(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 June 2009 (04.06.2009)

PCT

(10) International Publication Number
WO 2009/070041 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/NZ2008/000322

(22) International Filing Date:
28 November 2008 (28.11.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
563922 30 November 2007 (30.11.2007) NZ
2007237260 30 November 2007 (30.11.2007) AU

(71) Applicant *(for all designated States except US)*: **ELECTRONIC TRANSACTION SERVICES LIMITED** [NZ/NZ]; Level 23, ASB Bank Centre, 135 Albert Street, Auckland1 1010 (NZ).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GILL, Jason Nigel** [NZ/NZ]; 65 Kittiwake Drive, Schnapper Rock, North Shore City 0632 (NZ). **DUTT, Rajeshwar** [NZ/NZ]; 797 Dominion Road, Mount Eden, Auckland 1041 (NZ). **SOMA, Sanjay Magan** [NZ/NZ]; 3/33 Ladies Mile, Remuera, Auckland 1050 (NZ).

(74) Agents: **ADAMS, Matthew, D** et al.; A J Park, 6th Floor Huddart Parker Building, PO Box 949, Wellington 6015 (NZ).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

(54) Title: PAYMENT SYSTEM AND METHOD OF OPERATION

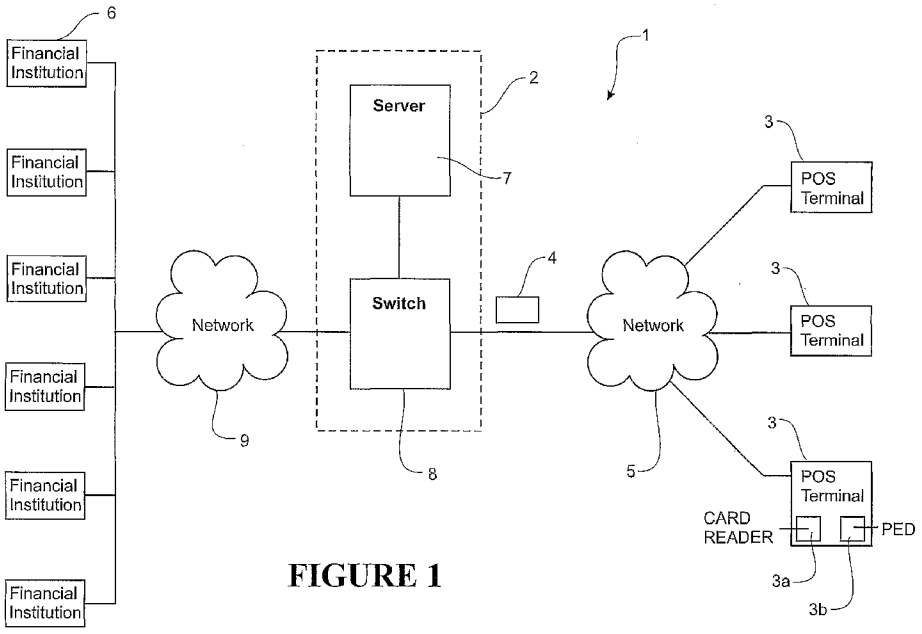

FIGURE 1

(57) Abstract: The present invention relates to a method and system for transferring funds between a merchant and purchaser. The transaction is initiated using a POS terminal (3). An encrypted transaction message is sent between the POS terminal (3) and a switch (8) that arranges a transfer of funds. The POS terminal (3) obtains a master key from a web server (7) for encrypting further key exchanges. The POS terminal (3) also receives configuration data from the switch 8 for configuring operation of the POS terminal (3).

WO 2009/070041 A2

PAYMENT SYSTEM AND METHOD OF OPERATION

FIELD OF THE INVENTION

The present invention relates to a payment system and method for electronic transactions.

BACKGROUND TO THE INVENTION

It is now common place for consumers to pay for their goods and services via electronic transactions. Typically, a merchant will have a point-of-sale (POS) terminal that is connected to a payment system via a network, such as a telephony network. When a customer wishes to purchase goods or services, a debit, credit or payment card is inserted or swiped through the terminal and the cost for the goods or services is entered into the POS terminal by the retailer. The customer then authorises the payment either through entering a pin number or by signing an authorisation slip. Once authorisation is complete, the POS terminal sends a transaction message to the payment system, which facilitates the transfer of funds from the customers account to the retailers account.

Due to changes in technology, the retailer POS terminals can become obsolete. This means that, in time, the POS terminals might not be able to function correctly with an upgraded payment system. Alternatively, the POS terminals might not be able to provide additional features and functionality as they become available.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide an improved method or system or computer or apparatus for facilitating the electronic transfer of funds in response to a purchase.

An improved system of the invention can do one or more of: increasing security through mutual authentication and/or message encryption, increasing the flexibility of POS terminals and their ability to be updated.

The payment system might relate to the computer systems that communicate with the terminals and financial institutions to facilitate electronic transactions. The payment system might also be considered to also comprise the terminals when connected to such a computer system, and any other features (such as networks) that might from such a payment system.

In one aspect the present invention may be said to consist in a method of reconfiguring a POS terminal comprising:

receiving at a computer system configuration data indicating operating configuration of a POS terminal,

verifying at the computer system that the operating configuration matches the required operating configuration of the POS terminal, and if not,

providing from the computer system different configuration data to the POS terminal to reconfigure the POS terminal with the required operating configuration.

Preferably the POS terminal comprises EMV tags that can be activated and de-activated to configure the POS terminal's configuration, wherein the configuration data provided from the computer system triggers activation/de-activation of the required EMV tags to reconfigure the POS terminal with the required operating configuration.

In another aspect the present invention may be said to consist in a method of transferring funds electronically between financial institutions in response to a transaction between a merchant and customer comprising:

receiving at a computer system configuration data indicating operating configuration of a POS terminal,

verifying at the computer system that the operating configuration matches the required operating configuration of the POS terminal, and if not,

providing from the computer system different configuration data to the POS terminal to reconfigure the POS terminal with the required operating configuration,

receiving at the computer system a transaction message indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arranging transfer of the transaction amount from the payer's financial institution to the payee's institution using the computer system.

Preferably the POS terminal comprises EMV tags that can be activated and de-activated to configure the POS terminal's configuration, wherein the configuration data provided from the computer system triggers activation and/or de-activation of the required EMV tags to reconfigure the POS terminal with the required operating configuration.

In another aspect the present invention may be said to consist in a POS terminal for transferring funds electronically between financial institutions of a merchant and customer, the terminal adapted to:

transmit configuration data to the computer system indicating operating configuration of the POS terminal, the computer system being adapted to verify that the received operating configuration matches the required operating configuration of the POS terminal, and

if the POS terminal operating configuration does not match the required operating configuration, receive configuration data from the computer system to reconfigure the POS terminal with the required operating configuration.

Preferably the POS terminal comprises EMV tags that can be activated and de-activated to configure the POS terminal's configuration, wherein the POS terminal is further adapted to:

reconfigure itself with the required operating configuration by activation and/or de-activation of the required EMV tags based on the configuration data received from the computer system.

In another aspect the present invention may be said to consist in a payment system for transferring funds electronically between financial institutions of a merchant and customer comprising:

a computer system connected to or for connection to a plurality of POS terminals and adapted to receive a transaction messages from the POS terminals, the computer system adapted to:

receive configuration data from a POS terminal indicating operating configuration of the POS terminal,

verify that the operating configuration matches the required operating configuration of the POS terminal, and if not,

provide from the computer system different configuration data to the POS terminal to reconfigure the POS terminal with the required operating configuration.

In another aspect the present invention may be said to consist in a payment system for transferring funds electronically between financial institutions of a merchant and customer comprising:

a computer system connected to or for connection to a plurality of POS terminals and adapted to receive a transaction messages from the POS terminals, the computer system adapted to:

receive configuration data from a POS terminal indicating operating configuration of the POS terminal,

verify that the operating configuration matches the required operating configuration of the POS terminal, and if not,

provide from the computer system different configuration data to the POS terminal to reconfigure the POS terminal with the required operating configuration,

receive a transaction message from the POS terminal indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arrange transfer of the transaction amount from the payer's financial institution to the payee's institution.

Preferably each POS terminal comprises EMV tags that can be activated and de-activated to configure the POS terminal's configuration, wherein the configuration data provided from the computer system triggers activation and/or de-activation of the required EMV tags to reconfigure the POS terminal with the required operating configuration.

In another aspect the present invention may be said to consist in a computer system for transferring funds electronically between financial institutions of a merchant and customer, the computer system adapted to:

receive configuration data from a POS terminal indicating operating configuration of the POS terminal,

verify that the operating configuration matches the required operating configuration of the POS terminal, and if not,

provide from the computer system different configuration data to the POS terminal to reconfigure the POS terminal with the required operating configuration,

receive a transaction message from the POS terminal indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arrange transfer of the transaction amount from the payer's financial institution to the payee's institution.

Preferably the POS terminal comprises EMV tags that can be activated and de-activated to configure the POS terminal's configuration, wherein the configuration data provided from the computer system triggers activation and/or de-activation of the required EMV tags to reconfigure the POS terminal with the required operating configuration.

In another aspect the present invention may be said to consist in a POS terminal connected or for connection to a computer system forming part of a payment system for transferring funds electronically between financial institutions between a merchant and customer, the POS terminal being adapted to send transaction messages to the computer system, a transaction message having encrypted data fields and indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions, wherein the POS terminal is adapted to do one or more of:

a) prior to sending the transaction message, obtain a master key from the computer system using mutual authentication,

b) prior to sending the transaction message, transmit configuration data indicating operating configuration of the POS terminal, which is verified by the computer system against a database that the operating configuration matches the required operating configuration, and if not, receive configuration data from the computer system to reconfigure the POS terminal with the required operating configuration,

c) encrypt the content in the message data fields using a transaction message key.

In another aspect the present invention may be said to consist in a method of arranging communication for a transaction with a POS terminal comprising:

receiving at a computer system a request from a POS terminal that initiates a key exchange process,

authenticating the POS terminal at the computer system,

providing from the computer system signed data to the POS terminal to enable authentication of the computer system by the POS terminal, and

providing from the computer system a master key to the POS terminal, wherein the master key can be utilised by the POS terminal for securing further key exchanges with the computer system.

In another aspect the present invention may be said to consist in a method of transferring funds electronically between financial institutions in response to a transaction between a merchant and customer comprising:

receiving at a computer system a request from a POS terminal that initiates a key exchange process,

authenticating the POS terminal at the computer system,

providing from the computer system signed data to the POS terminal to enable authentication of the computer system by the POS terminal, and

providing from the computer system a master key to the POS terminal, wherein the master key can be utilised by the POS terminal for securing further key exchanges with the computer system,

receiving at the computer system a transaction message indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arranging transfer of the transaction amount from the payer's financial institution to the payee's institution using the computer system.

Preferably the method further comprises:

receiving at the computer system a request from the POS terminal to obtain a transaction message key,

generating at the computer system a transaction message key and encrypting it with the master key, and

providing from the computer system the encrypted transaction message key to the POS terminal,

wherein the received transaction message is received from the POS terminal and is encrypted with the transaction key.

In another aspect the present invention may be said to consist in a payment system for transferring funds electronically between financial institutions of a merchant and customer comprising:

a computer system connected to or for connection to a plurality of POS terminals and adapted to receive a transaction messages from the POS terminals, the computer system adapted to:

receive a request from a POS terminal that initiates a key exchange process,

authenticate the POS terminal,

provide signed data to the POS terminal to enable authentication of the computer system by the POS terminal, and

provide a master key to the POS terminal, wherein the master key can be utilised by the POS terminal for securing further key exchanges with the computer system.

In another aspect the present invention may be said to consist in a payment system for transferring funds electronically between financial institutions of a merchant and customer comprising:

a computer system connected to or for connection to a plurality of POS terminals and adapted to receive a transaction messages from the POS terminals, the computer system adapted to:

receive a request from a POS terminal that initiates a key exchange process,

authenticate the POS terminal,

provide signed data to the POS terminal to enable authentication of the computer system by the POS terminal, and

provide a master key to the POS terminal, wherein the master key can be utilised by the POS terminal for securing further key exchanges with the computer system.

receive a transaction message indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arrange transfer of the transaction amount from the payer's financial institution to the payee's institution.

Preferably the computer system is further adapted to:

receive a request from the POS terminal to obtain a transaction message key,

generate a transaction message key and encrypt it with the master key, and

provide the encrypted transaction message key to the POS terminal,

wherein the received transaction message is encrypted with the transaction key.

In another aspect the present invention may be said to consist in a POS terminal for transferring funds electronically between financial institutions of a merchant and customer, the terminal adapted to:

send a request from to a computer system that initiates a key exchange process, the computer system being adapted to authenticate the POS terminal,

receive signed data from the computer system to enable authentication of the computer system by the POS terminal, and

receive a master key from the computer system, wherein the master key can be utilised by the POS terminal for securing further key exchanges with the computer system.

In another aspect the present invention may be said to consist in a computer system for transferring funds electronically between financial institutions of a merchant and customer, the computer system adapted to:

receive a request from a POS terminal that initiates a key exchange process,

authenticate the POS terminal,

provide signed data to the POS terminal to enable authentication of the computer system by the POS terminal, and

provide a master key to the POS terminal, wherein the master key can be utilised by the POS terminal for securing further key exchanges with the computer system.

receive a transaction message indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arrange transfer of the transaction amount from the payer's financial institution to the payee's institution.

Preferably the computer system is further adapted to:

receive a request from the POS terminal to obtain a transaction message key,

generate a transaction message key and encrypt it with the master key, and

provide the encrypted transaction message key to the POS terminal,

wherein the received transaction message is encrypted with the transaction key.

In another aspect the present invention may be said to consist in a method of transferring funds electronically between financial institutions in response to a transaction between a merchant and customer comprising:

receiving at a computer system a transaction message indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arranging transfer of the transaction amount from the payer's financial institution to the payee's institution using the computer system,

wherein the transaction message is comprises a header and message portion, the message portion having data fields with encrypted content.

Preferably the transaction message is received from a POS terminal over a non-secure network.

Preferably prior to receiving the transaction message, the method further comprises:

receiving at the computer system a request from a POS terminal that initiates a key exchange process,

authenticating the POS terminal at the computer system,

providing from the computer system signed data to the POS terminal to enable authentication of the computer system by the POS terminal, and

providing from the computer system a master key to the POS terminal,

wherein the master key can be utilised by the POS terminal for securing further key exchanges with the computer system.

Preferably the method further comprises:

receiving at the computer system a request from the POS terminal to obtain a transaction message key.

generating at the computer system a transaction message key and encrypting it with the master key, and

providing from the computer system the encrypted transaction message key to the POS terminal,

wherein the content of the data fields is encrypted with the transaction message key.

Preferably prior to receiving the transaction message, the method comprises:

receiving at the computer system configuration data indicating operating configuration of the POS terminal,

verifying at the computer system that the operating configuration matches the required operating configuration of the POS terminal, and if not,

providing from the computer system different configuration data to the POS terminal to reconfigure the POS terminal with the required operating configuration.

Preferably the configuration data comprises EMV tags to specify at least some of the types of data provided in a transaction message.

In another aspect the present invention may be said to consist in a method of transferring funds electronically between financial institutions in response to a transaction between a merchant and customer comprising:

receiving at a computer system a transaction message indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arranging transfer of the transaction amount from the payer's financial institution to the payee's institution,

wherein the transaction message is comprises encrypted data fields.

In another aspect the present invention may be said to consist in a payment system for transferring funds electronically between financial institutions of a merchant and customer comprising:

a computer system connected to or for connection to a plurality of POS terminals and adapted to receive a transaction messages from the POS terminals, the computer system adapted to:

receive a transaction message from a POS terminal indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arrange transfer of the transaction amount from the payer's financial institution to the payee's institution,

wherein the transaction message is comprises a header and message portion, the message portion having data fields with encrypted content.

In another aspect the present invention may be said to consist in a payment system according to claim 29 further comprising a plurality of POS terminals connected to the computer system via one or more networks.

Preferably the computer system communicates with a plurality of financial institutions via one or more networks.

Preferably the computer system comprises a switch for arranging funds transfers and a server for exchanging keys with the POS terminals.

In another aspect the present invention may be said to consist in a computer system for transferring funds electronically between financial institutions of a merchant and customer, the computer system adapted to:

receive a transaction message from a POS terminal indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arrange transfer of the transaction amount from the payer's financial institution to the payee's institution,

wherein the transaction message is comprises a header and message portion, the message portion having data fields with encrypted content.

Preferably the computer system communicates with a plurality of financial institutions via one or more networks.

Preferably the computer system comprises a switch for arranging funds transfers and a server for exchanging keys with the POS terminals.

In another aspect the present invention may be said to consist in a method of transferring funds electronically between financial institutions in response to a transaction between a merchant and customer comprising:

receiving at a computer system a transaction message indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arranging transfer of the transaction amount from the payer's financial institution to the payee's institution,

wherein the transaction message is comprises encrypted data fields.

In this specification where reference has been made to patent specifications, other external documents, or other sources of information, this is generally for the purpose of providing a context for discussing the features of the invention. Unless specifically stated otherwise, reference to such external documents is not to be construed as an admission that such documents, or such sources of information, in any jurisdiction, are prior art, or form part of the common general knowledge in the art

The term "comprising" as used in this specification means "consisting at least in part of". Related terms such as "comprise" and "comprised" are to be interpreted in the same manner.

To those skilled in the art to which the invention relates, many changes in construction and widely differing embodiments and applications of the invention will suggest themselves without

departing from the scope of the invention as defined in the appended claims. The disclosures and the descriptions herein are purely illustrative and are not intended to be in any sense limiting

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the invention will be described with reference to the following drawings, of which:

Figure 1 is a block diagram showing an overview of a payment system according to the invention,

Figure 2 is a process diagram showing an overview of the payment system,

Figures 3a, 3b, 4 are flow diagrams showing the mutual authentication and master key exchange,

Figure 5 is a table of example EMV tags,

Figure 6 is a table of a message structure with EMV tags,

Figure 7 is a flow diagram of an encryption process/data exchange process,

Figures 8, 9 are schematic diagrams of a message structure,

Figure 10 is a process diagram of the EMV tag update process.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Overall system

Figure 1 shows a simplified overview of a payment system 1 according to the invention. The payment system comprises a computer system 2 that facilitates electronic funds transfers. It comprises a switch 8 that independently communicates with a number of merchant POS terminals 3 and receives electronic transaction requests from them. The requests are received in the form of transaction messages e.g. 4 transmitted from the respective POS terminals 3. The switch 8 is also in communication with a number of financial institutions 6, such as banks, via network 9. The switch 8 facilitates the transfer of funds between the financial institutions 6 of respective parties (merchant/customer or payee/payer) involved in the electronic transactions. The computer system 2 also comprises a server 8 for carrying out logon, key exchange and other system administration procedures. In particular, the server carries out POS terminal key loading services. These comprise key generation, key loading, key management, key activation and key assignment. There is also security infrastructure. The switch 7 and server 8 might be located remotely from each other, or provided in the same location. The POS terminals 3 communicate with the central computer system 2 via a network 5, such as a telephony network. This could be a dial-up network, leased line, fixed IP, broadband IP, GPRS, CDMA or any other suitable telephony network. Each POS terminal 3 comprises a PIN entry device (PED) 3a and a card reader device 3b. The POS terminal has the ability to load terminal master keys. It also is pre-loaded with a manufacturer key. The payment

system 1 might be considered to be the computer system alone, or some combination of one or more of the computer system, the POS terminals, the networks and other aspects that enable electronic transactions.

Briefly, the payment system 1 works in the following manner. A POS terminal 3 logs on to the system 1 upon installation in order to receive the required keys to operate. Then periodically, the POS terminal logs on to the computer system 2 to identify itself and to receive required session keys (including transaction message keys), updated configuration data, and other required data for operation. The POS terminal operates in the normal manner for a POS terminal 3 from a user perspective. But, it can also operate in new ways in accordance with the received configuration and other data. In effect, the POS terminal is adapted to exploit the various new features of the system, including the ability to update its operation. The periodic logon can happen automatically or manually. It might, for example, occur every 24 hours or when a particular POS terminal is turned on, such as at the beginning of a retail day. . Each POS terminal 3 is adapted to work with the payment system 1 and utilise the re-configuration features. When a customer approaches the retailer to purchase goods and/or services, the POS terminal is operated and a transaction message 4 is created. This is done by introducing the customer's card to the card reader, and entering transaction details into the unit via a keypad. The transaction message is sent to the computer system 2 (and more particularly the switch 8), which in turn arranges electronic transfer of funds between the customer and the retailer's bank accounts 6. It then returns a transaction complete message to the POS terminal 3. The entire process is termed and "transaction" and comprises all or some of receiving card details to trigger a transaction, creating and sending a transaction message, arranging funds transfer, and providing confirmation.

The system contains a number of features that offer advantages over other specifications. Private keys for use in sending transaction messages can be securely loaded remotely. EMV applications, public keys and transaction and other message tags can be remotely managed according to POS terminal requirements. Transaction messages 4 can be more comprehensively encrypted, allowing them be sent over any network. Each POS terminal 3 in the payment system 1 is also designed to operate with all major card schemes and proprietary debit formats. Therefore, a POS terminal 3 can connect with minimal manual intervention, be re-configured remotely to behave in different ways and support the varied needs of multiple acquiring banks. As a result, the POS terminals 3 do not have to be returned to "base" for reconfiguration and a single POS terminal can accept local debit cards as well as other cards. The present invention allows for POS terminals 3 to be remotely configured to function as either a full EMV POS terminal, a standard magnetic strip terminal, or a combination of both based on the card scheme, acquirer and merchant requirements. A merchant can use a single POS terminal adapted to be configured and reconfigured according to the present invention to carry out all these functionalities.

For example, a POS terminal 3 of the payment system 1 can be configured to behave in the following ways:

1. To act as magnetic stripe only POS terminal.
2. To act as a full EMV terminal.
3. To act as a mixed magnetic stripe or EMV terminal dependant on the card present.
4. To accept off-line transactions for any or all cards processed.
5. To maintain EMV public keys as required for the EMV functions present.

Each POS terminal can be configured or re-configured with one or more of the above functionalities without any onsite reprogramming. The configuration is determined by the merchant/acquiring bank requirements or other local market features. It can have different requirements configured concurrently for each of the different card schemes it supports. These features are not limited to any particular POS terminal brand or proprietary POS terminal management system. All POS terminals 3 operating to the prescribed payment system 1 standard can operate in this manner. POS terminals require sufficient memory to store the flexible configuration. The functionality of the present invention is implemented in software in the terminal.

The combination of remotely configurable POS terminal 3 behaviour and the ability to operate over any network (particularly IP based networks) offers a flexible POS terminal environment that can meet the needs of multiple merchants, card schemes, issuers and acquirers all driven from a single platform. Direct integration with the processing platform enables all POS terminals to be configured in the same way, to avoid mismatched configuration or need to re-enter data, which occurs if an existing standalone-type POS terminal management system is used for each terminal type.

The result is a flexible payment system that can be adapted to meet a variety of merchant and acquirer requirements. It is possible to configure POS terminals 3 for one acquirer to behave quite differently from another and then re-configure their behaviour relatively easily. The flexibility of the system is based around the interactions that take place between the POS terminal 3 and the computer system 2.

Figure 2 shows in a general sense the nature of the interaction 26 that takes place between a POS terminal 3 and the computer system 2 prior to and during a transaction. Initially, the POS terminal is preconfigured with the manufacturer key and serial number. This occurs during manufacture of the POS terminal. Once on-site at the merchant premises, the POS terminal 3 can be installed and initialized. This first involves connecting the POS terminal to the computer system 2 in a way the merchant chooses through a variety of communications methods (dial, broadband, GPRS, CDMA, specialist IP service) 5. As part of the installation/initialization process 26, the POS terminal checks whether it has a master key, step 21. If it does not, the POS terminal then logs on to the server and initiates a key exchange process. The POS terminal and server undergo key

exchange process, which comprises a mutual authentication process, steps 20-21. As a result of this, a master key is downloaded from the computer system 2 to the POS terminal 3, for encrypting subsequent transaction messages 4.

During the periodic log on, the POS terminal 3 provides configuration data indicating its operating configuration to the switch 8, step 22. This comprises version details of software being executed, and other data as appropriate. This information is sent in an 0800 message in accordance with the AS2805 specification for network management. In response, the switch 8 checks the configuration data to see it matches the required configurations for that POS terminal 3. This information is stored in a database in the switch. The required configuration for a POS terminal 3 might change periodically, due to card issuer requirements, functionality updates and the like. If the configuration of the POS terminal 3 does not match the required configuration specified for that POS terminal, then the switch 8 provides (and the POS terminal downloads) various configuration data that is used to configure operation of the POS terminal 3 as part of the overall payment/transaction system, step 23. This includes enabling support for optionally providing EMV transactions via the POS terminal. The configuration data also comprises data specifying the requirement to change the secure session keys after a defined period or number of transactions or both. The information is sent in a 0300 message in accordance with the AS2805 specification for network management

At this point, the POS terminal 3 is then ready to facilitate transactions, steps 24, 25 in response to purchase of merchant goods/services by a customer. These transactions proceed in a manner to be described later, although appear to proceed in the usual way from a user/customer perspective. For example, such a transaction could proceed by way of a card swipe or dip, step 24. The POS terminal 3 then initiates a transaction using downloaded parameters from the previous steps to determine how the transaction occurs. A transaction message is sent to the switch, detailing among other things, the value of the transaction and the merchant who has undertaken the transaction and to whom the funds should be transferred. Information relating to the purchaser's card is also sent. The merchant information and purchaser's card information provide information for identifying the respective payer's (purchaser) and payee's (merchant) financial institutions and corresponding accounts within those financial institutions. For example, the information is used by the switch 8 to identify the bank account numbers of the payer and payee in a table of such information. The information is sent as a 0100 or 0200 message to the switch 8 in accordance with the AS2805 specification for network management. The switch 8 actions the funds transfer in accordance with the transaction message.

The switch 8 responds with a 110 or 210 message in accordance with the AS2805 specification for network management, as appropriate and EMV processing scripts if required. If required, the host can force a logoff and initiate the sequence again at step 22 if parameters have

been changed. That is, at any time, the POS terminal 3 can be centrally re-configured to support new operational and/or system features, such as a new bank acquirer, new card scheme, or to amend the merchant's trading parameters. This is by way of a manual or automatic update process, steps 22, 23.

The various functions of the system and method will now be described in further detail.

Mutual authentication and master key exchange process

As shown in Figure 2 in steps 20 to 21, the POS terminal 3 undergoes an initialisation/installation process with the server of the computer system 2. First, the POS terminal 3 checks if it already has a master key from the computer system step 20, and if not undergoes a key exchange process to obtain a master key. This process is termed "remote key injection" (RKI). A mutual authentication process steps 21, 22, Figure 2 is undertaken to obtain the key. The master key is used for encrypting various communications between the POS terminal 3 and the server 7 or switch 8. In particular, it is used to encrypt the transaction message session keys (to be described later) when they are exchanged between the switch 8 and the POS terminal 3 during the periodic logon.

The RKI process carries out mutual authentication of both parties (server 7 and POS terminal 3) involved in the transaction to reduce the risk of compromise in the process. It also incorporates a secure communication method with equipment manufacturers that allows for the exchange of sensitive data that assists in securing the process. The long process differs from others in the field in that it uses strong mutual authentication of parties at all stages. The file received from POS terminal suppliers (the Key Data File) is signed with a public/private key pair and then not only does the PED device authenticate itself to the computer system 2, but the terminal verifies that the computer system 2 is the authorised source for the master key. The Key Data File from the vendor contains records that match the PED serial number to the manufacturer's key for each device.

Figures 3a-4 show the flow diagrams of the RKI process, corresponding to steps 20, 21 of Figure 2. The process, comprises sign on (Figure 3a), master key exchange (Figure 3b) and sign off (Figure 4). These processes take place as follows.

Referring to Figure 3a, first the sign on takes place. The POS terminal 3 initiates the key download process, step 30, by sending the computer system 2 (more particularly the server 7) a request that contains the POS terminal's PED's software version, manufacturer ID, vendor ID and unique serial number. The PED's unique serial number is digitally signed with the PED's private key. This digital signature will be appended to field 60 of a network management request between the POS terminal and the server.

Next, the server 7 verifies the digital signature of the PED's unique serial number using the PED's public key, step 31. It then checks the PED's software version against a list of permitted software versions in an "allowed versions" database, step 32. If the PED's software version is a permitted version, the computer system verifies the authenticity of the PED by verifying the manufacturer ID, vendor ID and unique serial number against the data provided by the vendor in the key data file, step 33.

The server then generates a statistically random public/private key pair Key^{rki_ped} and a randomly generated secret number Sn^{rki}, step 34. The public/private key pair is then linked to the PED's unique serial number by the computer system. The serial number is sent from the POS terminal to the computer system, but also contained in the Key Data File as a cross check. That is, the server can check authenticity of the POS terminal using the information it receives, plus by using the serial number in the Key Data File, to which it has access. Looking at the Key Data File provides a back-up to checking the received serial number. Both the public/private key and the secret number (Key^{rki_ped} and Sn^{rki}) are signed with the computer system's private key ${}_{prv}Key^{rki}$, step 35. The secret number Sn^{rki} is encrypted using the PED's public key ${}_{pub}Key^{ped}$. The public/private key pair ${}_{pub}Key^{rki\_ped}$ and the secret number Sn^{rki} are returned to the POS terminal in a message, step 36.

Following a successful sign on, a master key is exchanged between the computer system 2 and the POS terminal 3 as follows, with reference to Figure 3b. First, the POS terminal verifies the server's signature with ${}_{pub}Key^{rki}$, step 37. If the key is valid, the POS terminal stores the ${}_{pub}Key^{rki\_ped}$ for later use. Then, the POS terminal 3 responds with a message that contains the Sn^{rki} and the type of key it requires, step 38. The server 7 receives the message and confirms that the Sn^{rki} associated with the PED unique serial number is same as the Sn^{rki} received in the message. It does this by checking the database, step 39. Then the computer system 2 responds with a message containing the type of POS terminal master key Key^{rki_tm} requested by the POS terminal (this could also be a 3rd party POS terminal master key). The Key^{rki_tm} is encrypted with the ${}_{pub}Key^{ped}$ and signed using the ${}_{prv}Key^{rki\_ped}$, step 40. The POS terminal 3 verifies the signature of the encrypted Key^{rki_tm} using ${}_{pub}Key^{rki\_ped}$ and decrypts the Key^{rki_tm} using ${}_{prv}Key^{ped}$, and loads Key^{rki_tm} into the appropriate key slot, step 41. The master key Key^{rki_tm} is then ready for use in obtaining session keys. More particularly, it is used in the logon process to create the three session keys for encryption during the transaction process.

Following a successful master key exchange process, a sign off process is undertaken, as shown in Figure 4. On successful Key^{rki_tm} loading, the POS terminal then sends an acknowledgment message to the RKI server, MAC'ed with the master key Key^{rki_tm} (symmetric key), step 42. This provides verification – if encryption is wrong then the MAC addresses do not match. On receipt of the acknowledgement, the server validates the message MAC using the master key

Key^{tki_tm}, and sends an activation message for the merchant and terminal ID combination to server 7, step 43. The server 7 then sends back a message to the POS terminal 3 to confirm that the master key loading process is complete, step 44. The message contains a MAC from the computer system calculated using the master key Key^{tki_tm}. Unless multiple keys are required, the POS terminal is required to end communications session (i.e. close socket or hang up phone line) on receipt of the sign off message, step 35.

EMV tag download

Once initialisation/installation is complete, then the device periodically logons to the switch, step 22, 23 of Figure 2. This might automatically happen every 24 hours, for example. During logon, transaction message session keys are obtained. These are transferred in an encrypted form using the master key. The transaction message session keys can be used to encrypt transaction messages communicated between the POS terminal and switch. During logon, PIN session keys and MAC keys are also generated and sent from the computer system to the POS terminal.

At each 24 hour log on, new session keys are generated by the switch 8, which returns the new session keys to the POS terminal encrypted under variants of the POS terminal master key.

Various configuration data can also be transferred from the switch to the POS terminal to update/reconfigure its functionality at this time. For example, activation of EMV tags can be updated.

The transaction message is created with fields in accordance with EMV tags where a smart "chip" card is used by a customer for a transaction. These tags are specified by the EMV standard. EMV has approximately 170 elements of "tag" data that can be required to be sent from a POS terminal to an acquiring network. These can be mandated by the card issuer so that they can specify the information that is received when conducting a transaction using their card. Each card issuer can stipulate different EMV tags to be used in relation to transactions involving their cards. Each POS terminal 3 can be configured and reconfigured with different sets of EMV tags to alter the nature of the information contained in a transaction message. Those EMV tags can be activated and de-activated remotely to alter terminal functionality, as required.

For example, activation/de-activation any of the tags detailed in Figure 5 can be altered for each card scheme application defined in the POS terminal to match the requirements of that particular card scheme. The requirements of the card scheme and how the POS terminal operates for that card is defined by the card issuer. Should these requirements change, the appropriate EMV tags used in the changed card scheme can be activated/de-activated remotely in the POS terminal, without the terminal application being reloaded and/or reconfigured manually by the terminal owner or technician.

Therefore, a particular POS terminal 3 might have different "sets" of EMV tags for each respective card issuer. A particular transaction message 4 created in response to a transaction for a particular card type will have data relating to the EMV tags specified for that card type. Figure 5 shows some typical (although not all) EMV tags and a definition/description of their data/functionality. A full set of EMV tags need not be described as these are published in the EMV specification and are known by those skilled in the art. Figure 6 shows an example of a transaction message 4 (such as that shown in Figure 9 later) with a number of field containing transaction data. The EMV tags are specified in the integrated chip card (ICC) data field 55. As can be seen in Figure 6, field 55 specifies the EMV tags in 5, along with content for those tags.

The EMV tag activation process is indicated in Figure 2, steps 22, 23. This forms part of the overall interaction process that takes place between the POS terminal 3 and computer system 2 (switch 8 and server 7). The requirements for this data can vary for each different card scheme and may change over time. The present invention proposes to keep POS terminals 3 deployed over several years hence has included a methodology to configure the EMV tags required remotely from the switching platform. This allows POS terminals 3 to change the tag data sent as part of a transaction without the need to change the POS terminal application or undergo re-certification. This has significant speed/flexibility implications when meeting future mandate or tag requirements.

Figure 7 shows the process in more detail. The POS terminal 3 is preloaded with the various EMV tags it may need to utilize. The POS terminal 3 then connects to the switch 8 during the periodic logon, step 70. In doing so it supplies a version number for the currently enabled configuration/application file that it is operating with. The configuration/application file is a joint file that controls the configuration and applications available in the POS terminal. It also supplies the currently enabled public keys, which are the public keys for the particular chip cards the POS terminal will work with. Public keys are provided for each of the card schemes, such as VISA, Mastercard and the like. Card prefix records are also supplied, which specify rules on how and when cards will be accepted for use. The switch 8 then verifies if the currently enabled application, public keys and card prefix records match those held by the host, step 71. It does this by checking the database held by the switch 8. This database specifies the configuration parameters that the requesting POS terminal 3 should be configured with. These may have been updated since the POS terminal 3 was last reconfigured. The update might be due, for example, to changes in operation, improved features, the requirements of a particular application changing, new cards being released, or other occurrence. For example, where a merchant has agreed to accept cards from a new card scheme, their EMV applications records and the operating parameters can be downloaded to the terminal. Similarly, should a new card scheme emerge, then keys, EMV application, and operating parameters can be attached to all terminals and downloaded. Activation and/or de-activation of preloaded EMV tags can be triggered over download also.

If the records do not match, the switch 8 returns a new set of application, public key and card prefix records and downloads these to the POS terminal, step 72 in a message. These messages contain a record for each supported EMV application and the EMV tags required for that application. The acitivation/de-activation of the terminal EMV tags to implement the new application is triggered as part of an 0300 message download sequence. This is in accordance with the AS2805 specification for network management. The POS terminal 3 uses the new application, public key, activated/de-activated EMV tags and card prefix records to specify the nature of the transaction message and how the transaction proceeds, step 73.

The EMV tags required for each card scheme application are held in a master application record on the switch 8 for each acquiring bank 6 belonging to that scheme. For each EMV application the POS terminal 3 is triggered by a downloaded message from the system to activate/de-activate the EMV tags required. When an EMV transaction is initiated for that application the tags are requested from the Chip Card and later activated/de-activated in the transaction message. These are the EMV tags that are specified for transfer when using that card scheme, and which have been activated/de-actived in the terminal during the download process. With the flexibility to vary tags to acquirer level, the terminal can ensure that it sends only tags that an acquirer can process but the same terminal can send a different set of tags if merchant changes to a different acquirer and retains the same equipment.

Enhanced message encryption (EME)

Once authentication and key exchange has taken place, and the periodic logon has taken place, the POS terminal 3 can then initiate transactions 4 on the payment system 1 (step 24, Figure 2). This takes place by a merchant operating the POS terminal 3 to request an electronic transfer of funds, and the customer authorising that by using their card in the card reader and entering a PIN number. Once operated, the POS terminal sends a transaction message 4 (such as that shown in Figure 6) to the switch 8 that contains information to trigger/facilitate the transfer. The message 4 is encrypted in a manner termed "enhanced message encryption" (EME). Figures 8 and 9 show an example of a message structure and Figure 10 is a flow diagram showing the enhanced message encryption process. Messages are encrypted using standard financial encryption protocols allowing messages to be sent over any open network. However, the present invention is faster to establish connections than other Internet based protocols and it also takes advantage of the secure master key loaded in each POS terminal 3 to enhance the encryption of the message to eliminate the risk of certain security attacks. The use of a mutual authentication process and master key dispenses with the need for a SSL secure session between the POS terminal 3 and the switch 8. This speeds up communication, allowing for the use of enhanced message encryption.

The transaction message 4 transferred from the POS terminal 3 to the switch 8 has a structure comprising a number of fields. Each field specifies certain information that is transferred to facilitate the transaction. An example of a transaction message, the fields it contains, and the type of information in those fields is shown in Figure 6. Figure 8 shows some other typical fields that could be used in the transaction message. The fields comprise field 55, which is an integrated circuit card (ICC) data field. This field contains data relating to a number of EMV tags which specify operation functionality of the POS terminal 3 and the transaction message 4 as described above. The tags for field 55 can be different for different POS terminals and types of POS terminals, and the tags used in any particular POS terminal might change over time after reconfiguration in response to system/protocol updates. The updating of the EMV tags is described above, in respect of Figures 5 and 6.

Figure 9 shows the actual structure of the message 90. All information is encrypted prior to sending the transaction message, except for fields used for routing the message through the network 5. It comprises a transport protocol data unit (TPDU) header 90a and routing fields 90b which form the header 91 A payload 90c is attached to the head comprising the message content. The header 91 remains unencrypted, but the message field 90c is encrypted using the transaction message session keys. This creates the encrypted transaction message 92.

Figure 10 shows the encryption process. This is undertaken by a computer program embedded in or downloaded into the hardware or firmware of the POS terminal 3. The EME process uses a separate data encryption (transaction) session key to take the transaction messages and then encrypt it (including all data fields) them using a standard 3DES process. The resulting secure message can then be routed over any network. The use of 3DES to secure all the message fields in the message as part of a standard message process is different to other encryption processes and different from a 'privacy key' approach that secures card data fields only. Certain fields are not encrypted to assist with routing by third party nodes that will not be privy to the decryption keys. This allows for routing of the transaction messages over a range of network types, where security is uncertain or cannot be controlled by the payment system administrator.

Referring to Figure 10, the encryption process contains the following steps. First, the POS terminal 3 receives the transaction request and the transaction message 4 is generated for sending to the computer system, step 100. The encryption process is triggered. The software then fetches the encryption transaction session key from its memory, step 101. This has been downloaded from the computer system 2 on a previous occasion, during the periodic logon process. The POS terminal 3 then determines if the transaction session key is still valid, step 102. The key is specified as being valid for a number of transactions, or a certain time period as configured by the computer system 2 for the POS terminal 3. If the session key is not still valid, the POS terminal 3 obtains another session key from the computer system 2 (more particularly, the switch 8) in the normal manner,

using the periodic logon process, step 103. Once the POS terminal 3 has a valid session key, it encrypts the transaction message, step 104. The message is encrypted under triple DES in ECB mode (as per AS 2805.5.4 – 2000 and AS2805.5.2). To aid with routing the message through third party nodes, the following (header) fields are not encrypted:

a. Encryption indicator
b. A copy of field 41, Card Acceptor Terminal ID
c. A copy of field 42, Card Acceptor ID Code
d. A copy of field 11, STAN
e. The Message Type

Once encrypted, the transaction message can be sent to the computer system 2 for facilitating the funds transfer, step 105. The computer system 2 decrypts the message 4 using the private session key and the message 4 is processed as normal to effect funds transfer by the switch 8.

Effects of combination of features

The POS terminal 3 and transaction features described above can be combined to provide an improved payment system 1. Private keys can be securely loaded remotely, EMV applications, public keys and tags can be remotely managed according to POS terminal requirements, and transaction messages are encrypted so they can be sent over any network. The POS terminal is adapted to operate with all major card schemes and proprietary debit formats. In summary, the system operates in the following manner.

1. The POS terminal is preconfigured with the manufacturer key and serial number.
2. The POS terminal is plugged in at the merchant site. The merchant can choose one or a number of communications methods such as dial-up, broadband, GPRS, CDMA, specialist IP service.
3. The private keys are download to the POS terminal
4. The POS terminal logs on to the network.
5. The POS terminal then downloads
    a. configuration records
    b. Application tables that determine how the POS terminal will behave for each card range and control:
        i. The application display text
        ii. The EMV action codes for the POS terminal (in each mode)
        iii. Online PIN capability
        iv. Offline PIN capability
        v. Whether the PIN can be bypassed
        vi. Whether the cardholder verification can be disabled

vii. The EMV tags to be sent with the transaction

c. Card tables that determine

i. Accounts available

ii. Purchase amounts (in various modes)

iii. Cash amounts

iv. Checking parameters

v. Offline behavior

vi. The pan truncation algorithm to be used on the receipt

d. Public keys for supported EMV schemes

6. Downloaded are the requirements to change the secure session keys after a defined period or number of transactions (or both).

7. EMV support can be only switched on for relevant schemes (or turned off entirely), offline operational parameters can are determined (and can be turned off)

8. The merchant can then transact

a. Both magnetic stripe and EMV operation can be supported

b. EMV cards for the schemes the merchant belongs to are supported

c. The transaction can be on-line or offline

d. Stored transaction are encrypted under a storage key

e. Messages when sent are fully encrypted

f. If transactions cannot be sent an temporary electronic offline function is available

9. The POS terminal can be centrally re-configured at any point to support a new bank acquirer, new card scheme or to amend the merchant's trading parameters.

CLAIMS

1. A method of reconfiguring a POS terminal comprising:

receiving at a computer system configuration data indicating operating configuration of a POS terminal,

verifying at the computer system that the operating configuration matches the required operating configuration of the POS terminal, and if not,

providing from the computer system different configuration data to the POS terminal to reconfigure the POS terminal with the required operating configuration.

2. A method according to claim 1 wherein the POS terminal comprises EMV tags that can be activated and de-activated to configure the POS terminal's configuration, wherein the configuration data provided from the computer system triggers activation/de-activation of the required EMV tags to reconfigure the POS terminal with the required operating configuration.

3. A method of transferring funds electronically between financial institutions in response to a transaction between a merchant and customer comprising:

receiving at a computer system configuration data indicating operating configuration of a POS terminal,

verifying at the computer system that the operating configuration matches the required operating configuration of the POS terminal, and if not,

providing from the computer system different configuration data to the POS terminal to reconfigure the POS terminal with the required operating configuration,

receiving at the computer system a transaction message indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arranging transfer of the transaction amount from the payer's financial institution to the payee's institution using the computer system.

4. A method according to claim 3 wherein the POS terminal comprises EMV tags that can be activated and de-activated to configure the POS terminal's configuration, wherein the configuration data provided from the computer system triggers activation and/or de-activation of the required EMV tags to reconfigure the POS terminal with the required operating configuration.

5. A POS terminal for transferring funds electronically between financial institutions of a merchant and customer, the terminal adapted to:

transmit configuration data to the computer system indicating operating configuration of the POS terminal, the computer system being adapted to verify that the received operating configuration matches the required operating configuration of the POS terminal, and

if the POS terminal operating configuration does not match the required operating configuration, receive configuration data from the computer system to reconfigure the POS terminal with the required operating configuration.

6. A POS terminal according to claim 5 wherein the POS terminal comprises EMV tags that can be activated and de-activated to configure the POS terminal's configuration, wherein the POS terminal is further adapted to:

reconfigure itself with the required operating configuration by activation and/or de-activation of the required EMV tags based on the configuration data received from the computer system.

7. A payment system for transferring funds electronically between financial institutions of a merchant and customer comprising:

a computer system connected to or for connection to a plurality of POS terminals and adapted to receive a transaction messages from the POS terminals, the computer system adapted to:

receive configuration data from a POS terminal indicating operating configuration of the POS terminal,

verify that the operating configuration matches the required operating configuration of the POS terminal, and if not,

provide from the computer system different configuration data to the POS terminal to reconfigure the POS terminal with the required operating configuration.

8. A payment system for transferring funds electronically between financial institutions of a merchant and customer comprising:

a computer system connected to or for connection to a plurality of POS terminals and adapted to receive a transaction messages from the POS terminals, the computer system adapted to:

receive configuration data from a POS terminal indicating operating configuration of the POS terminal,

verify that the operating configuration matches the required operating configuration of the POS terminal, and if not,

provide from the computer system different configuration data to the POS terminal to reconfigure the POS terminal with the required operating configuration,

receive a transaction message from the POS terminal indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arrange transfer of the transaction amount from the payer's financial institution to the payee's institution.

9. A payment system according to claim 7 or 8 wherein each POS terminal comprises EMV tags that can be activated and de-activated to configure the POS terminal's configuration, wherein the configuration data provided from the computer system triggers activation and/or de-activation of the required EMV tags to reconfigure the POS terminal with the required operating configuration.

10. A computer system for transferring funds electronically between financial institutions of a merchant and customer, the computer system adapted to:

receive configuration data from a POS terminal indicating operating configuration of the POS terminal,

verify that the operating configuration matches the required operating configuration of the POS terminal, and if not,

provide from the computer system different configuration data to the POS terminal to reconfigure the POS terminal with the required operating configuration,

receive a transaction message from the POS terminal indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arrange transfer of the transaction amount from the payer's financial institution to the payee's institution.

11. A computer system according to claim 10 wherein the POS terminal comprises EMV tags that can be activated and de-activated to configure the POS terminal's configuration, wherein the configuration data provided from the computer system triggers activation and/or de-activation of the required EMV tags to reconfigure the POS terminal with the required operating configuration.

12. A POS terminal connected or for connection to a computer system forming part of a payment system for transferring funds electronically between financial institutions between a merchant and customer, the POS terminal being adapted to send transaction messages to the computer system, a transaction message having encrypted data fields and indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions, wherein the POS terminal is adapted to do one or more of:

a) prior to sending the transaction message, obtain a master key from the computer system using mutual authentication,

b) prior to sending the transaction message, transmit configuration data indicating operating configuration of the POS terminal, which is verified by the computer system against a database that the operating configuration matches the required operating configuration, and if not, receive configuration data from the computer system to reconfigure the POS terminal with the required operating configuration,

c) encrypt the content in the message data fields using a transaction message key.

13. A method of arranging communication for a transaction with a POS terminal comprising:

receiving at a computer system a request from a POS terminal that initiates a key exchange process,

authenticating the POS terminal at the computer system,

providing from the computer system signed data to the POS terminal to enable authentication of the computer system by the POS terminal, and

providing from the computer system a master key to the POS terminal, wherein the master key can be utilised by the POS terminal for securing further key exchanges with the computer system.

14. A method of transferring funds electronically between financial institutions in response to a transaction between a merchant and customer comprising:

receiving at a computer system a request from a POS terminal that initiates a key exchange process,

authenticating the POS terminal at the computer system,

providing from the computer system signed data to the POS terminal to enable authentication of the computer system by the POS terminal, and

providing from the computer system a master key to the POS terminal, wherein the master key can be utilised by the POS terminal for securing further key exchanges with the computer system,

receiving at the computer system a transaction message indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arranging transfer of the transaction amount from the payer's financial institution to the payee's institution using the computer system.

15. A method according to claim 13 or 14 further comprising:

receiving at the computer system a request from the POS terminal to obtain a transaction message key,

generating at the computer system a transaction message key and encrypting it with the master key, and

providing from the computer system the encrypted transaction message key to the POS terminal,

wherein the received transaction message is received from the POS terminal and is encrypted with the transaction key.

16. A payment system for transferring funds electronically between financial institutions of a merchant and customer comprising:

a computer system connected to or for connection to a plurality of POS terminals and adapted to receive a transaction messages from the POS terminals, the computer system adapted to:

receive a request from a POS terminal that initiates a key exchange process,

authenticate the POS terminal,

provide signed data to the POS terminal to enable authentication of the computer system by the POS terminal, and

provide a master key to the POS terminal, wherein the master key can be utilised by the POS terminal for securing further key exchanges with the computer system.

17. A payment system for transferring funds electronically between financial institutions of a merchant and customer comprising:

a computer system connected to or for connection to a plurality of POS terminals and adapted to receive a transaction messages from the POS terminals, the computer system adapted to:

receive a request from a POS terminal that initiates a key exchange process,

authenticate the POS terminal,

provide signed data to the POS terminal to enable authentication of the computer system by the POS terminal, and

provide a master key to the POS terminal, wherein the master key can be utilised by the POS terminal for securing further key exchanges with the computer system.

receive a transaction message indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arrange transfer of the transaction amount from the payer's financial institution to the payee's institution.

18. A payment system according to claim 16 or 17 wherein the computer system is further adapted to:

receive a request from the POS terminal to obtain a transaction message key,

generate a transaction message key and encrypt it with the master key, and

provide the encrypted transaction message key to the POS terminal,

wherein the received transaction message is encrypted with the transaction key.

19. A POS terminal for transferring funds electronically between financial institutions of a merchant and customer, the terminal adapted to:

send a request from to a computer system that initiates a key exchange process, the computer system being adapted to authenticate the POS terminal,

receive signed data from the computer system to enable authentication of the computer system by the POS terminal, and

receive a master key from the computer system, wherein the master key can be utilised by the POS terminal for securing further key exchanges with the computer system.

20. A computer system for transferring funds electronically between financial institutions of a merchant and customer, the computer system adapted to:

receive a request from a POS terminal that initiates a key exchange process,

authenticate the POS terminal,

provide signed data to the POS terminal to enable authentication of the computer system by the POS terminal, and

provide a master key to the POS terminal, wherein the master key can be utilised by the POS terminal for securing further key exchanges with the computer system.

receive a transaction message indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arrange transfer of the transaction amount from the payer's financial institution to the payee's institution.

21. A computer system according to claim 20 further adapted to:

receive a request from the POS terminal to obtain a transaction message key,

generate a transaction message key and encrypt it with the master key, and

provide the encrypted transaction message key to the POS terminal,

wherein the received transaction message is encrypted with the transaction key.

22. A method of transferring funds electronically between financial institutions in response to a transaction between a merchant and customer comprising:

receiving at a computer system a transaction message indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arranging transfer of the transaction amount from the payer's financial institution to the payee's institution using the computer system,

wherein the transaction message is comprises a header and message portion, the message portion having data fields with encrypted content.

23. A method according to claim 22 wherein the transaction message is received from a POS terminal over a non-secure network.

24. A method according to claim 22 or 23 wherein prior to receiving the transaction message, the method further comprises:

receiving at the computer system a request from a POS terminal that initiates a key exchange process,

authenticating the POS terminal at the computer system,

providing from the computer system signed data to the POS terminal to enable authentication of the computer system by the POS terminal, and

providing from the computer system a master key to the POS terminal,

wherein the master key can be utilised by the POS terminal for securing further key exchanges with the computer system.

25. A method according to claim 24 further comprising:

receiving at the computer system a request from the POS terminal to obtain a transaction message key,

generating at the computer system a transaction message key and encrypting it with the master key, and

providing from the computer system the encrypted transaction message key to the POS terminal,

wherein the content of the data fields is encrypted with the transaction message key.

26. A method according to any preceding claim wherein prior to receiving the transaction message, the method comprises:

receiving at the computer system configuration data indicating operating configuration of the POS terminal,

verifying at the computer system that the operating configuration matches the required operating configuration of the POS terminal, and if not,

providing from the computer system different configuration data to the POS terminal to reconfigure the POS terminal with the required operating configuration.

27. A method according to claim 26 wherein the configuration data comprises EMV tags to specify at least some of the types of data provided in a transaction message.

28. A method of transferring funds electronically between financial institutions in response to a transaction between a merchant and customer comprising:

receiving at a computer system a transaction message indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arranging transfer of the transaction amount from the payer's financial institution to the payee's institution,

wherein the transaction message is comprises encrypted data fields.

29. A payment system for transferring funds electronically between financial institutions of a merchant and customer comprising:

a computer system connected to or for connection to a plurality of POS terminals and adapted to receive a transaction messages from the POS terminals, the computer system adapted to:

receive a transaction message from a POS terminal indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arrange transfer of the transaction amount from the payer's financial institution to the payee's institution,

wherein the transaction message is comprises a header and message portion, the message portion having data fields with encrypted content.

30. A payment system according to claim 29 further comprising a plurality of POS terminals connected to the computer system via one or more networks.

31. A payment system according to claim 29 or 30 further wherein the computer system communicates with a plurality of financial institutions via one or more networks.

32. A payment system according to any one of claims 29 to 31 wherein the computer system comprises a switch for arranging funds transfers and a server for exchanging keys with the POS terminals.

33. A computer system for transferring funds electronically between financial institutions of a merchant and customer, the computer system adapted to:

receive a transaction message from a POS terminal indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arrange transfer of the transaction amount from the payer's financial institution to the payee's institution,

wherein the transaction message is comprises a header and message portion, the message portion having data fields with encrypted content.

34. A computer system according to claim 33 wherein the computer system communicates with a plurality of financial institutions via one or more networks.

35. A computer system according to claim 33 or 34 wherein the computer system comprises a switch for arranging funds transfers and a server for exchanging keys with the POS terminals.

36. A method of transferring funds electronically between financial institutions in response to a transaction between a merchant and customer comprising:

receiving at a computer system a transaction message indicating a transaction amount and containing information for identifying the payer's and payee's financial institutions,

arranging transfer of the transaction amount from the payer's financial institution to the payee's institution,

wherein the transaction message is comprises encrypted data fields.

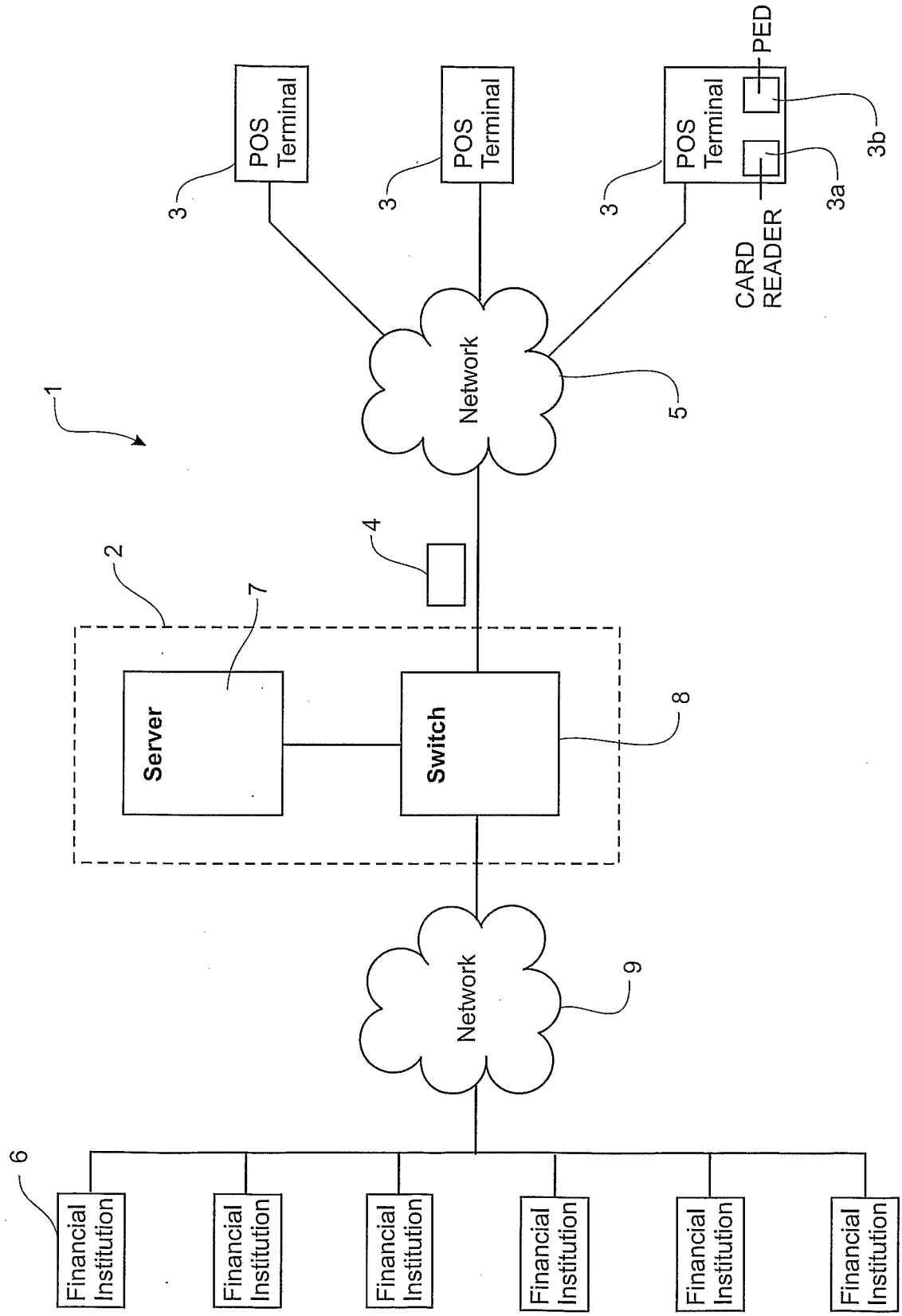
POS Terminal
POS Terminal
POS Terminal
PED
3b
3a
CARD READER
3
3
3
Network
5
1
4
2
7
Server
Switch
8
Network
9
6
Financial Institution
Financial Institution
Financial Institution
Financial Institution
Financial Institution
Financial Institution

FIGURE 1

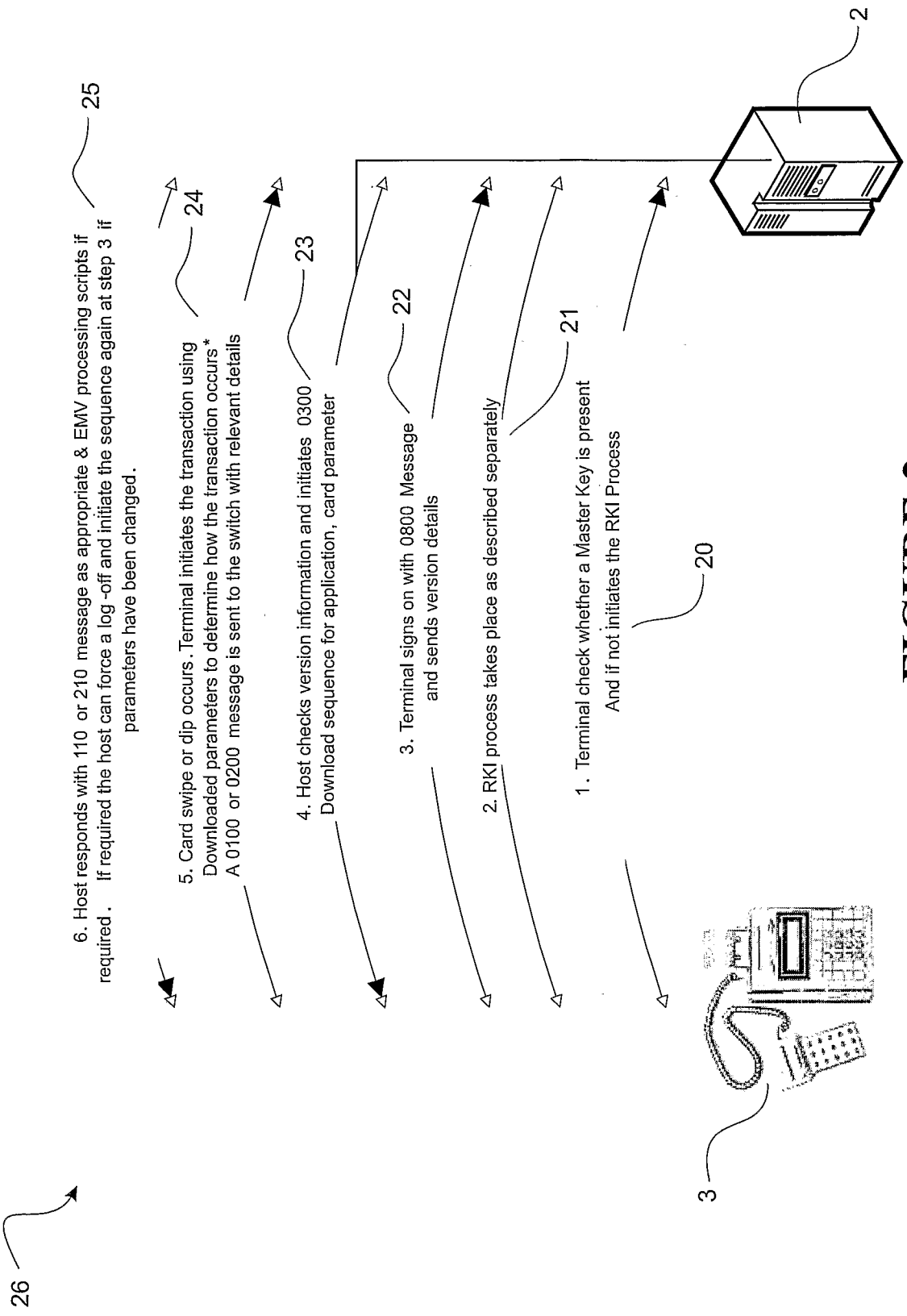
26
25
6. Host responds with 110 or 210 message as appropriate & EMV processing scripts if required . If required the host can force a log -off and initiate the sequence again at step 3 if parameters have been changed.
24
5. Card swipe or dip occurs. Terminal initiates the transaction using Downloaded parameters to determine how the transaction occurs* A 0100 or 0200 message is sent to the switch with relevant details
23
4. Host checks version information and initiates 0300 Download sequence for application, card parameter
22
3. Terminal signs on with 0800 Message and sends version details
21
2. RKI process takes place as described separately
20
1. Terminal check whether a Master Key is present And if not initiates the RKI Process
2
3

FIGURE 2

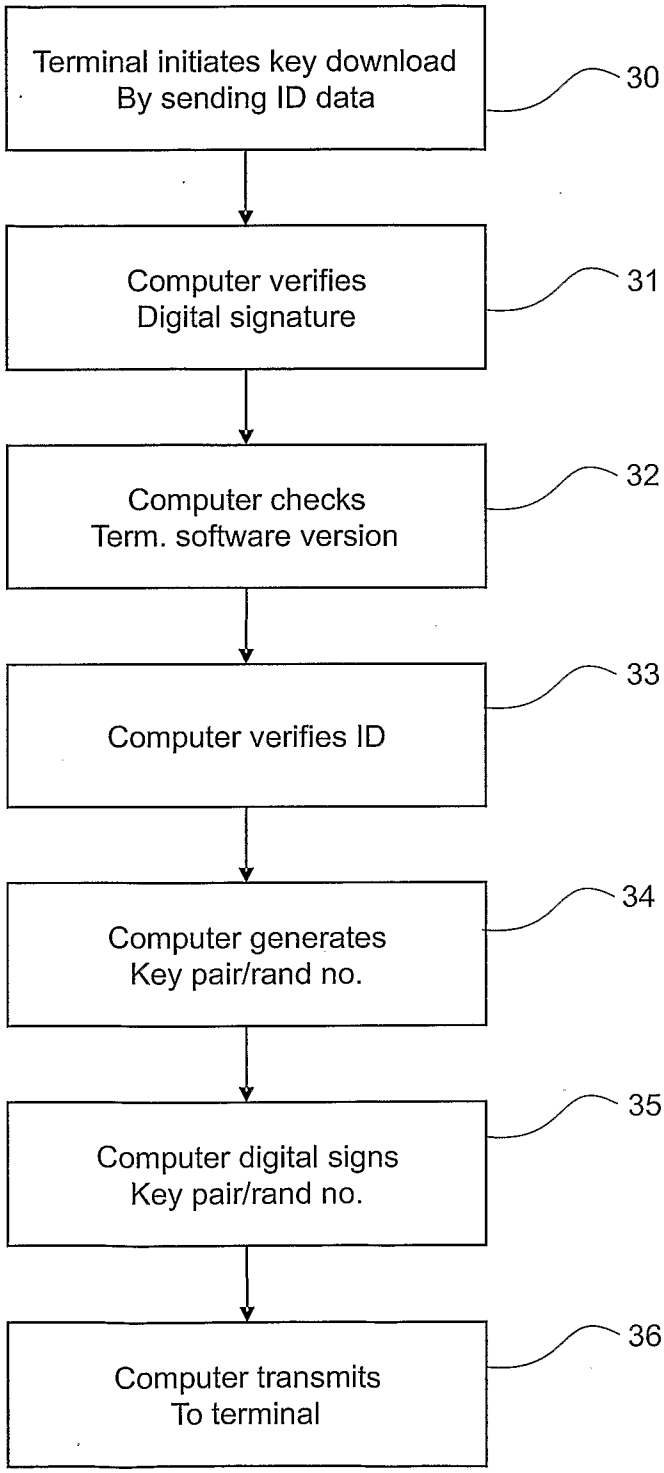
Terminal initiates key download
By sending ID data
30
Computer verifies
Digital signature
31
Computer checks
Term. software version
32
Computer verifies ID
33
Computer generates
Key pair/rand no.
34
Computer digital signs
Key pair/rand no.
35
Computer transmits
To terminal
36

FIGURE 3a

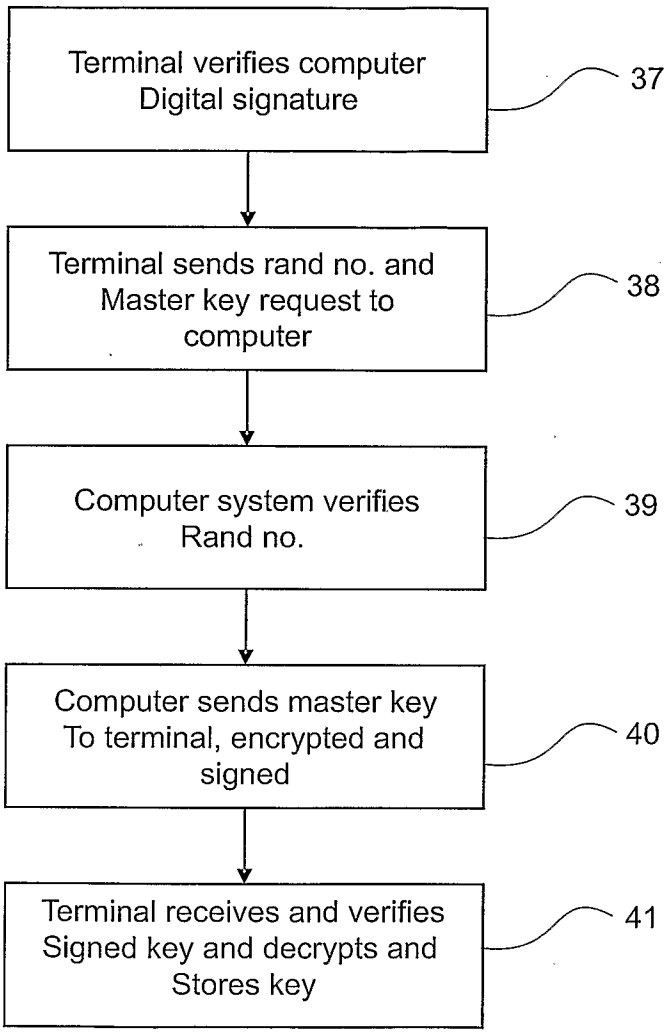
Terminal verifies computer Digital signature
37
Terminal sends rand no. and Master key request to computer
38
Computer system verifies Rand no.
39
Computer sends master key To terminal, encrypted and signed
40
Terminal receives and verifies Signed key and decrypts and Stores key
41

FIGURE 3b

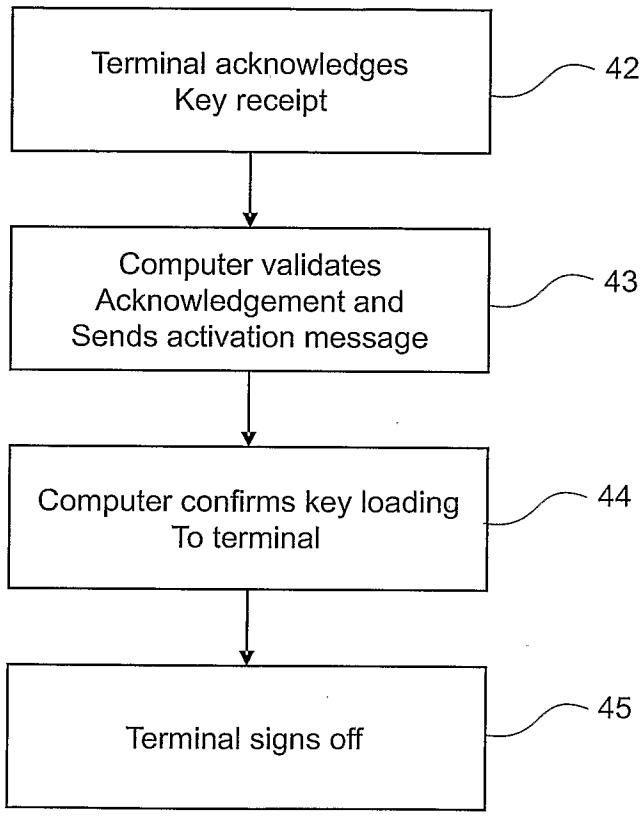
Terminal acknowledges
Key receipt
42
Computer validates
Acknowledgement and
Sends activation message
43
Computer confirms key loading
To terminal
44
Terminal signs off
45

FIGURE 4

EMV Tags

- 9F40 Additional Terminal Capabilities
- 9F02 Amount Authorised
- 9F03 Amount Other
- 9F26 Application Cryptogram
- 5F25 Application Effective Date
- 5F24 Application Expiration Date
- 9F06 Application Identifier (AID)
- 82 Application Interchange Profile
- 5F34 Application Primary Account Number (PAN) Sequence Number
- 9F36 Application Transaction Counter
- 9F09 Application Version Number
- 8A Authorisation Response Code
- 9F34 Cardholder Verification Method (CVM) Results
- 9F27 Cryptogram Information Data
- 9F1E Interface Device (IFD) Serial Number
- 9F10 Issuer Application Data
- 91 Issuer Authentication Data
- 5F28 Issuer Country Code
- 9F5B Issuer Script Results
- 71 Issuer Script Template 1
- 72 Issuer Script Template 2
- 9F33 Terminal Capabilities
- 9F1A Terminal Country Code
- 9F35 Terminal Type
- 95 Terminal Verification Results
- 5F2A Transaction Currency Code
- 9A Transaction Date
- 9B Transaction Status Information
- 9C Transaction Type
- 9F37 Unpredictable Number

FIGURE 5

Financial Transaction Request (0200)

Field	Message Fields	Data
Field 3	Processing Code	003000
Field 4	Amount Transaction	000000000100
Field 11	Systems Trace Audit Number	000112
Field 22	Point of Service Entry Mode	051
Field 24	Network International Identifier	001
Field 25	Point of Service Condition Code	00
Field 35	Customer Card Track 2 Data	4761739001010010D1012201114387808 9
Field 41	Card Acceptor Terminal ID	00980617
Field 42	Card Acceptor ID	00980617
Field 52	Customer PIN Data	DBC45773EC2C4FDA
Field 55	Integrated Circuit Card (ICC) Data	9F40:05:F000F0A001
		9F02:06:000000000100
		9F03:06:000000000000
		9F26:08:09C2505CD5BCD3CF
		5F25:03:950701
		5F24:03:101231
		9F06:07:A0000000031010
		82:02:5C00
		5F34:01:01
		9F36:02:02FF
		9F09:02:0084
		9F34:03:020300
		9F27:01:80
		9F1E:08:12345678
		9F10:07:06010A03A00000
		5F28:02:0840
		9F33:03:E0F0C8
		9F1A:02:0554
		9F35:01:22
		95:05:0000048000
		5F2A:02:0554
		9A:03:071029
		9B:02:E800
		9C:01:00
		9F37:04:0A02657A
Field 61	Last Completed Trans	000101
Field 64	Message Authentication Code	F9E0E42A00000000

FIGURE 6

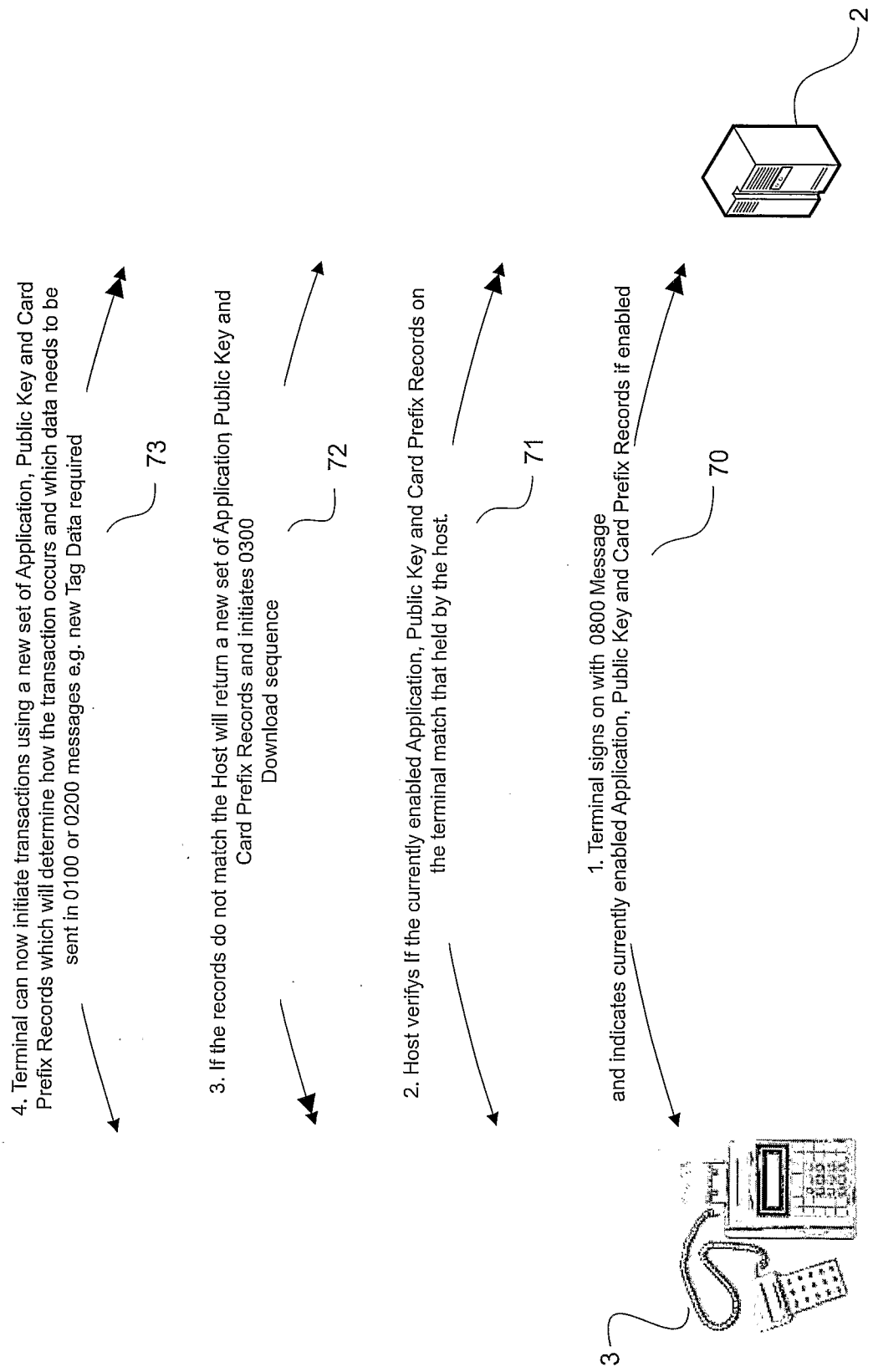
4. Terminal can now initiate transactions using a new set of Application, Public Key and Card Prefix Records which will determine how the transaction occurs and which data needs to be sent in 0100 or 0200 messages e.g. new Tag Data required
73
3. If the records do not match the Host will return a new set of Application, Public Key and Card Prefix Records and initiates 0300 Download sequence
72
2. Host verifys If the currently enabled Application, Public Key and Card Prefix Records on the terminal match that held by the host.
71
1. Terminal signs on with 0800 Message and indicates currently enabled Application, Public Key and Card Prefix Records if enabled
70
2
3

FIGURE 7

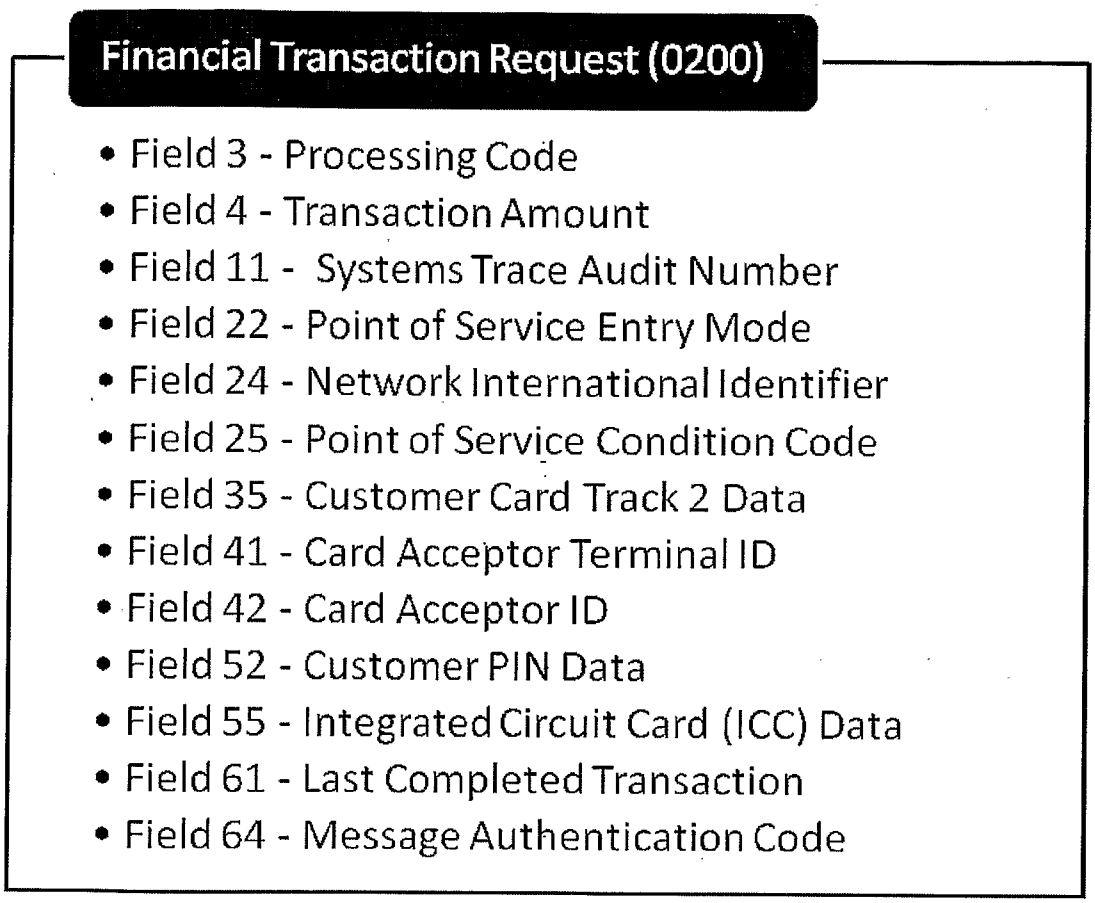
Financial Transaction Request (0200)
• Field 3 - Processing Code
• Field 4 - Transaction Amount
• Field 11 - Systems Trace Audit Number
• Field 22 - Point of Service Entry Mode
• Field 24 - Network International Identifier
• Field 25 - Point of Service Condition Code
• Field 35 - Customer Card Track 2 Data
• Field 41 - Card Acceptor Terminal ID
• Field 42 - Card Acceptor ID
• Field 52 - Customer PIN Data
• Field 55 - Integrated Circuit Card (ICC) Data
• Field 61 - Last Completed Transaction
• Field 64 - Message Authentication Code

FIGURE 8

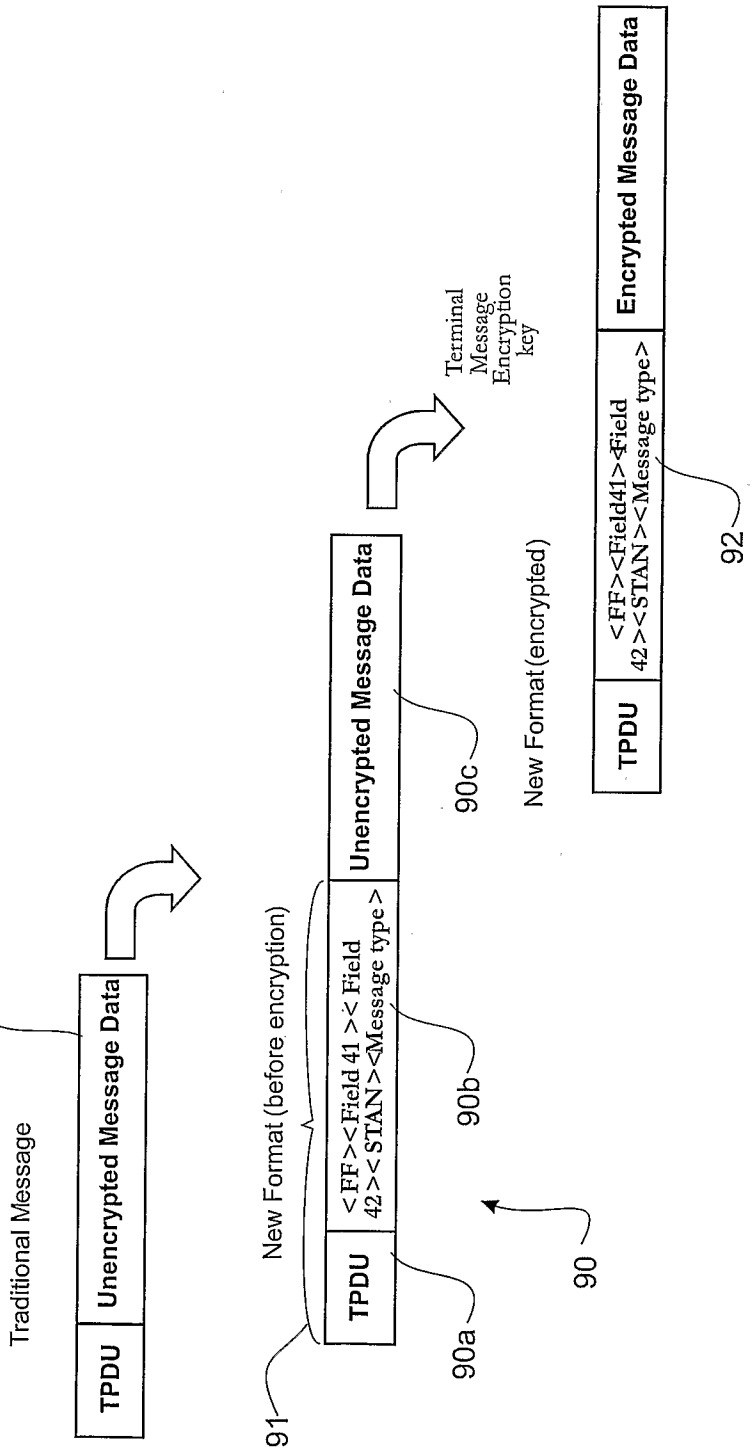
Traditional Message
57
TPDU
Unencrypted Message Data
New Format (before encryption)
91
TPDU
< FF >< Field 41 >< Field 42 >< STAN >< Message type >
Unencrypted Message Data
90a
90b
90c
90
Terminal Message Encryption key
New Format (encrypted)
TPDU
< FF >< Field41 >< Field 42 >< STAN >< Message type >
Encrypted Message Data
92

FIGURE 9

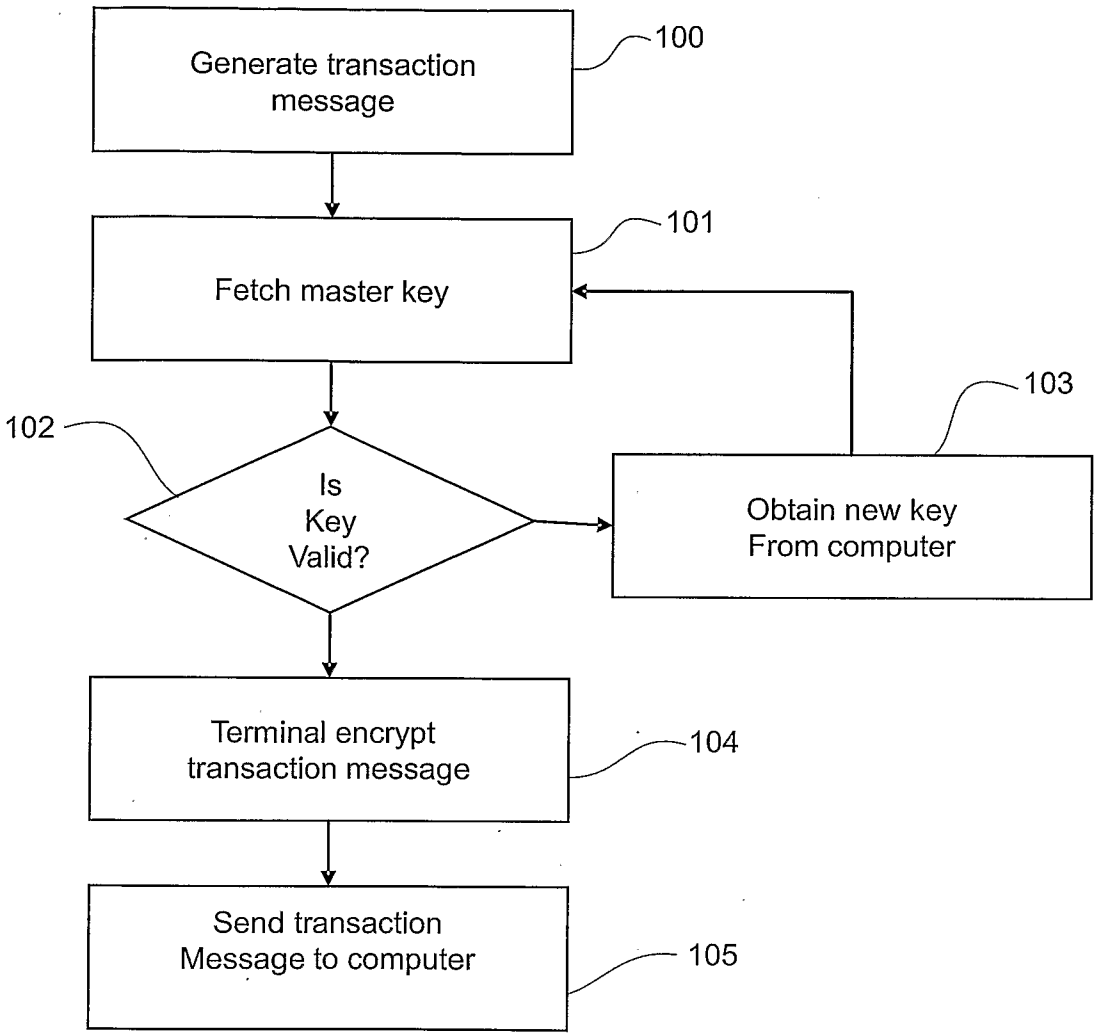
Generate transaction message
100
Fetch master key
101
102
Is Key Valid?
103
Obtain new key From computer
Terminal encrypt transaction message
104
Send transaction Message to computer
105

FIGURE 10