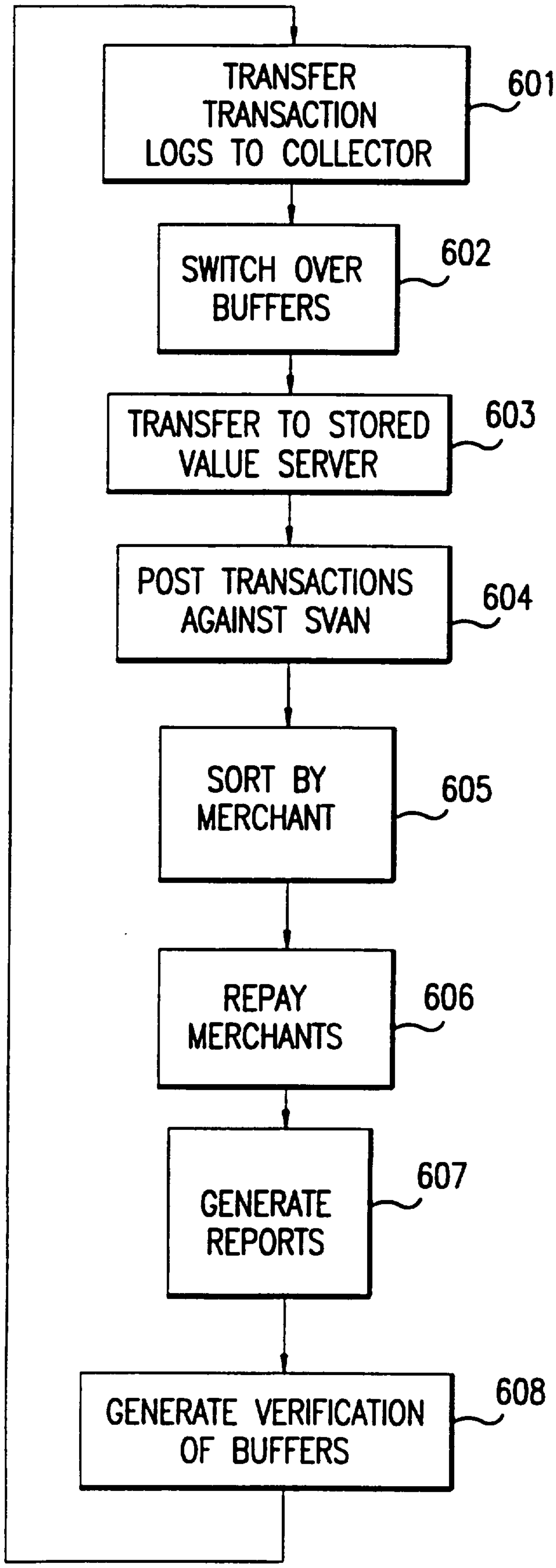

TRANSFER TRANSACTION LOGS TO COLLECTOR
601
SWITCH OVER BUFFERS
602
TRANSFER TO STORED VALUE SERVER
603
POST TRANSACTIONS AGAINST SVAN
604
SORT BY MERCHANT
605
REPAY MERCHANTS
606
GENERATE REPORTS
607
GENERATE VERIFICATION OF BUFFERS
608

FIG.6

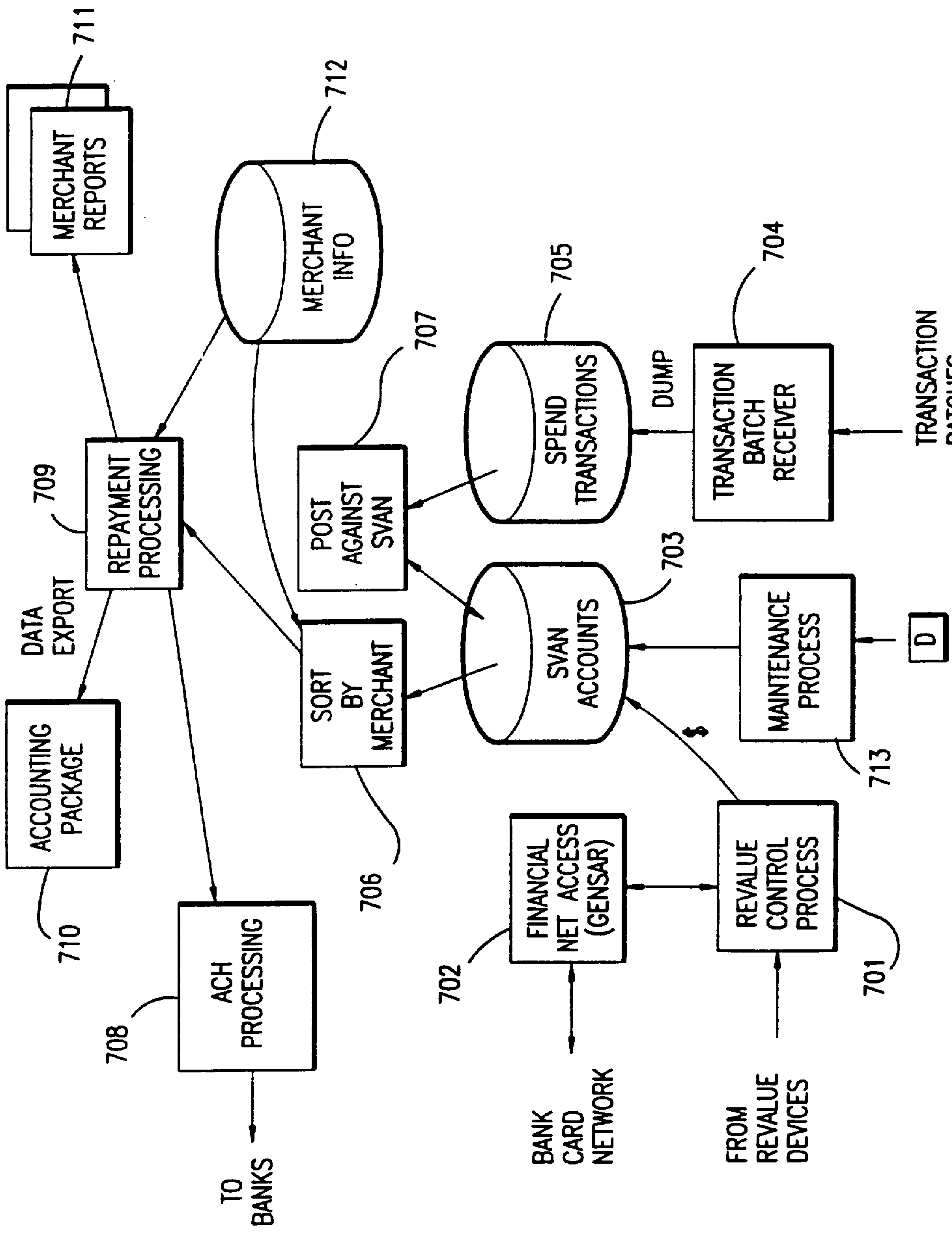

MERCHANT REPORTS
711
MERCHANT INFO
712
REPAYMENT PROCESSING
709
DATA EXPORT
ACCOUNTING PACKAGE
710
ACH PROCESSING
708
TO BANKS
POST AGAINST SVAN
707
SORT BY MERCHANT
706
SPEND TRANSACTIONS
705
DUMP
TRANSACTION BATCH RECEIVER
704
TRANSACTION BATCHES
SVAN ACCOUNTS
703
MAINTENANCE PROCESS
713
D
$
FINANCIAL NET ACCESS (GENSAR)
702
REVALUE CONTROL PROCESS
701
BANK CARD NETWORK
FROM REVALUE DEVICES

FIG.7

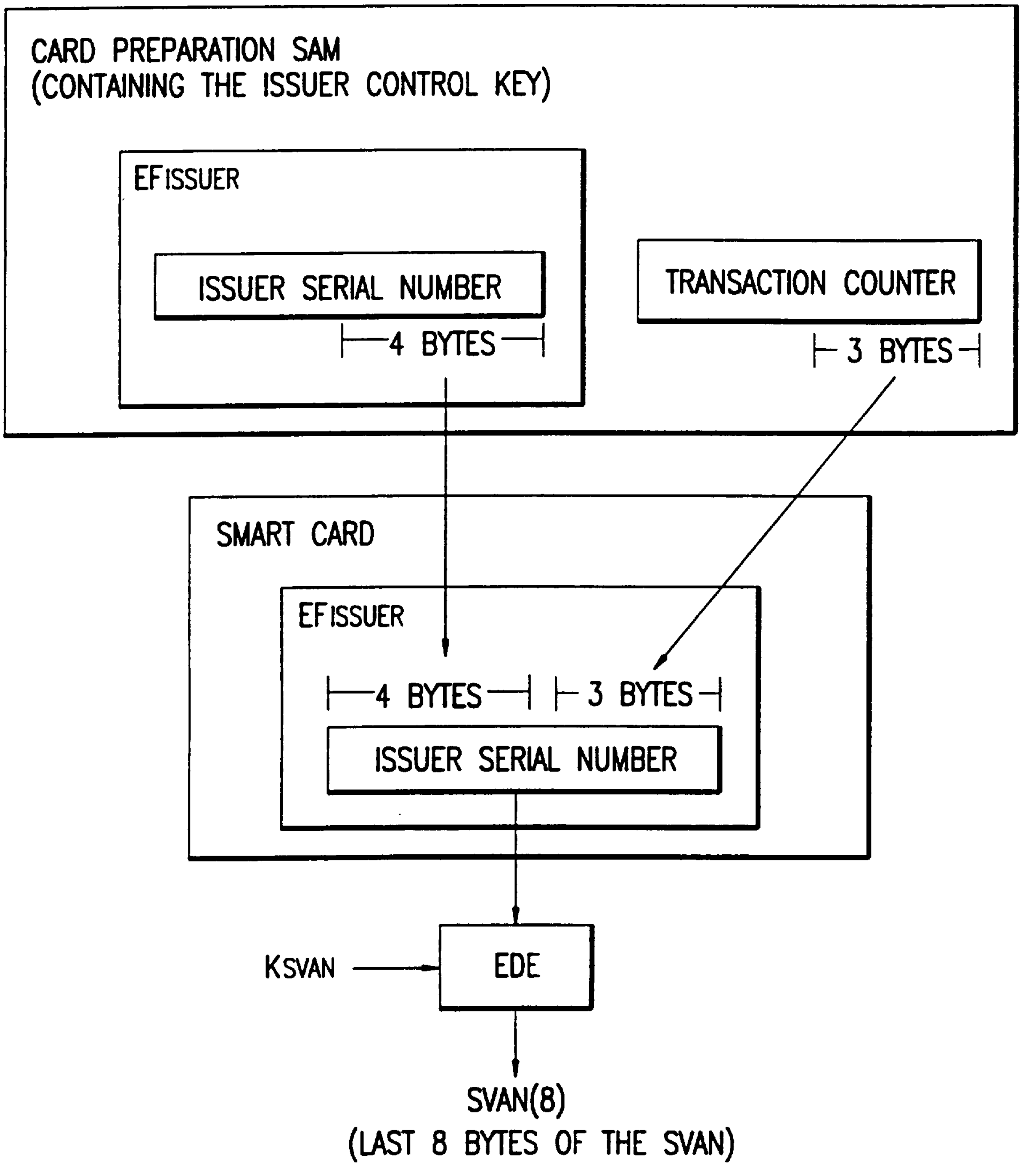

CARD PREPARATION SAM
(CONTAINING THE ISSUER CONTROL KEY)
EF ISSUER
ISSUER SERIAL NUMBER
4 BYTES
TRANSACTION COUNTER
3 BYTES
SMART CARD
EF ISSUER
4 BYTES
3 BYTES
ISSUER SERIAL NUMBER
KSVAN
EDE
SVAN(8)
(LAST 8 BYTES OF THE SVAN)

FIG.8

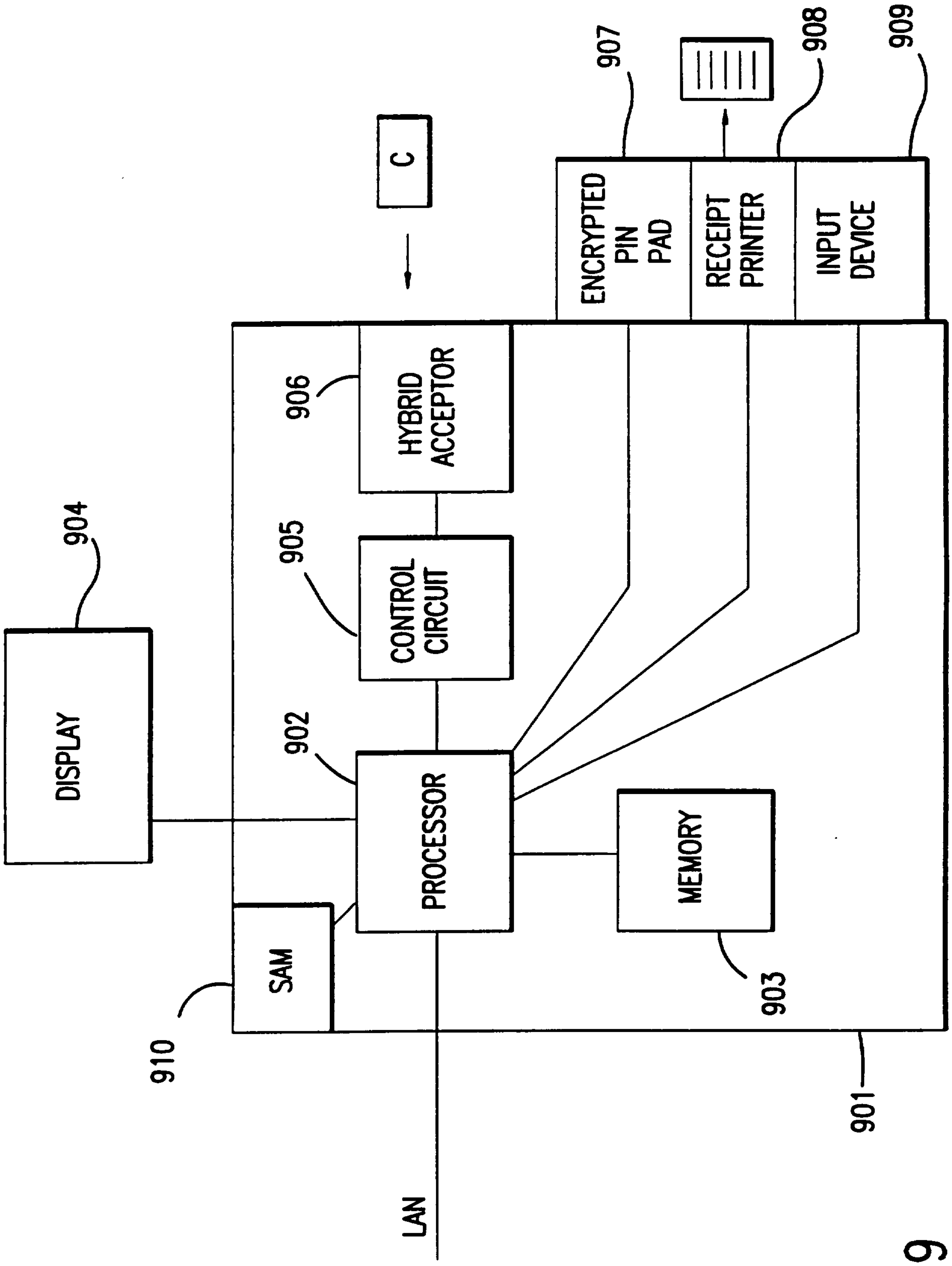

DISPLAY
904
C
906
HYBRID ACCEPTOR
905
CONTROL CIRCUIT
902
PROCESSOR
SAM
910
MEMORY
903
901
LAN
907
ENCRYPTED PIN PAD
RECEIPT PRINTER
908
INPUT DEVICE
909

FIG.9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/14414

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 17/60; G06K 5/00
US CL :235/379, 380
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)

U.S. : 235/379, 380

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)

APS, search terms: off-line, on-line, ic card, smart card

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 5,144,115 (Yoshida) 01 SEPTEMBER 1992. See entire document.	1-41
Y	US, A, 4,804,825 (BITOH) 14 FEBRUARY 1989, see the abstract.	1-41
Y	US, A, 4,630,201 (White) 16 December 1986, see column 6.	1-41

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier document published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search

27 NOVEMBER 1996

Date of mailing of the international search report

23 DEC 1996

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
JEFFREY R. FILIPEK
Telephone No. (703) 308-0956