

Walker
& Jocke a legal professional association

Ralph E. Jocke
Patent
&
Trademark Law

January 9, 2007
Via Federal Express

Ms. Cindy Fuller
Executive Director
Accredited Standards Committee X9, Inc.
3051 Rundelac Road
Annapolis, Maryland 21403

Re: **Supplemental Patent Statement of Diebold, Incorporated**

Dear Ms. Fuller:

I am writing to you on behalf of Diebold, Incorporated ("**Diebold**"). This Supplemental Patent Statement of Diebold supplements the Patent Statement submitted on August 11, 2003 and supplemented April 5, 2004 to Accredited Standards Committee X9, Inc. ("**X9**").

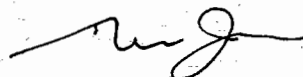
Diebold is the owner of U.S. Patent Numbers 6,854,645; 7,110,986; and 7,159,114. Copies of each of these patents are enclosed for your reference. Additional patent applications having disclosures that are the same as the enclosed patents, and/or those patents previously notified to X9, remain pending.

The U.S. Patents notified to X9 by Diebold, as well as the pending applications, may result in patent rights that encompass systems and methods utilized by persons practicing the X9.24 Part 2 Standard in conjunction with ATMs.

Diebold hereby restates that to the extent that the Standard cannot be practiced without a license to the patents referred to in Diebold's Patent Statement, Diebold hereby provides written assurance that licenses will be made available to applicants under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

If you have any questions concerning this matter, please do not hesitate to contact me.

Very truly yours,



Ralph E. Jocke

REJ/lch
Enclosures

330 • 721 • 0000
MEDINA

330 • 225 • 1669
CLEVELAND

330 • 722 • 6446
FACSIMILE

rej@walkerandjocke.com
E-MAIL



US007159114B1

(12) **United States Patent**
Zajkowski et al.

(10) **Patent No.:** US 7,159,114 B1
(45) **Date of Patent:** Jan. 2, 2007

(54) **SYSTEM AND METHOD OF SECURELY
INSTALLING A TERMINAL MASTER KEY
ON AN AUTOMATED BANKING MACHINE**

(75) **Inventors:** Timothy Zajkowski, Uniontown, OH
(US); Anne Doland, Uniontown, OH
(US); Mark D. Smith, North Canton,
OH (US)

(73) **Assignee:** Diebold, Incorporated, North Canton,
OH (US)

(*) **Notice:** Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 1002 days.

(21) **Appl. No.:** 10/126,728

(22) **Filed:** Apr. 19, 2002

Related U.S. Application Data

(60) Provisional application No. 60/285,724, filed on Apr.
23, 2001.

(51) **Int. Cl.**
H04K 1/00 (2006.01)
H04L 9/00 (2006.01)
G06Q 99/00 (2006.01)

(52) **U.S. Cl.** 713/171; 713/175; 713/176;
380/259; 705/73

(58) **Field of Classification Search** None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,918,728 A *	4/1990	Matyas et al.	380/280
4,941,176 A *	7/1990	Matyas et al.	380/280
4,972,472 A *	11/1990	Brown et al.	380/277
5,214,698 A *	5/1993	Smith et al.	380/280
5,428,684 A *	6/1995	Akiyama et al.	705/66
5,539,825 A *	7/1996	Akiyama et al.	705/68
5,787,403 A	7/1998	Randle	
6,085,177 A	7/2000	Semple et al.	
6,115,816 A	9/2000	Davis	

6,308,887 B1	10/2001	Korman et al.
6,396,928 B1	5/2002	Zheng
6,539,361 B1	3/2003	Richards et al.
6,539,364 B1 *	3/2003	Moribatake et al. 705/69
6,606,387 B1 *	8/2003	Abraham 380/277
6,705,517 B1 *	3/2004	Zajkowski et al. 235/379

(Continued)

OTHER PUBLICATIONS

"NCR Holistic Security: ATMIA ATM Security Best Practice Winner 2003". Oct. 27, 2003, Business Wire via Dialog Text Search, p. 1-2.*

"Triple DES: Options for Compliance", 2003, ATMmarketplace.com Guide, p. 1-40.*

(Continued)

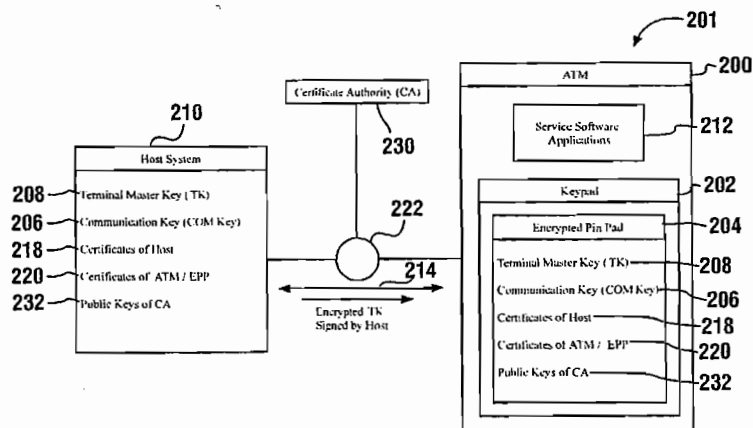
Primary Examiner—Christopher Revak

(74) *Attorney, Agent, or Firm*—Christopher L. Parmelee;
Ralph E. Jocke; Walker & Jocke LPA

(57) **ABSTRACT**

An automated banking machine (12, 200, 302) is provided. The machine may be operative to install a terminal master key (TK) therein in response to at least one input from a single operator. The machine may include an EPP (204) that is operative to remotely receive an encrypted terminal master key from a host system (210, 304). The machine may authenticate and decrypt the terminal master key prior to accepting the terminal master key. The machine may further output through a display device (30) of the machine a one-way hash of at least one public key associated with the host system. The machine may continue with the installation of the terminal master key in response to an operator confirming that the one-way hash of the public key corresponds to a value independently known by the operator to correspond to the host system.

43 Claims, 15 Drawing Sheets



US 7,159,114 B1

Page 2

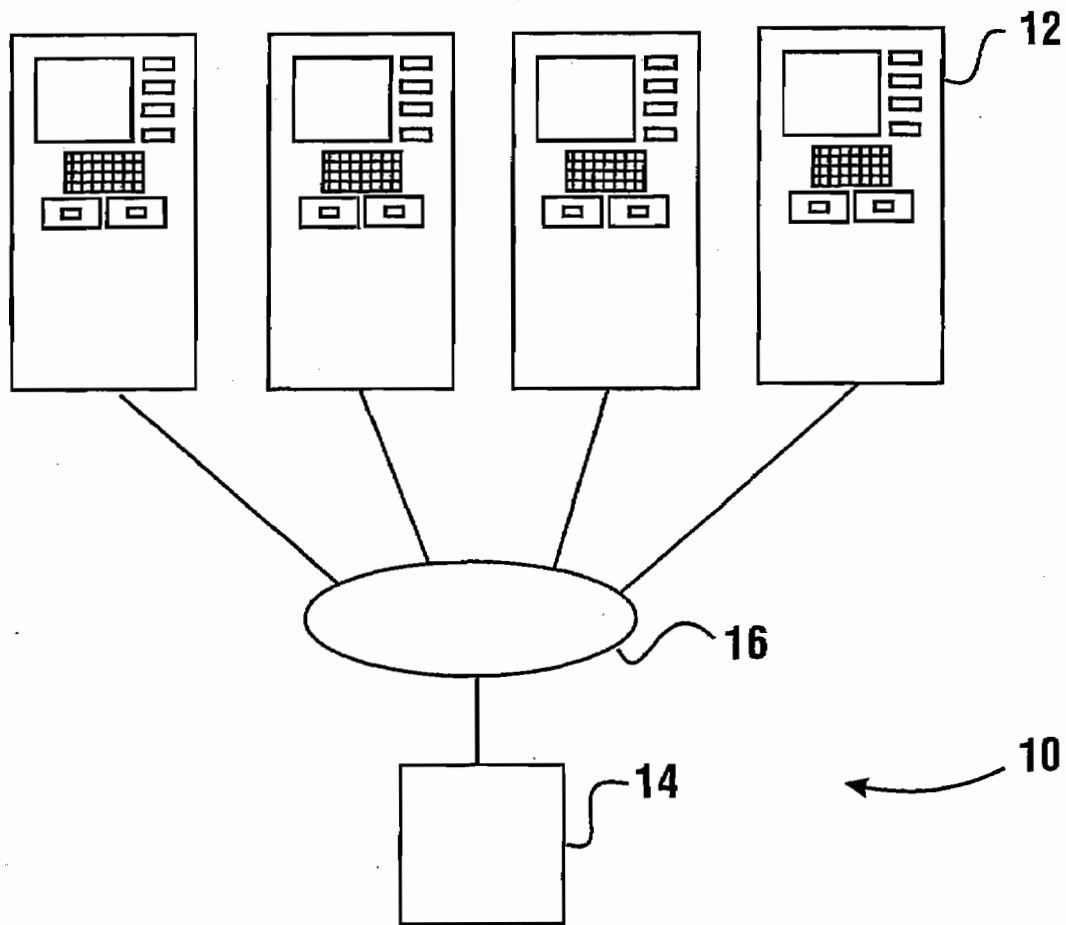
U.S. PATENT DOCUMENTS

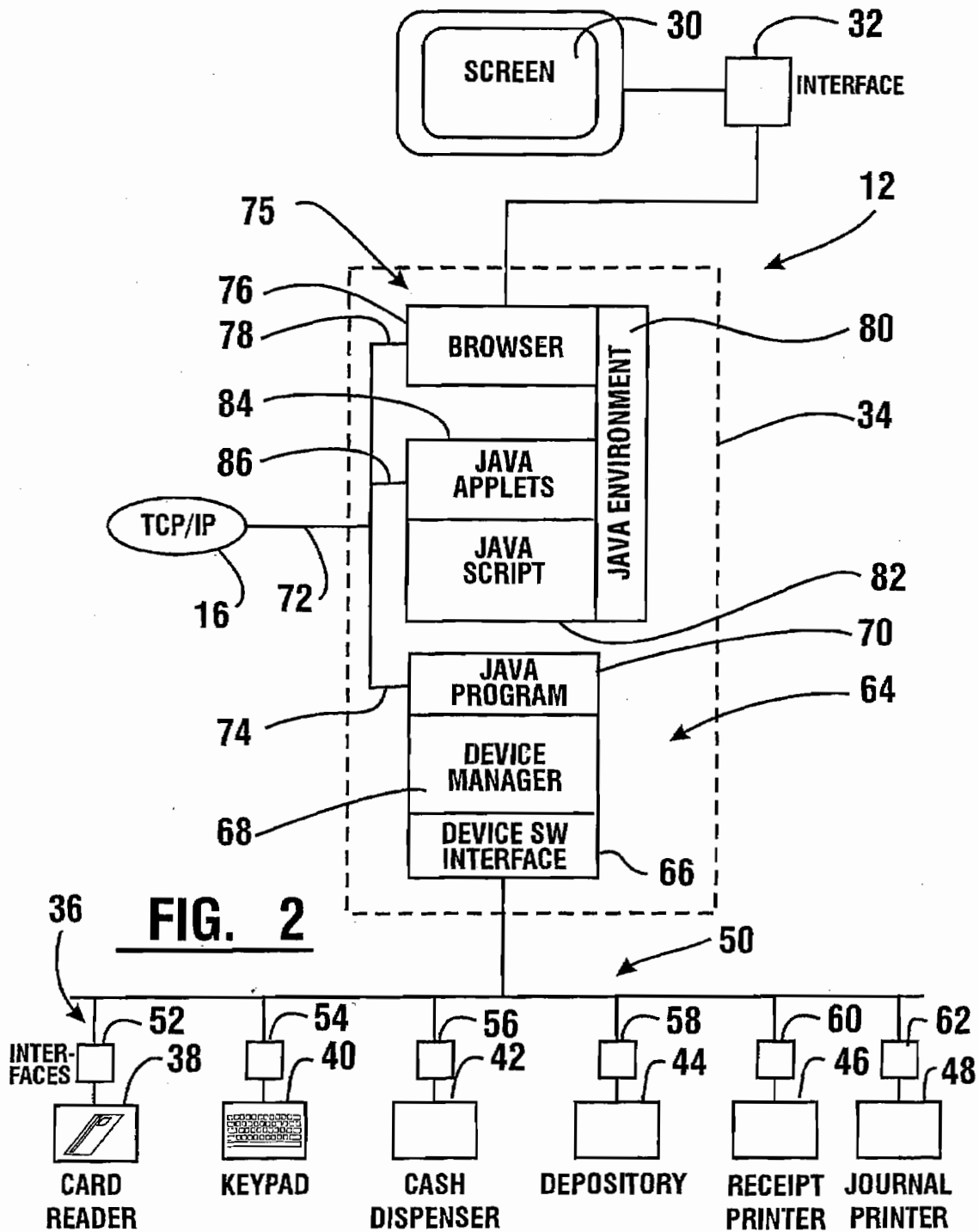
7,000,829	B1 *	2/2006	Harris et al.	235/379
2001/0026619	A1 *	10/2001	Howard et al.	380/279
2001/0049667	A1 *	12/2001	Moribatake et al.	705/69

OTHER PUBLICATIONS

"Effective Encryption Key Management Practices", Jul. 2003,
K3DES LLC, p. 1-23.*

* cited by examiner

FIG. 1



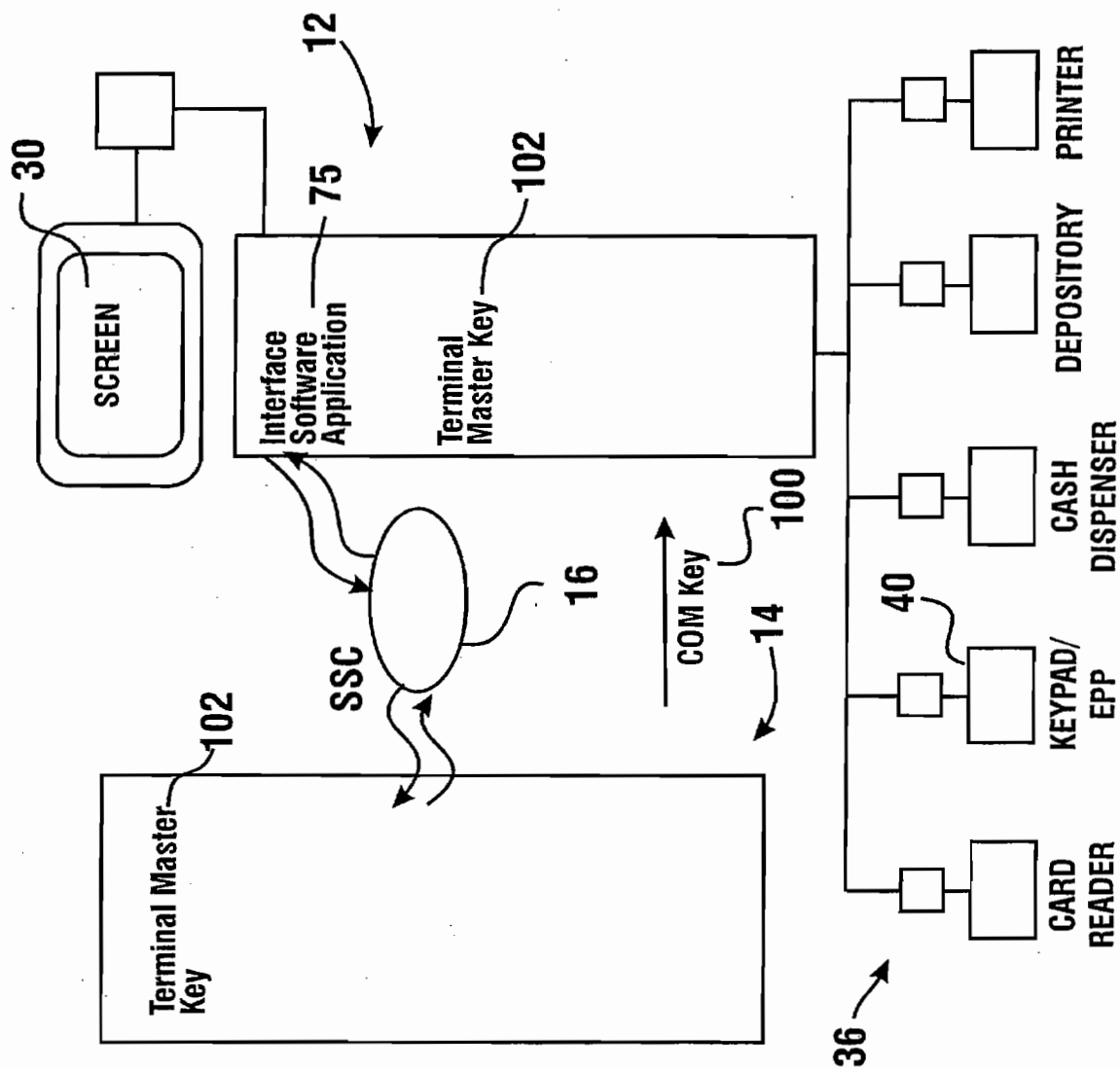


FIG. 3

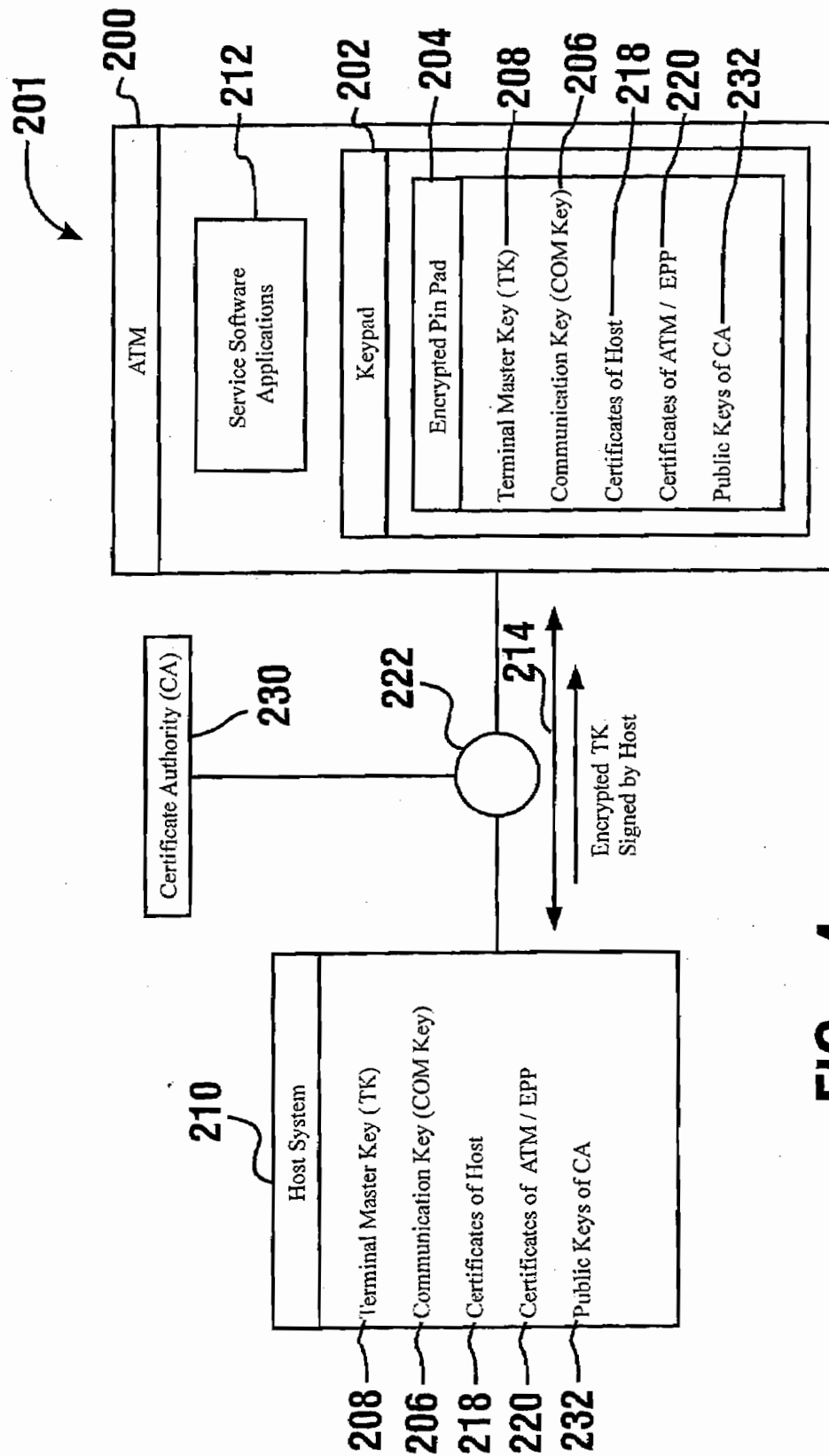


FIG. 4

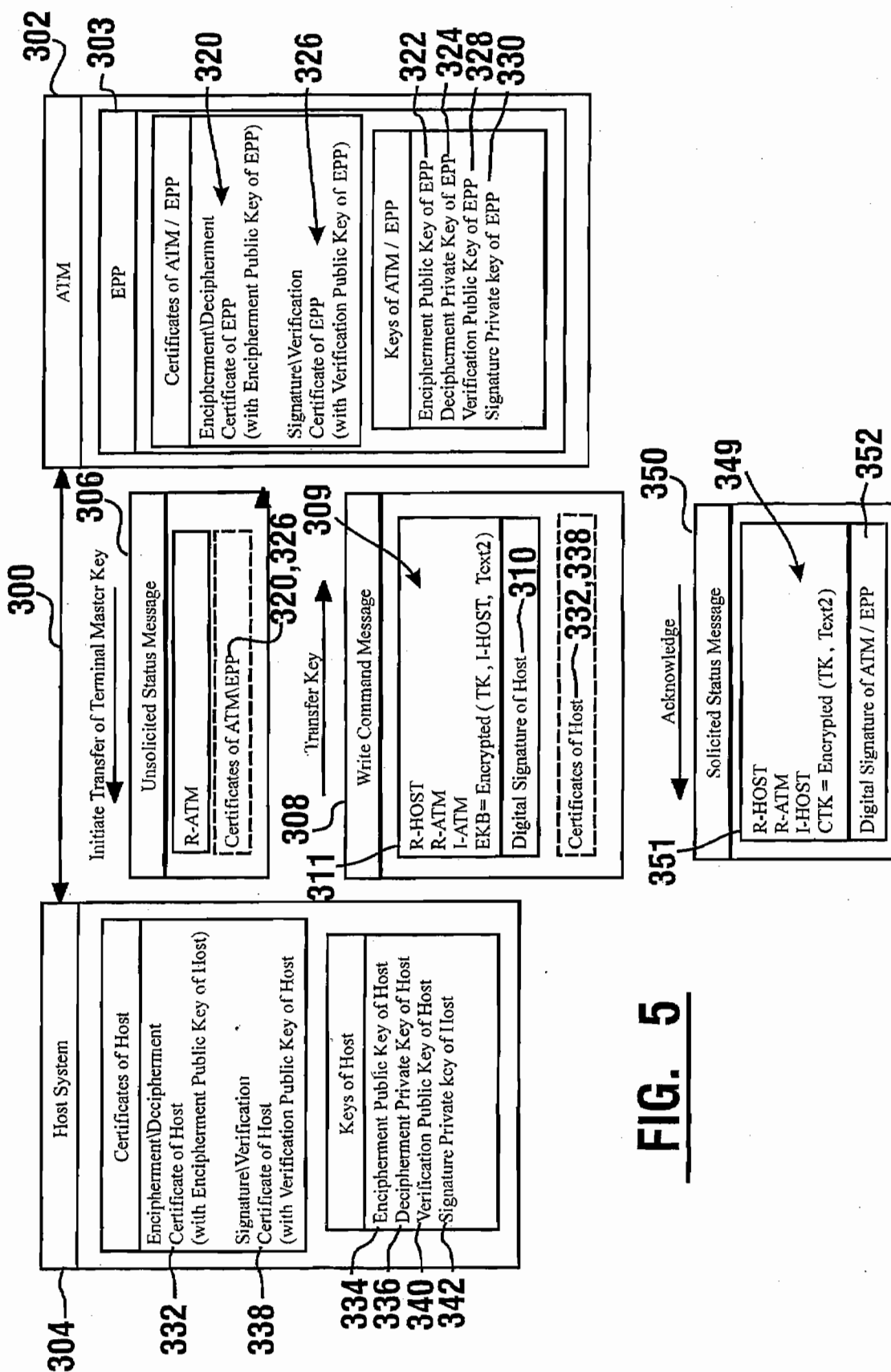


FIG. 5

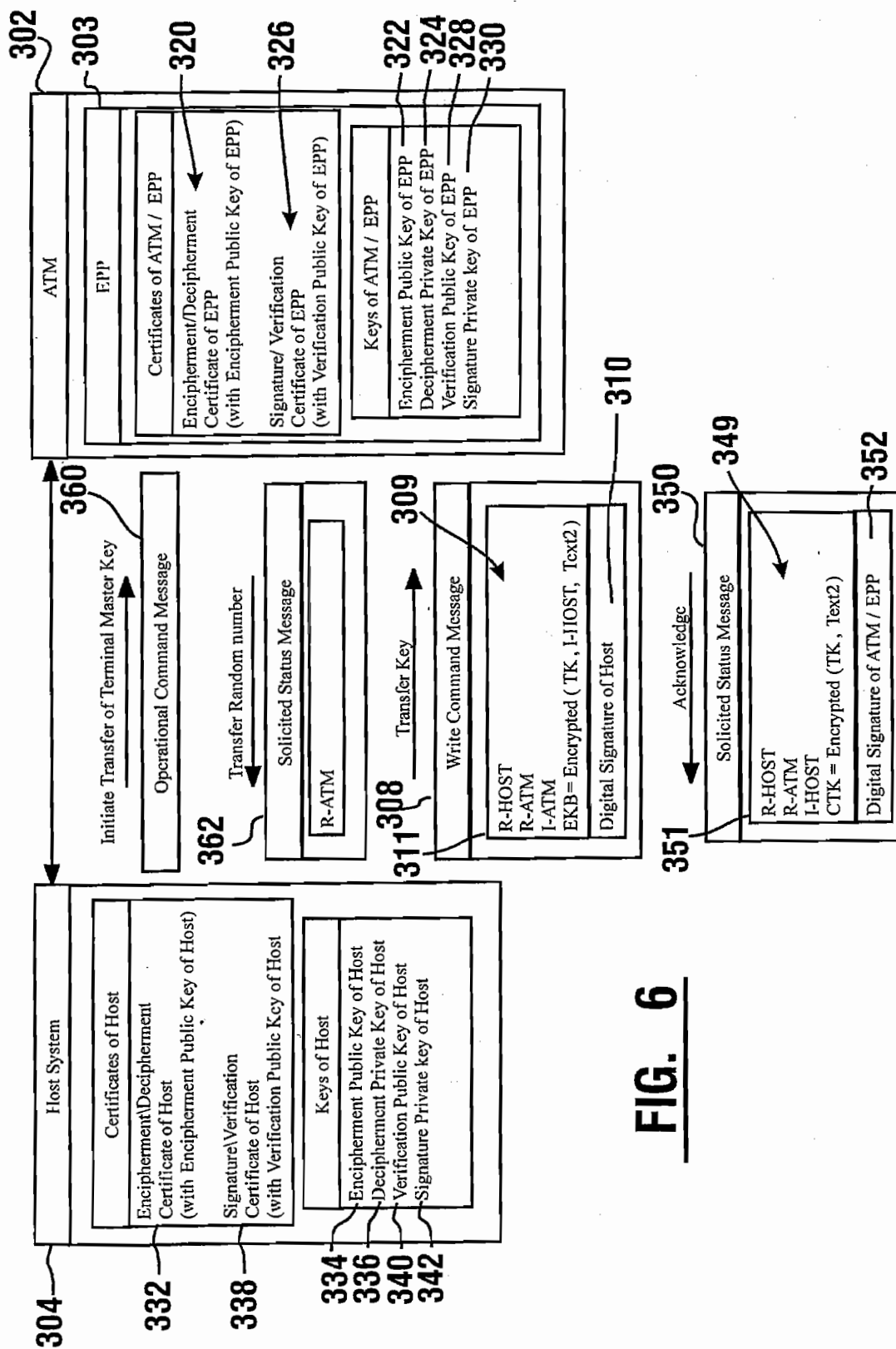


FIG. 6

306

Unsolicited Status Message

DESCRIPTION	CODE	NUMBER OF CHARACTERS
Protocol Dependent Header		VAR
Solicited/Unsolicited ID	'1'	1
Message Identifier	'2'	1
Field Separator (FS)	:1C	1
Logical Unit Number (LUNO)	---	3 or 9
Field Separator (FS)	:1C	1
Field Separator (FS)	:1C	1
Status Source	---	1
Status	---	VAR
Field Separator (FS)	:1C	1
/ Series/MDS Status	---	VAR
Field Separator (FS)	:1C	1
Maintenance Mode Log	---	VAR
Field Separator	:1C	1 [1]
Buffers to Follow ID	[9]	1 [1]
Buffer ID	---	3 [1]
Buffer Data	---	VAR [1]
Group Separator (GS)	:1D	1 [1]
Buffer ID	---	3 [1]
Buffer Data	---	VAR [1]
Protocol Dependent Trailer	VAR	VAR

305

307

FIG. 7

308

Write Command VII Message

DESCRIPTION	CODE	NUMBER OF CHARACTERS
Protocol Dependent Header		VAR
Write Command Identifier	'3'	1
Response Flag	[X]	1
Field Separator (FS)	:1C	1
Logical Unit Number (LUNO)	[X]	3
Field Separator (FS)	:1C	1
Message Sequence Number	[X]	3
Field Separator (FS)	:1C	1
Write Identifier (Encryption Key Change)	'3'	1
Key Change	[---]	1
Field Separator (FS)	:1C	1
New Key Data	[---]	VAR
Protocol Dependent Trailer		VAR

370

372

FIG. 8

Solicited Status Message

DESCRIPTION	CODE	NUMBER OF CHARACTERS
Protocol Dependent Header	VAR	Var
Solicited/Unsolicited ID	'2'	1
Message Identifier	'2'	1
Field Separator (FS)	:1C	1
Logical Unit Number (LUNO)	---	3 or 9
Field Separator (FS)	:1C	1
Message Sequence Number	---	8
Field Separator (FS)	:1C	1
Status Descriptor	---	1
Field Separator (FS)	:1C	1
Device Identifier (DID)	---	1
Status	---	VAR
Group Separator (GS)	:1D	111
Device Identifier (DID)	---	111
Status	---	VAR [1]
Field Separator (FS)	:1C	112
Amount of coins dispensed	---	312
Field Separator (FS)	:1C	113
MDS Status	---	VAR [3]
Field Separator	:1C	114
Buffers to Follow ID	[9]	114
Buffer ID	---	314
Buffer Data	---	VAR [4]
Group Separator (GS)	:1D	114
Buffer ID	---	314
Buffer Data	---	VAR [4]
Field Separator (FS)	:1C	115
Rollover 1 Count	---	315
Rollover 2 Count	---	315
Rollover 3 Count	---	315
Rollover 4 Count	---	315
Protocol Dependent Trailer	VAR	VAR

382

FIG. 9

Operational Command Message

DESCRIPTION	CODE	NUMBER OF CHARACTERS
Protocol Dependent Header		VAR
Operational Command Identifier	'1'	1
Response Flag	[X]	1
Field Separator (FS)	:1C	1
Logical Unit Number (LUNO)	[X]	3
Field Separator (FS)	:1C	1
Message Sequence Number	[X]	3
Field Separator (FS)	:1C	1
Command Code	---	1
Data Field	[---]	VAR
Field Separator (FS)	:1C[1]	1
Status Flag	[---][1]	1
Device Name	[---][1][2]	4
Protocol Dependent Trailer		VAR

363

FIG. 10

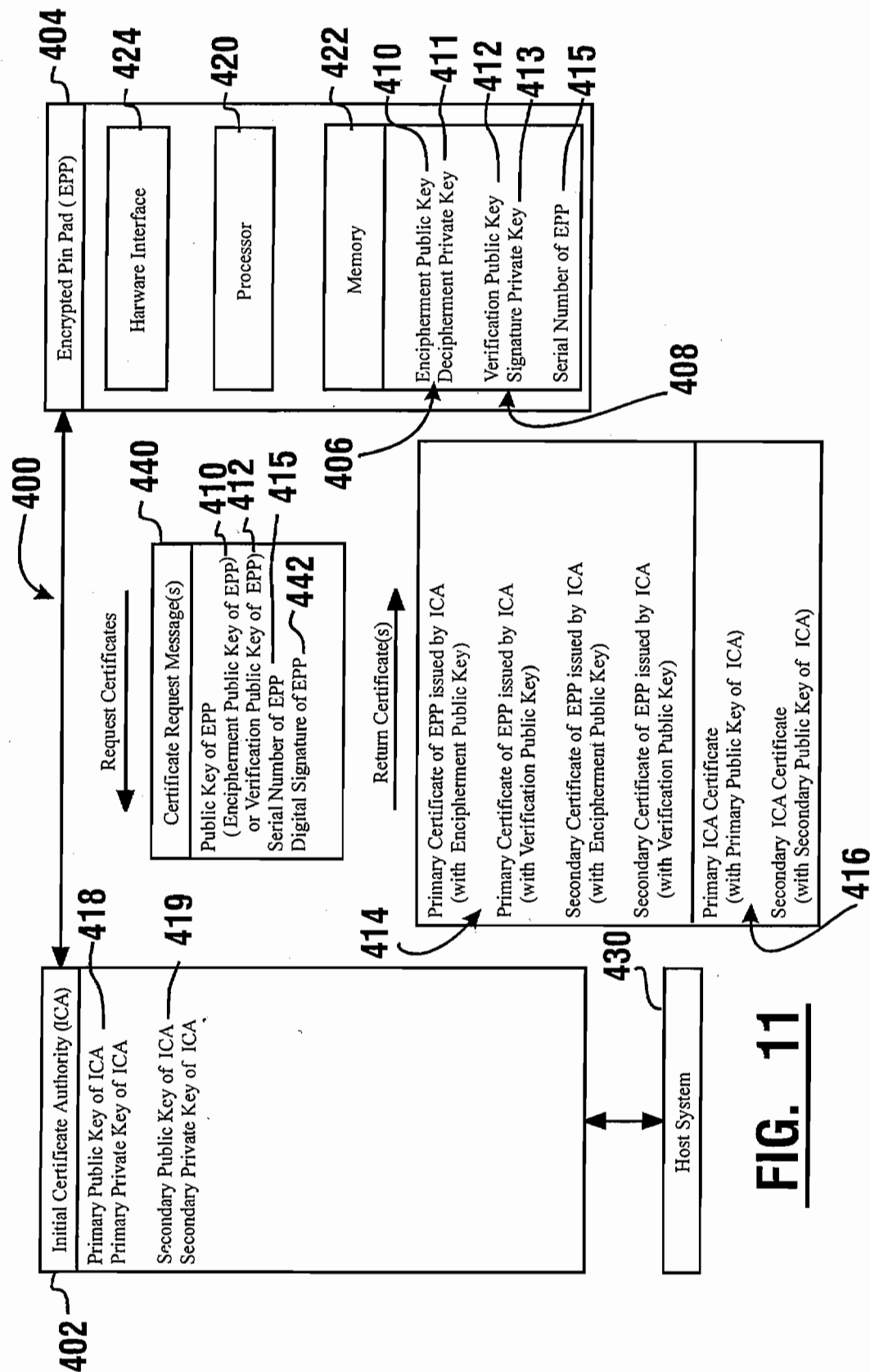


FIG. 11

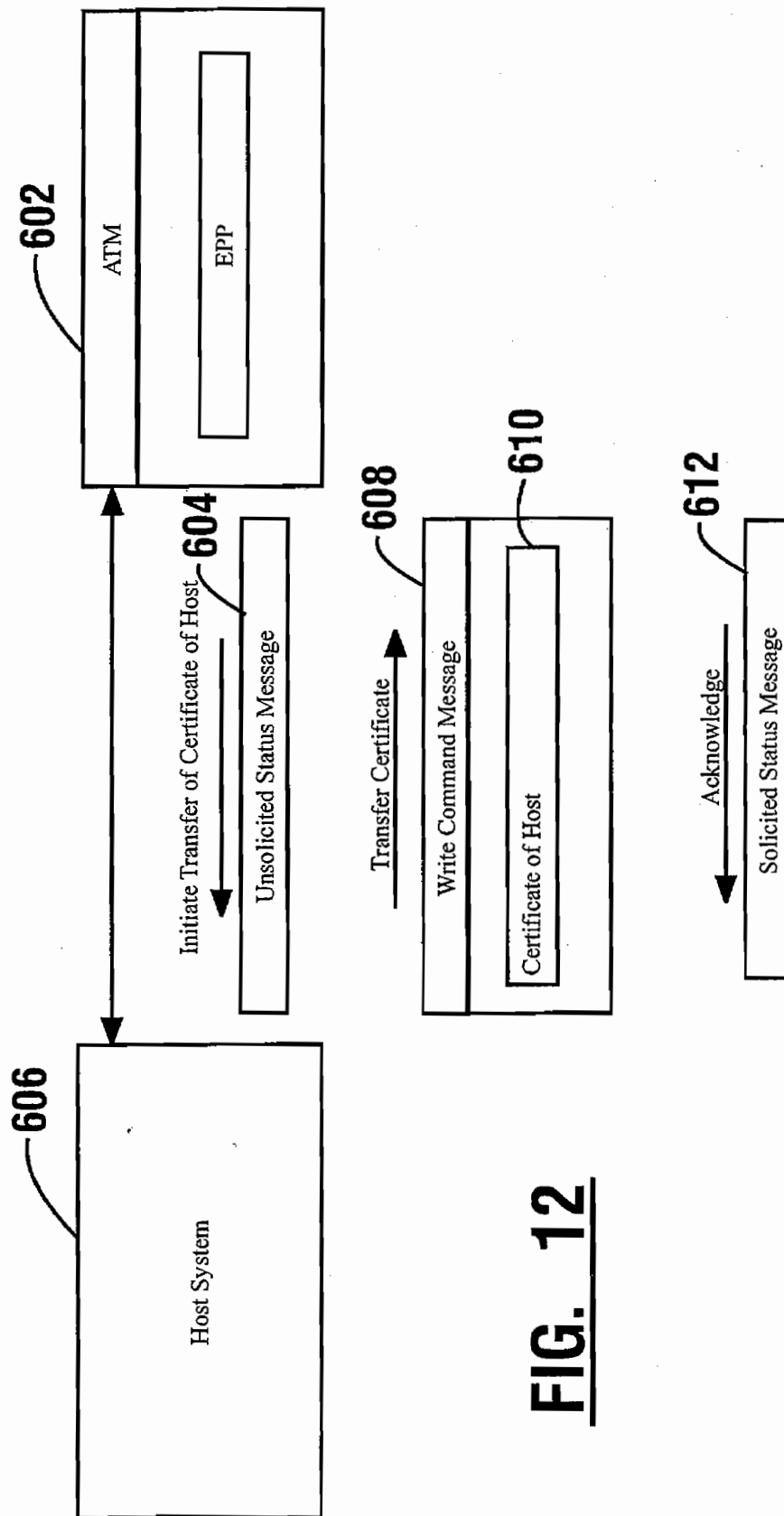


FIG. 12

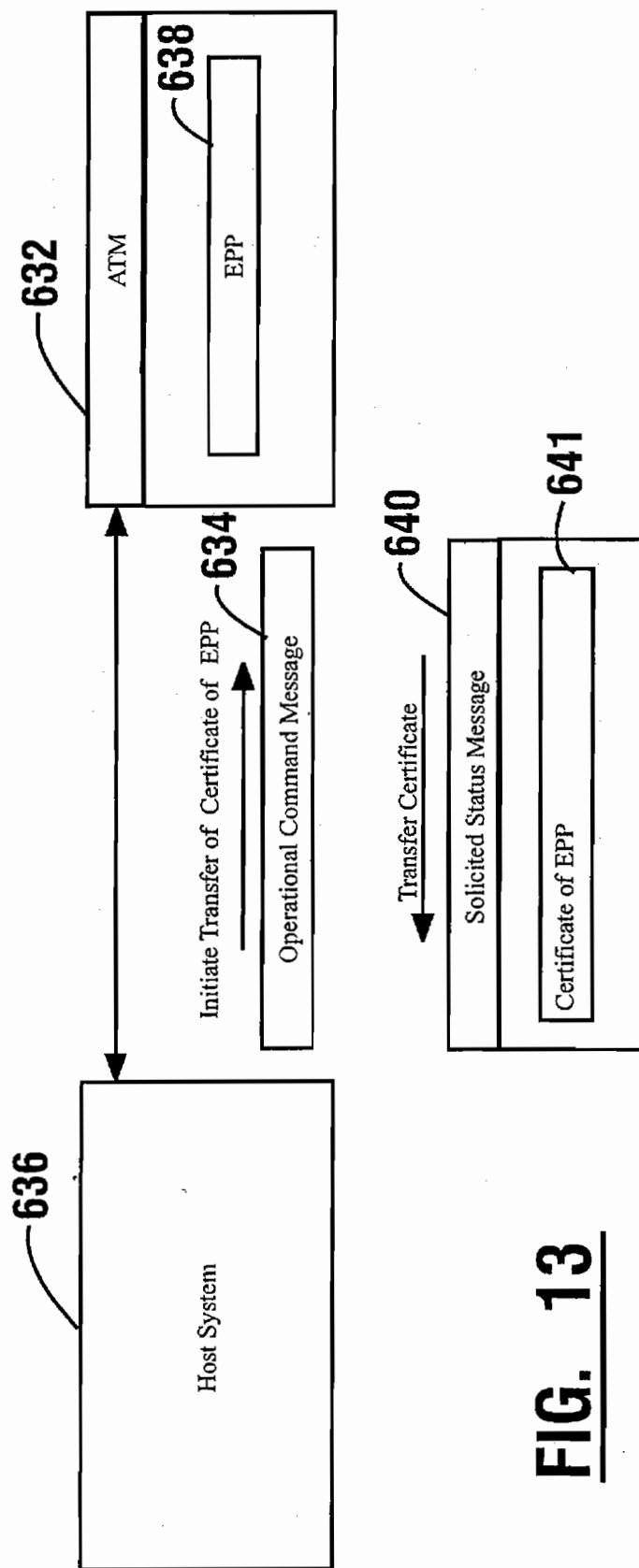


FIG. 13

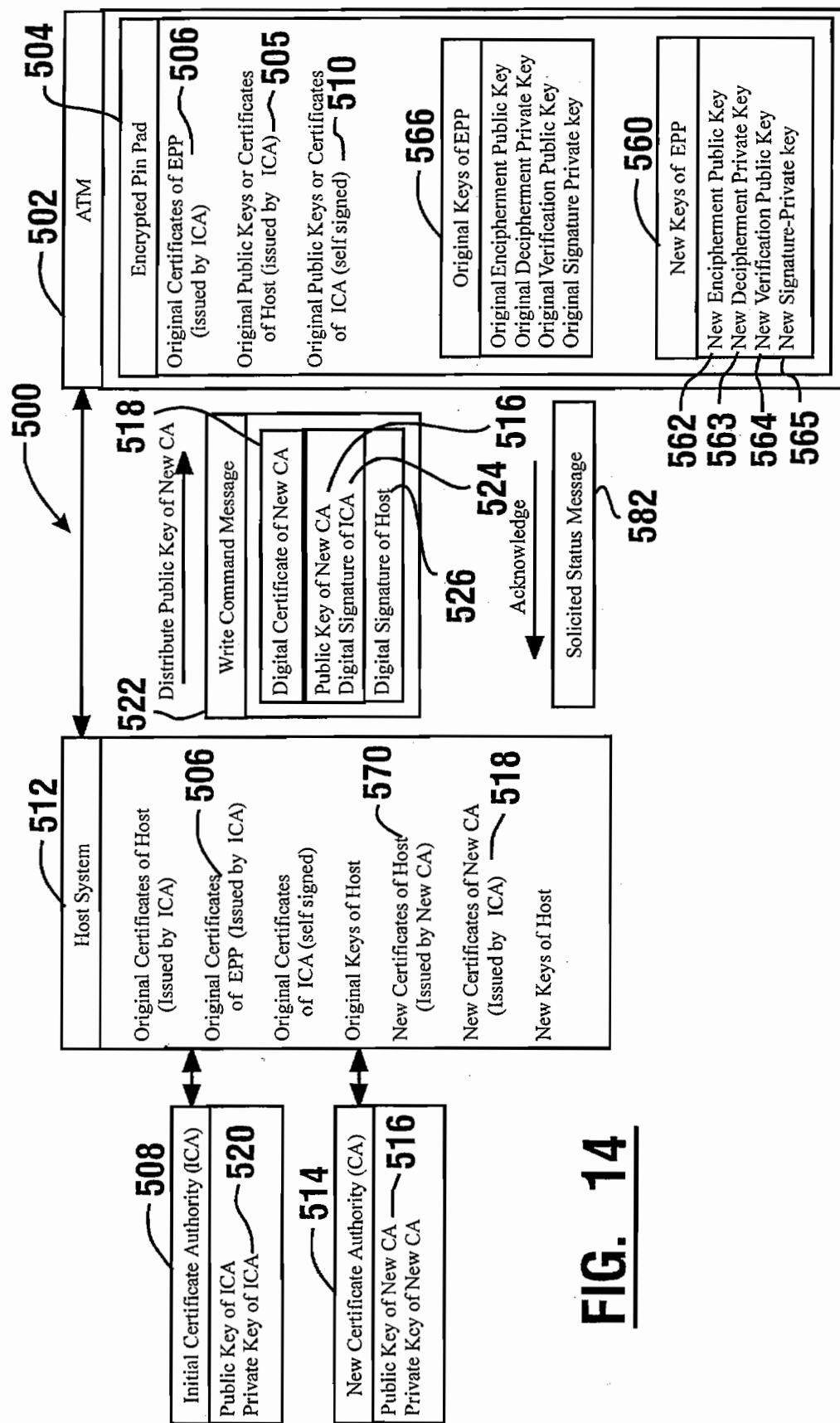


FIG. 14

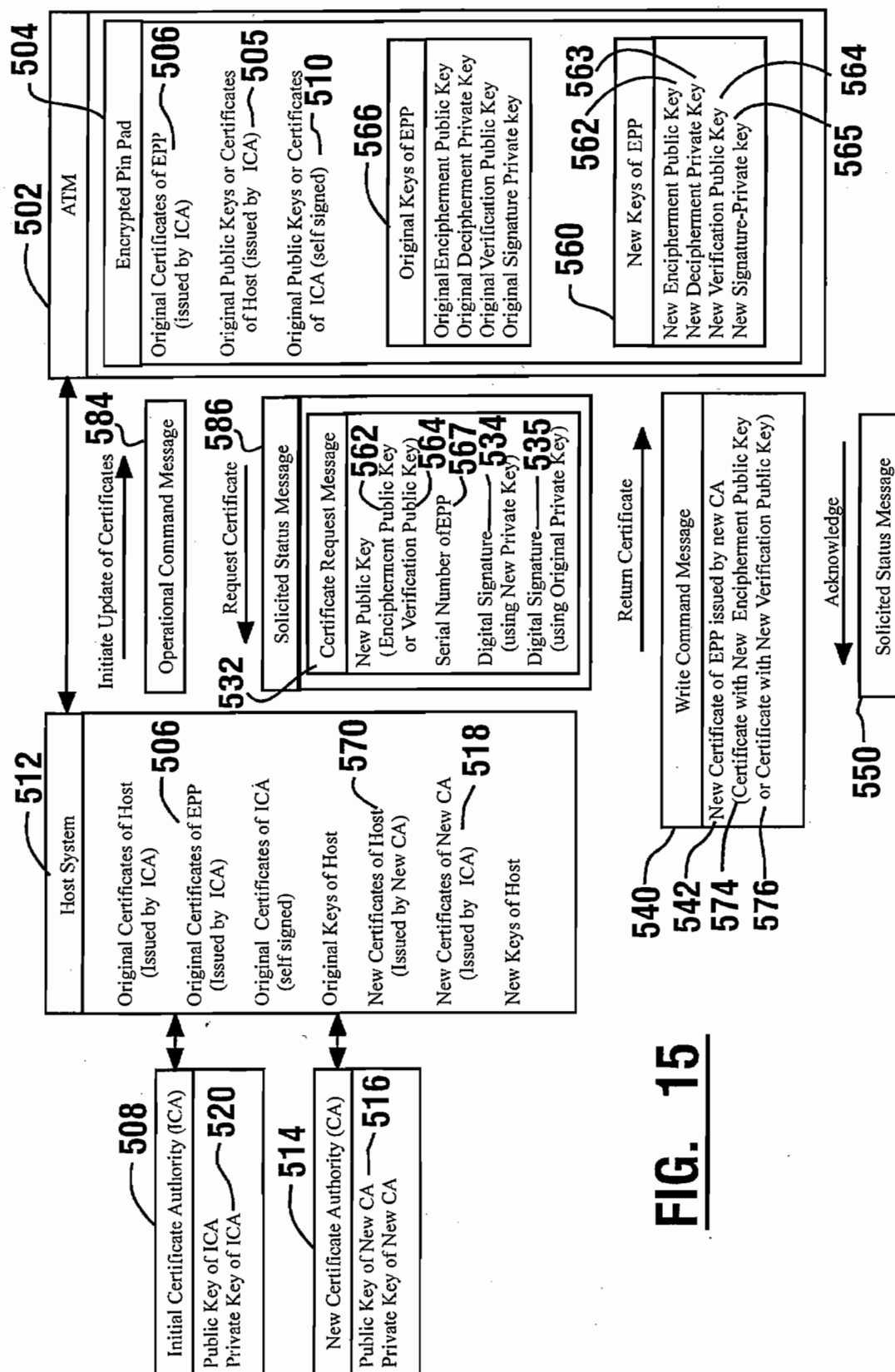


FIG. 15

1

SYSTEM AND METHOD OF SECURELY INSTALLING A TERMINAL MASTER KEY ON AN AUTOMATED BANKING MACHINE

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims benefit of U.S. Provisional Application Ser. No. 60/285,724 filed on Apr. 23, 2001.

TECHNICAL FIELD

This invention relates to automated banking machines. Specifically this invention relates to an automated banking machine system and method that is capable of configuring an automated banking machine with encryption keys.

BACKGROUND ART

Automated banking machines are well known. A common type of automated banking machine used by consumers is an automated teller machine ("ATM"). ATMs enable customers to carry out banking transactions. Common banking transactions that may be carried out with ATMs include the dispensing of cash, the making of deposits, the transfer of funds between accounts, the payment of bills and account balance inquiries. The types of banking transactions a customer can carry out are determined by capabilities of the particular banking machine and the programming of the institution operating the machine. Other types of automated banking machines may allow customers to charge against accounts or to transfer funds. Other types of automated banking machines may print or dispense items of value such as coupons, tickets, wagering slips, vouchers, checks, food stamps, money orders, scrip or traveler's checks. For purposes of this disclosure an ATM, an automated banking machine, or an automated transaction machine shall encompass any device which carries out transactions including transfers of value.

Many ATMs are configured to require consumers to enter a Personal Identification Number (PIN) with a keypad of the ATM prior to being granted permission to perform transaction functions with the ATM. The PIN is communicated to a host system by the ATM for purposes of authenticating the identity of the consumer. To prevent the PIN from being stolen by an unauthorized party, ATMs are operative to encrypt the PIN prior to sending the PIN to a host system. For many years Single-DES encryption has been used by ATMs to encrypt PINs using an 8 byte Communication (COM) secret key. Unfortunately, as the cost of computer processing power decreases over time, the risk of the encryption being cracked by unauthorized individuals or entities is increasing. Consequently, there exists a need for new and existing ATMs to include support for a more secure encryption protocol.

PIN information may be encrypted using a COM key known to both the ATM and the host system. The COM key may be securely sent to the ATM from the host system by encrypting the COM key with a terminal master key known to both the ATM and the host system. To maintain the secrecy of a terminal master key, when an ATM is being initially configured for operation, the initial terminal master key is often required to be manually installed by a two-person team at the ATM. Each person of the team has knowledge of only a portion of the information necessary to generate the initial terminal master key. To install the terminal master key successfully, each person must input

2

into the ATM his or her known portion of the terminal master key. Once installed, the inputted portions undergo a mathematical procedure that results in a sixteen (16) character key unknown to either person.

In general, financial institutions or other entities which operate ATMs, are responsible for inserting a unique initial terminal master key in their ATMs. Such entities are also responsible for periodically updating the COM key used for PIN encryption. Although the use of two-person teams to install the initial terminal master key increases the security of the system, in general such a protocol increases the maintenance costs per ATM and is generally cumbersome to manage. As a result, existing keys on ATMs are often not updated on a regular basis, which increases their vulnerability to being cracked. Consequently, there exists a need for a new system and method of installing the initial terminal master key which is less costly and less cumbersome to perform. There is a further need for a new system and method of installing a terminal master key on an ATM which is equally or more secure than a two-person team system.

DISCLOSURE OF INVENTION

It is an object of an exemplary form of the present invention to provide an automated banking machine at which a user may conduct transactions.

It is a further object of an exemplary form of the present invention to provide an automated banking machine which is more secure.

It is a further object of an exemplary form of the present invention to provide an automated banking machine which supports more secure encryption protocols.

It is a further object of an exemplary form of the present invention to provide a system and method for securely installing a terminal master key on an automated banking machine.

It is a further object of an exemplary form of the present invention to provide a system and method for securely and remotely installing a terminal master key on an automated banking machine.

It is a further object of an exemplary form of the present invention to provide a system and method for securely and remotely installing a terminal master key on an automated banking machine with the use of only a single operator at the ATM.

Further objects of exemplary forms of the present invention will be made apparent in the following Best Modes for Carrying Out Invention and the appended claims.

The foregoing objects are accomplished in an exemplary embodiment by an automated banking machine that includes output devices such as a display screen, and input devices such as a touch screen and/or a keyboard. The ATM further includes devices such as a cash dispenser mechanism for sheets of currency, a printer mechanism, a card reader/writer, a depository mechanism and other transaction function devices that are used by the machine in carrying out banking transactions. In the exemplary embodiment the ATM includes at least one computer. The computer is in operative connection with the output devices and the input devices, as well as with the cash dispenser mechanism, card reader and other physical transaction function devices in the banking machine. The computer is further operative to communicate with a host system located remotely from the ATM.

In the exemplary embodiment, the computer includes software programs that are executable therein. The software programs of the ATM are operative to cause the computer to

3

output user interface screens through a display device of the ATM. The user interface screens include consumer screens which provide a consumer with information for performing consumer operations such as banking functions with the ATM. The user interface screens further include service screens which provide a person servicing the ATM with information for performing service and maintenance operations with the ATM. In addition the ATM includes software programs operative in the computer for controlling and communicating with hardware devices of the ATM including the transaction function devices.

In an exemplary embodiment, the ATM includes encryption software and/or hardware which is operative to encrypt PIN information with DES keys securely received from the host system. In one exemplary embodiment, the ATM includes a keypad or encrypting pin pad (EPP) input device which is operative to encrypt a consumer entered PIN within a secure module directly at the keypad. The EPPs of exemplary embodiments are further operative to perform either Single-DES or Triple-DES encryption operations for message authentication, local PIN verification and key transport.

In the exemplary embodiment, the EPP and/or other hardware/software in the computer may be operative to establish a secure communication session between the ATM and a host system environment for transferring terminal master keys to the ATM from the host system. In the exemplary embodiment, individual authentication may be required from both the ATM and the host system to establish the secure communication session. Authentication may be achieved in one exemplary embodiment using digital certificates and digital signatures. Both the ATM and the host system each have individual certificates which may be exchanged between the ATM and host system in a point-to-point communication. The exchanged certificates enable the ATM and the host system to authenticate each other and establish a secure session through a Public Key Infrastructure (PKI). The secure session enables DES keys to be remotely installed and updated on an ATM by a host system. In the exemplary embodiment, the host system may be operative to coordinate the remote key management of DES keys for a plurality of ATMs connected to the host system.

To facilitate authentication and key management, both the ATM and host system may each include a pair of certificates. A first one of the certificates may be used for enciphering and deciphering information sent between the host system and the ATM. A second one of the certificates may be used for generating digital signatures and verifying digital signatures on information passed between the host system and ATM. In the exemplary embodiment, the ATM or a device of the ATM such as an encrypting keypad or encrypting pin pad (EPP) may be manufactured to include an initial set of the certificates which are issued by an initial certificate authority (CA). The exemplary ATM or a EPP device of the ATM may also be manufactured to include the public keys of the initial CA. In addition a host system connected to the ATM may include certificates issued by the initial CA and the public keys of the initial CA.

In the exemplary embodiment, an operator at the ATM may be enabled to cause the ATM to initiate the exchange of certificates between the ATM and the host system. To prevent a possible man-in-the-middle attack on the ATM and host, exemplary embodiments may include the ATM outputting through a display device of the ATM, a one-way hash of the public key of the host system found on each certificate of the host system. The operator may then independently verify that each displayed one-way hash corresponds to a

4

hash of the expected public key found in an authentic certificate of the host system.

In an exemplary embodiment, a financial institution may be operative to replace the initial CA with a new CA and may be operative to remotely cause the ATM and the host system to receive new sets of certificates issued by the new CA.

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 is a schematic view of an exemplary embodiment of an ATM system.

FIG. 2 is a schematic view of a further exemplary embodiment of an ATM system.

FIG. 3 is a schematic view of an exemplary embodiment of a system for remotely transferring terminal keys from a host system to an ATM.

FIG. 4 is a further schematic view of an exemplary embodiment of a system for remotely transferring terminal keys from a host system to an ATM.

FIG. 5 schematically represents an exemplary embodiment of a system and method for transferring a terminal master key from a host system to an ATM.

FIG. 6 schematically represents an exemplary embodiment of a system and method for transferring a terminal master key from a host system to an ATM.

FIG. 7 schematically represents an exemplary embodiment of a format for an unsolicited status message.

FIG. 8 schematically represents an exemplary embodiment of a format for a write command message.

FIG. 9 schematically represents an exemplary embodiment of a format for a solicited status message.

FIG. 10 schematically represents an exemplary embodiment of a format for an operational command message.

FIG. 11 schematically represents an exemplary embodiment of a system and method for installing certificates in an exemplary embodiment of an EPP.

FIG. 12 schematically represents an exemplary embodiment of a system for transferring certificates of a host system to an EPP.

FIG. 13 schematically represents an exemplary embodiment of a system for transferring certificates of an EPP to a host system.

FIG. 14 schematically represents an exemplary embodiment of a system for distributing new certificate for a new certificate authority to an EPP.

FIG. 15 schematically represents an exemplary embodiment of a system for updating original certificates of an EPP with new certificates of the EPP signed by a new certificate authority.

BEST MODES FOR CARRYING OUT INVENTION

Referring now to the drawings and particularly to FIG. 1, there is shown therein a network configuration schematically indicated 10, which includes the automated banking machine apparatus and system of an exemplary embodiment. Network 10 includes a plurality of automated banking machines 12 which in the exemplary embodiment of the invention are ATMs. ATMs 12 are connected to a computer system of a host system schematically indicated 14. Host system 14 includes a computer system that may be operated by the bank or other institution which has primary responsibility for the ATMs 12. Host banking system 14 may be connected to the ATMs 12 through a network 16. Network 16 may include a local or proprietary network or a public network such as the Internet which provides communication

5

between the computer system 14 and the banking machines 12. In one exemplary embodiment the messages are transmitted through the network 16 in the Transmission Control Protocol/Internet Protocol ("TCP/IP") format. In addition, the messages sent through network 16 may be sent in an encrypted or unencrypted form depending on the nature of the system and the security needs of the home bank.

FIG. 2 shows a schematic view of the ATM 12 used in connection with an exemplary embodiment of the invention. ATM 12 may include a touch screen 30. Touch screen 30 includes a display screen which serves as an output device for communication with a user of the machine. Touch screen 30, because it is a touch screen, also serves as an input device for receiving input instructions from a user. Touch screen 30 may be connected through an interface 32 to a computer 34 which is preferably housed within the machine. Alternative exemplary embodiments of the invention may include other output devices such as audio speakers and/or other display screens which may or may not be integrated with input devices. Alternative exemplary embodiments may also include other input devices such as function keys and keyboards which may or may not be integrated with output devices.

Computer 34 may also be in connection with a plurality of transaction function devices 36 which are included in ATM 12. Devices 36 may include for example, a card reader/writer mechanism 38 and a keypad 40. Devices 36 may further include a cash dispenser mechanism 42 which is operative to dispense sheets, which in some embodiments of the invention are currency or bank notes. Exemplary devices 36 may also include a depository 44 for accepting deposits into a secure location in the machine. A receipt printer 46 for providing transaction receipts to customers may also be included among devices 36. A journal printer 48 may also be included among the devices for keeping a hard copy record of transaction information. In other exemplary embodiments other or additional transaction function devices which carry out other transaction functions may be used. Other exemplary embodiments may include fewer transaction function devices. It should be further understood that while the described exemplary embodiment of the invention is an automated banking machine, the principles of the invention may be employed in many types of transaction machines that do not necessarily carry out banking transactions.

Each of the devices may be operatively connected to an internal control bus 50 within the banking machine 12. The control bus 50 outputs the internal messages to the particular devices. Each device may have an appropriate hardware interface which enables the particular device to operate to carry out its respective function in response to the messages transmitted to it on control bus 50. Card reader/writer 38 may have a hardware interface schematically shown as 52. Hardware interfaces 54, 56, 58, 60 and 62 may be respectively operative to connect key pad 40, cash dispenser mechanism 42, depository mechanism 44, receipt printer mechanism 46 and journal printer mechanism 48 to the control bus 50.

Computer 34 may have several software programs that are executable therein. In an exemplary embodiment these software programs may include a device interfacing software portion generally indicated 64. Device interfacing software portion 64 may include a software device interface 66 that communicates electronic messages with the control bus 50. The device interface software portion 64 may also include a device manager 68. The device manager may be operative to manage the various devices 36 and to control their various

6

states so as to be assured that they properly operate in sequence. In an exemplary embodiment, the device manager may also be operative to coordinate device objects in the software so as to enable operation of the devices by at least one object-oriented program 70. The object oriented program portion 70, for example may include an application written in the JAVA® language by Sun Microsystems or an application designed to operate according to Microsoft's .Net platform. Program 70 may work in conjunction with the device manager to receive object-oriented JAVA® or .NET messages which cause the devices to operate, and to transmit device operation messages indicative of a manner in which devices are operating and/or are receiving input data.

The device interfacing software portion 64 in the described exemplary embodiment may operate on computer 34 and may communicate through a physical TCP/IP connection 72 with the network 16. The physical connection may be analog dial-up, serial port, DSL, ISDN connection or other suitable network connection. In the configuration of the system as shown, device interfacing software portion 64 may communicate at the IP address of computer 34 and at an IP port or socket indicated 74 that is different from the other software applications. In other embodiments of the invention, device interfacing software portion 64 may operate in a different computer than the other software applications of the invention.

In further exemplary embodiments, the device interfacing portion 64 may also be based on an open standard platform such as WOSA/XFS (Windows Open Services Architecture/Extensions for Financial Services) or J/XFS (Java/Extensions for Financial Services). Such platforms include an open XFS manager which provides a uniform API for communication with the devices 36. When using an XFS manager, the device interfacing portion may communicate with the hardware interfaces 52, 54, 56, 58, 60 and 62 through software components such as service provider (SP) interfaces supplied by the vendors of the devices 36.

It should further be understood that although in this described exemplary embodiment the device interfacing portion 64 may be software, in other embodiments of the invention all or portions of the instruction steps executed by software portion 64 may be resident in firmware or in other program media in connection with one or more computers, which are operative to communicate with devices 36. For purposes of the invention all such forms of executable instructions shall be referred to as software.

Other software may also operate in computer 34. This software may include interface applications 75 which are operative to output interface screens through the output device 30 which provide information and instructions to consumers and/or operators for operating the ATM 12. In one exemplary embodiment the interface applications may include software for handling mark up language documents. In the exemplary embodiment the interface applications may include HyperText Markup Language (HTML) document processing software such as a browser, schematically indicated 76. In this described exemplary embodiment of the invention, the HTML document handling software includes a browser provided by Netscape®. However, in other embodiments other HTML document handling and communicating software and browser software, such as Internet Explorer™ from Microsoft, may be used. It should be understood that in some exemplary embodiments browsers which process markup language documents to provide visible and/or audible outputs as well as other outputs, as well as browsers which do not provide human perceivable out-

puts, may be used. Browser 76 may communicate in computer 34 at an IP port indicated by 78.

In an exemplary embodiment, the browser 76 may be in operative connection with JAVA® environment software 80 which enables computer 34 to run JAVA® language programs. However, other exemplary embodiments may use different types of software programs including Microsoft .NET applications and proprietary and platform specific terminal control software.

The JAVA® environment software 80 enables computer 34 to execute instructions in JAVA® script, schematically indicated 82. The instructions that are executed by the computer in JAVA® script may be embedded JAVA® script commands that are included in the HTML documents or other markup language documents which are received through the browser 76. The browser 76 in connection with the JAVA® environment software 80 which executes instructions in the embedded JAVA® script 82, serve as an HTML document handling software portion for transmitting and receiving HTML documents and TCP/IP messages through the IP port indicated by 78.

Computer 34 may also have executable software therein having a device application portion 84. The device application portion 84 may contain executable instructions related to operation of the devices 36. In one exemplary embodiment of the invention, the device application portion may include a plurality of JAVA® applets. In the described embodiment the applets include programs operable to control and keep track of the status of the devices with which they are associated. Certain applets may be operable to configure the browser to communicate messages. Certain applets may manage security and authenticate entities that use the ATM. It should be understood that this approach is exemplary and in other embodiments other approaches may be used. For example, other embodiments may use .Net components and objects rather than or in addition to JAVA® applets.

In the described form of the invention, JAVA® applets may be associated with functions such as enabling the card reader mechanism, notifying the browser when a user's card data has been entered, operating the receipt printer mechanism, operating the journal printer mechanism, enabling the customer keyboard and receiving data input through the keyboard, operating the sheet dispenser mechanism, operating the depository, navigating to document addresses, timing device functions, verifying digital signatures, handling encryption of messages, controlling the mix of bills dispensed from multiple cash dispenser mechanisms, calculating foreign exchange, and ending a transaction and instructing the browser to return to communication with a server. Of course, in other embodiments, other applets or components may be used to control devices and use data to carry out various desired functions with the machine. The device application portion 84 may communicate in the computer 34 at an IP port indicated 86.

In the described embodiment of the invention, the device application portion 84 of the software may not communicate its messages directly to the device interfacing software portion 64. However, it should be understood that some embodiments of the invention may provide for the device application portion 84 to directly communicate device operation messages to the device program 70. This may be done either internally using TCP/IP, by delivery of messages in a conventional manner through a queue established in the operating system of the computer that is associated with the software that interfaces with the devices, or by direct call to this software.

FIG. 3 shows an exemplary embodiment of the ATM 12 in communication through the network 16 with a financial transaction processing system which in this example includes the host system 14. Host system 14 includes at least one server computer and may be operative to keep track of debiting or crediting customers' accounts when they conduct transactions at the automated banking machines. In addition host system 14 may be operative to track transactions for purposes of accomplishing settlements with other institutions who are participants in the system and whose customers conduct transactions at the ATMs 12. In an exemplary embodiment the host system 14 may be operative to communicate messages to the ATM 12 through network 16 using a secure socket connection ("SSC") so as to minimize the risk of interception of the messages. Of course other techniques, including encryption message techniques, may be used to minimize the risk of interception of the messages. It should be understood that the make of ATM 12 is exemplary and other types of ATMs may be used with exemplary embodiments.

In the exemplary embodiment messages sent to the ATM 12 may include the instructions and information for the ATM to verify that the messages it receives are genuine. This may include digital signatures which when transferred using public key or private key encryption techniques verify the messages as genuine. The machine checks to be sure the signature in the messages received from the host system or another system corresponds to the digital signature for that address stored in memory, and enables operation with the transaction devices, such as the cash dispenser 42, or the keypad 40 only when such correspondence is present. Of course various approaches to verifying and encrypting messages may be used in various embodiments. As used herein signatures or signed records encompass any indicia which is included in or is derivable from a record, such as a message or document which is indicative that it is authorized.

When performing transactions for a consumer, an exemplary embodiment of the interface application 75 may be operative to prompt a consumer to input his/her Personal Identification Number (PIN) using an input device such as keypad 40 of the ATM 12. The exemplary embodiment of the ATM 12 includes encryption software and/or hardware which is operative to encrypt PIN information with a Communication (COM) secret key and a corresponding encryption algorithm and protocol. Examples of encryption algorithms and protocols which an exemplary embodiment may use to encrypt PIN information include symmetric cryptography algorithms such as Single-DES encryption and double-length key Triple-DES encryption. In other alternative exemplary embodiments, other symmetric or asymmetric cryptographic algorithms and protocols may be used.

When the exemplary embodiment of the ATM 12 is initially configured to perform transactions with the host system 14, a communication (COM) key 100 may be securely sent from the host system 14 to the ATM 12 through the network 16. To prevent the COM key 100 from being stolen by an unauthorized third party, the COM key may be encrypted with a terminal master key 102 known to both the host system and the ATM. In the exemplary embodiment the terminal master key 102 may be a DES secret key, however in alternative exemplary embodiments the terminal master key may correspond to the one or more encryption keys for use with other symmetric or asymmetric encryption algorithms and protocols.

As discussed previously, a current practice for installing the terminal master key on an ATM includes having a two-person team manually input two different key compo-

nents which are used by the ATM to construct the terminal master key. The described exemplary embodiment may be operative to install the terminal master key on an ATM remotely from the host system without the use of a two-person team.

FIG. 4 shows a schematic view of an exemplary embodiment of an ATM 200. ATM 200 includes a keypad 202. The keypad 202 includes an EPP 204 which may be operative to perform the encryption of inputs through the keypad and the encryption/decryption of information being sent in messages between the ATM and a host system. For example in exemplary embodiments, the EPP may be operative to encrypt an input such as an inputted PIN using the COM key 206. The EPP 204 of the exemplary embodiment may further be operative to perform steps necessary to securely acquire the COM key 206 from the host system 210 using a terminal master key 208. In addition, the exemplary embodiment of the EPP 204 may be operative to perform steps necessary to securely acquire the terminal master key 208 from the host system 210.

To securely transfer the terminal master key 208 from the host system 210 to the ATM 200, the exemplary ATM 200 is operatively programmed to cause the EPP 204 to establish a secure communication session, socket, and/or channel 214 between the ATM 200 and the host system 210 that may be used to securely transfer the terminal master key 208 through a network 222. The exemplary ATM 200 may include a service software application 212. The service software application 212 may be operative responsive to commands inputted into the ATM 200 by a single operator to cause the ATM 200 to establish the secure communication session 214 for securely transferring the terminal master key 208 to the EPP 204.

In the exemplary embodiment, individual authentication may be required from both the ATM 200 and the host system 210. Authentication may be achieved in one exemplary embodiment using certificates and a Public Key Infrastructure generally indicated 201. In this described exemplary embodiment, both the ATM 200 and the host system 210 each are associated with their own digital certificates 218, 220. The secure communication session 214 may be initiated by exchanging the certificates 218 of the host and the certificates of the ATM 220 between the ATM 200 and the host system 210. In one exemplary embodiment, the certificates 218, 220 may be authenticated by both the ATM 200 and the host system 210 using a public key 232 of a trusted certificate authority (CA) 230.

Once the certificates 218, 220 have been exchanged and authenticated, the exemplary embodiment of the ATM and host system may pass encrypted and digitally signed information between them. Such information for example may include signed messages, encrypted secret keys, updated CA public keys, and updated certificates. As shown in FIG. 4 the exemplary ATM 200 and host system 210 may be further operative to use the exemplary PKI system 201 to securely transfer the terminal master key 208 to the ATM 200. This may be achieved in one exemplary embodiment by having the host system 210 encrypt the terminal master key 208 using a public key associated with at least one certificate 220 of the ATM. The host system 210 may then send a digitally signed message to the ATM 200 which includes the encrypted terminal master key 216. In the exemplary embodiment, the ATM 200 may be operative to decrypt the encrypted terminal master key 216 using a corresponding private key of the ATM 200. In addition the ATM 200 may be operative to authenticate the digital signature of the host system using a public key from one the certificates 218 of

the host system. Using this described exemplary process, an exemplary host system may be operative in accordance with its programming to coordinate the remote key management of terminal master keys for a plurality of ATMs 200 connected to the host system.

When certificates are initially exchanged between the ATM 200 and the host system 210, there exists a possibility that an unauthorized entity may perform a man-in-the-middle hacking attack to uncover information being passed between the ATM and host system. During such an attack the unauthorized entity may simultaneously impersonate both the ATM and the host system by exchanging imposter messages for the original messages being transferred between the ATM and host system. To reduce the risk of this type of attack, the service software application 212 may be operatively programmed to cause the ATM 200 to display through a display device, a one-way hash or digest of the public key of the host system found on the certificate 218 of the host system. The exemplary one-way hash of the public key of the host system may be calculated by the exemplary ATM 200 using a one-way hash function such as MD5 or SHA-1. The operator may then independently verify that the displayed one-way hash is identical to a one-way hash of the public key of the host system known by the operator to correspond to an authentic certificate of the host system.

In the exemplary embodiment, to facilitate both authentication and key management, the host system 210 may include two certificates 218 and the ATM 200 may include two certificates 220. A first one of the certificates may be associated with a first set of private/public key pairs which are used for encrypting and deciphering the terminal master key and other information sent between the host system and the ATM. A second one of the certificates may be associated with a second set of private/public key pairs used for signing and verifying digital signatures on information passed between the host system and the ATM. In the exemplary embodiment, the EPP 204 of the ATM 200 may be manufactured to include the initial set of certificates 220 of the ATM stored therein. Such certificates 220 of the ATM which may be stored in a memory of the EPP 204 are issued by the CA 230. The certificates 218 of the host system may also be issued by the CA 230. However, it is to be understood that in alternative exemplary embodiments the certificates 218, 220 may be issued by different certificate authorities.

In the exemplary embodiment, the EPP 204 may include the necessary processing capabilities and programming to validate/authenticate the certificates 218 received from the host system 210 by validating/authenticating the digital signature of the CA 230 found on the certificates 218 of host system 210. In the exemplary embodiment, the EPP 204 may be manufactured to include the public keys 232 of the CA 230. The public keys 232 of the CA may be used by the EPP 204 to validate/authenticate the digital signatures of the CA found on the certificates of the host 218. Likewise, the host system 210 may be operative to validate/authenticate the certificates 220 of the ATM using the public keys 232 of the CA.

In exemplary embodiments, the terminal master key may be transferred between the host and an ATM using a remote key transport process based on protocols such as the key transport mechanism 5 of ISO/IEC 11770-3 and the three-pass authentication mechanism of ISO/IEC 9798-3. These protocols may be used to transfer two shared secret keys in three passes and provide mutual entity authentication and key confirmation.

In exemplary embodiments, the EPP may be constructed so as prevent the secret encryption keys stored therein from

11

being retrieved from the EPP by an unauthorized user, entity, software program, hardware device, or other probing or sniffing device. Exemplary embodiments of the EPP may further be operative to destroy and/or delete the secret keys from the memory of the EPP in response to the EPP being tampered with. For example, an exemplary embodiment of the EPP may destroy all or portions of the EPP memory in response to the packaging or outer enclosure of the EPP being opened or altered.

FIG. 5 shows a schematic view of system and method by which a single operator at an ATM 302 may initiate the process of transferring a terminal master key to the ATM 302 from the host system 304. This method comprises a plurality of messages 306, 308, 350 being sent between the ATM and the host system which establish a secure communication session, socket, and/or channel 300 between the host system 304 and the ATM 302 which is used to transfer the terminal master key across a network. In this exemplary embodiment, a modified key transport mechanism may be employed which is based on the ISO/IEC 11770-3 and ISO/IEC 9798-3 protocols and which provides unilateral key transport from the host system to the ATM. In this described exemplary embodiment, ATM 302 may enable a single operator to input a command through an input device of the ATM which causes the ATM to initiate the remote transfer of a terminal master key to the ATM. In exemplary embodiments the key transfer may also be initiated by the host system.

In the exemplary embodiment, the ATM 302 and/or an EPP 303 of the ATM may generate a random number (R-ATM) in response to receiving the input from the operator. The random number (R-ATM) may be sent by the ATM 302 to the host system 304 as part of at least one message 306 which may include for example an unsolicited status message or other types of messages capable of being sent by an ATM to a host system. In this described exemplary embodiment, certificates of the ATM and the host system may have been previously exchanged with each other as will be discussed below. However, in an alternative exemplary embodiment, if certificates of the ATM have not yet been exchanged with the host system, the exemplary ATM 302 may be operative to include a certificate 320 associated with encipherment/decipherment of the ATM/EPP and a certificate 326 associated with signature/verification 326 of the ATM/EPP with the message 306 at this time.

FIG. 7 shows an example format for the unsolicited status message in a Diebold 91X ATM message protocol environment that may be used for message 306. Here the random number (R-ATM) may be stored in the buffer data field 307 of the unsolicited status message. The status field 305 may include data which indicates that the unsolicited status message corresponds to a request to initiate the process of transferring the terminal master key.

In response to receiving the message 306 from the ATM, the exemplary host system may be operative to generate and return to the ATM at least one message 308 including for example a write command message or other types of message that an ATM is capable of receiving from a host system. The message 308 from the host system includes a terminal master key (TK) encrypted within an Encipherment Key Block (EKB). In the exemplary embodiment, the host system may generate the Encipherment Key Block (EKB) by encrypting the terminal master key (TK) and identifying data associated with the host system such as a host distinguishing identifier (I-Host) using a public encipherment transformation associated with the ATM and/or EPP of the ATM. The host distinguishing identifier (I-Host) may correspond to a unique number, name or other indicia which is

12

associated with the host 304. In the exemplary embodiment the public encipherment transformation associated with the ATM/EPP may include encrypting the information (TK and I-Host) using an encipherment public key 322 associated with the encryption/decryption certificate 320 of the ATM/EPP.

In addition to sending the encrypted terminal master key (TK) and host distinguishing identifier (I-Host), the host system may be operative to send as part of the message 308 a random number generated by the host (R-Host), the random number received from the ATM (R-ATM), and identifying data associated with the ATM such as an ATM distinguishing identifier (I-ATM). The ATM distinguishing identifier corresponds to a unique number, name or other indicia associated with the ATM 302 or the EPP 303 of the ATM.

In the exemplary embodiment, the message data 309 corresponding to the random number generated by the host system (R-Host), the random number received from the ATM (R-ATM), the ATM distinguishing identifier (I-ATM), and the Encipherment Key Block (EKB) may be digitally signed by the host system 304 to form a digital signature 310 using a private signature transformation associated with the host system. In the exemplary embodiment the private signature transformation associated with the host system may include signing the message using a signature private key 342 of the host system.

The resulting signed message 311 may use the PKCS #7: Cryptographic Message Syntax Standard format. The message syntax may use Abstract Syntax Notation One (ASN.1) with Basic Encoding Rules (BER) and Distinguished Encoding Rules (DER). In exemplary embodiments where the message of the host system is being transmitted over a 7-bit ASCII network such as in a Diebold 91X ATM message protocol environment, the binary output of the Abstract Syntax Notation One (ASN.1) may be converted to 7-bit ASCII for transmission within the write command message. In an exemplary embodiment an encoding algorithm such as Base64 encoding may be used by the host system which is operative to convert octets (bytes) into printable ASCII characters. In other exemplary embodiments other encoding algorithms may be used which are operative to produce 7-bit ASCII from binary.

FIG. 8 shows an exemplary format for a write command message in a Diebold 91X ATM message protocol environment that may be used to transfer the information described as being included in the message 308 being sent to the ATM. Here the write command message 308 corresponds to a 91X Write Command VII message. The key change field 370 of the Write Command VII message may include data which indicates that the write command message corresponds to the remote transfer of a terminal master key. The encrypted and signed message data 311 which includes the terminal master key may be included in the new key data field 372 of the Write Command VII message. Referring back to FIG. 5, in an alternative exemplary embodiment, if certificates of the host system have not yet been exchanged with the ATM, the exemplary host system 304 may be operative to attach certificates 332, 338 of the host system to the message 308.

Once the message 308 is received by the ATM, the ATM and/or the EPP of the ATM may be operative to validate the digital signature 310 of the host system using the public verification transformation associated with the host system. In the exemplary embodiment the public verification transformation associated with the host may include validating the digital signature using a verification public key 340 associated with the signature/verification certificate 338 of

13

the host. A positive validation of the digital signature may indicate that the message 308 from the ATM has not been tampered with prior to being received by the ATM 302. Also, a positive validation of the digital signature may indicate that the information in the message 308 originates from the host system and not a third party hacker.

After validating the digital signature 310, the ATM and/or the EPP of the ATM may be operative to verify that the ATM distinguishing identifier data (I-ATM) in the message 308 corresponds to the identity of the ATM 302 and that the random number (R-ATM) in the message 308 corresponds to the original random number (R-ATM) sent to the host system in the message 306. In addition to these validations, the exemplary ATM 302 and/or an EPP 303 of the ATM may be operative to decrypt the Enciphered Key Block (EKB) using the private decipherment transformation associated with the ATM/EPP. In the exemplary embodiment the private decipherment transformation associated with the ATM/EPP includes decrypting the information (TK and I-Host) using a decipherment private key 324 stored in the memory of the EPP.

Decrypting the Enciphered Key Block (EKB) produces the terminal master key (TK) and the host distinguishing identifier (I-Host). If the decrypted host distinguishing identifier (I-Host) corresponds to the correct host system, the ATM 302 and/or the EPP of the ATM may be operative to accept the terminal master key (TK). In the exemplary embodiment, if the ATM and/or EPP of the ATM has been previously set to use a single-length key such as Single-DES encryption and the new terminal master key (TK) correspond to a double length key, the ATM and/or the EPP of the ATM may be operative to automatically switch to an algorithm which use double-length keys such as double-length key Triple-DES encryption. In addition if the ATM and/or EPP of the ATM has been previously set to use double-length keys and the new terminal master key (TK) correspond to a single length key, the ATM and/or EPP of the ATM may be operative to automatically switch to an algorithm which use single length keys such as Single-DES encryption.

As shown in FIG. 5, the exemplary embodiment of the ATM 302 may be operative to confirm the acceptance of the terminal master key (TK) by sending to the host system 304 at least one message 350 including for example a solicited status message or other types of messages capable of being sent by an ATM to a host system. In this described exemplary embodiment, the message data 349 transferred within the message 350 may include the random numbers (R-ATM, R-Host) and the host distinguishing identifier (I-Host). The message data 349 may be further signed by the ATM and/or the EPP of the ATM using a private signature transformation associated with the ATM/EPP. In the exemplary embodiment the private signature transformation associated with the ATM/EPP may include signing the message using a signature private key 330 stored in the memory of the EPP.

The resulting signed message data 351 may use the PKCS #7: Cryptographic Message Syntax Standard format. As discussed previously, this message syntax may use the Abstract Syntax Notation One (ASN.1) with Basic Encoding Rules (BER) and Distinguished Encoding Rules (DER) which is converted from octet (byte) strings to 7-bit ASCII using Base64 encoding. FIG. 9 shows an exemplary format for a solicited status message in a Diebold 91X ATM message protocol environment which may be used to transfer information corresponding to the described message 350. Here the solicited status message may include the signed message data 351 within a buffer data field 382.

14

In alternative exemplary embodiments, the message 350 may further include a cryptographic check value (CTK) for the terminal master key (TK). The cryptographic check value (CTK) may be generated with the ATM and/or the EPP of the ATM by encrypting the received Terminal Master Key (TK) with a verification number or a random number (text2) using a public encipherment transformation associated with the host system. In the exemplary embodiment the public encipherment transformation includes encrypting the information (TK, text2) using an encipherment public key 334 associated with the encryption/decryption certificate 332 of the host system. In this described alternative embodiment, the random number (text2) may originally have been generated by the host system 304 and sent to the ATM 302 in the Enciphered Key Block (EKB) of the message 308 from the host system.

After receiving the message 350 from the ATM, the host system 304 may be operative to verify the digital signature 352 using the public verification transformation associated with the ATM/EPP. In the exemplary embodiment the public verification transformation associated with the ATM/EPP may include verifying the digital signature 352 using a verification public key 328 associated with the signature/verification certificate 326 of the ATM/EPP. Once the digital signature 352 is verified, the host system 304 may be operative to verify that the distinguishing identifier (I-Host) and the random numbers (R-ATM and R-Host) agree with the corresponding values sent by the host system in the message 308. In the event that any one of the verifications performed by the ATM/EPP and host system fail, the exemplary ATM/EPP and host system may be operative to destroy the terminal master key (TK). Also in the exemplary embodiment, each time this exemplary protocol is executed, a new terminal master key (TK) may be generated.

In alternative embodiments, where the message 350 from the ATM includes a cryptographic check value (CTK), the exemplary embodiment of the host system 304 may be operative to decrypt the cryptographic check value (CTK) using a private decipherment transformation associated with the host system. In the exemplary embodiment the private decipherment transformation may include decrypting the cryptographic check value (CTK) using the decipherment private key 336 of the host system. The resulting decrypted terminal master key (TK) and verification number (text2) may then be verified with the original values sent in the message 308 to further verify the integrity of the secure session 300.

In addition to enabling a single operator at an ATM to initiate the remote transfer of a terminal master key to an ATM, an exemplary embodiment of the present system may further include a transfer of the terminal master key which is initiated by the host system. FIG. 6 shows a schematic view of an exemplary embodiment where the host system 304 may be operative to initiate the transfer of the terminal master key by sending to the ATM 302 at least one message 360 including for example an operational command message or other types of messages an ATM is capable of receiving from a host system. FIG. 10 shows an example of the operational command message for a Diebold 91X ATM message protocol environment that may be used to transfer information corresponding to the described message 360. Here, the operational command message may include a command code field 363 which includes data representative of a command to initiate the remote transfer of terminal key.

Referring back to FIG. 6, the ATM 632 may respond to receiving the message 360, by sending to the host system one or messages 362 including for example a solicited status

15

message or other messages which an ATM is capable of sending to a host system. The messages 362 may contain the previously described random number (R-ATM). In a Diebold 91X ATM message protocol environment, for example, the data corresponding to the random number (R-ATM) may be included in a buffer data field of the solicited status message. After the host system 304 has received the message 362 with the random number (R-ATM), the messages 308, 350 may be transferred between the host system and ATM as previously described.

In this described exemplary embodiment the encipherment and decipherment transformations may be performed using public and private key pair sets and an asymmetric cryptography algorithm such as the RSA cryptography algorithm. In addition, the signature and verification transformations may be performed using a second set of public and private key pair sets and the RSA cryptography algorithm and a one-way hash function such as MD5 or SHA-1. The RSA modulus for this exemplary embodiment may be 2048 bits. In alternative exemplary embodiments, other encryption and signature protocols and algorithms may be used including DSA, and AES (Rijndael). Also in this described exemplary embodiment, cryptographic calculations of the ATM may be performed by a processor in the EPP 303 of the ATM 302. However, in other exemplary embodiments of the ATM, all or portions of the cryptographic calculations may be performed by other hardware devices, and computer processors of the ATM.

As discussed previously, many ATMs require a two-person team to install a terminal master key. The exemplary embodiment includes upgrading such ATMs to support receiving a terminal master key from a host system. In one exemplary embodiment, this upgrade may be performed by accessing the interior portion of an ATM and removing an existing EPP or other device designed to receive and/or hold a terminal master key constructed from two values manually inputted into the ATM by a two-person team. Once the existing EPP has been removed, an alternate EPP may be installed in its place. The alternate EPP may be operative to receive the terminal master key from the host system according to the previously described protocols. In this described embodiment the alternate EPP is operative to perform encryption, decryption, signature, and verification functions with the public and private keys of the EPP and the public keys associated with the host system and certificate authority stored in the EPP. In one exemplary embodiment, the alternate EPP may further be operative to encrypt inputted PIN values using either single-DES or triple-DES algorithms and protocols.

In an exemplary embodiment, the EPP may be manufactured to include the certificate associated with encipherment/decipherment 320 and the certificate associated with signature/verification 326 stored therein. In this described exemplary embodiment these certificates may be issued by an initial CA and are digitally signed using a primary private key of the initial CA. The certificates 332, 338 of the host system are likewise issued and signed by the initial CA.

In a further exemplary embodiment, the EPP may be manufactured to include a secondary set of the certificates 320 and 326 signed with a secondary private key of the initial CA. The secondary set of certificates is intended to be used as a backup, in the event that the secrecy of the primary private key of the initial CA is compromised. In such cases, the primary set of certificates may be revoked and the secondary set of certificates may be used in their place to sign/verify messages and encipher/decipher messages at the EPP and host system.

16

The revocation of the primary certificates may be initiated by the host system. The host system may send to the ATMs a secondary set of certificates of the host system signed with the secondary private key of the initial CA. When the exemplary EPP receives a secondary set of certificates from the host system, the EPP may be operative to return its secondary certificates to the host system. In alternative exemplary embodiments, the EPP and host system may initially exchange both primary and secondary sets of certificates. When it is necessary to revoke the primary set of certificates issued by the initial CA, the host system may send a message to each ATM which is representative of a command to stop using the primary certificates and to begin using the secondary certificates.

In addition to storing its own primary and secondary sets of certificates, the exemplary EPP may further be operative to store the primary and secondary public keys of the initial CA. These primary and secondary public keys of the initial CA may be included on respective primary and secondary certificates of the initial CA. The primary and secondary certificates of the CA may be self signed.

FIG. 11 shows a schematic view of an exemplary process 400 that may be used in one exemplary embodiment to configure an EPP 404 with certificates generated by the initial CA 402. Here, the exemplary EPP 404 includes a processor 420, a memory 422 in operative connection with the processor, and a hardware interface 424 in operative connection with the processor. The exemplary processor 420 of the EPP 404 may be operative to communicate with external devices and servers such as a host system, a processor of an ATM, or the initial CA through the hardware interface 424. When the EPP is initially manufactured and/or is re-commissioned, the hardware interface 424 may be connected to a system that is capable of sending messages between the EPP and the initial CA 402. The system for initializing the EPP may include communication hardware, software and a network connection that is in communication with the initial CA and is operative to transfer messages between the EPP and the initial CA. In alternative exemplary embodiments, a system for initializing the EPP may include an ATM and host system that is in operative communication with the initial CA. The hardware interface of the EPP may be operative to communicate with the initial CA through the network interface of the ATM after being installed in the ATM.

When the exemplary EPP 404 is initially powered up, the processor 420 may be operatively programmed to generate a set of encipherment/decipherment public/private key pairs 406 and a set of signature/verification public/private key pairs 408. These keys 406, 408 may be stored by the processor in the memory 422. In the exemplary embodiment these keys 406, 408 may be RSA keys. However, it is to be understood that in alternative exemplary embodiments, keys for other encryption and digital signature algorithms and protocols may be generated.

After the sets of keys 406, 408 have been generated, the processor 420 may be operative to generate two certificate request messages 440 each containing one of the two generated public keys 410, 412 from the generated sets of keys 406, 408. These certificate request messages 440 may be signed using the respective private keys 411, 413 which correspond to the public keys 410, 412 in each certificate request message 440. Also, these messages may include a serial number or other unique identifier of the EPP. In an exemplary embodiment, the certificate request messages may be constructed according to the PKCS #10 Certification Request Syntax Standard format. The exemplary embodi-

ment of the EPP may be operative to output the certificate request messages through its hardware interface 424 for purposes of communicating the certificate request messages to the initial CA.

In response to receiving the certificate request messages 440 the initial CA 402 may be operative to verify that the EPP has possession of the private keys 411 413 by verifying the digital signatures 442 of the messages 440 using the corresponding public key 410, 412 received in the messages 440. After verifying the digital signatures of the messages 440, the initial CA may generate and sign corresponding primary and secondary certificates 114 for each of the two public keys 410, 412 of the EPP. In addition, each of the certificates may include the serial number 415 of the EPP.

The EPP 404 may be operative to receive the newly generated primary and secondary certificates 114 through the hardware interface 424. The EPP may also be operative to receive the primary and secondary certificates 416 of the initial CA through the hardware interface. These certificates 416 of the initial CA may include the primary and secondary public keys 418, 419 of the initial CA and may be self-signed with the private keys corresponding to the public keys 418, 419 of the initial CA.

The EPP is operative to use the public keys 418 and 419 from the certificates 416 of the initial CA to validate the certificates 414 of the EPP. Further, the EPP may verify that the public keys in the certificates 414 of the EPP match the original public keys 410, 412 generated by the EPP. Also, the EPP may verify that the serial number in the certificates matches the original serial number 415 of the EPP.

The EPP 404 may store the received certificates 414 of the EPP in the memory 422. Also, the EPP 404 may store the public keys 418, 419 and/or the certificates 416 of the initial CA 402 in the memory 422. The memory 422 may be comprised of a nonvolatile memory that is operative to preserve the keys 406, 408 and certificates 414, 416 in the memory 422, during periods when the power has been removed from the EPP 404. In the described exemplary embodiment, the public keys 410, 412 of the EPP may each be sent to the initial CA 402 in their own respective certificate request messages 440. However, in alternative exemplary embodiments, both public keys 410, 412 of the EPP may be included in a single certificate request message.

In the exemplary embodiment, the host system 430 may also be operative to communicate with the initial CA 402 using the process previously described with respect to the EPP. The host system may generate its own sets of encipherment/decipherment public/private key pairs and signature/verification public/private key pairs. The host system may then enable one or more certificate request messages to be sent to an initial CA which includes the generated public keys of the host. The initial CA may issue corresponding encipherment/decipherment and signature/verification certificates for the host system. These certificates for the host system may be received by the host system along with the certificates of the initial CA for storage at the host system. In addition the initial CA may further issue both primary and secondary sets of the host certificates, where the first set is signed by the primary private key of the initial CA and the second set is signed by the secondary private key of the initial CA.

In the exemplary embodiment, the primary and secondary sets of certificates for the EPP include the same set of public keys of the EPP. However, in alternative exemplary embodiments, the EPP may generate both a primary set and a secondary set of encipherment/decipherment public/private key pairs and signature/verification public/private key pairs.

The corresponding public keys from the primary set of keys may be forwarded to the initial CA to be integrated into the primary set of certificates of the EPP issued by the CA. The corresponding public keys from the secondary set of keys may be forwarded to the initial CA to be integrated into the secondary set of certificates of the EPP issued by the CA. In addition the exemplary primary and secondary host certificates may likewise be associated with separate sets of primary and secondary sets of encipherment/decipherment public/private key pairs and signature/verification public/private key pairs.

As discussed previously the certificates issued by the initial CA are exchanged between the host system 430 and the EPP 404. The public keys 418, 419 of the initial CA may be used by the host system 430 and the EPP 404 to authenticate the exchanged certificates of the EPP and host system. The exemplary embodiment may use a large key size for the keys 418, 419 of the initial CA so as to make the forging of the certificates much more difficult. However to further increase security, the exemplary EPP and/or the host system may be operative to limit the number of initial certificate exchanges in order to prevent possible future exchanges using forged certificates. In addition, in the exemplary embodiment, initial certificate exchanges may be locked out once a remote terminal master key transfer has been completed. However, prior to the terminal master key transport, multiple certificate exchanges may be permitted between the host and the ATM for testing purposes.

In the exemplary embodiment, the initial certificate exchange between the host system and EPP may be initiated by an operator inputting commands into the ATM, which causes the ATM to communicate with a host system and begin the certificate exchange. FIG. 12 schematically shows the certificate exchange process between an ATM 602 and a host system 606 that is initiated by an operator. Here exemplary embodiments of the ATM 602 may generate and send to the host system 606 at least one message 604 in response to receiving a command from an operator to initiate the certificate exchange. In the exemplary embodiment, the message 604 may include for example an unsolicited status message or other types of messages which an ATM is capable of sending to a host system. In a Diebold 91X ATM message protocol environment, for example, the unsolicited status message may include data in a status field which corresponds to "new network certificate required". The unsolicited status message may also include data in a device ID field which corresponds to the EPP.

In response to receiving the message 604, the host system may return to the ATM, a certificate containing the public key of the host system. In exemplary embodiments the host system may also be capable of initiating the sending of the certificate of the host to the ATM without first receiving a message 604 from the ATM.

As shown in FIG. 12, the host certificate 610 may be included in at least one message 608 being sent to the ATM. Such a message 608 may include for example a write command message or other types of messages which an ATM is capable of receiving from a host system. In a Diebold 91X ATM message protocol environment, for example, the write command message may correspond to a Write Command VII message with data in a key change field that includes the certificate 610 of the host system 606. Such data for the certificate may use the PKCS #7: Cryptographic Message Syntax Standard format. This message syntax may use the Abstract Syntax Notation One (ASN.1) with Basic Encoding Rules (BER) and Distinguished Encoding Rules

(DER) which is converted from octet (8-bit) strings to 7-bit ASCII using Base64 encoding.

In response to receiving the certificate 604 of the host system, the EPP may retrieve the public key of the initial CA from the memory of the EPP and use the retrieved public key to validate the signature on the certificate 610 of the host system. Also as discussed previously, the exemplary ATM may be operative to display a one-way hash of the public key of the host through a display device of the ATM. The ATM may require an operator to enter an input through an input device of the ATM which corresponds to a confirmation that the one-way hash number is valid. To verify the displayed one-way hash number, the operator may compare the displayed one-way hash number to another hash number that the operator independently knows corresponds to the public key of the host. If these described verifications are successful, the EPP may store the certificate of the host system 604 and/or the public key of the host in a memory of the EPP.

Also, the ATM 602 may return to the host system 606 at least one message 612 which includes data that is representative of a successful completion of the certificate transfer. Such a message 612 may include for example a solicited status message or other types of messages which an ATM is capable of sending to a host system. If the verifications of the certificate of the host system are unsuccessful, the message 612 may be returned with data representative of an error. In this described exemplary embodiment the ATM 602 may send messages 612 for each of the certificates (encipherment/decipherment or signature/verification) of the host system. In other exemplary embodiments, the ATM may request both certificates in a single message.

The EPP may also send its certificates to the host system. FIG. 13 schematically shows the certificate exchange process between an ATM 632 and a host system 636 that is initiated by the host system. Here the host system 306 may send to the ATM 632 at least one message 634 which requests one of the certificates of the EPP 638 of the ATM. Such a message 634 may include for example an operational command message or other types of messages which an ATM is capable of receiving from a host system. In a Diebold 91X ATM message protocol environment, for example, the operational command message may include a command code that corresponds to requesting a certificate. The contents of the data field may indicate which public key certificate (encipherment/decipherment or signature/verification) is requested. The ATM 632 may respond by sending at least one message 640 containing the particular certificate 641 of the EPP that was requested by the host system. Such messages 640 may include for example a solicited status message or other types of messages which an ATM is capable of sending to a host system. In a Diebold 91X ATM message protocol environment, for example, the data corresponding to the certificate may be included in the buffer data field. As discussed previously, the data corresponding to the certificate may use the PKCS #7: Cryptographic Message Syntax Standard format. The message syntax may use the Abstract Syntax Notation One (ASN.1) with Basic Encoding Rules (BER) and Distinguished Encoding Rules (DER) which is converted from octet (8-bit) strings to 7-bit ASCII using Base64 encoding.

The host system may validate the digital signature of the EPP using its copy of the public key of the initial CA. In this described exemplary embodiment the host system may send operational command messages for each of the certificates (encipherment/decipherment or signature/verification) of

the EPP of the ATM. In other exemplary embodiments, the host system may request both certificates in a single request message.

As shown in FIG. 14, an exemplary embodiment of the EPP 504 may be manufactured to include the original public keys and/or original certificates 510 of an initial CA 508. As discussed previously, the EPP may further acquire its own initial set of original certificates 506 that are issued by the initial CA 508. Such original certificates may include the respective public encipherment and verification keys generated by the EPP. Also as discussed previously, the EPP may acquire the original public keys and/or certificates 505 of the host system that were issued by the initial CA 508.

As described herein, the EPP may store copies of the certificates of host systems and certificate authorities in a memory of the EPP. However, it is to be understood that in other exemplary embodiments, only the public keys included in the certificates of certificate authorities and host systems may be stored in the EPP. Other contents of the certificates of the certificate authorities and host systems may be discarded after validation of the certificates and storage of the public keys by the EPP.

In exemplary embodiments, the original certificates 506 of the EPP which were signed by the initial CA 508 may be used for terminal master key transfers. However, the institution or other entity operating the ATM 502 with the EPP 504 may wish to replace the initial CA 508 with a new CA 514. As a result, exemplary embodiments of the EPP 504 may further be operative to replace the public keys and/or certificates of the initial CA 508 with new public keys and/or certificates of a new CA 514. FIG. 14 shows an exemplary process 500 for replacing public keys and/or certificates in an EPP 504 of an ATM 502 when the initial or subsequent CA is replaced.

In an exemplary embodiment a host system 512 may initiate the replacement of the original public keys and/or certificates 510 of the initial CA 508 stored in the EPP. An exemplary embodiment of the host system 512 may send to the ATM 502 at least one message 522 including for example a write command message or other types of messages which an ATM is capable of receiving from a host system. The message 522 may include a new certificate 518 of the new CA 514. In embodiments where the EPP requires both primary and secondary certificates of the new CA, the host system may send separate messages 522 for each certificate or may include both primary and secondary certificates in a single message. In the following description of the systems shown in FIGS. 10 and 11, each of the messages 522, 532, 540, 550 may refer to transferring only individual certificates or individual keys in the messages. However, it is to be understood that in other exemplary embodiments, the messages 522, 532, 540, 550 may be constructed to send multiple certificates or keys in each message.

In this described exemplary embodiment the new certificate 518 of the new CA 514 includes the new public key 516 of the new CA. In addition the new certificate 518 may be signed by the initial CA 508 using the private key 520 of the initial CA 508 to form the digital signature 524. In a Diebold 91X ATM message protocol environment, for example, the data corresponding to the new certificate 518 of the new CA may be included in the New Key Data field of a Write Command VII Message. As discussed previously, the data corresponding to the certificate may use the PKCS #7: Cryptographic Message Syntax Standard format. The message syntax may use the Abstract Syntax Notation One (ASN.1) with Basic Encoding Rules (BER) and Distinguished

21

guished Encoding Rules(DER) which is converted from octet (8-bit) strings to 7-bit ASCII using Base64 encoding.

In the exemplary embodiment, the certificate of the new CA may be further signed by the host system 512 to form the digital signature 526. Upon receipt of the message 522 by the ATM 502, the exemplary EPP 504 is operative to validate the digital signature 524 of the initial CA and validate the digital signature 526 of the host system. In exemplary embodiments, the EPP may validate the digital signature 524 of the initial CA using the original public key and/or original certificate 510 of the initial CA. In addition the exemplary EPP 502 may validate the digital signature 526 of the host system using the original public key and/or original certificate 505 of the host system.

Once the new certificate 518 of the new CA has been validated, the new public key 516 and/or certificate 518 of the new CA may be stored in the EPP for use with authenticating new certificates issued by the new CA. Although the original public key and/or certificate 510 of the initial CA could be discarded after the new certificate 518 has been accepted, exemplary embodiments of the EPP may also retain the original public key and/or certificate 510 for use in re-commissioning the EPP.

After the new public keys 516 and/or new certificate 518 of the new CA 514 have been accepted by the EPP 504, the exemplary ATM 502 may send to the host system 512 a message 582 which indicates that the replacement of the certificates for the CA was successful. Such a message 582 may include for example a solicited status message or other types of messages which an ATM is capable of sending to a host system. When the verification of the new certificate of the CA is unsuccessful, the message 582 returned may indicate an error.

After the EPP has received the new public keys 516 of the new CA 514, the exemplary EPP 504 may require new certificates for the EPP which are signed by the new CA. To enhance security of the system, the exemplary embodiment of the EPP may also generate new public/private encipherment/decipherment and signature/validation key pairs 560 to replace the original key pairs 566.

FIG. 15 schematically shows the process for updating the original public/private key pairs 566 of the EPP and corresponding original certificates 506 of the EPP. Here, the host system 512 may send to the ATM 502 at least one message 584 which includes data representative of a request that the EPP 504 generate new public/private key pairs 506. Such a message 584 may include an operational command message or other types of messages which an ATM is capable of receiving from a host system. In the exemplary embodiment, the message 584 may include a field which specifies which of the encipherment/decipherment or signature/validation keys pairs to update. In other exemplary embodiments, the message 584 may correspond to a request that both types of key pairs to be updated.

Once one of the new key pairs 560 has been generated, the ATM 502 may send to the host system 512 at least one message 586 which includes a certificate request message 532. Such a message 586 may include for example a solicited status message or other types of messages which an ATM is capable of sending to a host system. The certificate request message 532 may request the issue of a new certificate for one or both of the corresponding newly generated public keys 562, 564. In a Diebold 91X ATM message protocol environment, for example, the data corresponding to the certificate request message may be included in the buffer data field of the solicited status message.

22

The exemplary certificate request message 532 may include one or both of the corresponding newly generated public key 562, 564 of the EPP 504. The certificate request messages 532 may also include the serial number 567 or other unique identifier of the EPP. In this described exemplary embodiment, the new public verification key 564 and the new public 151 encipherment key 562 are sent to the host system in separate certificate request messages responsive to receiving separate messages 584 from the host which individually specify which of the key pairs to update. However, it is to be understood that in alternative exemplary embodiments, both public keys 562, 564 may be sent in a common certificate request message or the message 586 from the ATM may include separate certificate request messages for each public key.

When the certificate request message contains the new verification public key 564, the EPP may sign the certificate request message 532 with the new private signature key 565 to form digital signature 534. Also to authenticate the message to the host, the EPP may sign the certificate request 532 with its original private signature key of the original keys 566 to form the digital signature 535. When the certificate request message contains the new encipherment public key 562 of the EPP, the certificate request message may first be signed with the new decipherment private key 563, and may then be signed with the original decipherment private key from the original keys 566 to authenticate the message with the host.

In an exemplary embodiment the certificate request message 532 may include both the PKCS #10: Certification Request Syntax Standard format and the PKCS #7: Cryptographic Message Syntax Standard format. The messages may use the PKCS #7 Signed-data content for the outer signature (using the original private signature or decryption key). The message may use the PKCS #10 certificate request format for the inner data (using the new private signature or decryption key). Also as discussed previously, the message syntax may use the Abstract Syntax Notation One (ASN.1) with Basic Encoding Rules (BER) and Distinguished Encoding Rules(DER) which is converted from octet (8-bit) strings to 7-bit ASCII using Base64 encoding.

Upon receipt of the certificate request messages 532, the exemplary host system may validate the EPP signatures 534, 535 of the messages. After validating the signatures 534, 535, the host system may cause the new CA 514 to issue an updated certificate 542 which includes the corresponding new public key 562, 564 of the EPP received in the certificate request message 532. The updated certificate 542 may also include the serial number 567 or other unique identifier of the EPP.

The host system may be operative to send a message 540 to the ATM 502 which includes the updated certificate 542. Such a message 540 may include for example write command messages or other types of messages that an ATM is capable of receiving from a host system. In a Diebold 91X ATM message protocol environment, for example, the data corresponding to the updated certificate 542 for the EPP may be included in the new key data field of a Write Command VII Message. In an exemplary embodiment the messages 540 for sending an updated certificate of the EPP may include the PKCS #7: Cryptographic Message Syntax Standard format. The messages may use the degenerate "certificate only" case of the Signed-data content type in which the inner content's data field is omitted and there are no signers.

The exemplary embodiment of the host system is operative to send at least one message 540 with one new certificate 542 of the EPP for each certificate request messages

532. In alternative exemplary embodiments, the host system may send both the new encipherment/decipherment and signature/verification certificates 574, 576 in a single message 540 responsive to receiving one or more certificate request messages 522 that includes both public keys 562, 564 in a single message 586 from the ATM.

Before accepting the new certificate 542, the EPP may verify that the new certificate was signed by the current CA, which in this described embodiment is the new CA 514. In addition the EPP may verify that the public key in the new certificate 542 matches the current public key which in this described embodiment is one of the newly generated public keys 562, 564. Also the EPP may verify that the serial number in the new certificate 542 matches the original serial number of the EPP. If the received new certificate is determined to be valid, the EPP may store it in the memory of the EPP. In addition the EPP may replace the original keys 566 with the newly generated public/private encipherment/decipherment or signature/validation key pairs 560 that correspond to the new certificate 542.

Upon accepting the new certificate 542, the exemplary EPP may return to the host system at least one message 550 which indicates that the new certificate 542 was successfully received. Such a message 550 may include for example a solicited status message 550 or other types of message which an ATM is capable of sending to a host system. In one exemplary embodiment, when the message 550 has been received and represents the acceptance of the new certificate 542, the host system may replace the copy of the original certificate 506 of the EPP stored at the host system with the new certificate 542 of the EPP. In other exemplary embodiments, the original ATM certificates 506 stored at the host system may be replaced with new certificates 542 of the EPP by having the EPP of the ATM 504 send the new certificates to the host system. As discussed previously with respect to FIG. 13, the host system 536 may send a message 634 to the ATM 632 which requests one of the new certificates of the EPP. In response, the EPP 638 may return the requested new certificate in a message 640.

In addition, the exemplary host system 512 may further send to the EPP, a set of new certificates 570 for the host system which are digitally signed by the new CA. This process may be initiated by the host system or an operator at the ATM. As discussed previously with respect to FIG. 12, when an operator initiates the transfer of the updated certificate of the host system to the ATM 502, the ATM is operative to output a one-way hash of the new public key contained in the new certificate of the host through a display device of the ATM which can be independently verified by the operator. If the one-way hash is indicated to be valid by the operator, the EPP may accept and store the new public key and/or the new certificate of the host system in the memory of the EPP.

As with the certificates issued by the initial CA, the EPP 504 and host system 512 are further operative to use the exchanged new public keys and/or new certificates 542, 570 issued by the new CA to perform the steps involved with securely transferring a terminal master key from the host system 512 to the EPP 504. In the exemplary embodiment, the steps described with respect to updating the CA and certificates may be performed a plurality of times whenever there is a requirement to change the CA and/or the public keys associated with the CA.

In exemplary embodiments, the EPP may be decommissioned in the field. Such a decommissioning may include clearing the public and private key pairs of the EPP and any public keys of the host system and a new CA. When the EPP

is re-commissioned it may generate new public and private key pairs. The EPP may then generate new certificate request messages to be sent to the initial CA which include the newly generated public keys and the serial number of the EPP. As discussed previously, the initial CA may issue corresponding primary and secondary certificates for each of the new public keys of the EPP.

Computer software used in operating the automated transaction machines and connected computers may be loaded from articles of various types into the respective computers. Such computer software may be included on and loaded from one or more articles such as diskettes or compact disks. Such software may also be included on articles such as hard disk drives, tapes or ready only memory devices. Other articles which include data representative of the instructions for operating computers in the manner described herein are suitable for use in achieving operation of transaction machines and systems in accordance with exemplary embodiments.

The exemplary embodiments of the automated banking machines and systems described herein have been described with reference to particular software components and features. Other embodiments of the invention may include other or different software components which provide similar functionality.

Thus the new automated banking machine and system and method achieves one or more of the above stated objectives, eliminates difficulties encountered in the use of prior devices and systems, solves problems and attains the desirable results described herein.

In the foregoing description certain terms have been used for brevity, clarity and understanding. However no unnecessary limitations are to be implied therefrom because such terms are for descriptive purposes and are intended to be broadly construed. Moreover the descriptions and illustrations herein are by way of examples and the invention is not limited to the details shown and described.

In the following claims any feature described as a means for performing a function shall be construed as encompassing any means capable of performing the recited function and shall not be deemed limited to the particular means shown in the foregoing description or mere equivalents thereof. The description of the exemplary embodiment included in the Abstract included herewith shall not be deemed to limit the invention to features described therein.

Having described the features, discoveries and principles of the invention, the manner in which it is constructed and operated and the advantages and useful results attained; the new and useful structures, devices, elements, arrangements, parts, combinations, systems, equipment, operations, methods, processes and relationships are set forth in the appended claims.

We claim:

1. A method comprising:

- a) receiving at least one first input with an automated banking machine that includes a cash dispenser, wherein the at least one first input corresponds to a command to initiate a transfer of a terminal master key to the automated banking machine;
- b) sending from the automated banking machine at least one first message to a host system, wherein the at least one first message includes first data representative of a request to transfer the terminal master key to the automated banking machine;

25

- c) receiving with the automated banking machine at least one second message from the host system, wherein the at least one second message includes an encrypted terminal master key;
- d) validating the second message; and
- e) decrypting the terminal master key with a first private key of the automated banking machine.
- 2. The method according to claim 1, wherein in step (d) the second message is validated using a first public key of the host system, and wherein prior to step (d) further comprising:
 - f) receiving with the automated banking machine, the first public key of the host system from the host system.
- 3. The method according to claim 2, wherein in step (a) the at least one first input is received from a single operator through at least one input device of the machine, and wherein further comprising:
 - g) calculating a one-way hash of the first public key of the host system;
 - h) outputting through a display device of the automated banking machine the one-way hash; and
 - i) receiving at least one second input through the at least one input device of the automated banking machine that corresponds to a command to accept the first public key of the host system.
- 4. The method according to claim 2, wherein in step (f) the first public key of the host system is included in a certificate of the host system, wherein further comprising:
 - g) validating the certificate of the host system using a public key associated with a certificate authority (CA).
- 5. The method according to claim 4, and further comprising:
 - h) generating at least one third message, wherein the at least one third message includes second data;
 - i) signing the second data with a second private key of the automated banking machine; and
 - j) sending with the automated banking machine the at least one third message to the host system.
- 6. The method according to claim 5, and further comprising:
 - k) sending through operation of the automated banking machine at least two certificates of the automated banking machine to the host system, wherein a first of the at least two certificates includes a first public key of the automated banking machine that corresponds to the first private key of the automated banking machine, wherein a second of the at least two certificates includes a second public key of the automated banking machine that corresponds to the second private key of the automated banking machine.
- 7. The method according to claim 5, wherein prior to step (h) further comprising
 - k) receiving with the automated banking machine from the host system a second public key of the host system; and
 - l) encrypting the terminal master key with the second public key of the host system; and
 wherein in step (h), the second data includes at least a portion of the terminal master key encrypted with the second public key of the host system.
- 8. The method according to claim 7, wherein in step (c) the second message includes an encrypted first information, wherein step (e) includes decrypting the first information, wherein step (l) includes encrypting both the terminal master key and the first information with the second public key of the host system, wherein in step (h) the second data includes

26

the terminal master key and the first information encrypted with the public key of the host system.

9. The method according to claim 5, wherein in step (c) the second message includes an identity data for the host system, wherein in step (h) the second data includes the identity data.

10. The method according to claim 9, wherein in step (c) the identity data is encrypted in the second message, wherein step (e) includes decrypting the identity data, wherein in step (h) the second data includes the decrypted identity data information.

11. The method according to claim 10, wherein in step (c) the second message includes a random number associated with the host system, wherein in step (h) the second data includes the random number.

12. The method according to claim 6, wherein prior to step (k) further comprising:

l) converting the certificates to a 7-bit ASCII format.

13. The method according to claim 1, wherein prior to step (b) further comprising:

f) generating a first random number; and

wherein in step (b) the first message includes the first random number, wherein step (c) the second message includes a second number, wherein step (d) includes verifying that the first random number corresponds to the second number received in the second message.

14. The method according to claim 1, wherein in step (a) the at least one first input corresponds to at least one third message received from the host system by the automated banking machine.

15. The method according to claim 14, wherein in step (a) the third message corresponds to a Diebold 91X operational command message, wherein in step (b) the first message corresponds to a Diebold 91X solicited status message.

16. The method according to claim 1, wherein in step (b) the first message corresponds to a Diebold 91X Unsolicited Status Message, wherein in step (c) the second message corresponds to a Diebold 91X Write Command Message.

17. The method according to claim 1, wherein steps (d) and (e) are performed with an encrypting pin pad (EPP) of the automated banking machine.

18. The method according to claim 17, further comprising:

f) determining that the terminal master key is a double-length key; and

g) switching in the EPP a current encryption algorithm from a Single-DES encryption algorithm to a double-length Triple-DES encryption algorithm.

19. The method according to claim 17, further comprising:

f) determining that the terminal master key is a single-length key; and

g) switching in the EPP a current encryption algorithm from a double-length Triple-DES encryption algorithm to a Single-DES encryption algorithm.

20. The method according to claim 17, further comprising:

f) receiving at least one third message from the host system;

g) decrypting the at least one third message to uncover a communication key using the terminal master key;

h) receiving the input of a personal identification number (PIN) through operation of the EPP of the automated banking machine;

i) encrypting with the EPP the PIN using the communication key; and

27

j) sending with the automated banking machine at least one fourth message to the host system, wherein the at least one fourth message includes the encrypted PIN.

21. The method according to claim 20, wherein in step (i) the PIN is encrypted using a double-length key Triple-DES encryption algorithm, wherein in step (e) the terminal master key is decrypted using an RSA algorithm.

22. The method according to claim 20, further comprising:

k) dispensing cash with the cash dispenser of the automated banking machine.

23. Computer readable media bearing instructions which are operative to cause at least one computer in the automated banking machine to cause the automated banking machine to carry out the method steps recited in claim 1.

24. An automated banking machine apparatus comprising: an automated banking machine, wherein the automated banking machine is operative to communicate with a host system, wherein the automated banking machine is operative to receive from the host system: a signed and encrypted terminal master key, an encrypted communication key, and at least one certificate of the host system, wherein the at least one certificate of the host system includes a verification public key of the host system wherein the automated banking machine includes:

at least one first processor; and

an encrypting pin pad (EPP) in operative connection with at least one first processor, wherein the EPP includes:

at least one second processor;

a hardware interface in operative connection with the at least one second processor, wherein the at least one second processor is operative to communicate with at least the first processor through the hardware interface;

a memory in operative connection with the at least one second processor, wherein the memory includes at least one public key of a certificate authority (CA) and at least one decipherment private key of the EPP; and

a keypad in operative connection with the at least one second processor, wherein the at least one second processor is operative to validate the certificate of the host system using the public key of the CA, wherein the at least one second processor is operative to validate the signed encrypted terminal master key using the verification public key of the host system, wherein the at least one second processor is operative to decrypt the signed encrypted terminal master key using the decipherment private key of the EPP, wherein the at least one second processor is operative to decrypt the encrypted communication key using the terminal master key, wherein the at least one second processor is operative to encrypt a personal identification number (PIN) inputted through the keypad using the communication key.

25. The machine according to claim 24, wherein the automated banking machine includes:

at least one input device in operative connection with the at least one first processor;

a cash dispenser in operative connection with the at least one first processor, wherein the at least one first processor is operative to cause the cash dispenser to dispense currency responsive to at least one first input received through the at least one input device.

28

26. The machine according to claim 25, wherein the automated banking machine further includes:

at least one output device in operative connection with the at least one first processor, wherein the at least one first processor is operative to output through the at least one output device a one-way hash of the verification public key of the host system, wherein the at least one first processor is operative to inform the at least one second processor that the one-way hash of the verification public key of the host system has been verified by an operator responsive to at least one second input received through the at least one input device that is representative of a confirmation that the public key of the certificate of the host system is valid.

27. The machine according to claim 25, wherein the at least one second processor is operative to encrypt the PIN using a double-length key Triple-DES algorithm.

28. The machine according to claim 25, wherein the at least one second processor is operative to decrypt the signed terminal master key, validate the signed terminal master key, and validate the certificate of the host system using RSA algorithms.

29. The machine according to claim 24, wherein the at least one second processor is operative to generate the at least one decipherment private key of the EPP and at least one encipherment public key of the EPP.

30. The machine according to claim 29, wherein the at least one second processor is operative to generate at least one signature private key of the EPP and at least one verification public key of the EPP, wherein the at least one second processor is operative to sign messages being sent to the host system using the at least one signature private key of the EPP.

31. The machine according to claim 30, wherein the at least one second processor is operative to receive through the hardware interface, a primary encipherment/decipherment certificate of the EPP and a secondary encipherment/decipherment certificate of the EPP, wherein both the primary encipherment/decipherment certificate of the EPP and the secondary encipherment/decipherment certificate of the EPP include the at least one encipherment public key of the EPP, wherein the at least one second processor is operative to receive through the hardware interface both a primary signature/verification certificate of the EPP and a secondary signature/verification certificate of the EPP, wherein both the primary signature/verification certificate of the EPP and the secondary signature/verification certificate of the EPP include the at least one verification public key of the EPP.

32. The machine according to claim 24, wherein the at least one second processor is operative to switch from using a Single-DES algorithm to a double-length Triple-DES algorithm for encrypting inputted PINs responsive to determining that the terminal master key received from the host system is a double-length key.

33. A method for improving the encryption capabilities of an automated banking machine that is operative to configure the machine with a terminal master key through the manual operations of a two-person team, wherein a first person must manually input a first value into the machine and a second person must manually input a second value into the machine, and wherein the machine constructs the terminal master key using both the first and second values, the method comprising:

a) disengaging an existing encrypting pin pad (EPP) from the automated banking machine, wherein the existing EPP is operative to receive at least a portion of a terminal master key constructed from two separate

29

values manually inputted into the machine through at least one input device of the machine; and

- b) installing an alternate EPP in the automated banking machine, wherein the alternate EPP is operative to receive an encrypted terminal master key from a host system.

34. The method according to claim 33, wherein the alternate EPP installed in step (b) includes at least one first certificate stored therein.

35. The method according to claim 34, wherein the alternate EPP installed in step (b) is operative to decrypt the terminal master key using a private key stored in the EPP.

36. The method according to claim 35, wherein the alternate EPP installed in step (b) is operative to send the at least one first certificate to the host system.

37. The method according to claim 36, wherein the alternate EPP installed in step (b) is operative to receive at least one second certificate from the host system.

38. The method according to claim 37, wherein the alternate EPP installed in step (b) is operative to authenticate the terminal master key using a public key associated with the at least one second certificate.

39. The method according to claim 38, wherein the alternate EPP installed in step (b) is operative to authenticate the at least one second certificate using a public key associated with a certificate authority (CA), wherein the public key associated with the CA is stored in the EPP.

40. The method according to claim 36, wherein the alternate EPP installed in step (b) is operative to digitally

30

sign a message using a private key associated with a public key in the at least one first certificate and is further operative to send the signed message to the host system.

41. The method according to claim 36, wherein the alternate EPP installed in step (b) is operative to replace the at least one first certificate with at least one second certificate received from the host system.

42. The method according to claim 34, wherein the alternate EPP installed in step (b) is operative to generate at least one public key and private RSA key pair.

43. A method of modifying an automated banking machine including a cash dispenser, which automated banking machine is operative to receive at least one encryption key used in the encryption of messages sent from the machine, and wherein the machine is adapted to receive the at least one encryption key through at least one manual input device on the machine, the method comprising:

- a) disengaging an existing encryption key holding device from the machine, which existing encryption key holding device is adapted to hold the at least one encryption key received through the at least one manual input device; and

- b) installing an encrypting pin pad on the machine, wherein the encrypting pin pad is adapted to hold at least one remotely delivered encryption key received by the machine from a remote host system.

* * * * *



US007110986B1

D-1077+20 RY

(12) **United States Patent**
Zajkowski et al.

(10) **Patent No.:** US 7,110,986 B1
(45) **Date of Patent:** Sep. 19, 2006

(54) **AUTOMATED BANKING MACHINE
SYSTEM AND METHOD**

(75) **Inventors:** Timothy Zajkowski, Uniontown, OH
(US); Anne Doland, Uniontown, OH
(US); Mark D. Smith, North Canton,
OH (US)

(73) **Assignee:** Diebold, Incorporated, North Canton,
OH (US)

(*) **Notice:** Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 782 days.

(21) **Appl. No.:** 10/126,729

(22) **Filed:** Apr. 19, 2002

Related U.S. Application Data

(60) **Provisional application No.** 60/285,724, filed on Apr.
23, 2001.

(51) **Int. Cl.**
H04L 9/28 (2006.01)
G06Q 90/00 (2006.01)

(52) **U.S. Cl.** 705/64; 705/42; 713/156;
713/168

(58) **Field of Classification Search** 705/18,
705/42-44, 50-54, 64-67, 70-79; 713/156-162,
713/164-189, 200-202; 380/277-285, 28-30;
707/9-10

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,605,820 A * 8/1986 Campbell, Jr. 705/71
4,659,877 A * 4/1987 Dorsey et al. 379/88.14
4,933,971 A * 6/1990 Bestock et al. 380/44
5,787,403 A 7/1998 Randle

6,085,177 A 7/2000 Semple et al.
6,115,816 A 9/2000 Davis
6,226,618 B1 * 5/2001 Downs et al. 705/1
6,308,887 B1 10/2001 Korman et al.
6,396,928 B1 5/2002 Zheng
6,539,361 B1 3/2003 Richards et al.
6,594,758 B1 * 7/2003 Okui 713/163
2002/0062440 A1 * 5/2002 Akama 713/171

FOREIGN PATENT DOCUMENTS

EP 138320 A2 * 4/1985

OTHER PUBLICATIONS

Forcht et al., "Security Issues and Concern with the Internet",
Internet Research v5n3, pp. 23-31, 1995, ISSN: 1066-2243.*

* cited by examiner

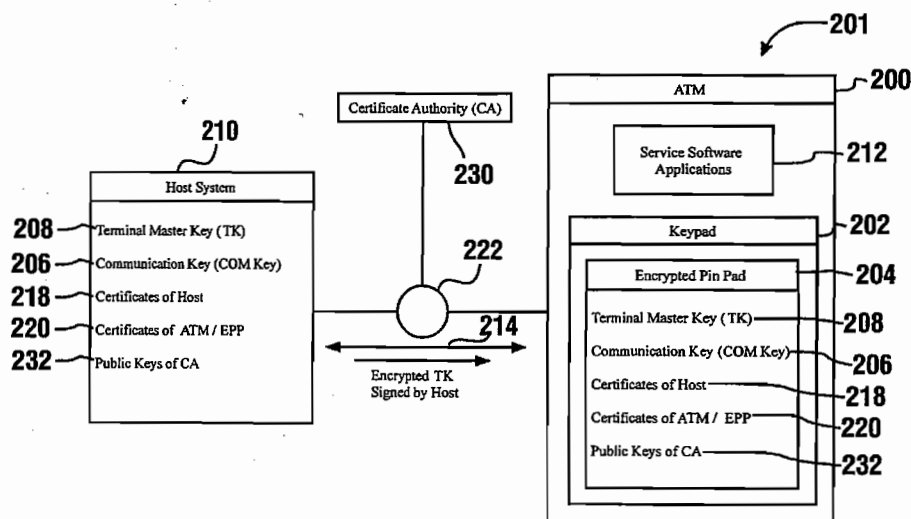
Primary Examiner—Mary D. Cheung

(74) **Attorney, Agent, or Firm**—Christopher L. Parmelee;
Ralph E. Jocke; Walker & Jocke

(57) **ABSTRACT**

An automated banking machine (12, 200, 302) is provided. The machine may be operative to install a terminal master key (TK) therein in response to at least one input from a single operator. The machine may include an EPP (204) that is operative to remotely receive an encrypted terminal master key from a host system (210, 304). The machine may authenticate and decrypt the terminal master key prior to accepting the terminal master key. The machine may further output through a display device (30) of the machine a one-way hash of at least one public key associated with the host system. The machine may continue with the installation of the terminal master key in response to an operator confirming that the one-way hash of the public key corresponds to a value independently known by the operator to correspond to the host system.

39 Claims, 15 Drawing Sheets



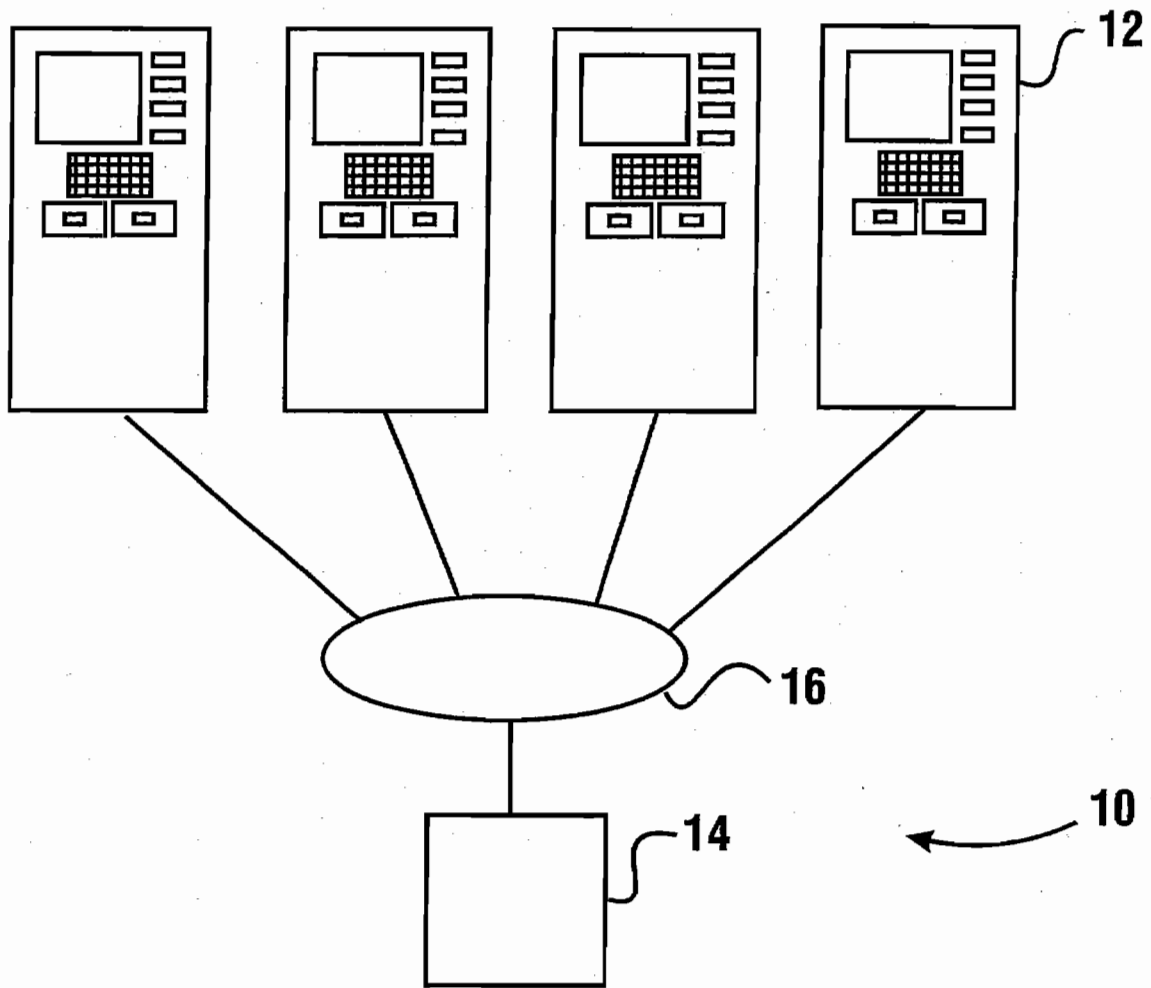
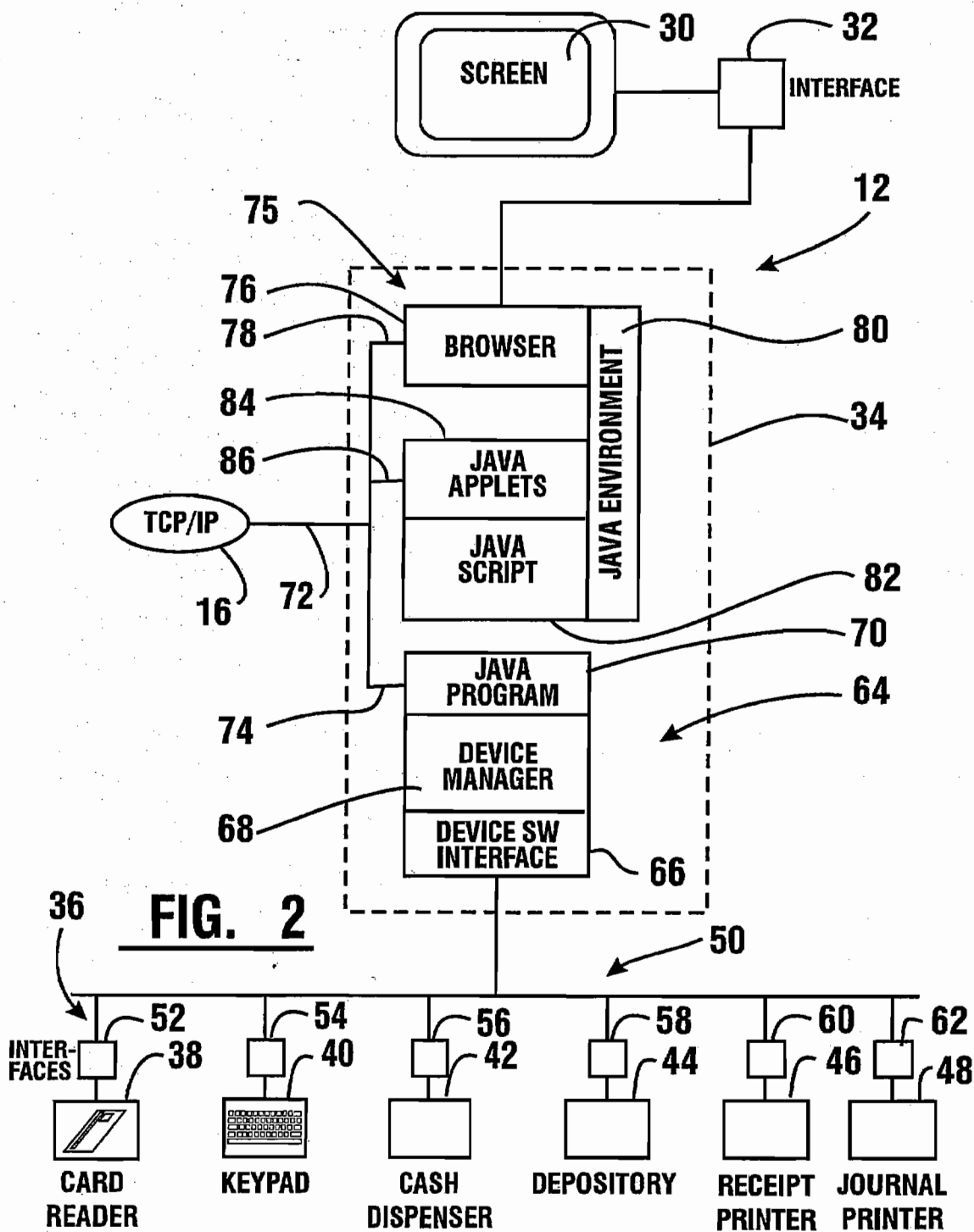


FIG. 1



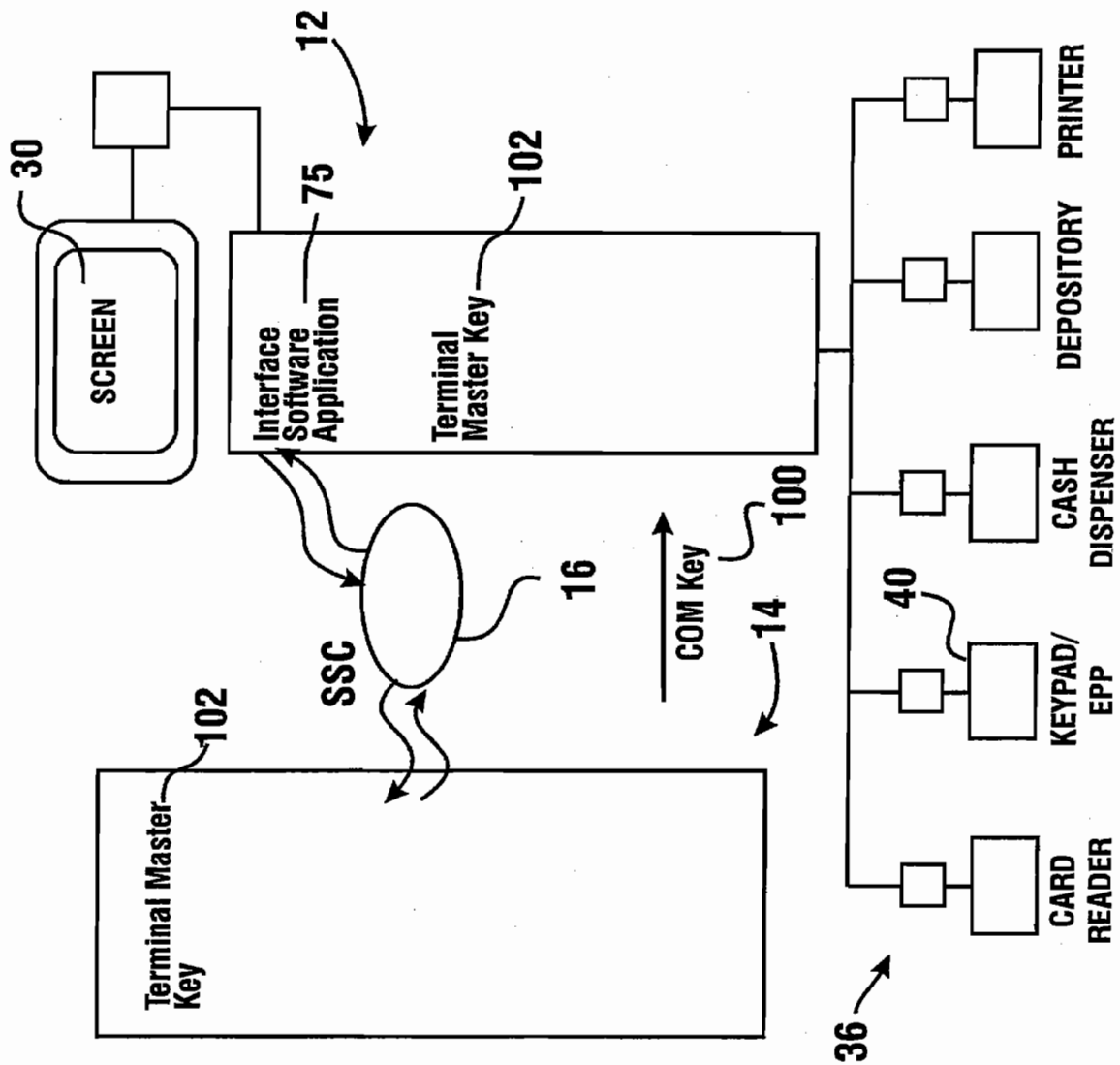


FIG. 3

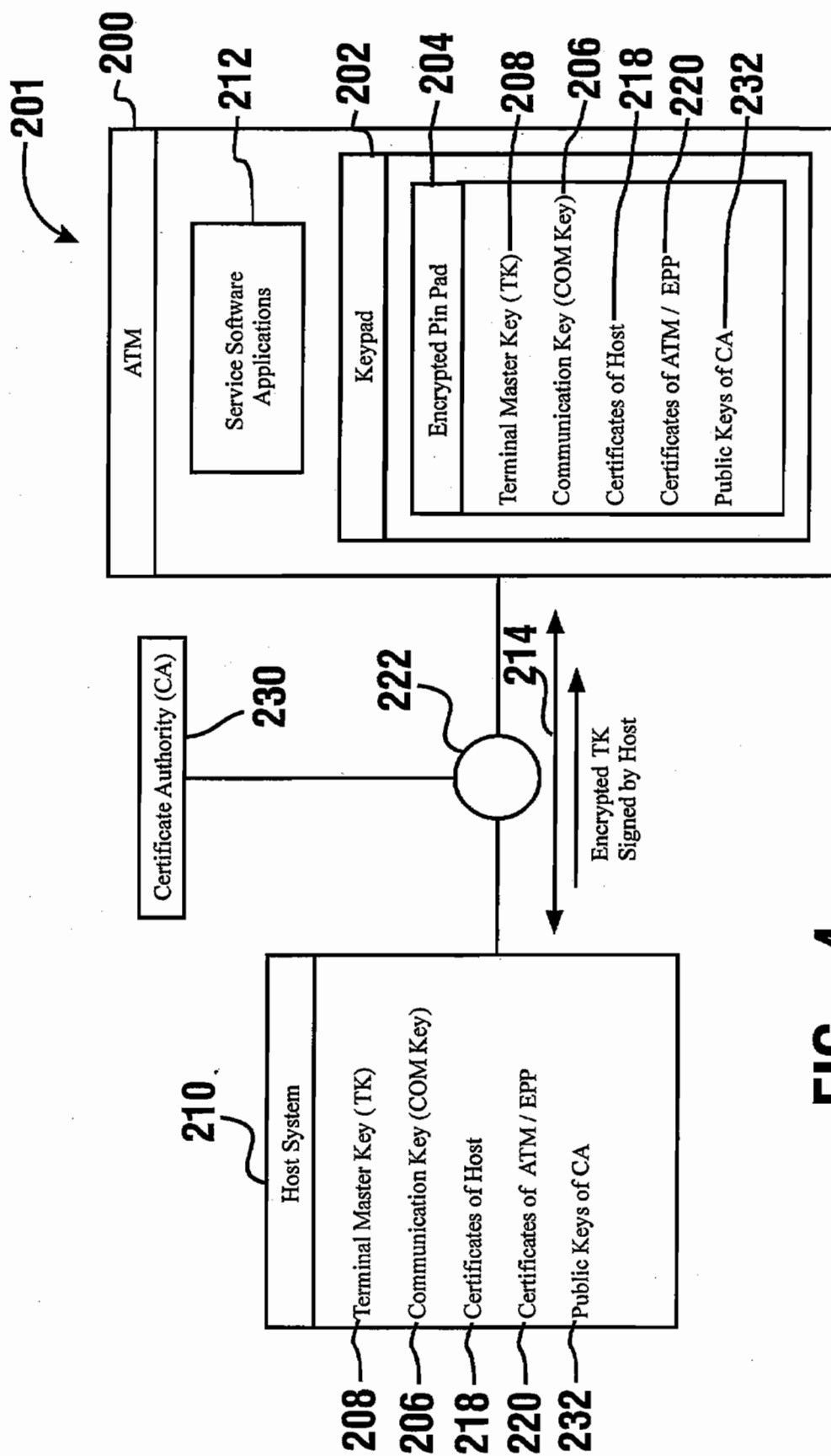


FIG. 4

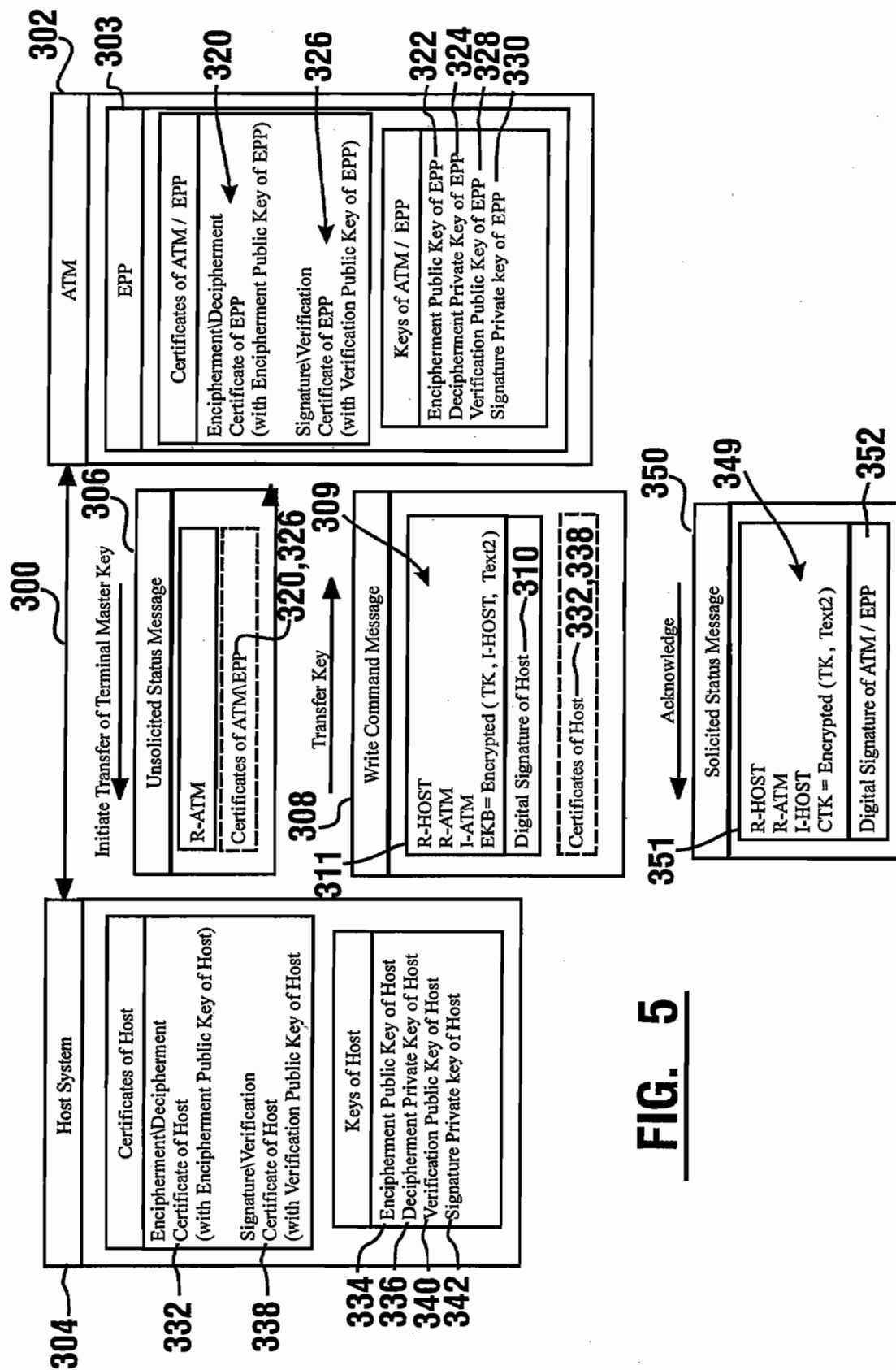
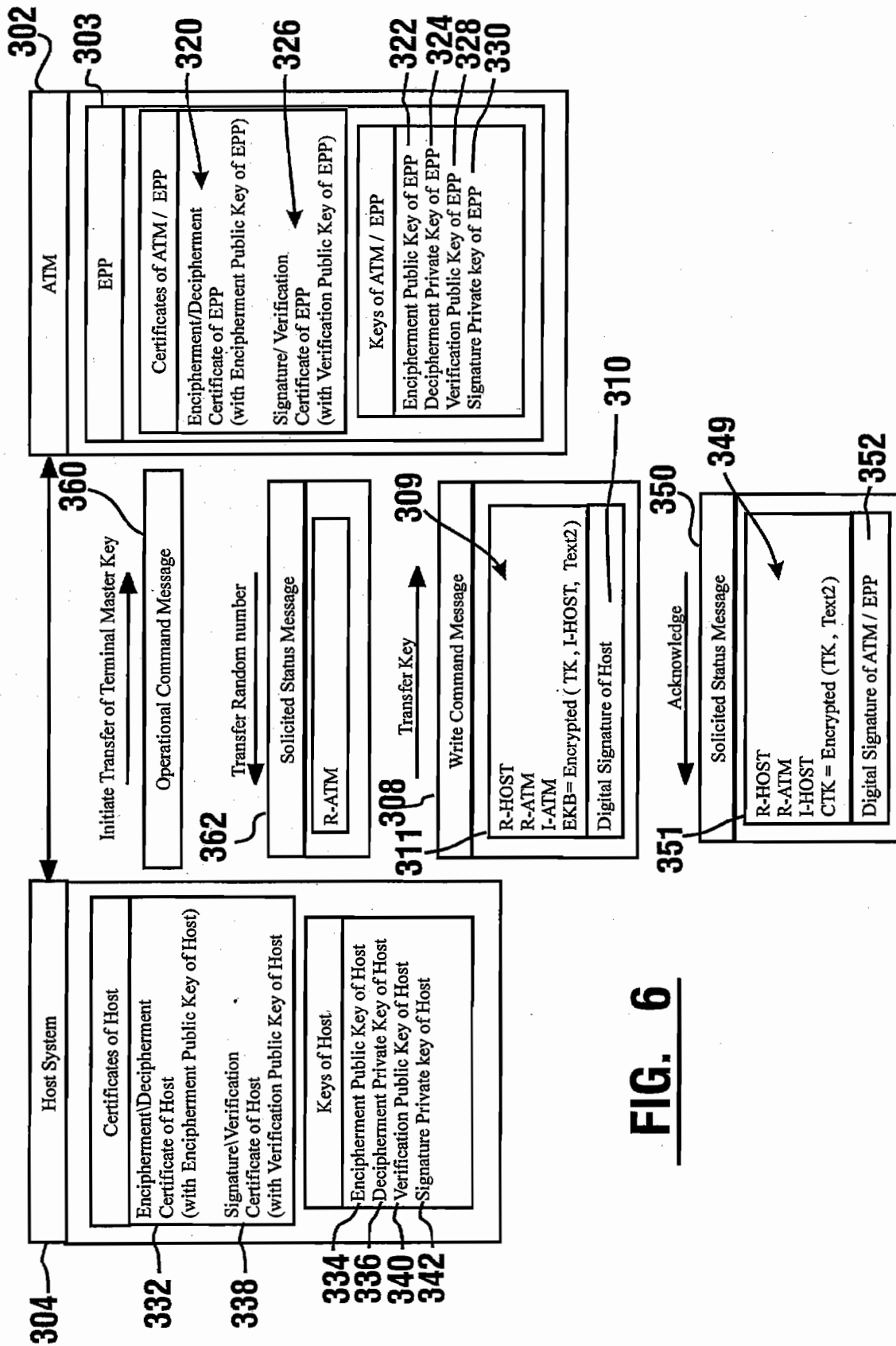


FIG. 5

**FIG. 6**

306

Unsolicited Status Message

DESCRIPTION	CODE	NUMBER OF CHARACTERS
Protocol Dependent Header		VAR
Solicited/Unsolicited ID	'1'	1
Message Identifier	'2'	1
Field Separator (FS)	:1C	1
Logical Unit Number (LUNO)	---	3 or 9
Field Separator (FS)	:1C	1
Field Separator (FS)	:1C	1
Status Source	---	1
Status	---	VAR
Field Separator (FS)	:1C	1
/ Series/MDS Status	---	VAR
Field Separator (FS)	:1C	1
Maintenance Mode Log	---	VAR
Field Separator	:1C	1 [1]
Buffers to Follow ID	[9]	1 [1]
Buffer ID	---	3 [1]
Buffer Data	---	VAR [1]
Group Separator (GS)	:1D	1 [1]
Buffer ID	---	3 [1]
Buffer Data	---	VAR [1]
Protocol Dependent Trailer	VAR	VAR

305

307

FIG. 7

308

Write Command VII Message

DESCRIPTION	CODE	NUMBER OF CHARACTERS
Protocol Dependent Header		VAR
Write Command Identifier	'3'	1
Response Flag	[X]	1
Field Separator (FS)	:1C	1
Logical Unit Number (LUNO)	[X]	3
Field Separator (FS)	:1C	1
Message Sequence Number	[X]	3
Field Separator (FS)	:1C	1
Write Identifier (Encryption Key Change)	'3'	1
Key Change	[---]	1
Field Separator (FS)	:1C	1
New Key Data	[---]	VAR
Protocol Dependent Trailer		VAR

370

372

FIG. 8

Solicited Status Message

DESCRIPTION	CODE	NUMBER OF CHARACTERS
Protocol Dependent Header	VAR	Var
Solicited/Unsolicited ID	'2'	1
Message Identifier	'2'	1
Field Separator (FS)	:1C	1
Logical Unit Number (LUNO)	---	3 or 9
Field Separator (FS)	:1C	1
Message Sequence Number	---	8
Field Separator (FS)	:1C	1
Status Descriptor	---	1
Field Separator (FS)	:1C	1
Device Identifier (DID)	---	1
Status	---	VAR
Group Separator (GS)	:1D	1[1]
Device Identifier (DID)	---	1[1]
Status	---	VAR [1]
Field Separator (FS)	:1C	1[2]
Amount of coins dispensed	---	3[2]
Field Separator (FS)	:1C	1[3]
MDS Status	---	VAR [3]
Field Separator	:1C	1[4]
Buffers to Follow ID	[9]	1[4]
Buffer ID	---	3[4]
Buffer Data	---	VAR [4]
Group Separator (GS)	:1D	1[4]
Buffer ID	---	3[4]
Buffer Data	---	VAR [4]
Field Separator (FS)	:1C	1[5]
Rollover 1 Count	---	3[5]
Rollover 2 Count	---	3[5]
Rollover 3 Count	---	3[5]
Rollover 4 Count	---	3[5]
Protocol Dependent Trailer	VAR	VAR

382

FIG. 9

Operational Command Message

DESCRIPTION	CODE	NUMBER OF CHARACTERS
Protocol Dependent Header		VAR
Operational Command Identifier	'1'	1
Response Flag	[X]	1
Field Separator (FS)	:1C	1
Logical Unit Number (LUNO)	[X]	3
Field Separator (FS)	:1C	1
Message Sequence Number	[X]	3
Field Separator (FS)	:1C	1
Command Code	---	1
Data Field	[---]	VAR
Field Separator (FS)	:1C[1]	1
Status Flag	[---][1]	1
Device Name	[---][1][2]	4
Protocol Dependent Trailer		VAR

363

FIG. 10

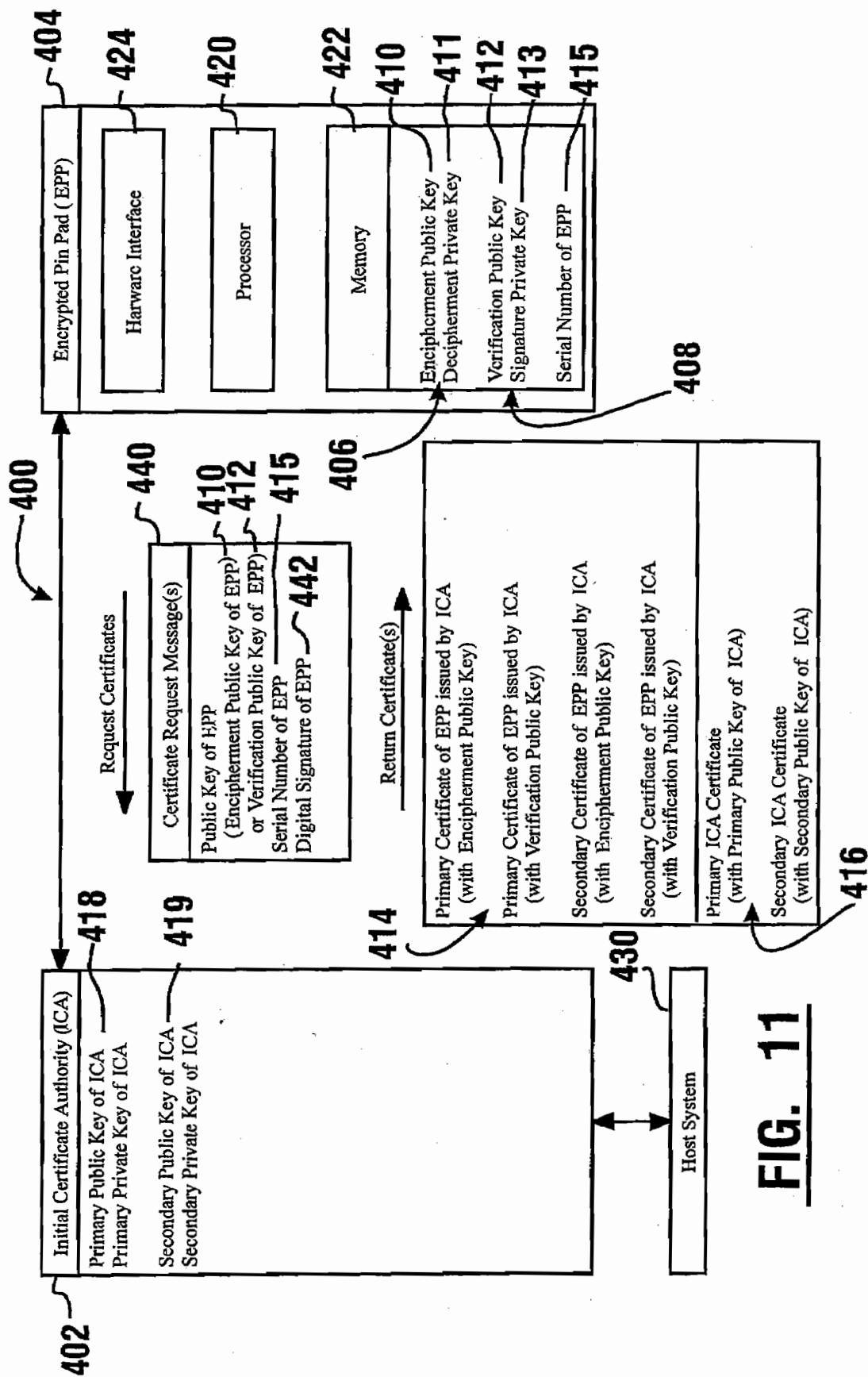


FIG. 11

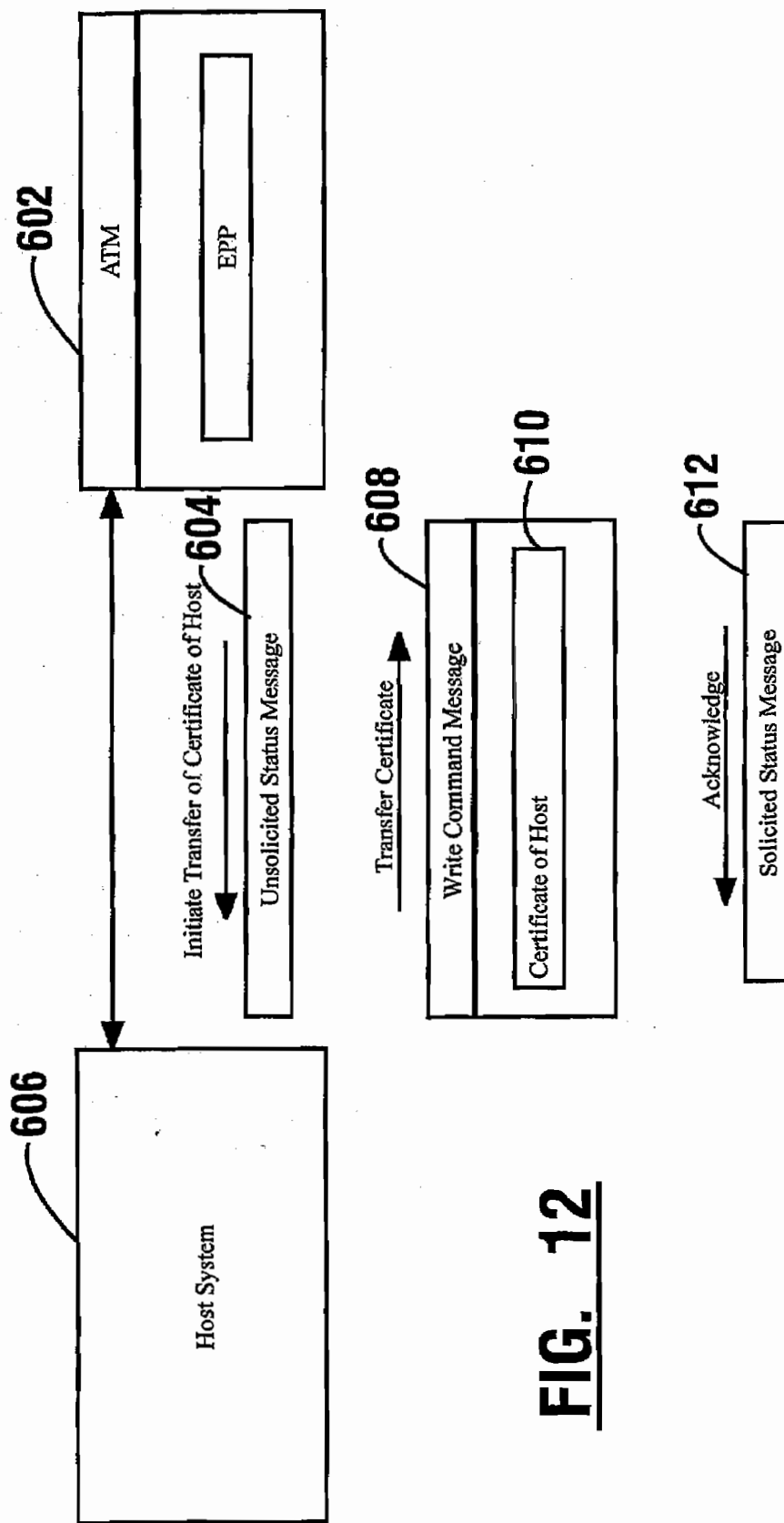


FIG. 12

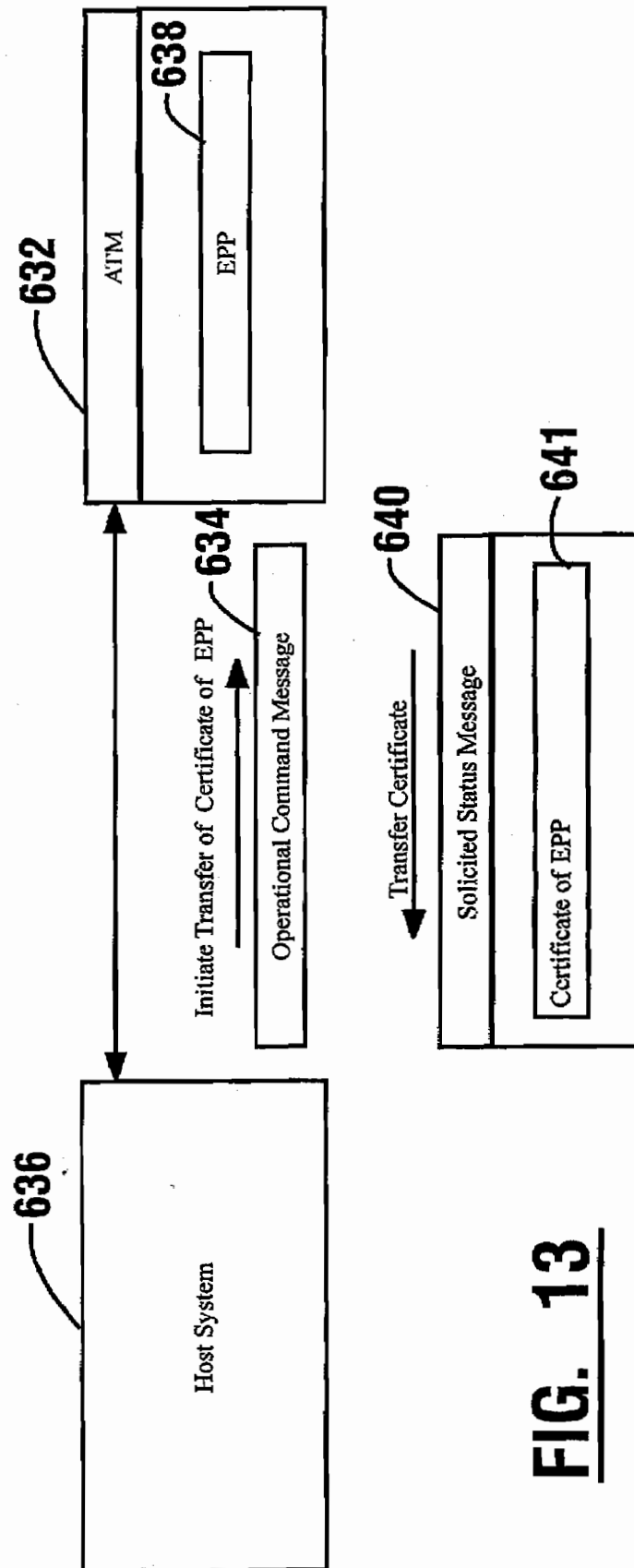


FIG. 13

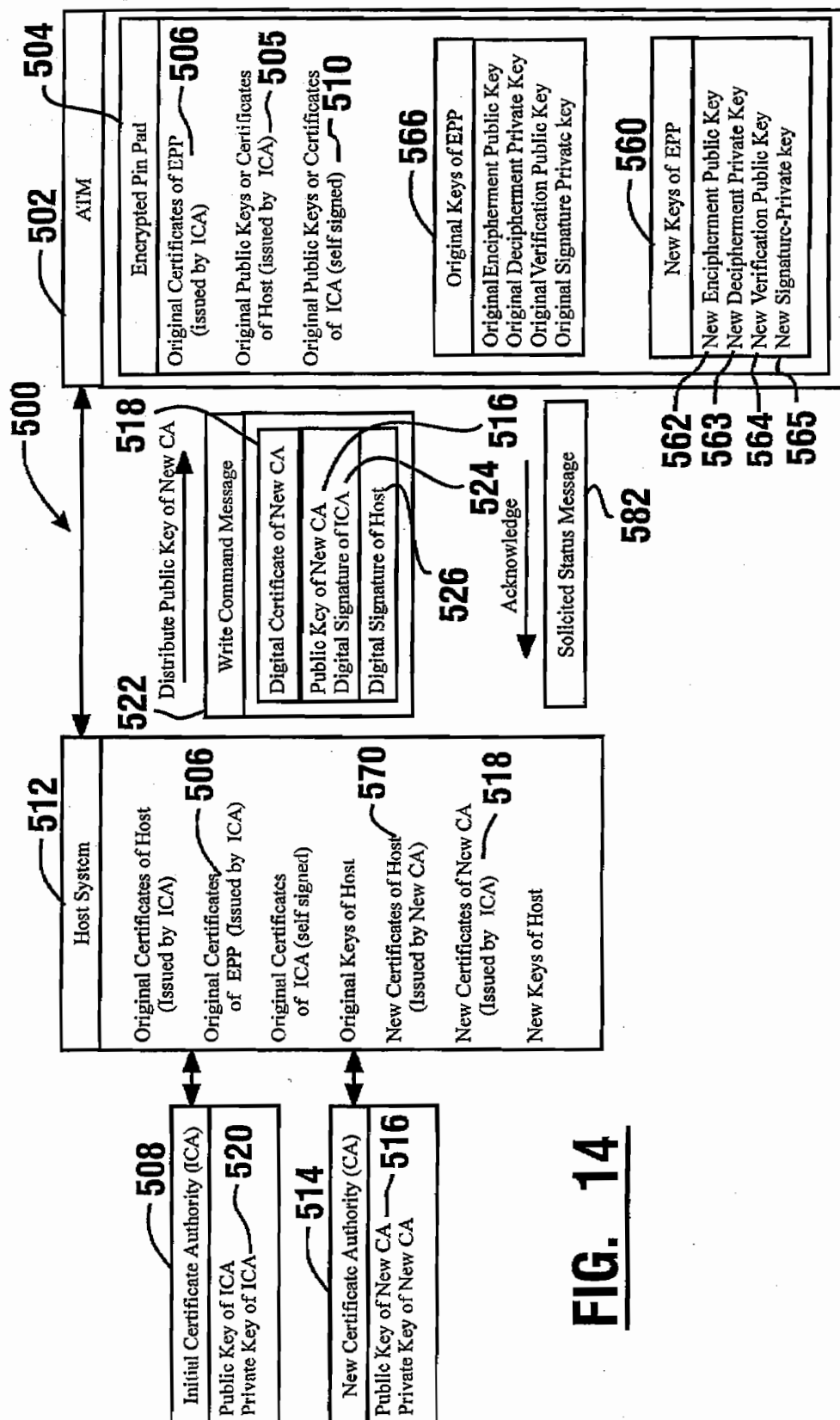


FIG. 14

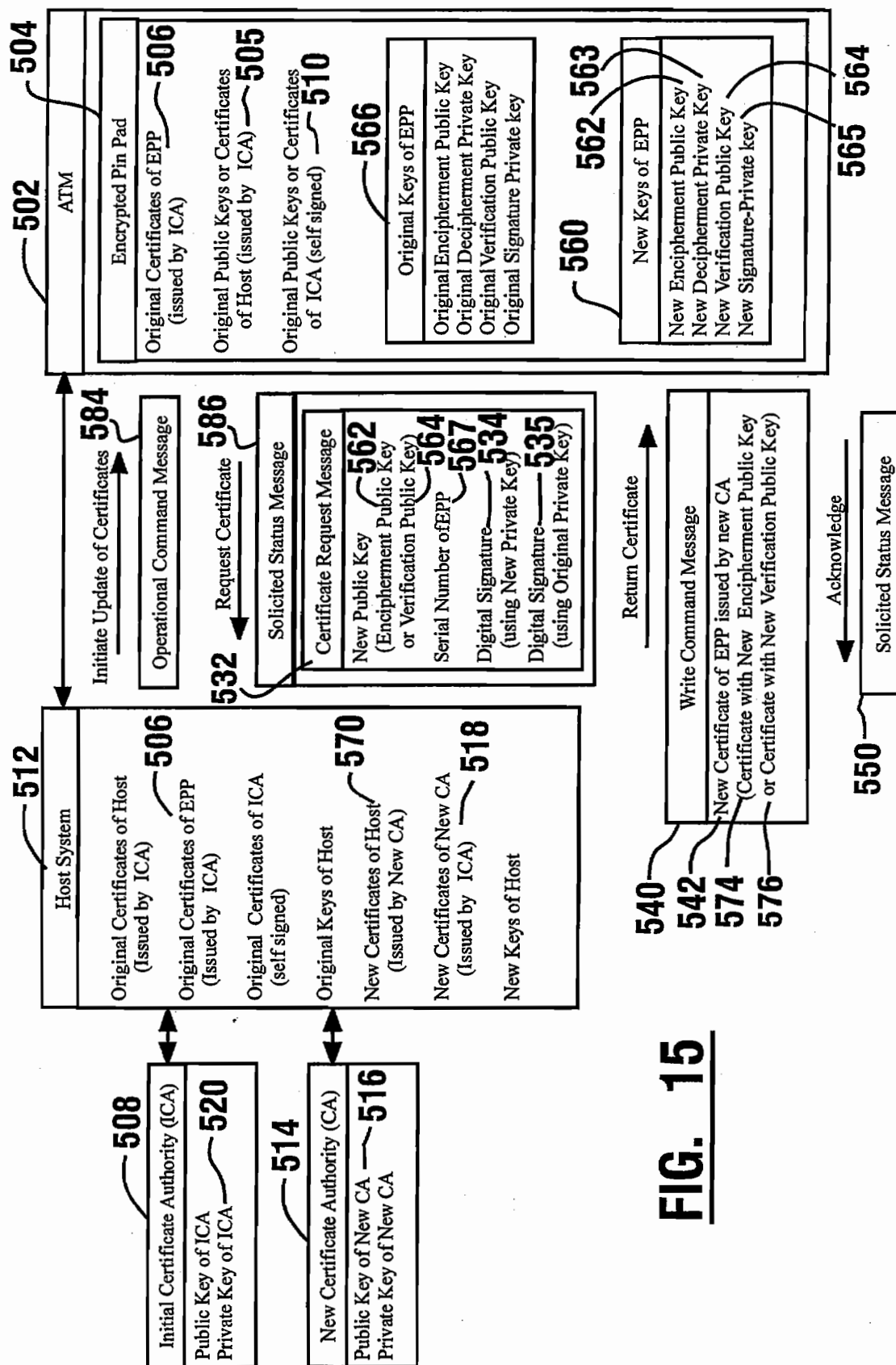


FIG. 15

1

AUTOMATED BANKING MACHINE SYSTEM AND METHOD

CROSS REFERENCE TO RELATED APPLICATIONS

This application claims benefit of U.S. Provisional Application Ser. No. 60/285,724 filed on Apr. 23, 2001.

TECHNICAL FIELD

This invention relates to automated banking machines. Specifically this invention relates to an automated banking machine system and method that is capable of configuring an automated banking machine with encryption keys.

BACKGROUND ART

Automated banking machines are well known. A common type of automated banking machine used by consumers is an automated teller machine ("ATM"). ATMs enable customers to carry out banking transactions. Common banking transactions that may be carried out with ATMs include the dispensing of cash, the making of deposits, the transfer of funds between accounts, the payment of bills and account balance inquiries. The types of banking transactions a customer can carry out are determined by capabilities of the particular banking machine and the programming of the institution operating the machine. Other types of automated banking machines may allow customers to charge against accounts or to transfer funds. Other types of automated banking machines may print or dispense items of value such as coupons, tickets, wagering slips, vouchers, checks, food stamps, money orders, scrip or traveler's checks. For purposes of this disclosure an ATM, an automated banking machine, or an automated transaction machine shall encompass any device which carries out transactions including transfers of value.

Many ATMs are configured to require consumers to enter a Personal Identification Number (PIN) with a keypad of the ATM prior to being granted permission to perform transaction functions with the ATM. The PIN is communicated to a host system by the ATM for purposes of authenticating the identity of the consumer. To prevent the PIN from being stolen by an unauthorized party, ATMs are operative to encrypt the PIN prior to sending the PIN to a host system. For many years Single-DES encryption has been used by ATMs to encrypt PINs using an 8 byte Communication (COM) secret key. Unfortunately, as the cost of computer processing power decreases over time, the risk of the encryption being cracked by unauthorized individuals or entities is increasing. Consequently, there exists a need for new and existing ATMs to include support for a more secure encryption protocol.

PIN information may be encrypted using a COM key known to both the ATM and the host system. The COM key may be securely sent to the ATM from the host system by encrypting the COM key with a terminal master key known to both the ATM and the host system. To maintain the secrecy of a terminal master key, when an ATM is being initially configured for operation, the initial terminal master key is often required to be manually installed by a two-person team at the ATM. Each person of the team has knowledge of only a portion of the information necessary to generate the initial terminal master key. To install the terminal master key successfully, each person must input into the ATM his or her known portion of the terminal master

2

key. Once installed, the inputted portions undergo a mathematical procedure that results in a sixteen (16) character key unknown to either person.

In general, financial institutions or other entities which operate ATMs, are responsible for inserting a unique initial terminal master key in their ATMs. Such entities are also responsible for periodically updating the COM key used for PIN encryption. Although the use of two-person teams to install the initial terminal master key increases the security of the system, in general such a protocol increases the maintenance costs per ATM and is generally cumbersome to manage. As a result, existing keys on ATMs are often not updated on a regular basis, which increases their vulnerability to being cracked. Consequently, there exists a need for a new system and method of installing the initial terminal master key which is less costly and less cumbersome to perform. There is a further need for a new system and method of installing a terminal master key on an ATM which is equally or more secure than a two-person team system.

DISCLOSURE OF INVENTION

It is an object of an exemplary form of the present invention to provide an automated banking machine at which a user may conduct transactions.

It is a further object of an exemplary form of the present invention to provide an automated banking machine which is more secure.

It is a further object of an exemplary form of the present invention to provide an automated banking machine which supports more secure encryption protocols.

It is a further object of an exemplary form of the present invention to provide a system and method for securely installing a terminal master key on an automated banking machine.

It is a further object of an exemplary form of the present invention to provide a system and method for securely and remotely installing a terminal master key on an automated banking machine.

It is a further object of an exemplary form of the present invention to provide a system and method for securely and remotely installing a terminal master key on an automated banking machine with the use of only a single operator at the ATM.

Further objects of exemplary forms of the present invention will be made apparent in the following Best Modes for Carrying Out Invention and the appended claims.

The foregoing objects are accomplished in an exemplary embodiment by an automated banking machine that includes output devices such as a display screen, and input devices such as a touch screen and/or a keyboard. The ATM further includes devices such as a cash dispenser mechanism for sheets of currency, a printer mechanism, a card reader/writer, a depository mechanism and other transaction function devices that are used by the machine in carrying out banking transactions. In the exemplary embodiment the ATM includes at least one computer. The computer is in operative connection with the output devices and the input devices, as well as with the cash dispenser mechanism, card reader and other physical transaction function devices in the banking machine. The computer is further operative to communicate with a host system located remotely from the ATM.

In the exemplary embodiment, the computer includes software programs that are executable therein. The software programs of the ATM are operative to cause the computer to output user interface screens through a display device of the

3

ATM. The user interface screens include consumer screens which provide a consumer with information for performing consumer operations such as banking functions with the ATM. The user interface screens further include service screens which provide a person servicing the ATM with information for performing service and maintenance operations with the ATM. In addition the ATM includes software programs operative in the computer for controlling and communicating with hardware devices of the ATM including the transaction function devices.

In an exemplary embodiment, the ATM includes encryption software and/or hardware which is operative to encrypt PIN information with DES keys securely received from the host system. In one exemplary embodiment, the ATM includes a keypad or encrypting pin pad (EPP) input device which is operative to encrypt a consumer entered PIN within a secure module directly at the keypad. The EPPs of exemplary embodiments are further operative to perform either Single-DES or Triple-DES encryption operations for message authentication, local PIN verification and key transport.

In the exemplary embodiment, the EPP and/or other hardware/software in the computer may be operative to establish a secure communication session between the ATM and a host system environment for transferring terminal master keys to the ATM from the host system. In the exemplary embodiment, individual authentication may be required from both the ATM and the host system to establish the secure communication session. Authentication may be achieved in one exemplary embodiment using digital certificates and digital signatures. Both the ATM and the host system each have individual certificates which may be exchanged between the ATM and host system in a point-to-point communication. The exchanged certificates enable the ATM and the host system to authenticate each other and establish a secure session through a Public Key Infrastructure (PKI). The secure session enables DES keys to be remotely installed and updated on an ATM by a host system. In the exemplary embodiment, the host system may be operative to coordinate the remote key management of DES keys for a plurality of ATMs connected to the host system.

To facilitate authentication and key management, both the ATM and host system may each include a pair of certificates. A first one of the certificates may be used for enciphering and deciphering information sent between the host system and the ATM. A second one of the certificates may be used for generating digital signatures and verifying digital signatures on information passed between the host system and ATM. In the exemplary embodiment, the ATM or a device of the ATM such as an encrypting keypad or encrypting pin pad (EPP) may be manufactured to include an initial set of the certificates which are issued by an initial certificate authority (CA). The exemplary ATM or a EPP device of the ATM may also be manufactured to include the public keys of the initial CA. In addition a host system connected to the ATM may include certificates issued by the initial CA and the public keys of the initial CA.

In the exemplary embodiment, an operator at the ATM may be enabled to cause the ATM to initiate the exchange of certificates between the ATM and the host system. To prevent a possible man-in-the-middle attack on the ATM and host, exemplary embodiments may include the ATM outputting through a display device of the ATM, a one-way hash of the public key of the host system found on each certificate of the host system. The operator may then independently verify that each displayed one-way hash corresponds to a

4

hash of the expected public key found in an authentic certificate of the host system.

In an exemplary embodiment, a financial institution may be operative to replace the initial CA with a new CA and may be operative to remotely cause the ATM and the host system to receive new sets of certificates issued by the new CA.

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 is a schematic view of an exemplary embodiment of an ATM system.

FIG. 2 is a schematic view of a further exemplary embodiment of an ATM system.

FIG. 3 is a schematic view of an exemplary embodiment of a system for remotely transferring terminal keys from a host system to an ATM.

FIG. 4 is a further schematic view of an exemplary embodiment of a system for remotely transferring terminal keys from a host system to an ATM.

FIG. 5 schematically represents an exemplary embodiment of a system and method for transferring a terminal master key from a host system to an ATM.

FIG. 6 schematically represents an exemplary embodiment of a system and method for transferring a terminal master key from a host system to an ATM.

FIG. 7 schematically represents an exemplary embodiment of a format for an unsolicited status message.

FIG. 8 schematically represents an exemplary embodiment of a format for a write command message.

FIG. 9 schematically represents an exemplary embodiment of a format for a solicited status message.

FIG. 10 schematically represents an exemplary embodiment of a format for an operational command message.

FIG. 11 schematically represents an exemplary embodiment of a system and method for installing certificates in an exemplary embodiment of an EPP.

FIG. 12 schematically represents an exemplary embodiment of a system for transferring certificates of a host system to an EPP.

FIG. 13 schematically represents an exemplary embodiment of a system for transferring certificates of an EPP to a host system.

FIG. 14 schematically represents an exemplary embodiment of a system for distributing new certificate for a new certificate authority to an EPP.

FIG. 15 schematically represents an exemplary embodiment of a system for updating original certificates of an EPP with new certificates of the EPP signed by a new certificate authority.

BEST MODES FOR CARRYING OUT INVENTION

Referring now to the drawings and particularly to FIG. 1, there is shown therein a network configuration schematically indicated 10, which includes the automated banking machine apparatus and system of an exemplary embodiment. Network 10 includes a plurality of automated banking machines 12 which in the exemplary embodiment of the invention are ATMs. ATMs 12 are connected to a computer system of a host system schematically indicated 14. Host system 14 includes a computer system that may be operated by the bank or other institution which has primary responsibility for the ATMs 12. Host banking system 14 may be connected to the ATMs 12 through a network 16. Network 16 may include a local or proprietary network or a public network such as the Internet which provides communication

5

between the computer system 14 and the banking machines 12. In one exemplary embodiment the messages are transmitted through the network 16 in the Transmission Control Protocol/Internet Protocol ("TCP/IP") format. In addition, the messages sent through network 16 may be sent in an encrypted or unencrypted form depending on the nature of the system and the security needs of the home bank.

FIG. 2 shows a schematic view of the ATM 12 used in connection with an exemplary embodiment of the invention. ATM 12 may include a touch screen 30. Touch screen 30 includes a display screen which serves as an output device for communication with a user of the machine. Touch screen 30, because it is a touch screen, also serves as an input device for receiving input instructions from a user. Touch screen 30 may be connected through an interface 32 to a computer 34 which is preferably housed within the machine. Alternative exemplary embodiments of the invention may include other output devices such as audio speakers and/or other display screens which may or may not be integrated with input devices. Alternative exemplary embodiments may also include other input devices such as function keys and keyboards which may or may not be integrated with output devices.

Computer 34 may also be in connection with a plurality of transaction function devices 36 which are included in ATM 12. Devices 36 may include for example, a card reader/writer mechanism 38 and a keypad 40. Devices 36 may further include a cash dispenser mechanism 42 which is operative to dispense sheets, which in some embodiments of the invention are currency or bank notes. Exemplary devices 36 may also include a depository 44 for accepting deposits into a secure location in the machine. A receipt printer 46 for providing transaction receipts to customers may also be included among devices 36. A journal printer 48 may also be included among the devices for keeping a hard copy record of transaction information. In other exemplary embodiments other or additional transaction function devices which carry out other transaction functions may be used. Other exemplary embodiments may include fewer transaction function devices. It should be further understood that while the described exemplary embodiment of the invention is an automated banking machine, the principles of the invention may be employed in many types of transaction machines that do not necessarily carry out banking transactions.

Each of the devices may be operatively connected to an internal control bus 50 within the banking machine 12. The control bus 50 outputs the internal messages to the particular devices. Each device may have an appropriate hardware interface which enables the particular device to operate to carry out its respective function in response to the messages transmitted to it on control bus 50. Card reader/writer 38 may have a hardware interface schematically shown as 52. Hardware interfaces 54, 56, 58, 60 and 62 may be respectively operative to connect key pad 40, cash dispenser mechanism 42, depository mechanism 44, receipt printer mechanism 46 and journal printer mechanism 48 to the control bus 50.

Computer 34 may have several software programs that are executable therein. In an exemplary embodiment these software programs may include a device interfacing software portion generally indicated 64. Device interfacing software portion 64 may include a software device interface 66 that communicates electronic messages with the control bus 50. The device interface software portion 64 may also include a device manager 68. The device manager may be operative to manage the various devices 36 and to control their various

6

states so as to be assured that they properly operate in sequence. In an exemplary embodiment, the device manager may also be operative to coordinate device objects in the software so as to enable operation of the devices by at least one object-oriented program 70. The object oriented program portion 70, for example may include an application written in the JAVA® language by Sun Microsystems or an application designed to operate according to Microsoft's .Net platform. Program 70 may work in conjunction with the device manager to receive object-oriented JAVA® or .NET messages which cause the devices to operate, and to transmit device operation messages indicative of a manner in which devices are operating and/or are receiving input data.

The device interfacing software portion 64 in the described exemplary embodiment may operate on computer 34 and may communicate through a physical TCP/IP connection 72 with the network 16. The physical connection may be analog dial-up, serial port, DSL, ISDN connection or other suitable network connection. In the configuration of the system as shown, device interfacing software portion 64 may communicate at the IP address of computer 34 and at an IP port or socket indicated 74 that is different from the other software applications. In other embodiments of the invention, device interfacing software portion 64 may operate in a different computer than the other software applications of the invention.

In further exemplary embodiments, the device interfacing portion 64 may also be based on an open standard platform such as WOSA/XFS (Windows Open Services Architecture/ eXtensions for Financial Services) or J/XFS (Java/eXtensions for Financial Services). Such platforms include an open XFS manager which provides a uniform API for communication with the devices 36. When using an XFS manager, the device interfacing portion may communicate with the hardware interfaces 52, 54, 56, 58, 60 and 62 through software components such as service provider (SP) interfaces supplied by the vendors of the devices 36.

It should further be understood that although in this described exemplary embodiment the device interfacing portion 64 may be software, in other embodiments of the invention all or portions of the instruction steps executed by software portion 64 may be resident in firmware or in other program media in connection with one or more computers, which are operative to communicate with devices 36. For purposes of the invention all such forms of executable instructions shall be referred to as software.

Other software may also operate in computer 34. This software may include interface applications 75 which are operative to output interface screens through the output device 30 which provide information and instructions to consumers and/or operators for operating the ATM 12. In one exemplary embodiment the interface applications may include software for handling mark up language documents. In the exemplary embodiment the interface applications may include HyperText Markup Language (HTML) document processing software such as a browser, schematically indicated 76. In this described exemplary embodiment of the invention, the HTML document handling software includes a browser provided by Netscape®. However, in other embodiments other HTML document handling and communicating software and browser software, such as Internet Explorer™ from Microsoft, may be used. It should be understood that in some exemplary embodiments browsers which process markup language documents to provide visible and/or audible outputs as well as other outputs, as well as browsers which do not provide human perceivable out-

puts, may be used. Browser 76 may communicate in computer 34 at an IP port indicated by 78.

In an exemplary embodiment, the browser 76 may be in operative connection with JAVA® environment software 80 which enables computer 34 to run JAVA® language programs. However, other exemplary embodiments may use different types of software programs including Microsoft NET applications and proprietary and platform specific terminal control software.

The JAVA® environment software 80 enables computer 34 to execute instructions in JAVA® script, schematically indicated 82. The instructions that are executed by the computer in JAVA® script may be embedded JAVA® script commands that are included in the HTML documents or other markup language documents which are received through the browser 76. The browser 76 in connection with the JAVA® environment software 80 which executes instructions in the embedded JAVA® script 82, serve as an HTML document handling software portion for transmitting and receiving HTML documents and TCP/IP messages through the IP port indicated by 78.

Computer 34 may also have executable software therein having a device application portion 84. The device application portion 84 may contain executable instructions related to operation of the devices 36. In one exemplary embodiment of the invention, the device application portion may include a plurality of JAVA® applets. In the described embodiment the applets include programs operable to control and keep track of the status of the devices with which they are associated. Certain applets may be operable to configure the browser to communicate messages. Certain applets may manage security and authenticate entities that use the ATM. It should be understood that this approach is exemplary and in other embodiments other approaches may be used. For example, other embodiments may use .Net components and objects rather than or in addition to JAVA® applets.

In the described form of the invention, JAVA® applets may be associated with functions such as enabling the card reader mechanism, notifying the browser when a user's card data has been entered, operating the receipt printer mechanism, operating the journal printer mechanism, enabling the customer keyboard and receiving data input through the keyboard, operating the sheet dispenser mechanism, operating the depository, navigating to document addresses, timing device functions, verifying digital signatures, handling encryption of messages, controlling the mix of bills dispensed from multiple cash dispenser mechanisms, calculating foreign exchange, and ending a transaction and instructing the browser to return to communication with a server. Of course, in other embodiments, other applets or components may be used to control devices and use data to carry out various desired functions with the machine. The device application portion 84 may communicate in the computer 34 at an IP port indicated 86.

In the described embodiment of the invention, the device application portion 84 of the software may not communicate its messages directly to the device interfacing software portion 64. However, it should be understood that some embodiments of the invention may provide for the device application portion 84 to directly communicate device operation messages to the device program 70. This may be done either internally using TCP/IP, by delivery of messages in a conventional manner through a queue established in the operating system of the computer that is associated with the software that interfaces with the devices, or by direct call to this software.

FIG. 3 shows an exemplary embodiment of the ATM 12 in communication through the network 16 with a financial transaction processing system which in this example includes the host system 14. Host system 14 includes at least one server computer and may be operative to keep track of debiting or crediting customers' accounts when they conduct transactions at the automated banking machines. In addition host system 14 may be operative to track transactions for purposes of accomplishing settlements with other institutions who are participants in the system and whose customers conduct transactions at the ATMs 12. In an exemplary embodiment the host system 14 may be operative to communicate messages to the ATM 12 through network 16 using a secure socket connection ("SSC") so as to minimize the risk of interception of the messages. Of course other techniques, including encryption message techniques, may be used to minimize the risk of interception of the messages. It should be understood that the make of ATM 12 is exemplary and other types of ATMs may be used with exemplary embodiments.

In the exemplary embodiment messages sent to the ATM 12 may include the instructions and information for the ATM to verify that the messages it receives are genuine. This may include digital signatures which when transferred using public key or private key encryption techniques verify the messages as genuine. The machine checks to be sure the signature in the messages received from the host system or another system corresponds to the digital signature for that address stored in memory, and enables operation with the transaction devices, such as the cash dispenser 42, or the keypad 40 only when such correspondence is present. Of course various approaches to verifying and encrypting messages may be used in various embodiments. As used herein signatures or signed records encompass any indicia which is included in or is derivable from a record, such as a message or document which is indicative that it is authorized.

When performing transactions for a consumer, an exemplary embodiment of the interface application 75 may be operative to prompt a consumer to input his/her Personal Identification Number (PIN) using an input device such as keypad 40 of the ATM 12. The exemplary embodiment of the ATM 12 includes encryption software and/or hardware which is operative to encrypt PIN information with a Communication (COM) secret key and a corresponding encryption algorithm and protocol. Examples of encryption algorithms and protocols which an exemplary embodiment may use to encrypt PIN information include symmetric cryptography algorithms such as Single-DES encryption and double-length key Triple-DES encryption. In other alternative exemplary embodiments, other symmetric or asymmetric cryptography algorithms and protocols may be used.

When the exemplary embodiment of the ATM 12 is initially configured to perform transactions with the host system 14, a communication (COM) key 100 may be securely sent from the host system 14 to the ATM 12 through the network 16. To prevent the COM key 100 from being stolen by an unauthorized third party, the COM key may be encrypted with a terminal master key 102 known to both the host system and the ATM. In the exemplary embodiment the terminal master key 102 may be a DES secret key, however in alternative exemplary embodiments the terminal master key may correspond to the one or more encryption keys for use with other symmetric or asymmetric encryption algorithms and protocols.

As discussed previously, a current practice for installing the terminal master key on an ATM includes having a two-person team manually input two different key compo-

nents which are used by the ATM to construct the terminal master key. The described exemplary embodiment may be operative to install the terminal master key on an ATM remotely from the host system without the use of a two-person team.

FIG. 4 shows a schematic view of an exemplary embodiment of an ATM 200. ATM 200 includes a keypad 202. The keypad 202 includes an EPP 204 which may be operative to perform the encryption of inputs through the keypad and the encryption/decryption of information being sent in messages between the ATM and a host system. For example in exemplary embodiments, the EPP may be operative to encrypt an input such as an inputted PIN using the COM key 206. The EPP 204 of the exemplary embodiment may further be operative to perform steps necessary to securely acquire the COM key 206 from the host system 210 using a terminal master key 208. In addition, the exemplary embodiment of the EPP 204 may be operative to perform steps necessary to securely acquire the terminal master key 208 from the host system 210.

To securely transfer the terminal master key 208 from the host system 210 to the ATM 200, the exemplary ATM 200 is operatively programmed to cause the EPP 204 to establish a secure communication session, socket, and/or channel 214 between the ATM 200 and the host system 210 that may be used to securely transfer the terminal master key 208 through a network 222. The exemplary ATM 200 may include a service software application 212. The service software application 212 may be operative responsive to commands inputted into the ATM 200 by a single operator to cause the ATM 200 to establish the secure communication session 214 for securely transferring the terminal master key 208 to the EPP 204.

In the exemplary embodiment, individual authentication may be required from both the ATM 200 and the host system 210. Authentication may be achieved in one exemplary embodiment using certificates and a Public Key Infrastructure generally indicated 201. In this described exemplary embodiment, both the ATM 200 and the host system 210 each are associated with their own digital certificates 218, 220. The secure communication session 214 may be initiated by exchanging the certificates 218 of the host and the certificates of the ATM 220 between the ATM 200 and the host system 210. In one exemplary embodiment, the certificates 218, 220 may be authenticated by both the ATM 200 and the host system 210 using a public key 232 of a trusted certificate authority (CA) 230.

Once the certificates 218, 220 have been exchanged and authenticated, the exemplary embodiment of the ATM and host system may pass encrypted and digitally signed information between them. Such information for example may include signed messages, encrypted secret keys, updated CA public keys, and updated certificates. As shown in FIG. 4 the exemplary ATM 200 and host system 210 may be further operative to use the exemplary PKI system 201 to securely transfer the terminal master key 208 to the ATM 200. This may be achieved in one exemplary embodiment by having the host system 210 encrypt the terminal master key 208 using a public key associated with at least one certificate 220 of the ATM. The host system 210 may then send a digitally signed message to the ATM 200 which includes the encrypted terminal master key 216. In the exemplary embodiment, the ATM 200 may be operative to decrypt the encrypted terminal master key 216 using a corresponding private key of the ATM 200. In addition the ATM 200 may be operative to authenticate the digital signature of the host system using a public key from one the certificates 218 of

the host system. Using this described exemplary process, an exemplary host system may be operative in accordance with its programming to coordinate the remote key management of terminal master keys for a plurality of ATMs 200 connected to the host system.

When certificates are initially exchanged between the ATM 200 and the host system 210, there exists a possibility that an unauthorized entity may perform a man-in-the-middle hacking attack to uncover information being passed between the ATM and host system. During such an attack the unauthorized entity may simultaneously impersonate both the ATM and the host system by exchanging imposter messages for the original messages being transferred between the ATM and host system. To reduce the risk of this type of attack, the service software application 212 may be operatively programmed to cause the ATM 200 to display through a display device, a one-way hash or digest of the public key of the host system found on the certificate 218 of the host system. The exemplary one-way hash of the public key of the host system may be calculated by the exemplary ATM 200 using a one-way hash function such as RD5 or SHA-1. The operator may then independently verify that the displayed one-way hash is identical to a one-way hash of the public key of the host system known by the operator to correspond to an authentic certificate of the host system.

In the exemplary embodiment, to facilitate both authentication and key management, the host system 210 may include two certificates 218 and the ATM 200 may include two certificates 220. A first one of the certificates may be associated with a first set of private/public key pairs which are used for encrypting and deciphering the terminal master key and other information sent between the host system and the ATM. A second one of the certificates may be associated with a second set of private/public key pairs used for signing and verifying digital signatures on information passed between the host system and the ATM. In the exemplary embodiment, the EPP 204 of the ATM 200 may be manufactured to include the initial set of certificates 220 of the ATM stored therein. Such certificates 220 of the ATM which may be stored in a memory of the EPP 204 are issued by the CA 230. The certificates 218 of the host system may also be issued by the CA 230. However, it is to be understood that in alternative exemplary embodiments the certificates 218, 220 may be issued by different certificate authorities.

In the exemplary embodiment, the EPP 204 may include the necessary processing capabilities and programming to validate/authenticate the certificates 218 received from the host system 210 by validating/authenticating the digital signature of the CA 230 found on the certificates 218 of host system 210. In the exemplary embodiment, the EPP 204 may be manufactured to include the public keys 232 of the CA 230. The public keys 232 of the CA may be used by the EPP 204 to validate/authenticate the digital signatures of the CA found on the certificates of the host 218. Likewise, the host system 210 may be operative to validate/authenticate the certificates 220 of the ATM using the public keys 232 of the CA.

In exemplary embodiments, the terminal master key may be transferred between the host and an ATM using a remote key transport process based on protocols such as the key transport mechanism 5 of ISO/IEC 11770-3 and the three-pass authentication mechanism of ISO/IEC 9798-3. These protocols may be used to transfer two shared secret keys in three passes and provide mutual entity authentication and key confirmation.

In exemplary embodiments, the EPP may be constructed so as prevent the secret encryption keys stored therein from

being retrieved from the EPP by an unauthorized user, entity, software program, hardware device, or other probing or sniffing device. Exemplary embodiments of the EPP may further be operative to destroy and/or delete the secret keys from the memory of the EPP in response to the EPP being tampered with. For example, an exemplary embodiment of the EPP may destroy all or portions of the EPP memory in response to the packaging or outer enclosure of the EPP being opened or altered.

FIG. 5 shows a schematic view of system and method by which a single operator at an ATM 302 may initiate the process of transferring a terminal master key to the ATM 302 from the host system 304. This method comprises a plurality of messages 306, 308, 350 being sent between the ATM and the host system which establish a secure communication session, socket, and/or channel 300 between the host system 304 and the ATM 302 which is used to transfer the terminal master key across a network. In this exemplary embodiment, a modified key transport mechanism may be employed which is based on the ISO/IEC 11770-3 and ISO/IEC 9798-3 protocols and which provides unilateral key transport from the host system to the ATM. In this described exemplary embodiment, ATM 302 may enable a single operator to input a command through an input device of the ATM which causes the ATM to initiate the remote transfer of a terminal master key to the ATM. In exemplary embodiments the key transfer may also be initiated by the host system.

In the exemplary embodiment, the ATM 302 and/or an EPP 303 of the ATM may generate a random number (R-ATM) in response to receiving the input from the operator. The random number (R-ATM) may be sent by the ATM 302 to the host system 304 as part of at least one message 306 which may include for example an unsolicited status message or other types of messages capable of being sent by an ATM to a host system. In this described exemplary embodiment, certificates of the ATM and the host system may have been previously exchanged with each other as will be discussed below. However, in an alternative exemplary embodiment, if certificates of the ATM have not yet been exchanged with the host system, the exemplary ATM 302 may be operative to include a certificate 320 associated with encipherment/decipherment of the ATM/EPP and a certificate 326 associated with signature/verification 326 of the ATM/EPP with the message 306 at this time.

FIG. 7 shows an example format for the unsolicited status message in a Diebold 91X ATM message protocol environment that may be used for message 306. Here the random number (R-ATM) may be stored in the buffer data field 307 of the unsolicited status message. The status field 305 may include data which indicates that the unsolicited status message corresponds to a request to initiate the process of transferring the terminal master key.

In response to receiving the message 306 from the ATM, the exemplary host system may be operative to generate and return to the ATM at least one message 308 including for example a write command message or other types of message that an ATM is capable of receiving from a host system. The message 308 from the host system includes a terminal master key (TK) encrypted within an Encipherment Key Block (EKB). In the exemplary embodiment, the host system may generate the Encipherment Key Block (EKB) by encrypting the terminal master key (TK) and identifying data associated with the host system such as a host distinguishing identifier (I-Host) using a public encipherment transformation associated with the ATM and/or EPP of the ATM. The host distinguishing identifier (I-Host) may correspond to a unique number, name or other indicia which is

associated with the host 304. In the exemplary embodiment the public encipherment transformation associated with the ATM/EPP may include encrypting the information (TK and I-Host) using an encipherment public key 322 associated with the encryption/decryption certificate 320 of the ATM/EPP.

In addition to sending the encrypted terminal master key (TK) and host distinguishing identifier (I-Host), the host system may be operative to send as part of the message 308 a random number generated by the host (R-Host), the random number received from the ATM (R-ATM), and identifying data associated with the ATM such as an ATM distinguishing identifier (I-ATM). The ATM distinguishing identifier corresponds to a unique number, name or other indicia associated with the ATM 302 or the EPP 303 of the ATM.

In the exemplary embodiment, the message data 309 corresponding to the random number generated by the host system (R-Host), the random number received from the ATM (R-ATM), the ATM distinguishing identifier (I-ATM), and the Encipherment Key Block (EKB) may be digitally signed by the host system 304 to form a digital signature 310 using a private signature transformation associated with the host system. In the exemplary embodiment the private signature transformation associated with the host system may include signing the message using a signature private key 342 of the host system.

The resulting signed message 311 may use the PKCS #7: Cryptographic Message Syntax Standard format. The message syntax may use Abstract Syntax Notation One (ASN.1) with Basic Encoding Rules (BER) and Distinguished Encoding Rules (DER). In exemplary embodiments where the message of the host system is being transmitted over a 7-bit ASCII network such as in a Diebold 91X ATM message protocol environment, the binary output of the Abstract Syntax Notation One (ASN.1) may be converted to 7-bit ASCII for transmission within the write command message. In an exemplary embodiment an encoding algorithm such as Base64 encoding may be used by the host system which is operative to convert octets (bytes) into printable ASCII characters. In other exemplary embodiments other encoding algorithms may be used which are operative to produce 7-bit ASCII from binary.

FIG. 8 shows an exemplary format for a write command message in a Diebold 91X ATM message protocol environment that may be used to transfer the information described as being included in the message 308 being sent to the ATM. Here the write command message 308 corresponds to a 91X Write Command VII message. The key change field 370 of the Write Command VII message may include data which indicates that the write command message corresponds to the remote transfer of a terminal master key. The encrypted and signed message data 311 which includes the terminal master key may be included in the new key data field 372 of the Write Command VII message. Referring back to FIG. 5, in an alternative exemplary embodiment, if certificates of the host system have not yet been exchanged with the ATM, the exemplary host system 304 may be operative to attach certificates 332, 338 of the host system to the message 308.

Once the message 308 is received by the ATM, the ATM and/or the EPP of the ATM may be operative to validate the digital signature 310 of the host system using the public verification transformation associated with the host system. In the exemplary embodiment the public verification transformation associated with the host may include validating the digital signature using a verification public key 340 associated with the signature/verification certificate 338 of

13

the host. A positive validation of the digital signature may indicate that the message 308 from the ATM has not been tampered with prior to being received by the ATM 302. Also a positive validation of the digital signature may indicate that the information in the message 308 originates from the host system and not a third party hacker.

After validating the digital signature 310, the ATM and/or the EPP of the ATM may be operative to verify that the ATM distinguishing identifier data (I-ATM) in the message 308 corresponds to the identity of the ATM 302 and that the random number (R-ATM) in the message 308 corresponds to the original random number (R-ATM) sent to the host system in the message 306. In addition to these validations, the exemplary ATM 302 and/or an EPP 303 of the ATM may be operative to decrypt the Enciphered Key Block (EKB) using the private decipherment transformation associated with the ATM/EPP. In the exemplary embodiment the private decipherment transformation associated with the ATM/EPP includes decrypting the information (TK and I-Host) using a decipherment private key 324 stored in the memory of the EPP.

Decrypting the Enciphered Key Block (EKB) produces the terminal master key (TK) and the host distinguishing identifier (I-Host). If the decrypted host distinguishing identifier (I-Host) corresponds to the correct host system, the ATM 302 and/or the EPP of the ATM may be operative to accept the terminal master key (TK). In the exemplary embodiment, if the ATM and/or EPP of the ATM has been previously set to use a single-length key such as Single-DES encryption and the new terminal master key (TK) correspond to a double length key, the ATM and/or the EPP of the ATM may be operative to automatically switch to an algorithm which use double-length keys such as double-length key Triple-DES encryption. In addition if the ATM and/or EPP of the ATM has been previously set to use double-length keys and the new terminal master key (TK) correspond to a single length key, the ATM and/or EPP of the ATM may be operative to automatically switch to an algorithm which use single length keys such as Single-DES encryption.

As shown in FIG. 5, the exemplary embodiment of the ATM 302 may be operative to confirm the acceptance of the terminal master key (TK) by sending to the host system 304 at least one message 350 including for example a solicited status message or other types of messages capable of being sent by an ATM to a host system. In this described exemplary embodiment, the message data 349 transferred within the message 350 may include the random numbers (R-ATM, R-Host) and the host distinguishing identifier (I-Host). The message data 349 may be further signed by the ATM and/or the EPP of the ATM using a private signature transformation associated with the ATM/EPP. In the exemplary embodiment the private signature transformation associated with the ATM/EPP may include signing the message using a signature private key 330 stored in the memory of the EPP.

The resulting signed message data 351 may use the PKCS #7: Cryptographic Message Syntax Standard format. As discussed previously, this message syntax may use the Abstract Syntax Notation One (ASN.1) with Basic Encoding Rules (BER) and Distinguished Encoding Rules (DER) which is converted from octet (byte) strings to 7-bit ASCII using Base64 encoding. FIG. 9 shows an exemplary format for a solicited status message in a Diebold 91X ATM message protocol environment which may be used to transfer information corresponding to the described message 350. Here the solicited status message may include the signed message data 351 within a buffer data field 382.

14

In alternative exemplary embodiments, the message 350 may further include a cryptographic check value (CTK) for the terminal master key (TK). The cryptographic check value (CTK) may be generated with the ATM and/or the EPP of the ATM by encrypting the received Terminal Master Key (TK) with a verification number or a random number (text2) using a public encipherment transformation associated with the host system. In the exemplary embodiment the public encipherment transformation includes encrypting the information (TK, text2) using an encipherment public key 334 associated with the encryption/decryption certificate 332 of the host system. In this described alternative embodiment, the random number (text2) may originally have been generated by the host system 304 and sent to the ATM 302 in the Enciphered Key Block (EKB) of the message 308 from the host system.

After receiving the message 350 from the ATM, the host system 304 may be operative to verify the digital signature 352 using the public verification transformation associated with the ATM/EPP. In the exemplary embodiment the public verification transformation associated with the ATM/EPP may include verifying the digital signature 352 using a verification public key 328 associated with the signature/verification certificate 326 of the ATM/EPP. Once the digital signature 352 is verified, the host system 304 may be operative to verify that the distinguishing identifier (I-Host) and the random numbers (R-ATM and R-Host) agree with the corresponding values sent by the host system in the message 308. In the event that any one of the verifications performed by the ATM/EPP and host system fail, the exemplary ATM/EPP and host system may be operative to destroy the terminal master key (TK). Also in the exemplary embodiment, each time this exemplary protocol is executed, a new terminal master key (TK) may be generated.

In alternative embodiments, where the message 350 from the ATM includes a cryptographic check value (CTK), the exemplary embodiment of the host system 304 may be operative to decrypt the cryptographic check value (CTK) using a private decipherment transformation associated with the host system. In the exemplary embodiment the private decipherment transformation may include decrypting the cryptographic check value (CTK) using the decipherment private key 336 of the host system. The resulting decrypted terminal master key (TK) and verification number (text2) may then be verified with the original values sent in the message 308 to further verify the integrity of the secure session 300.

In addition to enabling a single operator at an ATM to initiate the remote transfer of a terminal master key to an ATM, an exemplary embodiment of the present system may further include a transfer of the terminal master key which is initiated by the host system. FIG. 6 shows a schematic view of an exemplary embodiment where the host system 304 may be operative to initiate the transfer of the terminal master key by sending to the ATM 302 at least one message 360 including for example an operational command message or other types of messages an ATM is capable of receiving from a host system. FIG. 10 shows an example of the operational command message for a Diebold 91X ATM message protocol environment that may be used to transfer information corresponding to the described message 360. Here, the operational command message may include a command code field 363 which includes data representative of a command to initiate the remote transfer of terminal key.

Referring back to FIG. 6, the ATM 632 may respond to receiving the message 360, by sending to the host system one or messages 362 including for example a solicited status

message or other messages which an ATM is capable of sending to a host system. The messages 362 may contain the previously described random number (R-ATM). In a Diebold 91X ATM message protocol environment, for example, the data corresponding to the random number (R-ATM) may be included in a buffer data field of the solicited status message. After the host system 304 has received the message 362 with the random number (R-ATM), the messages 308, 350 may be transferred between the host system and ATM as previously described.

In this described exemplary embodiment the encipherment and decipherment transformations may be performed using public and private key pair sets and an asymmetric cryptography algorithm such as the RSA cryptography algorithm. In addition, the signature and verification transformations may be performed using a second set of public and private key pair sets and the RSA cryptography algorithm and a one-way hash function such as MD5 or SHA-1. The RSA modulus for this exemplary embodiment may be 2048 bits. In alternative exemplary embodiments, other encryption and signature protocols and algorithms may be used including DSA, and AES (Rijndael). Also in this described exemplary embodiment, cryptographic calculations of the ATM may be performed by a processor in the EPP 303 of the ATM 302. However, in other exemplary embodiments of the ATM, all or portions of the cryptographic calculations may be performed by other hardware devices, and computer processors of the ATM.

As discussed previously, many ATMs require a two-person team to install a terminal master key. The exemplary embodiment includes upgrading such ATMs to support receiving a terminal master key from a host system. In one exemplary embodiment, this upgrade may be performed by accessing the interior portion of an ATM and removing an existing EPP or other device designed to receive and/or hold a terminal master key constructed from two values manually inputted into the ATM by a two-person team. Once the existing EPP has been removed, an alternate EPP may be installed in its place. The alternate EPP may be operative to receive the terminal master key from the host system according to the previously described protocols. In this described embodiment the alternate EPP is operative to perform encryption, decryption, signature, and verification functions with the public and private keys of the EPP and the public keys associated with the host system and certificate authority stored in the EPP. In one exemplary embodiment, the alternate EPP may further be operative to encrypt inputted PIN values using either single-DES or triple-DES algorithms and protocols.

In an exemplary embodiment, the EPP may be manufactured to include the certificate associated with encipherment/decipherment 320 and the certificate associated with signature/verification 326 stored therein. In this described exemplary embodiment these certificates may be issued by an initial CA and are digitally signed using a primary private key of the initial CA. The certificates 332, 338 of the host system are likewise issued and signed by the initial CA.

In a further exemplary embodiment, the EPP may be manufactured to include a secondary set of the certificates 320 and 326 signed with a secondary private key of the initial CA. The secondary set of certificates is intended to be used as a backup, in the event that the secrecy of the primary private key of the initial CA is compromised. In such cases, the primary set of certificates may be revoked and the secondary set of certificates may be used in their place to sign/verify messages and encipher/decipher messages at the EPP and host system.

The revocation of the primary certificates may be initiated by the host system. The host system may send to the ATMs a secondary set of certificates of the host system signed with the secondary private key of the initial CA. When the exemplary EPP receives a secondary set of certificates from the host system, the EPP may be operative to return its secondary certificates to the host system. In alternative exemplary embodiments, the EPP and host system may initially exchange both primary and secondary sets of certificates. When it is necessary to revoke the primary set of certificates issued by the initial CA, the host system may send a message to each ATM which is representative of a command to stop using the primary certificates and to begin using the secondary certificates.

In addition to storing its own primary and secondary sets of certificates, the exemplary EPP may further be operative to store the primary and secondary public keys of the initial CA. These primary and secondary public keys of the initial CA may be included on respective primary and secondary certificates of the initial CA. The primary and secondary certificates of the CA may be self signed.

FIG. 11 shows a schematic view of an exemplary process 400 that may be used in one exemplary embodiment to configure an EPP 404 with certificates generated by the initial CA 402. Here, the exemplary EPP 404 includes a processor 420, a memory 422 in operative connection with the processor, and a hardware interface 424 in operative connection with the processor. The exemplary processor 420 of the EPP 404 may be operative to communicate with external devices and servers such as a host system, a processor of an ATM, or the initial CA through the hardware interface 424. When the EPP is initially manufactured and/or is re-commissioned, the hardware interface 424 may be connected to a system that is capable of sending messages between the EPP and the initial CA 402. The system for initializing the EPP may include communication hardware, software and a network connection that is in communication with the initial CA and is operative to transfer messages between the EPP and the initial CA. In alternative exemplary embodiments, a system for initializing the EPP may include an ATM and host system that is in operative communication with the initial CA. The hardware interface of the EPP may be operative to communicate with the initial CA through the network interface of the ATM after being installed in the ATM.

When the exemplary EPP 404 is initially powered up, the processor 420 may be operatively programmed to generate a set of encipherment/decipherment public/private key pairs 406 and a set of signature/verification public/private key pairs 408. These keys 406, 408 may be stored by the processor in the memory 422. In the exemplary embodiment these keys 406, 408 may be RSA keys. However, it is to be understood that in alternative exemplary embodiments, keys for other encryption and digital signature algorithms and protocols may be generated.

After the sets of keys 406, 408 have been generated, the processor 420 may be operative to generate two certificate request messages 440 each containing one of the two generated public keys 410, 412 from the generated sets of keys 406, 408. These certificate request messages 440 may be signed using the respective private keys 411, 413 which correspond to the public keys 410, 412 in each certificate request message 440. Also, these messages may include a serial number or other unique identifier of the EPP. In an exemplary embodiment, the certificate request messages may be constructed according to the PKCS #10 Certification Request Syntax Standard format. The exemplary embodi-

ment of the EPP may be operative to output the certificate request messages through its hardware interface 424 for purposes of communicating the certificate request messages to the initial CA.

In response to receiving the certificate request messages 440 the initial CA 402 may be operative to verify that the EPP has possession of the private keys 411 413 by verifying the digital signatures 442 of the messages 440 using the corresponding public key 410, 412 received in the messages 440. After verifying the digital signatures of the messages 440, the initial CA may generate and sign corresponding primary and secondary certificates 114 for each of the two public keys 410, 412 of the EPP. In addition, each of the certificates may include the serial number 415 of the EPP.

The EPP 404 may be operative to receive the newly generated primary and secondary certificates 114 through the hardware interface 424. The EPP may also be operative to receive the primary and secondary certificates 416 of the initial CA through the hardware interface. These certificates 416 of the initial CA may include the primary and secondary public keys 418, 419 of the initial CA and may be self-signed with the private keys corresponding to the public keys 418, 419 of the initial CA.

The EPP is operative to use the public keys 418 and 419 from the certificates 416 of the initial CA to validate the certificates 414 of the EPP. Further, the EPP may verify that the public keys in the certificates 414 of the EPP match the original public keys 410, 412 generated by the EPP. Also, the EPP may verify that the serial number in the certificates matches the original serial number 415 of the EPP.

The EPP 404 may store the received certificates 414 of the EPP in the memory 422. Also, the EPP 404 may store the public keys 418, 419 and/or the certificates 416 of the initial CA 402 in the memory 422. The memory 422 may be comprised of a nonvolatile memory that is operative to preserve the keys 406, 408 and certificates 414, 416 in the memory 422, during periods when the power has been removed from the EPP 404. In the described exemplary embodiment, the public keys 410, 412 of the EPP may each be sent to the initial CA 402 in their own respective certificate request messages 440. However, in alternative exemplary embodiments, both public keys 410, 412 of the EPP may be included in a single certificate request message.

In the exemplary embodiment, the host system 430 may also be operative to communicate with the initial CA 402 using the process previously described with respect to the EPP. The host system may generate its own sets of encipherment/decipherment public/private key pairs and signature/verification public/private key pairs. The host system may then enable one or more certificate request messages to be sent to an initial CA which includes the generated public keys of the host. The initial CA may issue corresponding encipherment/decipherment and signature/verification certificates for the host system. These certificates for the host system may be received by the host system along with the certificates of the initial CA for storage at the host system. In addition the initial CA may further issue both primary and secondary sets of the host certificates, where the first set is signed by the primary private key of the initial CA and the second set is signed by the secondary private key of the initial CA.

In the exemplary embodiment, the primary and secondary sets of certificates for the EPP include the same set of public keys of the EPP. However, in alternative exemplary embodiments, the EPP may generate both a primary set and a secondary set of encipherment/decipherment public/private key pairs and signature/verification public/private key pairs.

The corresponding public keys from the primary set of keys may be forwarded to the initial CA to be integrated into the primary set of certificates of the EPP issued by the CA. The corresponding public keys from the secondary set of keys may be forwarded to the initial CA to be integrated into the secondary set of certificates of the EPP issued by the CA. In addition the exemplary primary and secondary host certificates may likewise be associated with separate sets of primary and secondary sets of encipherment/decipherment public/private key pairs and signature/verification public/private key pairs.

As discussed previously the certificates issued by the initial CA are exchanged between the host system 430 and the EPP 404. The public keys 418, 419 of the initial CA may be used by the host system 430 and the EPP 404 to authenticate the exchanged certificates of the EPP and host system. The exemplary embodiment may use a large key size for the keys 418, 419 of the initial CA so as to make the forging of the certificates much more difficult. However to further increase security, the exemplary EPP and/or the host system may be operative to limit the number of initial certificate exchanges in order to prevent possible future exchanges using forged certificates. In addition, in the exemplary embodiment, initial certificate exchanges may be locked out once a remote terminal master key transfer has been completed. However, prior to the terminal master key transport, multiple certificate exchanges may be permitted between the host and the ATM for testing purposes.

In the exemplary embodiment, the initial certificate exchange between the host system and EPP may be initiated by an operator inputting commands into the ATM, which causes the ATM to communicate with a host system and begin the certificate exchange. FIG. 12 schematically shows the certificate exchange process between an ATM 602 and a host system 606 that is initiated by an operator. Here exemplary embodiments of the ATM 602 may generate and send to the host system 606 at least one message 604 in response to receiving a command from an operator to initiate the certificate exchange. In the exemplary embodiment, the message 604 may include for example an unsolicited status message or other types of messages which an ATM is capable of sending to a host system. In a Diebold 91X ATM message protocol environment, for example, the unsolicited status message may include data in a status field which corresponds to "new network certificate required". The unsolicited status message may also include data in a device ID field which corresponds to the EPP.

In response to receiving the message 604, the host system may return to the ATM, a certificate containing the public key of the host system. In exemplary embodiments the host system may also be capable of initiating the sending of the certificate of the host to the ATM without first receiving a message 604 from the ATM.

As shown in FIG. 12, the host certificate 610 may be included in at least one message 608 being sent to the ATM. Such a message 608 may include for example a write command message or other types of messages which an ATM is capable of receiving from a host system. In a Diebold 91X ATM message protocol environment, for example, the write command message may correspond to a Write Command VII message with data in a key change field that includes the certificate 610 of the host system 606. Such data for the certificate may use the PKCS #7: Cryptographic Message Syntax Standard format. This message syntax may use the Abstract Syntax Notation One (ASN.1) with Basic Encoding Rules (BER) and Distinguished Encoding Rules

(DER) which is converted from octet (8-bit) strings to 7-bit ASCII using Base64 encoding.

In response to receiving the certificate 604 of the host system, the EPP may retrieve the public key of the initial CA from the memory of the EPP and use the retrieved public key to validate the signature on the certificate 610 of the host system. Also as discussed previously, the exemplary ATM may be operative to display a one-way hash of the public key of the host through a display device of the ATM. The ATM may require an operator to enter an input through an input device of the ATM which corresponds to a confirmation that the one-way hash number is valid. To verify the displayed one-way hash number, the operator may compare the displayed one-way hash number to another hash number that the operator independently knows corresponds to the public key of the host. If these described verifications are successful, the EPP may store the certificate of the host system 604 and/or the public key of the host in a memory of the EPP.

Also, the ATM 602 may return to the host system 606 at least one message 612 which includes data that is representative of a successful completion of the certificate transfer. Such a message 612 may include for example a solicited status message or other types of messages which an ATM is capable of sending to a host system. If the verifications of the certificate of the host system are unsuccessful, the message 612 may be returned with data representative of an error. In this described exemplary embodiment the ATM 602 may send messages 612 for each of the certificates (encipherment/decipherment or signature/verification) of the host system. In other exemplary embodiments, the ATM may request both certificates in a single message.

The EPP may also send its certificates to the host system. FIG. 13 schematically shows the certificate exchange process between an ATM 632 and a host system 636 that is initiated by the host system. Here the host system 306 may send to the ATM 632 at least one message 634 which requests one of the certificates of the EPP 638 of the ATM. Such a message 634 may include for example an operational command message or other types of messages which an ATM is capable of receiving from a host system. In a Diebold 91X ATM message protocol environment, for example, the operational command message may include a command code that corresponds to requesting a certificate. The contents of the data field may indicate which public key certificate (encipherment/decipherment or signature/verification) is requested. The ATM 632 may respond by sending at least one message 640 containing the particular certificate 641 of the EPP that was requested by the host system. Such messages 640 may include for example a solicited status message or other types of messages which an ATM is capable of sending to a host system. In a Diebold 91X ATM message protocol environment, for example, the data corresponding to the certificate may be included in the buffer data field. As discussed previously, the data corresponding to the certificate may use the PKCS #7: Cryptographic Message Syntax Standard format. The message syntax may use the Abstract Syntax Notation One (ASN.1) with Basic Encoding Rules (BER) and Distinguished Encoding Rules (DER) which is converted from octet (8-bit) strings to 7-bit ASCII using Base64 encoding.

The host system may validate the digital signature of the EPP using its copy of the public key of the initial CA. In this described exemplary embodiment the host system may send operational command messages for each of the certificates (encipherment/decipherment or signature/verification) of

the EPP of the ATM. In other exemplary embodiments, the host system may request both certificates in a single request message.

As shown in FIG. 14, an exemplary embodiment of the EPP 504 may be manufactured to include the original public keys and/or original certificates 510 of an initial CA 508. As discussed previously, the EPP may further acquire its own initial set of original certificates 506 that are issued by the initial CA 508. Such original certificates may include the respective public encipherment and verification keys generated by the EPP. Also as discussed previously, the EPP may acquire the original public keys and/or certificates 505 of the host system that were issued by the initial CA 508.

As described herein, the EPP may store copies of the certificates of host systems and certificate authorities in a memory of the EPP. However, it is to be understood that in other exemplary embodiments, only the public keys included in the certificates of certificate authorities and host systems may be stored in the EPP. Other contents of the certificates of the certificate authorities and host systems may be discarded after validation of the certificates and storage of the public keys by the EPP.

In exemplary embodiments, the original certificates 506 of the EPP which were signed by the initial CA 508 may be used for terminal master key transfers. However, the institution or other entity operating the ATM 502 with the EPP 504 may wish to replace the initial CA 508 with a new CA 514. As a result, exemplary embodiments of the EPP 504 may further be operative to replace the public keys and/or certificates of the initial CA 508 with new public keys and/or certificates of a new CA 514. FIG. 14 shows an exemplary process 500 for replacing public keys and/or certificates in an EPP 504 of an ATM 502 when the initial or subsequent CA is replaced.

In an exemplary embodiment a host system 512 may initiate the replacement of the original public keys and/or certificates 510 of the initial CA 508 stored in the EPP. An exemplary embodiment of the host system 512 may send to the ATM 502 at least one message 522 including for example a write command message or other types of messages which an ATM is capable of receiving from a host system. The message 522 may include a new certificate 518 of the new CA 514. In embodiments where the EPP requires both primary and secondary certificates of the new CA, the host system may send separate messages 522 for each certificate or may include both primary and secondary certificates in a single message. In the following description of the systems shown in FIGS. 10 and 11, each of the messages 522, 532, 540, 550 may refer to transferring only individual certificates or individual keys in the messages. However, it is to be understood that in other exemplary embodiments, the messages 522, 532, 540, 550 may be constructed to send multiple certificates or keys in each message.

In this described exemplary embodiment the new certificate 518 of the new CA 514 includes the new public key 516 of the new CA. In addition the new certificate 518 may be signed by the initial CA 508 using the private key 520 of the initial CA 508 to form the digital signature 524. In a Diebold 91X ATM message protocol environment, for example, the data corresponding to the new certificate 518 of the new CA may be included in the New Key Data field of a Write Command VII Message. As discussed previously, the data corresponding to the certificate may use the PKCS #7: Cryptographic Message Syntax Standard format. The message syntax may use the Abstract Syntax Notation One (ASN.1) with Basic Encoding Rules (BER) and Distinguished

guished Encoding Rules (DER) which is converted from octet (8-bit) strings to 7-bit ASCII using Base64 encoding.

In the exemplary embodiment, the certificate of the new CA may be further signed by the host system 512 to form the digital signature 526. Upon receipt of the message 522 by the ATM 502, the exemplary EPP 504 is operative to validate the digital signature 524 of the initial CA and validate the digital signature 526 of the host system. In exemplary embodiments, the EPP may validate the digital signature 524 of the initial CA using the original public key and/or original certificate 510 of the initial CA. In addition the exemplary EPP 502 may validate the digital signature 526 of the host system using the original public key and/or original certificate 505 of the host system.

Once the new certificate 518 of the new CA has been validated, the new public key 516 and/or certificate 518 of the new CA may be stored in the EPP for use with authenticating new certificates issued by the new CA. Although the original public key and/or certificate 510 of the initial CA could be discarded after the new certificate 518 has been accepted, exemplary embodiments of the EPP may also retain the original public key and/or certificate 510 for use in re-commissioning the EPP.

After the new public keys 516 and/or new certificate 518 of the new CA 514 have been accepted by the EPP 504, the exemplary ATM 502 may send to the host system 512 a message 582 which indicates that the replacement of the certificates for the CA was successful. Such a message 582 may include for example a solicited status message or other types of messages which an ATM is capable of sending to a host system. When the verification of the new certificate of the CA is unsuccessful, the message 582 returned may indicate an error.

After the EPP has received the new public keys 516 of the new CA 514, the exemplary EPP 504 may require new certificates for the EPP which are signed by the new CA. To enhance security of the system, the exemplary embodiment of the EPP may also generate new public/private encipherment/decipherment and signature/validation key pairs 560 to replace the original key pairs 566.

FIG. 15 schematically shows the process for updating the original public/private key pairs 566 of the EPP and corresponding original certificates 506 of the EPP. Here, the host system 512 may send to the ATM 502 at least one message 584 which includes data representative of a request that the EPP 504 generate new public/private key pairs 506. Such a message 584 may include an operational command message or other types of messages which an ATM is capable of receiving from a host system. In the exemplary embodiment, the message 584 may include a field which specifies which of the encipherment/decipherment or signature/verification keys pairs to update. In other exemplary embodiments, the message 584 may correspond to a request that both types of key pairs to be updated.

Once one of the new key pairs 560 has been generated, the ATM 502 may send to the host system 512 at least one message 586 which includes a certificate request message 532. Such a message 586 may include for example a solicited status message or other types of messages which an ATM is capable of sending to a host system. The certificate request message 532 may request the issue of a new certificate for one or both of the corresponding newly generated public keys 562, 564. In a Diebold 91X ATM message protocol environment, for example, the data corresponding to the certificate request message may be included in the buffer data field of the solicited status message.

The exemplary certificate request message 532 may include one or both of the corresponding newly generated public key 562, 564 of the EPP 504. The certificate request messages 532 may also include the serial number 567 or other unique identifier of the EPP. In this described exemplary embodiment, the new public verification key 564 and the new public encipherment key 562 are sent to the host system in separate certificate request messages responsive to receiving separate messages 584 from the host which individual specify which of the key pairs to update. However, it is to be understood that in alternative exemplary embodiments, both public keys 562, 564 may be sent in a common certificate request message or the message 586 from the ATM may include separate certificate request messages for each public key.

When the certificate request message contains the new verification public key 564, the EPP may sign the certificate request message 532 with the new private signature key 565 to form digital signature 534. Also to authenticate the message to the host, the EPP may sign the certificate request 532 with its original private signature key of the original keys 566 to form the digital signature 535. When the certificate request message contains the new encipherment public key 562 of the EPP, the certificate request message may first be signed with the new decipherment private key 563, and may then be signed with the original decipherment private key from the original keys 566 to authenticate the message with the host.

In an exemplary embodiment the certificate request message 532 may include both the PKCS #10: Certification Request Syntax Standard format and the PKCS #7: Cryptographic Message Syntax Standard format. The messages may use the PKCS #7 Signed-data content for the outer signature (using the original private signature or decryption key). The message may use the PKCS #10 certificate request format for the inner data (using the new private signature or decryption key). Also as discussed previously, the message syntax may use the Abstract Syntax Notation One (ASN.1) with Basic Encoding Rules (BER) and Distinguished Encoding Rules (DER) which is converted from octet (8-bit) strings to 7-bit ASCII using Base64 encoding.

Upon receipt of the certificate request messages 532, the exemplary host system may validate the EPP signatures 534, 535 of the messages. After validating the signatures 534, 535, the host system may cause the new CA 514 to issue an updated certificate 542 which includes the corresponding new public key 562, 564 of the EPP received in the certificate request message 532. The updated certificate 542 may also include the serial number 567 or other unique identifier of the EPP.

The host system may be operative to send a message 540 to the ATM 502 which includes the updated certificate 542. Such a message 540 may include for example write command messages or other types of messages that an ATM is capable of receiving from a host system. In a Diebold 91X ATM message protocol environment, for example, the data corresponding to the updated certificate 542 for the EPP may be included in the new key data field of a Write Command VII Message. In an exemplary embodiment the messages 540 for sending an updated certificate of the EPP may include the PKCS #7: Cryptographic Message Syntax Standard format. The messages may use the degenerate "certificate only" case of the Signed-data content type in which the inner content's data field is omitted and there are no signers.

The exemplary embodiment of the host system is operative to send at least one message 540 with one new certificate 542 of the EPP for each certificate request messages

532. In alternative exemplary embodiments, the host system may send both the new encipherment/decipherment and signature/verification certificates 574, 576 in a single message 540 responsive to receiving one or more certificate request messages 522 that includes both public keys 562, 564 in a single message 586 from the ATM.

Before accepting the new certificate 542, the EPP may verify that the new certificate was signed by the current CA, which in this described embodiment is the new CA 514. In addition the EPP may verify that the public key in the new certificate 542 matches the current public key which in this described embodiment is one of the newly generated public keys 562, 564. Also the EPP may verify that the serial number in the new certificate 542 matches the original serial number of the EPP. If the received new certificate is determined to be valid, the EPP may store it in the memory of the EPP. In addition the EPP may replace the original keys 566 with the newly generated public/private encipherment/decipherment or signature/validation key pairs 560 that correspond to the new certificate 542.

Upon accepting the new certificate 542, the exemplary EPP may return to the host system at least one message 550 which indicates that the new certificate 542 was successfully received. Such a message 550 may include for example a solicited status message 550 or other types of message which an ATM is capable of sending to a host system. In one exemplary embodiment, when the message 550 has been received and represents the acceptance of the new certificate 542, the host system may replace the copy of the original certificate 506 of the EPP stored at the host system with the new certificate 542 of the EPP. In other exemplary embodiments, the original ATM certificates 506 stored at the host system may be replaced with new certificates 542 of the EPP by having the EPP of the ATM 504 send the new certificates to the host system. As discussed previously with respect to FIG. 13, the host system 536 may send a message 634 to the ATM 632 which requests one of the new certificates of the EPP. In response, the EPP 638 may return the requested new certificate in a message 640.

In addition, the exemplary host system 512 may further send to the EPP, a set of new certificates 570 for the host system which are digitally signed by the new CA. This process may be initiated by the host system or an operator at the ATM. As discussed previously with respect to FIG. 12, when an operator initiates the transfer of the updated certificate of the host system to the ATM 502, the ATM is operative to output a one-way hash of the new public key contained in the new certificate of the host through a display device of the ATM which can be independently verified by the operator. If the one-way hash is indicated to be valid by the operator, the EPP may accept and store the new public key and/or the new certificate of the host system in the memory of the EPP.

As with the certificates issued by the initial CA, the EPP 504 and host system 512 are further operative to use the exchanged new public keys and/or new certificates 542, 570 issued by the new CA to perform the steps involved with securely transferring a terminal master key from the host system 512 to the EPP 504. In the exemplary embodiment, the steps described with respect to updating the CA and certificates may be performed a plurality of times whenever there is a requirement to change the CA and/or the public keys associated with the CA.

In exemplary embodiments, the EPP may be decommissioned in the field. Such a decommissioning may include clearing the public and private key pairs of the EPP and any public keys of the host system and a new CA. When the EPP

is re-commissioned it may generate new public and private key pairs. The EPP may then generate new certificate request messages to be sent to the initial CA which include the newly generated public keys and the serial number of the EPP. As discussed previously, the initial CA may issue corresponding primary and secondary certificates for each of the new public keys of the EPP.

Computer software used in operating the automated transaction machines and connected computers may be loaded from articles of various types into the respective computers. Such computer software may be included on and loaded from one or more articles such as diskettes or compact disks. Such software may also be included on articles such as hard disk drives, tapes or ready only memory devices. Other articles which include data representative of the instructions for operating computers in the manner described herein are suitable for use in achieving operation of transaction machines and systems in accordance with exemplary embodiments.

The exemplary embodiments of the automated banking machines and systems described herein have been described with reference to particular software components and features. Other embodiments of the invention may include other or different software components which provide similar functionality.

Thus the new automated banking machine and system and method achieves one or more of the above stated objectives, eliminates difficulties encountered in the use of prior devices and systems, solves problems and attains the desirable results described herein.

In the foregoing description certain terms have been used for brevity, clarity and understanding. However no unnecessary limitations are to be implied therefrom because such terms are for descriptive purposes and are intended to be broadly construed. Moreover the descriptions and illustrations herein are by way of examples and the invention is not limited to the details shown and described.

In the following claims any feature described as a means for performing a function shall be construed as encompassing any means capable of performing the recited function and shall not be deemed limited to the particular means shown in the foregoing description or mere equivalents thereof. The description of the exemplary embodiment included in the Abstract included herewith shall not be deemed to limit the invention to features described therein.

Having described the features, discoveries and principles of the invention, the manner in which it is constructed and operated and the advantages and useful results attained; the new and useful structures, devices, elements, arrangements, parts, combinations, systems, equipment, operations, methods, processes and relationships are set forth in the appended claims.

We claim:

1. A method comprising:

- a) receiving with a host system from an automated banking machine including a cash dispenser, a first public key of the automated banking machine, wherein a first certificate of the automated banking machine includes the first public key of the automated banking machine, wherein the first certificate of the automated banking machine is signed by a certificate authority (CA);
- b) validating with the host system the first certificate of the automated banking machine using a public key of the CA;
- c) receiving with the host system at least one first message from the automated banking machine, wherein the at

25

- least one first message includes data representative of a request to transfer a terminal master key to the automated banking machine;
- d) generating a terminal master key with the host system including generating with the host system first encrypted data using the first public key of the automated banking machine, wherein the first encrypted data includes the terminal master key;
 - e) sending from the host system at least one second message to the automated banking machine, wherein the at least one second message includes the first encrypted data;
 - f) receiving with the host system at least one third message from the automated banking machine, wherein the third message includes data representative of an acknowledgment that the terminal master key included in the first encrypted data has been accepted by the automated banking machine, wherein the at least one third message includes a digital signature of the automated banking machine;
 - g) validating with the host system the digital signature included in the at least one third message using a second public key of the automated banking machine.
2. A method comprising:
- a) receiving with a host system from an automated banking machine including a cash dispenser, a first public key of the automated banking machine, wherein a first certificate of the automated banking machine includes the first public key of the automated banking machine, wherein the first certificate of the automated banking machine is signed by a certificate authority (CA);
 - b) validating with the host system the first certificate of the automated banking machine using a public key of the CA;
 - c) receiving with the host system at least one first message from the automated banking machine, wherein the at least one first message includes data representative of a request to transfer a terminal master key to the automated banking machine;
 - d) generating a terminal master key with the host system including generating first encrypted data using the first public key of the automated banking machine, wherein the first encrypted data includes the terminal master key;
 - e) generating a random number through operation of the host system;
 - f) sending from the host system at least one second message to the automated banking machine, wherein the at least one second message includes the first encrypted data and the random number generated in (e) through operation of the host system;
 - g) receiving with the host system at least one third message from the automated banking machine, wherein the third message includes data representative of an acknowledgment that the terminal master key included in the first encrypted data has been accepted by the automated banking machine, wherein the at least one third message includes a first number;
 - h) verifying through operation of the host system that the random number generated through operation of the host system in (e) corresponds to the first number.
3. A method comprising:
- a) receiving with a host system from an automated banking machine including a cash dispenser, a first public key of the automated banking machine, wherein a first certificate of the automated banking machine

26

- includes the first public key of the automated banking machine, wherein the first certificate of the automated banking machine is signed by a certificate authority (CA);
- b) validating with the host system the first certificate of the automated banking machine using a public key of the CA;
 - c) receiving with the host system at least one first message from the automated banking machine, wherein the at least one first message includes data representative of a request to transfer a terminal master key to the automated banking machine, wherein the at least one first message corresponds to a Diebold 91X Unsolicited Status Message;
 - d) generating a terminal master key with the host system including generating first encrypted data using the first public key of the automated banking machine, wherein the first encrypted data includes the terminal master key;
 - e) sending from the host system at least one second message to the automated banking machine, wherein the at least one second message includes the first encrypted data, wherein the at least one second message corresponds to a Diebold 91X Write Command Message;
 - f) receiving with the host system at least one third message from the automated banking machine, wherein the third message includes data that is representative of an acknowledgment that the terminal master key included in the first encrypted data has been accepted by the automated banking machine, wherein the at least one third message corresponds to a Diebold 91X Solicited Status Message.
4. A method comprising:
- a) sending with a host system at least one first message to an automated banking machine including a cash dispenser, wherein the at least one first message includes data representative of a request to send a first certificate of the automated banking machine to the host system;
 - b) receiving with the host system the first certificate of the automated banking machine from the automated banking machine, wherein the first certificate of the automated banking machine includes a first public key of the automated banking machine, wherein the first certificate of the automated banking machine is signed by a certificate authority (CA);
 - c) through operation of the host system, validating the certificate of the automated banking machine using a public key of the CA;
 - d) receiving with the host system at least one second message from the automated banking machine, wherein the at least one second message includes data representative of a request to transfer a terminal master key to the automated banking machine;
 - e) generating a terminal master key with the host system including generating first encrypted data using the first public key of the automated banking machine, wherein the first encrypted data includes the terminal master key;
 - f) sending from the host system at least one third message to the automated banking machine, wherein the at least one third message includes the first encrypted data.
5. A method comprising:
- a) sending from a host system to an automated banking machine that includes a cash dispenser, at least one first message, wherein the at least one first message includes data representative of a command operative to cause

- the automated banking machine to send at least one second message to the host system, wherein the at least one first message corresponds to a Diebold 91X Operational Command Message;
- b) receiving with the host system the at least one second message from the automated banking machine, wherein the at least one second message includes data representative of a request to transfer a terminal master key to the automated banking machine, wherein the at least one second message corresponds to a Diebold 91X Solicited Status Message;
- c) generating a terminal master key through operation of the host system, including generating first encrypted data using a first public key of the automated banking machine, wherein the first encrypted data includes the terminal master key;
- d) sending from the host system at least one third message to the automated banking machine, wherein the at least one third message includes the first encrypted data, wherein the at least one third message corresponds to a Diebold 91X Write Command Message.
6. A method comprising:
- a) receiving with a host system from an automated banking machine that includes a cash dispenser, at least one first message, wherein the at least one first message includes data representative of a request to transfer a terminal master key to the automated banking machine;
- b) generating a terminal master key through operation of the host system, including generating first encrypted data using a first public key of the automated banking machine, wherein the first encrypted data includes the terminal master key;
- c) sending from the host system at least one second message to the automated banking machine, wherein the at least one second message includes the first encrypted data;
- d) generating a communication key through operation of the host computer, including generating second encrypted data using the terminal master key, wherein the second encrypted data includes the communication key; and
- e) sending from the host system at least one third message to the automated banking machine, wherein the at least one third message includes the second encrypted data.
7. A method comprising:
- a) receiving with a host system from an automated banking machine that includes a cash dispenser, at least one first message, wherein the at least one first message includes data representative of a request to transfer a terminal master key to the automated banking machine, wherein the host system includes a primary public key of a certificate authority (CA), a secondary public key of the CA, at least one primary certificate of the host system signed by the CA, at least one secondary certificate of the host system signed by the CA, and a primary certificate of the automated banking machine signed by the CA, wherein the primary public key of the CA is used to validate the primary certificate of the host system and the at least one primary certificate of the automated banking machine, wherein the secondary public key of the CA is used to validate the at least one secondary certificate of the host system;
- b) sending from the host system, at least one second message to the automated banking machine, wherein the at least one second message includes the at least one secondary certificate of the host system;

- c) receiving with the host system, at least one third message from the automated banking machine, wherein the at least one third message includes a secondary certificate of the automated banking machine;
- d) validating through operation of the host system the secondary certificate of the automated banking machine using the secondary public key of the CA;
- e) generating a terminal master key through operation of the host system including generating first encrypted data using a first public key of the automated banking machine, wherein the first encrypted data includes the terminal master key; and
- f) sending from the host system at least one fourth message to the automated banking machine, wherein the at least one fourth message includes the first encrypted data.
8. A method comprising:
- a) receiving with a host system, at least one first message from an automated banking machine that includes a cash dispenser, wherein the at least one first message includes at least one original certificate of the automated banking machine signed by an initial certificate authority (CA), wherein the at least one original certificate of the automated banking machine includes an original public key of the automated banking machine;
- b) validating the at least one original certificate of the automated banking machine using a public key of the initial CA through operation of the host system;
- c) receiving with the host system a new certificate of a new CA that is signed by the initial CA, wherein the new certificate of the new CA includes a public key of the new CA;
- d) through operation of the host system, signing the new certificate of the new CA with a private key of the host system to produce a digital signature of the host system;
- e) sending from the host system, at least one second message to the automated banking machine, wherein the at least one second message includes the new certificate of the new CA and the digital signature of the host system;
- f) receiving with the host system, at least one third message from the automated banking machine, wherein the at least one third message includes at least one certificate request message; wherein the at least one certificate request message includes a first public key of the automated banking machine, a first digital signature of the automated banking machine, and a second digital signature of the automated banking machine;
- g) through operation of the host system, validating the first digital signature of the automated banking machine using the first public key of the automated banking machine;
- h) through operation of the host system, validating the second digital signature of the automated banking machine using the original public key of the automated banking machine;
- i) providing to the host system a new certificate issued by the new CA for the automated banking machine, wherein the new certificate for the automated banking machine includes the first public key of the automated banking machine;
- j) sending from the host system, at least one fourth message to the automated banking machine, wherein the at least one fourth message includes the new certificate for the automated banking machine;

29

- k) subsequent to (j), receiving with the host system at least one fifth message from an automated banking machine, wherein the at least one fifth message includes data representative of a request to transfer a terminal master key to the automated banking machine; 5
 - l) generating a terminal master key through operation of the host system including generating first encrypted data using the first public key of the automated banking machine, wherein the first encrypted data includes the terminal master key; and 10
 - m) sending from the host system at least one sixth message to the automated banking machine, wherein the at least one sixth message includes the first encrypted data.
9. A method comprising: 15
- a) receiving with a host system from an automated banking machine that includes a cash dispenser, data corresponding to at least one certificate of the automated banking machine, wherein the at least one certificate of the automated banking machine is signed by a certificate authority (CA) and includes a first public key of the automated banking machine; 20
 - b) validating the at least one certificate of the automated banking machine using a public key of the CA;
 - c) receiving with the host system, data representative of a request to transfer a terminal master key to the automated banking machine; 25
 - d) generating a terminal master key;
 - e) generating first encrypted data using the first public key of the automated banking machine, wherein the first encrypted data includes data corresponding to the terminal master key; 30
 - f) sending data corresponding to the first encrypted data from the host system to the automated banking machine; 35
 - g) receiving with the host system at least one message from the automated banking machine, wherein the at least one message includes data representative of an acknowledgment that the terminal master key has been accepted by the automated banking machine, wherein the at least one message includes data corresponding to a digital signature of the automated banking machine; and 40
 - h) validating the digital signature corresponding to data included in the at least one message using a second public key of the automated banking machine. 45
10. The method according to claim 9, wherein prior to step (h) further comprising:
- i) receiving with the host system, the second public key of the automated banking machine from the automated banking machine. 50
11. The method according to claim 10, wherein in step (i) the second public key of the automated banking machine is included in a second certificate of the automated banking machine, wherein the second certificate of the automated banking machine is signed by the CA, further comprising: 55
- j) validating the second certificate of the automated banking machine system using the public key of the CA.
12. A method comprising:
- a) receiving with a host system from an automated banking machine that includes a cash dispenser, data corresponding to at least one certificate of the automated banking machine, wherein the at least one certificate of the automated banking machine is signed by a certificate authority (CA) and includes data corresponding to a first public key of the automated banking machine; 60

30

- b) validating the at least one certificate of the automated banking machine using a public key of the CA;
 - c) receiving with the host system at least one first message, wherein the at least one first message includes data representative of a request to transfer a terminal master key to the automated banking machine; 5
 - d) generating a terminal master key;
 - e) generating a random number through operation of the host system; 10
 - f) generating first encrypted data using the first public key of the automated banking machine, wherein the first encrypted data includes data corresponding to the terminal master key;
 - g) sending from the host system at least one second message to the automated banking machine, wherein the at least one second message includes data corresponding to the first encrypted data and the random number generated through operation of the host system; 15
 - h) receiving with the host system at least one third message from the automated banking machine, wherein the at least one third message includes data corresponding to a first number and data that is representative of an acknowledgment that the terminal master key has been accepted by the automated banking machine; and 20
 - i) verifying that the random number generated through operation of the host system and the first number have a corresponding relationship. 25
13. The method according to claim 12, wherein in step (f) the first encrypted data further includes data corresponding to first identity data corresponding to the host system, wherein in step (h), the at least one third message includes data corresponding to second identity data; further comprising: 30
- j) verifying that the first identity data corresponding to the host system has a corresponding relationship to the second identity data. 35
14. The method according to claim 13, wherein in step (g) the at least one second message further includes data corresponding to a random number generated through operation of the automated banking machine, and further comprising: 40
- k) signing at least portions of the at least one second message using a private key of the host system.
15. The method according to claim 14, wherein in step (h), the at least one third message includes data corresponding to a second number, further comprising: 45
- l) verifying that the random number generated through operation of the automated banking machine has a corresponding relationship with the second number.
16. The method according to claim 14, wherein in step (c) the at least one first message includes data corresponding to the random number generated through operation of the automated banking machine. 50
17. The method according to claim 14, wherein prior to step (h) further comprising: 55
- 1) sending to the automated banking machine data corresponding to a first certificate of the host system, wherein the first certificate of the host system includes data corresponding to a first public key of the host system, wherein the first public key of the host system is capable of being used by the automated banking machine to validate a digital signature of the host system.
18. The method according to claim 17, and prior to step (h) further comprising: 60
- m) sending to the automated banking machine data corresponding to a second certificate of the host system,

31

wherein the second certificate includes data corresponding to a second public key of the host system; wherein in step (h), the at least one third message includes data corresponding to second encrypted data, wherein the second encrypted data includes data corresponding to a key, 5 and further comprising:

- n) determining the key using the second encrypted data;
- o) verifying that the terminal master key corresponds to the key determined in (n).

19. The method according to claim 17, wherein in step (l) the first certificate of the host system is sent in a format which corresponds to the PKCS #7: Cryptographic Message Syntax Standard. 10

20. The method according to claim 14, wherein in step (g) the at least one second message further includes data corresponding to identity data representative of the automated banking machine. 15

21. A method comprising:

- a) receiving with a host system from an automated banking machine that includes a cash dispenser, data corresponding to at least one certificate of the automated banking machine, wherein the at least one certificate of the automated banking machine is signed by a certificate authority (CA) and includes data corresponding to a first public key of the automated banking machine; 25
- b) validating the at least one certificate of the automated banking machine using a public key of the CA;
- c) receiving with the host system at least one first message from the automated banking machine, wherein the at least one first message includes data representative of a request to transfer a terminal master key to the automated banking machine, wherein the at least one first message corresponds to a Diebold 91X Unsolicited Status Message; 30
- d) generating a terminal master key; 35
- e) generating first encrypted data using a first public key of the automated banking machine, wherein the first encrypted data includes data corresponding to the terminal master key; 40
- f) sending from the host system at least one second message to the automated banking machine, wherein the at least one second message includes data corresponding to the first encrypted data, wherein the at least one second message corresponds to a Diebold 91X Write Command Message; and 45
- g) receiving with the host system at least one third message from the automated banking machine, wherein the at least one third message includes data that is representative of an acknowledgment that the terminal master key has been accepted by the automated banking machine, wherein the at least one third message corresponds to a Diebold 91X Solicited Status Message. 50

22. A method comprising:

- a) receiving with a host system at least one first message, wherein the at least one first message includes data representative of a request to transfer a terminal master key to the automated banking machine, wherein the automated banking machine includes a cash dispenser; 60
- b) sending at least one second message to the automated banking machine, wherein the at least one second message includes data representative of a request to send a first certificate of the automated banking machine to the host system; 65
- c) receiving with the host system from the automated banking machine, data corresponding to the first cer-

32

tificate of the automated banking machine, wherein the first certificate of the automated banking machine is signed by a certificate authority (CA) and includes data corresponding to a first public key of the automated banking machine;

- d) validating the first certificate of the automated banking machine using a public key of the CA;
- e) generating a terminal master key;
- f) generating first encrypted data using the first public key of the automated banking machine, wherein the first encrypted data includes data corresponding to the terminal master key; and
- g) sending from the host system at least one second message to the automated banking machine, wherein the at least one second message includes data corresponding to the first encrypted data.

23. The method according to claim 22, wherein in step (c) the first certificate of the automated banking machine is received in a format which corresponds to the PKCS #7: Cryptographic Message Syntax Standard.

24. A method comprising:

- a) receiving with a host system at least one first message, wherein the at least one first message includes data representative of a request to transfer a terminal master key to an automated banking machine, wherein the automated banking machine includes a cash dispenser;
- b) generating a terminal master key;
- c) generating first encrypted data using a first public key of the automated banking machine, wherein the first encrypted data includes data corresponding to the terminal master key;
- d) sending from the host system at least one second message to the automated banking machine, wherein the at least one second message includes data corresponding to the first encrypted data;
- e) generating a communication key;
- f) generating second encrypted data using the terminal master key, wherein the second encrypted data includes data corresponding to the communication key; and
- g) sending from the host system at least one third message to the automated banking machine, wherein the at least one third message includes data corresponding to the second encrypted data.

25. The method according to claim 24, wherein in step (c) the first encrypted data is generated using an asymmetrical cryptography algorithm, and wherein in step (f) the second encrypted data is generated using a symmetric cryptography algorithm.

26. The method according to claim 25, wherein in step (c) the asymmetric cryptography algorithm includes an RSA algorithm, and wherein in step (f) the symmetric cryptography algorithm includes either a Single-DES encryption algorithm or a double-length Triple-DES encryption algorithm.

27. The method according to claim 25, further comprising:

- h) receiving at least one fourth message from the automated banking machine, wherein the at least one fourth message includes data corresponding to third encrypted data, wherein the third encrypted data includes data corresponding to a personal identification number (PIN) input at the automated banking machine,
- i) determining data corresponding to the PIN from the third encrypted data using the communication key; and
- j) authorizing the conduct of a transaction with the automated banking machine responsive to the data corresponding to the PIN.

28. The method according to claim 27, wherein in step (j) the transaction corresponds to a dispense of cash with the cash dispenser of the automated banking machine.

29. A method in which a host system includes a primary public key of a certificate authority (CA), a secondary public key of the CA, at least one primary certificate of the host system signed by the CA, at least one secondary certificate of the host system signed by the CA, and a primary certificate of an automated banking machine signed by the CA, wherein the primary public key of the CA is used to validate the primary certificate of the host system, and the primary certificate of the automated banking machine, wherein the secondary public key of the CA is used to validate the secondary certificate of the host system, wherein the automated banking machine includes a cash dispenser, the method comprising:

- a) sending from the host system, at least first message to the automated banking machine, wherein the at least one first message includes data corresponding to the secondary certificate of the host system;
- b) receiving with the host system, at least one second message from the automated banking machine, wherein the at least one second message includes data corresponding to a secondary certificate of the automated banking machine, wherein the secondary certificate of the automated banking machine includes data corresponding to a public key of the automated banking machine; and
- c) validating the secondary certificate of the automated banking machine using the secondary public key of the CA;
- d) receiving with a host system at least one third message, wherein the at least one third message includes data representative of a request to transfer a terminal master key to the automated banking machine;
- e) generating a terminal master key;
- f) generating first encrypted data using the public key of the automated banking machine, wherein the first encrypted data includes data corresponding to the terminal master key; and
- g) sending from the host system at least one fourth message to the automated banking machine, wherein the at least one fourth message includes data corresponding to the first encrypted data.

30. A method comprising:

- a) receiving with a host system, at least one first message from an automated banking machine that includes a cash dispenser, wherein the at least one first message includes data corresponding to at least one original certificate of the automated banking machine signed by an initial certificate authority (CA), wherein the at least one original certificate of the automated banking machine includes data corresponding to an original public key of the automated banking machine; and
- b) validating the original certificate of the automated banking machine using a public key of the initial CA;
- c) receiving a new certificate of a new CA that is signed by the initial CA, wherein the new certificate of the new CA includes a public key of the new CA;
- d) signing the new certificate of the new CA using a private key of the host system to produce data corresponding to a digital signature of the host system;
- e) sending from the host system, at least one second message to the automated banking machine, wherein the at least one second message includes data corre-

sponding to the new certificate of the new CA signed in (d) and the digital signature of the host system produced in (d);

- f) receiving with the host system, at least one third message from the automated banking machine, wherein the at least one third message corresponds to at least one certificate request message, wherein the at least one certificate request message includes data corresponding to a first public key of the automated banking machine, a first digital signature of the automated banking machine, and a second digital signature of the automated banking machine;
- g) validating the first digital signature of the automated banking machine using the first public key of the automated banking machine;
- h) validating the second digital signature of the automated banking machine using the original public key of the automated banking machine;
- i) causing the new certificate authority to issue a new certificate for the automated banking machine, wherein the new certificate for the automated banking machine includes data corresponding to the first public key of the automated banking machine;
- j) sending from the host system, at least one fourth message to the automated banking machine, wherein the at least one fourth message includes data corresponding to the new certificate for the automated banking machine caused to be issued in (i);
- k) receiving with a host system at least one fifth message, wherein the at least one fifth message includes data representative of a request to transfer a terminal master key to the automated banking machine;
- l) generating a terminal master key;
- m) generating first encrypted data using the first public key of the automated banking machine, wherein the first encrypted data includes data corresponding to the terminal master key; and
- n) sending from the host system at least one sixth message to the automated banking machine, wherein the at least one sixth message includes data corresponding to the first encrypted data.

31. The method according to claim 30, wherein in step (f) the at least one certificate request message includes data corresponding to a serial number of an encrypting pin pad (EPP) of the automated banking machine, wherein in step (i) the new certificate for the automated banking machine includes data corresponding to the serial number of the EPP.

32. The method according to claim 30, and prior to step (f) further comprising:

- o) receiving with the host system, at least one seventh message from the automated banking machine, wherein the at least one seventh message includes data representative of an acknowledgment that the new certificate of the new CA was accepted by the automated banking machine.

33. The method according to claim 30, wherein prior to step (i) further comprising:

- o) sending with the host system, at least one seventh message to the automated banking machine, wherein the at least one seventh message includes data representative of a command to cause the automated banking machine to send the at least one third message.

34. The method according to claim 33, further comprising:

- p) receiving with the host system, at least one eighth message from the automated banking machine, wherein the at least one eighth message includes data represen-

35

tative of an acknowledgment that the new certificate for the automated banking machine was accepted by the automated banking machine.

35. The method according to claim 30, and prior to step (f) further comprising:

- o) sending with the host system, at least one seventh message to the automated banking machine, wherein the at least one seventh message includes data corresponding to at least one new certificates of the host system that were issued by the new CA.

36. A method comprising:

- a) receiving with a host system from an automated banking machine including a cash dispenser, data corresponding to a public key associated with the automated banking machine;
- b) sending from the host system to the automated banking machine data corresponding to a public key associated with the host system;
- c) through operation of the host system, causing first encrypted data to be generated using the public key associated with the automated banking machine, wherein the first encrypted data includes data corresponding to at least one first key;
- d) sending from the host system to the automated banking machine, at least one message including data corresponding to the first encrypted data;
- e) sending from the host system to the automated banking machine, at least one message including data corre-

36

sponding to second encrypted data encrypted using the at least one first key, wherein the second encrypted data includes data corresponding to a second key;

- f) receiving with the host system from the automated banking machine at least one message including data corresponding to third encrypted data encrypted using the second key;
- g) through operation of the host system, determining that a banking transaction is authorized using data corresponding to the third encrypted data received in (f);
- h) responsive to (g) sending from the host system to the automated banking machine, a message including data indicating that the banking transaction is authorized to be performed.

37. The method according to claim 36, wherein in (g) the third encrypted data includes data corresponding to a PIN associated with a financial account.

38. The method according to claim 36, wherein in (f) the banking transaction includes dispensing cash through operation of the automated banking machine.

39. Computer readable media bearing computer executable instructions which are operative to cause at least one computer included in the host system to cause the host system to carry out the method steps recited in claim 36.

* * * * *



US006854645B1

D-1162 R2

(12) **United States Patent**
Somers, Jr. et al.

(10) Patent No.: **US 6,854,645 B1**
(45) Date of Patent: **Feb. 15, 2005**

(54) **AUTOMATED TELLER MACHINE,
SOFTWARE AND DISTRIBUTION METHOD**

(75) Inventors: **Charles H. Somers, Jr.**, North Canton,
OH (US); **Richard A. Steinmetz**, St.
Cloud, FL (US); **Richard P. Brunt**,
Springfield, MA (US); **Kenneth W.**
Zahorec, North Canton, OH (US)

(73) Assignee: **Diebold, Incorporated**, North Canton,
OH (US)

(*) Notice: Subject to any disclaimer, the term of this
patent is extended or adjusted under 35
U.S.C. 154(b) by 11 days.

(21) Appl. No.: **10/349,208**

(22) Filed: **Jan. 21, 2003**

Related U.S. Application Data

(60) Provisional application No. 60/351,257, filed on Jan. 22,
2002.

(51) Int. Cl.⁷ **G06F 17/60**

(52) U.S. Cl. **235/379; 235/381; 235/382;
705/43; 717/174**

(58) Field of Search **235/379, 381,
235/382, 382.5; 902/8, 14, 37, 38, 39, 40,
41; 705/43, 44, 35, 39; 713/100; 717/174;
709/221**

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,836,104 A * 11/1998 Epps 43/122
6,360,255 B1 * 3/2002 McCormack et al. 709/221
6,505,177 B1 * 1/2003 Drummond et al. 705/43
6,520,410 B2 * 2/2003 Putman et al. 235/380
6,672,505 B1 * 1/2004 Steinmetz et al. 235/379
6,676,018 B1 * 1/2004 Trelawney et al. 235/381
6,705,517 B1 * 3/2004 Zajkowski et al. 235/379

2003/0120597 A1 * 6/2003 Drummond et al. 705/43
2003/0120935 A1 * 6/2003 Teal et al. 713/188
2003/0126084 A1 * 7/2003 Drummond et al. 705/43
2003/0141360 A1 * 7/2003 De Leo et al. 235/379
2003/0200435 A1 * 10/2003 England et al. 713/172
2003/0216172 A1 * 11/2003 LeMay et al. 463/29
2004/0010597 A1 * 1/2004 Kirschner et al. 709/228
2004/0050927 A1 * 3/2004 Nozaki et al. 235/379

FOREIGN PATENT DOCUMENTS

JP 9-81416 A * 3/1997
JP 2001-154879 A * 6/2001

* cited by examiner

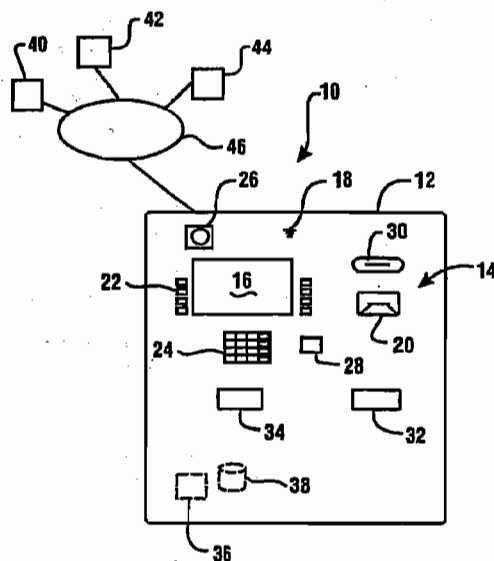
Primary Examiner—Jared J. Fureman

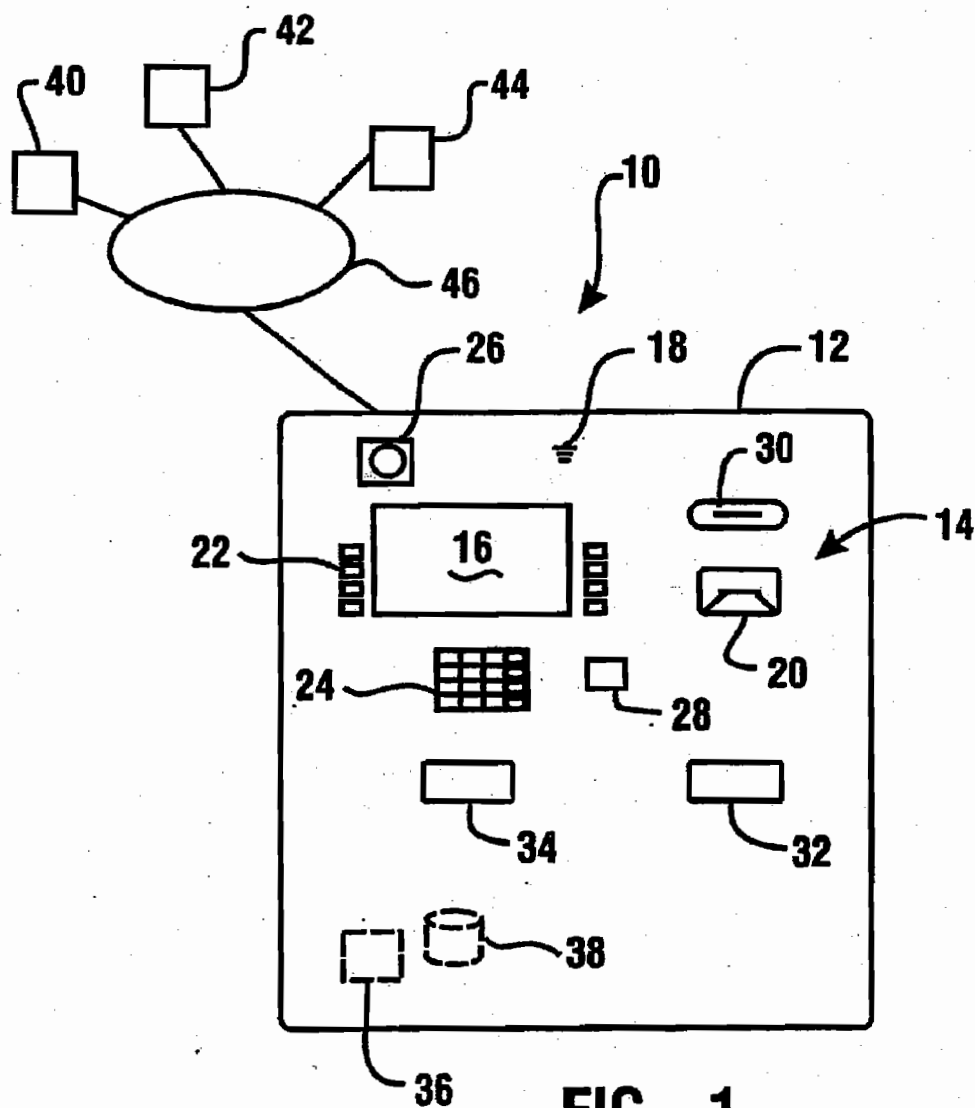
(74) Attorney, Agent, or Firm—Ralph E. Jocke; Christopher
L. Parmelee; Walker & Jocke

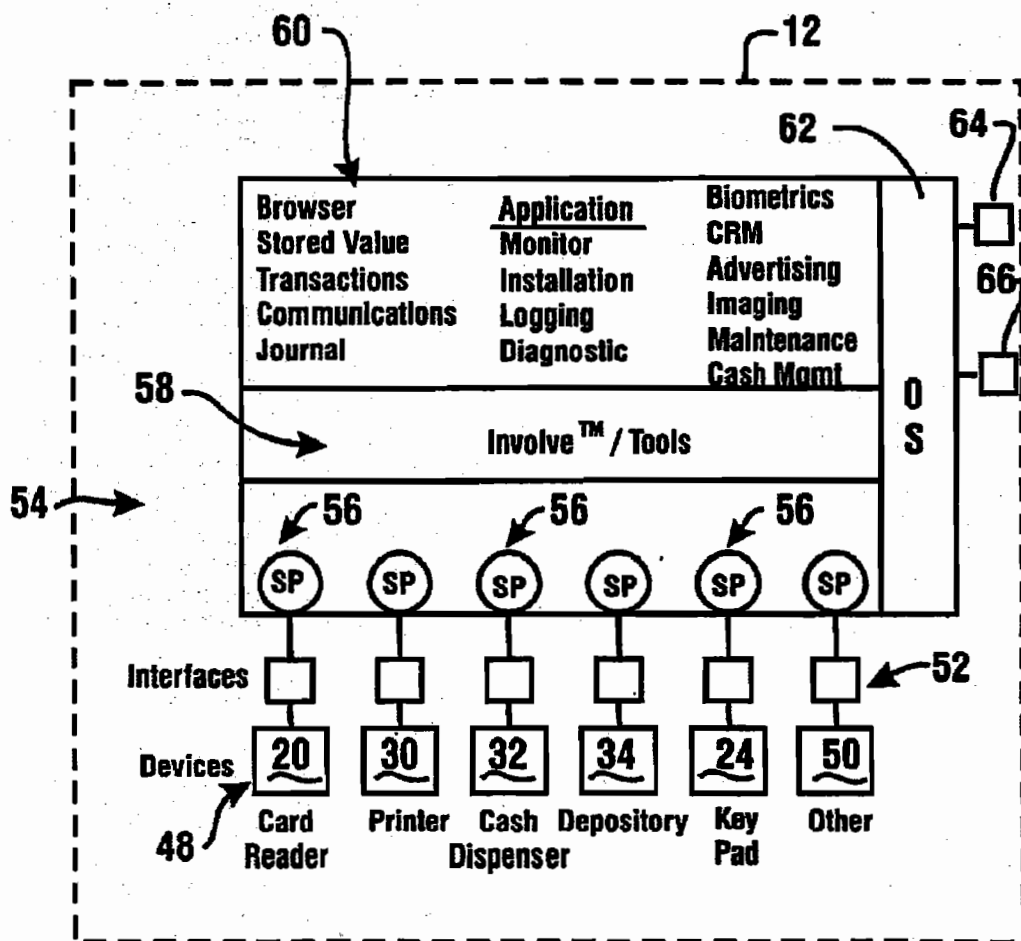
(57) **ABSTRACT**

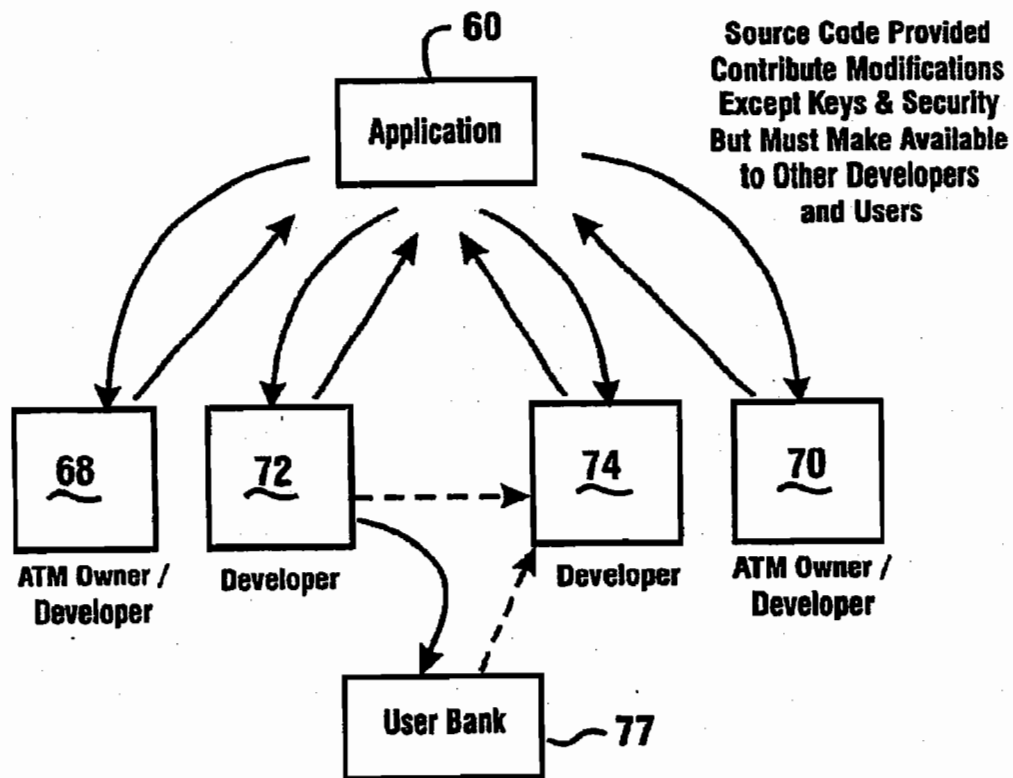
An automated teller machine (12) includes at least one processor (36) which operates to cause transaction function devices (16, 18, 20, 22, 24, 26, 28, 30, 32, 34) to operate to carry out banking transactions for users of the machine. A software environment (54) operates in the processor and includes a hardware independent software application (60) which application may be operated successfully in a plurality of brands of automated teller machine hardware. The automated teller machine verifies that the software application has been authorized by an appropriate authorizing entity before the application is enabled to cause operation of transaction function devices. In some distribution methods the software application is provided in source code form at generally no charge to ATM owners and software developers, who are required to contribute modifications to the entity offering the software, which modifications are further made available to facilitate the development and use of platform independent software applications in automated teller machines.

33 Claims, 7 Drawing Sheets



**FIG. 1**

**FIG. 2**

**FIG. 3**

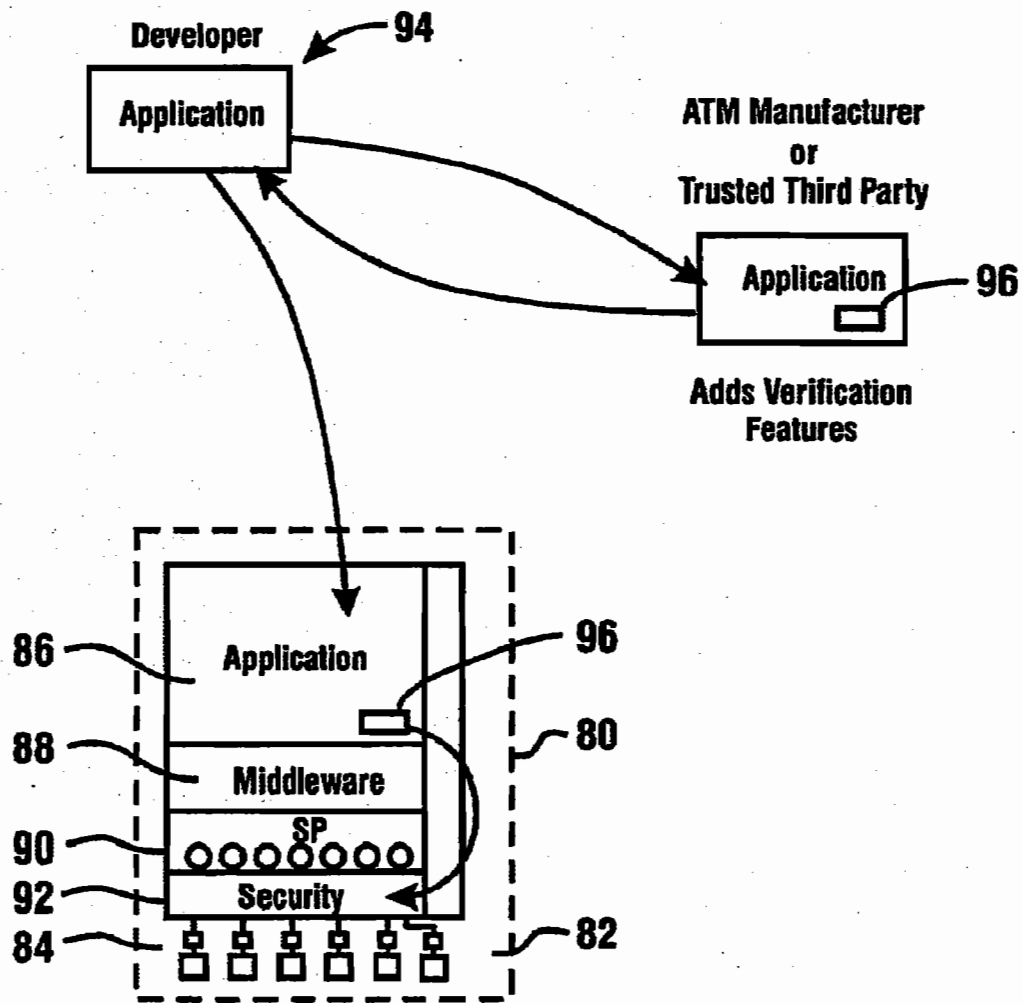


FIG. 4

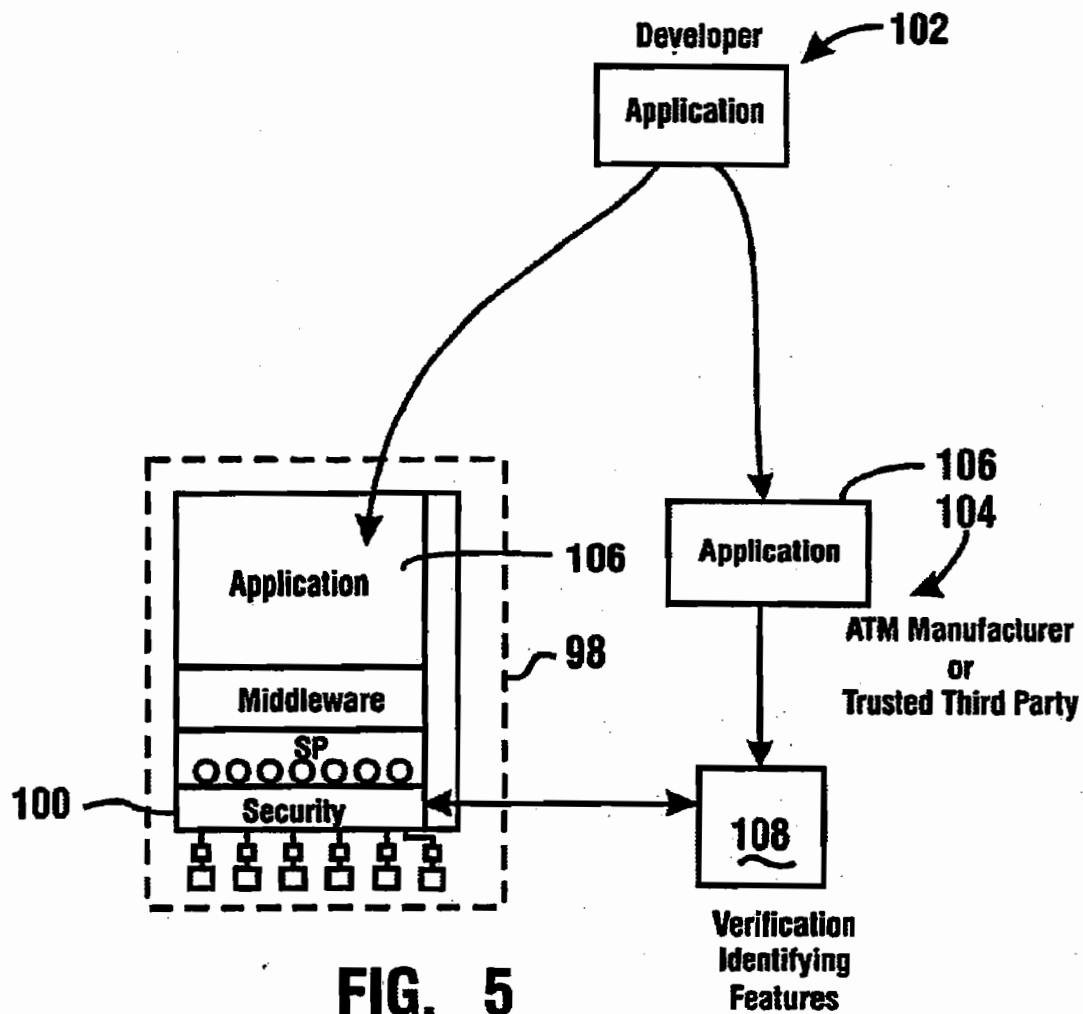
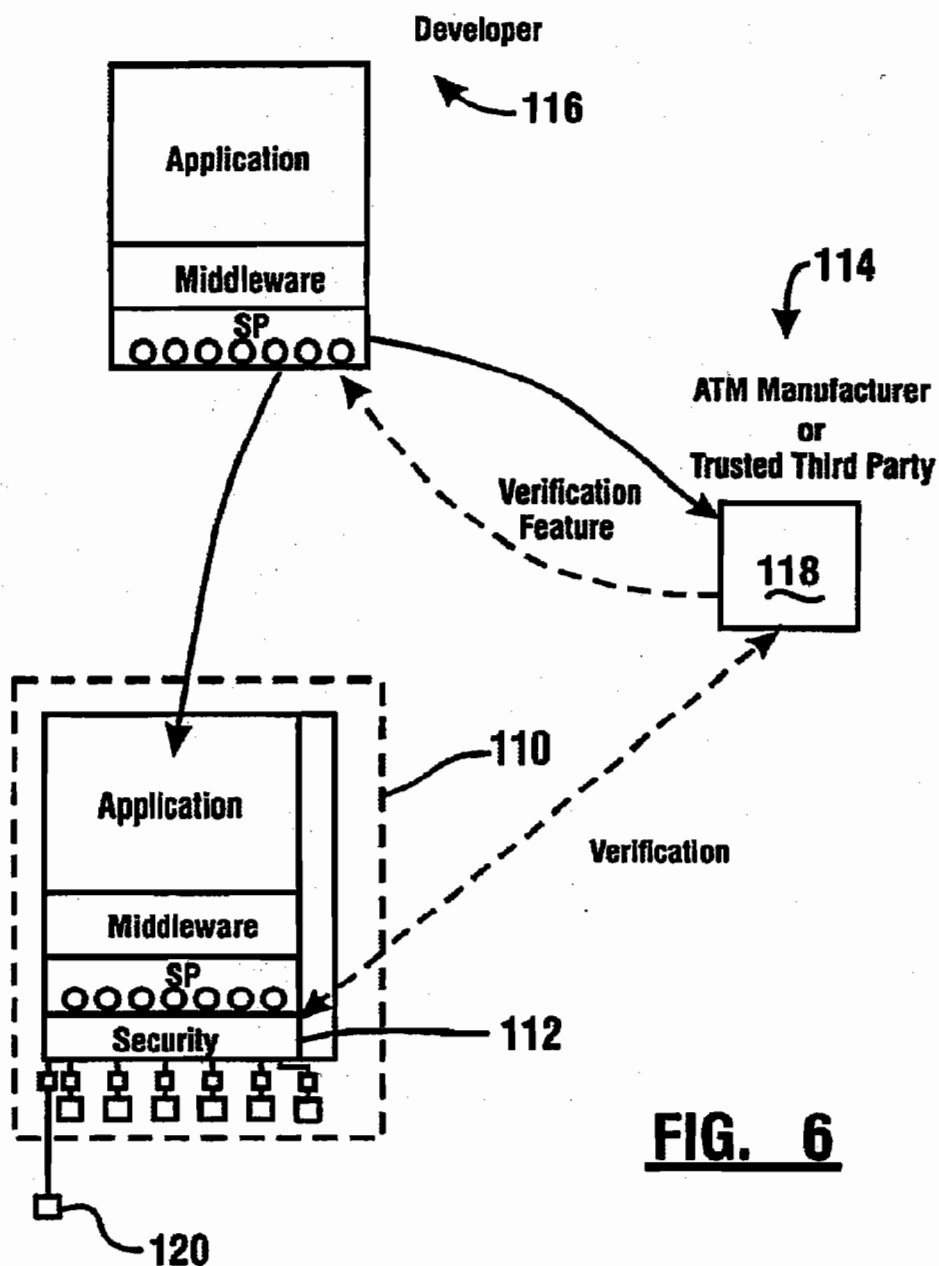


FIG. 5

**FIG. 6**

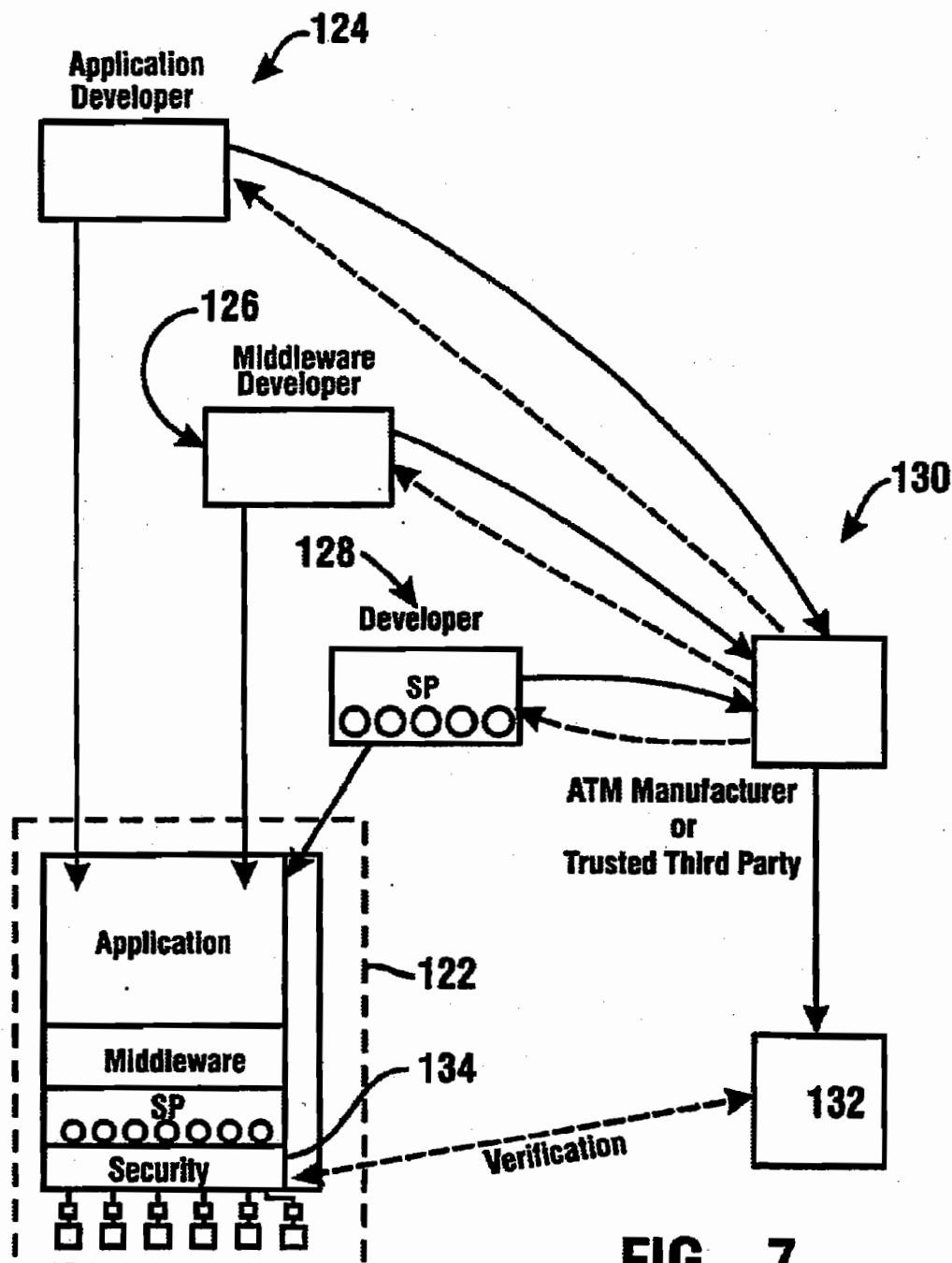


FIG. 7

1

AUTOMATED TELLER MACHINE, SOFTWARE AND DISTRIBUTION METHOD

CROSS REFERENCE TO RELATED APPLICATION

This Application claims benefit pursuant to 35 U.S.C. § 119(e) of Provisional Application Ser. No. 60/351,257 filed Jan. 22, 2002.

TECHNICAL FIELD

This invention relates to automated teller machines. Specifically this invention relates to devices and software used in the operation of automated teller machines and a method for operation and distribution thereof.

BACKGROUND ART

Automated teller machines (ATMs) are known in the prior art. Automated teller machines may be used by consumers to carry out banking and other functions. Such functions may include for example receiving cash, making deposits, checking account balances, cashing checks, printing checks, printing statements, printing money orders and other functions. For purposes of this disclosure an automated teller machine will be considered to include any device operative to carry out one or more types of financial transactions for users of the machine.

Automated teller machines usually include one or more internal processors which carry out software instructions and enable operation of the machine. Presently most automated teller machine software is proprietary to the particular machine manufacturer. As a result the software which causes one manufacturer's automated teller machine to operate will not operate another manufacturer's automated teller machine.

Recently organizations have begun to develop standards related to devices commonly found in automated teller machines. These standards provide a generally uniform set of instructions for operating each particular type of device which is likely to be found in an automated teller machine. For example these standards may provide a generally uniform set of instructions for operating a cash dispenser to dispense a bill. As a result an entity wishing to write software to operate an automated teller machine may theoretically write a suitable software application for controlling the devices in the machine by writing the software application in accordance with the standard. In addition software written in accordance with the standard should be able to operate in automated teller machines made by different manufacturers. An example of such a standard is known as the WOSA-XFS or XFS standard which has been developed by a committee of the CEN. Other standards are also being discussed and developed.

In order for the standards to have greater value, manufacturers of automated teller machines would need to produce software that will enable the devices in their machines to operate in response to the standardized instructions. Software which enables a particular manufacturer's transaction function devices in an ATM to operate in accordance with a standard is referred to in an XFS environment or other standardized environments, as a service provider or SP software. Some manufacturers of automated teller machines have developed SP software for the transaction function devices included in their machines. However, certain manufacturers place restrictions on the availability of their SP software. As a result it is not generally feasible for a software

2

developer to develop a hardware independent software application for operating automated teller machines produced by different manufacturers.

Further, the ability of application developers to develop applications may present issues related to maintaining the proper operation of the ATM. The ability of third party developers unassociated with an ATM manufacturer to write software that can be loaded onto and operate the ATM may present issues as to whether the software loaded on the ATM is authorized as well as whether such a developer has met commitments that they may have related to the manufacturer or other third parties.

A further issue may arise with regard to entities that wish to operate devices in conjunction with an automated teller machine that are not devices for which standard service provider interfaces have been developed and/or devices which require different relationships to other ATM transaction function devices than a device normally associated with such a service provider interface. In such cases it may not be cost effective for an ATM manufacturer to develop or support service provider software for devices that are not normally included in an automated teller machine. As a result the capabilities of automated teller machines to work in conjunction with such external devices may not be developed.

Further issues may arise when software components provided by different entities are installed on an ATM. Uncertainty may arise as to which software component (or transaction function device) is the cause of a malfunction of the ATM.

DISCLOSURE OF INVENTION

There exists a need for a system and method for facilitating the distribution of software for operating automated teller machines and which will make software more readily available to owners of automated teller machines and developers who wish to have a single software application that runs automated teller machines of different manufacturers. There further exists a need for a system and method for assuring that software which has been developed and/or modified by third parties, or that has been installed on ATMs is authorized by the manufacturer of the ATM or other authorizing entity. There further exists a need for assuring that third parties who develop or modify ATM software abide by commitments that they had made to the ATM manufacture, other authorizing entity or the user community in general. There further exists a need for verifying that multiple software components from different sources are authorized to work together on an ATM, and for more readily identifying the source of a malfunction. There further exists a need for a system and method for supporting devices that are not traditionally included in ATMs as adjunct devices to ATMs and to assure that such adjunct devices are authorized and supported.

It is an object of an exemplary embodiment of the present invention to provide a method.

It is a further object of an exemplary embodiment of the present invention to provide a method of distributing automated teller machine software.

It is a further object of an exemplary embodiment of the present invention to provide a method of distributing automated teller machine software that will enhance the ability of owners of automated teller machines to use software that can be run on automated teller machines produced by different manufacturers.

It is a further object of an exemplary embodiment of the present invention to provide a method in which advance-

3

ments in automated teller machine software are shared with the market so as to improve the quality of automated teller machine software.

It is a further object of an exemplary embodiment of the present invention to provide a method for distributing automated teller machine software that preserves heightened security for systems including automated teller machines.

It is a further object of an exemplary embodiment of the present invention to provide an automated teller machine that is operative to verify that software installed thereon has been authorized by an entity associated with the machine.

It is a further object of an exemplary embodiment to provide an automated teller machine which operates to more readily identify the source of malfunctions.

It is a further object of an exemplary embodiment of the present invention to provide an automated teller machine and system that is operative to verify that a plurality of software components installed on an automated machine have been indicated as suitable for operation together.

It is a further object of an exemplary embodiment of the present invention to provide an automated teller machine and method which enables the machine to work in conjunction with an external device not generally operated in an automated teller machine.

Further objects of exemplary embodiments of the present invention will be made apparent in the following Best Modes for Carrying Out Invention and the appended claims.

The foregoing objects are accomplished in a first exemplary embodiment by a method in which an entity develops a hardware independent software application for operating automated teller machines of different manufacturers. This may include for example, a software application that complies with the XFS or other standard. In accordance with the first exemplary method, the entity developing the application then offers to provide the right to use the software to all owners of automated teller machines regardless of brand at no charge.

In accordance with an exemplary form of the method, the entity originally developing the software application authorizes third parties, such as automated teller machine owners or software developers or others, to modify and/or distribute the original and modified forms of the software. The right to modify and/or distribute the software is offered in exchange for such third party's agreement to provide the source code for such modified software to the entity offering the application. The entity offering the application may then further make the modified forms of the software available in the same manner as the original application. In an exemplary embodiment to further assure that the third parties modifying the software make their modifications available, a condition to granting the rights to modify the software includes an obligation to make available the source code for such modified software to any third party upon request.

In some exemplary embodiments in order to assure security of automated teller machine systems, the requirement to provide modifications to the entity originally offering the application and/or to third parties, maybe restricted with regard to security software modifications. Such security software modifications may include modifications as may be specifically defined by agreement, but would normally include only those modifications which if provided and made publicly available may facilitate the compromise of security of an automated teller machine system. In some exemplary embodiments such security software modifications may not necessarily include techniques which rely on specific keys, certificates or other electronic security fea-

4

tures which provide security independent from the software itself and which are unique to the particular user. In one exemplary embodiment however, for security software modifications that are not contributed to the application provider for redistribution to third parties, the entity making such modifications is required to provide a general description of the security modifications made and the name of each entity to which the modified software has been provided. The entity offering the application would then make this information publicly available so that it could be found by third parties.

In addition or in the alternative, exemplary embodiments may require a party making security software modifications that are not contributed to the generally available application, to make the source code for such security modifications available to any user who has received the code or any person or entity that such a user has designated as their agent for receiving the code. This may include for example another developer which a user of such a system wishes to have further modify the software. Of course the obligations to contribute modifications and make available further security software modifications would apply to any subsequent modifications of the code.

In other exemplary embodiments entities requiring modifications to the software application are urged through technological measures to provide the modified forms of the software to the entity offering the original form of the software. This may be done for example, by including in the automated teller machine at least one software verification device that is operative to verify that a copy of the software installed on the machine has been provided to the entity. The software verification device may operate for example, by verifying one or more verification features that are included in the software application by the entity offering the original code after the third party had provided it to the entity. This may include for example, the third party providing the modified software to the entity, and the entity including verification features in the software such as a digital signature, and the entity then providing the software with the digital signature back to the developer or other entity who produced the modified version. In such a system the software verification device in the ATM may operate to read and analyze the digital signature included in the software after it is installed to verify that the signature is a valid signature of the authorizing entity.

In some alternative exemplary embodiments the ATM may include a software verification device that is operative to communicate with a remote computer operated under the auspices of the entity offering the software. In such systems remote communication caused through operation of the software verification device, between the machine and the remote computer is operative to determine that the software installed in the machine has been provided to the entity. This may be done for example, by comparing identifying features of the software in the machine with such features of software deposited with the entity. Such identifying features may include a hash of all or a portion of the software and/or comparing the magnitude of measurable parameters associated with the software and/or other features or combinations thereof. Such communication between the ATM and the remote computer associated with the entity is operative to determine at least one result indicative of the relationship between the identifying features which establishes whether the software has been provided to the entity and which is used by the machine as the basis for allowing or preventing the software from operating at least one device of the machine.

In other exemplary embodiments the principles described may be used to verify that software that is not made generally available for distribution and modification, is authorized by the manufacturer, licensor or other entity associated with the machine. This may include for example situations where an ATM manufacturer, an ATM operator such as a financial institution or other third party commissions an independent developer to produce software to operate an ATM. At least one software verification device may operate in the ATM to verify that the software which has been installed therein is the software that has been provided to or otherwise authorized by the entity. Such approaches may help to assure that independent developers or other third parties do not provide or install unauthorized software on ATMs. As can be appreciated, a requirement that the entity has received the software and in some manner authorized its use before the software will operate on the ATM to carry out at least one type of transaction function minimizes the risk of the use of unauthorized software.

In other exemplary embodiments the principles described herein may be used to facilitate the development of systems in which other devices not normally operated in automated teller machines are nonetheless used as an adjunct thereto. Such adjunct devices may include for example, specialized money order, check or ticket printers which provide special authentication or other types of features on items that they produce. Other devices may include ticket acceptors or token return devices which have special requirements not normally associated with financial transactions. Other devices may include for example, devices which provide goods or services of value such as for example, article rental devices which enable the user to rent or operate an article for a period of time through payment made through the ATM. Other examples may include devices which deliver various types of digital media such as video, music, text or other items. Other examples of devices may include tanning devices, aroma therapy devices, medication dispensing devices, oxygen delivery devices, beverage dispensing devices and other types of devices for which there is an associated financial transaction that can be conducted through a connected ATM.

In some exemplary embodiments entities such as the ATM manufacturer or other entity, may provide the source code of its service provider software to third parties and grant the right to make modifications thereto. Such third parties may develop modified forms of the service provider software so as to enable the support of specialized devices which are not normally included in the ATM. Such specialized device support may facilitate the development and support for such adjunct external devices which the ATM manufacturer may not otherwise support. To assure that the modified forms of the service provider software are suitable, some exemplary embodiments may require that such modified forms of the software be authorized by the entity such as the manufacturer of a machine. This enables the manufacturer of the machine or other entity to certify that the modified form of the software is appropriately suitable for operation in the machine and in the other associated device.

In some further exemplary embodiments multiple items of computer software may be installed in the ATM. In such exemplary embodiments the software verification device may operate to determine that all of such plurality of software items are authorized for operation on the machine by the entity. In addition, the machine may operate to verify that the plurality of software items that are installed on the machine are compatible or otherwise authorized for use together on the machine. Such capabilities are provided so

that the machine will not operate absent a determination that the items are authorized and suitable for use together. Other exemplary embodiments may include software components which operate independently to test the functionality of the component independently of other software components and/or devices.

This may facilitate the identification of a malfunctioning software or hardware component from among a plurality of components that are interdependent in their normal operation. Of course it should be understood that these features and approaches are exemplary and in other features and embodiments other approaches may be used.

The descriptions provided herein are exemplary and all other devices, methods and systems encompassed by any of the claims below are within the scope of the present invention.

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 is a schematic view of an automated teller machine system which may be used to carry out transactions.

FIG. 2 is a schematic view of hardware and software components in an exemplary automated teller machine.

FIG. 3 is a schematic view of a diagram representative of the distribution of software in an accordance with an exemplary embodiment.

FIG. 4 is a schematic view representative of a methodology in which an entity receives ATM software and assures that the software is authorized by the entity through inclusion of verification features in the software.

FIG. 5 is a schematic view of a methodology in which an entity assures receipt and authorizes software by verifying identifying features included in the software.

FIG. 6 is a schematic view of a further alternative methodology which multiple software items are authorized for use on an ATM.

FIG. 7 is a schematic view of a further alternative methodology in which multiple items of software are authorized for use on an ATM, and in which the system verifies compatibility of such multiple software items for use on the ATM.

BEST MODES FOR CARRYING OUT INVENTION

Referring now to the drawings and particularly FIG. 1, there is shown therein an automated teller machine system generally indicated 10. The system includes an automated teller machine 12. Automated teller machine 12 is alternatively referred to herein as an ATM. Automated teller machine 12 of the exemplary embodiment is used by consumers to carry out banking transactions. The exemplary ATM 12 is shown as including thereon a user interface generally indicated 14. User interface 14 includes one or more input devices and output devices. Input devices may be used by the operator of the machine to provide information or instructions to the machine. Output devices include devices for providing information and instructions to a user. In this exemplary embodiment user interface 14 includes an output screen 16 which serves an output device. User interface 14 of the exemplary embodiment further includes a speaker schematically indicated 18 for providing audible outputs to a user.

User interface 14 further includes a card reader schematically indicated 20. The card reader in the exemplary embodiment is operative to read cards or other articles provided to the machine by a user which may include information which

identifies the user, a user's account or other information. User interface 14 further includes function keys 22. Function keys 22 are positioned adjacent to screen 16 and enable a user to select options which may be presented to the user visually through the screen. A further input device in the exemplary embodiment includes a keypad 24. In this exemplary embodiment keypad 24 includes an alphanumeric keypad as well as certain function keys.

The exemplary embodiment also includes an image capture device 26. Image capture device 26 may be operative to capture images of portions of a user. This may include for example capturing images of the user's face for purposes of making a record of the transaction. Alternatively images of a user's face may be analyzed and used for purposes of identifying the user. In alternative embodiments the image capture device may comprise an iris scanner or other biometric reader for purposes of identifying a particular user carrying out a transaction. Other input devices may also be provided on user interface 14. For example a fingerprint reading device 28 is schematically represented. Fingerprint reading devices may be used in some embodiments to read fingerprint data from a user for purposes of identifying a user. It should be understood that fingerprint data, iris scan data or other biometric data may be used in some embodiments as an alternative or additional means for identifying the user. Such means may be used as a substitute for or as a check on data provided by a user to a card reader or other method for purposes of verifying the user's identity or accounts.

The exemplary ATM 12 further includes in its user interface, a receipt printer 30. In the exemplary embodiment receipt printer 30 is operative to provide users with receipts or other data related to transactions which are conducted at the machine. It should be understood that in other embodiments different or additional types of output devices may be provided including printers that provide users with statements or other documents.

The exemplary ATM 12 further includes a cash dispenser schematically indicated 32. The exemplary cash dispenser is operative to dispense cash in the form of bills or currency notes to a user who conducts a dispensing transaction. The exemplary ATM 12 further includes a depository schematically indicated 34. Depository 34 in the exemplary embodiment is operative to accept deposits input by a user in the course of certain types of transactions conducted at the machine.

It should be understood that the devices discussed in connection with ATM 12 are exemplary. In other embodiments of ATMs, different types and numbers of devices may be used. The type and character of the devices may depend on the particular type of ATM being operated and the character of the transaction types to be conducted.

As schematically represented in FIG. 1, ATM 12 includes therein at least one processor 36. Processor 36 is in operative connection with at least one data store schematically indicated 38. The devices included in ATM 12 are operated responsive to instructions carried out by the processor in accordance with computer software and data stored in the data store 38. The discussion of an exemplary automated teller machine, components and the operation thereof are included in U.S. Pat. No. 6,334,117 granted Dec. 25, 2001 and owned by the assignee of the present invention, which patent is incorporated herein by reference in its entirety as if fully rewritten herein. As can be appreciated the data store includes software instructions and data that can be executed and/or utilized by the at least one processor in the machine

to cause the machine to operate to carry out transactions for users of the machine. Software which includes the instructions may reside on and/or be loaded into the data store from articles such as floppy disks, CDs, hard drives, memory cartridges, tape or other types of articles or media capable of holding such instructions.

ATM 12 is operative to carry out transactions for users through communication with remote computers schematically indicated 40, 42 and 44. ATM 12 includes at least one communication device such as a modem or other network interface device to enable such communication. The remote computers communicate with ATM 12 through at least one network 46. The remote computers may be associated with financial institutions, sources of monetary value or other entities that can authorize the conduct of transactions by a user at the machine. Messages exchanged between the ATM 12 and the remote computers are operative to provide a remote computer which can authorize a transaction, with information concerning the requested transaction. This may include for example, the type of transaction, amount involved and the account or user requesting the transaction. When the remote computer receives the information necessary to determine if the transaction should be authorized, the remote computer operates in accordance with its programming to determine if the transaction should be authorized.

The remote computer then sends one or more messages through the network to indicate to the ATM 12 if the transaction should be carried out. In response to an indication that the transaction is authorized the ATM will operate responsive to the processor 36 to operate the transaction function devices and to complete the transaction. In the exemplary embodiment the processor then causes the ATM 12 to communicate with the remote computer which authorized the transaction to indicate that the transaction was completed or was not successfully completed. The remote computer in response to the message from the ATM may make the necessary deductions or additions from accounts, record information or otherwise appropriately account for the transactions conducted.

FIG. 2 is a schematic representation of some of the hardware and software included in ATM 12. As previously discussed ATM 12 includes transaction function devices generally referred to schematically as 48. The transaction function devices may include the devices previously discussed, only some of which are shown. These include for example the card reader 20, printer 30, cash dispenser 32, depository 34, keypad 24. Other or additional transaction function devices are represented schematically by the device 50. It should be understood that device 50 actually represents multiple items of transaction function device hardware, and that all transaction function device hardware components are not shown herein for purposes of simplicity.

As represented in FIG. 2, the hardware of each transaction function device generally has an associated software interface. These interfaces are schematically indicated 52. In some exemplary embodiments the interfaces 52 comprise firmware which is resident on processors associated with the respective transaction function device. It should be understood that the nature of the interface and its character as either hardware or software will depend on the particular transaction function device with which it is associated.

An exemplary software environment operating in processor 36 is schematically represented 54. Software environment 54 includes a plurality of service provider software or SPs indicated as SP software 56. As previously discussed the exemplary service provider software is operative to gener-

ally present an interface for each particular device that conforms to the requirements of the standard for the particular type of device. Thus, for example the service provider software associated with the cash dispenser presents an interface that enables the SP software to cause the cash dispenser of the particular brand and type of ATM to operate in response to commands that have been established as those which should cause a cash dispenser in an ATM to operate. The SP software 56 in the exemplary embodiment is operative to cause operation of the transaction function devices as well as to control certain relationships between such devices so as to avoid the need to account for such relationships in other software components. It should be understood that this approach is exemplary and in other embodiments the programming regarding relationships between devices may be included in other software layers as appropriate in accordance with the particular standards to which the software is written. Further, as later discussed additional software may be provided such as verification software which is operative to reduce the risk that unauthorized software is allowed to operate transaction function devices in the ATM.

In the exemplary embodiment of the software environment 54, a middle layer 58 is used. In the exemplary embodiment the middle layer includes INvolve™ software which is available from Nexus Software, Inc. of Raleigh, N.C. In alternative embodiments the middle layer may include APTRA™ software available from NCR Corporation or other middle layer software. The middle layer software is alternatively referred to herein as "middleware." In the exemplary embodiment the middle layer software is operative to account for any differences or special circumstances that may exist which may make the service provider software and associated commands different for different brands of hardware. For example the recognized standards for automated teller machine devices may not account for all of the features or functions available in a given transaction function device. Standards often leave open the opportunity for additional instructions or messages to accommodate such devices. Further, as later discussed certain machines may include or have operated in connection therewith devices for which there is no applicable published standard.

Exemplary middle layer 58 includes software which is operative to cause operation of at least some transaction function devices and to handle differences between various types of service provider software so as to avoid the need for the developer of the application to have knowledge of and/or to account for them. In addition the exemplary form of the middle layer 58 may include tools or other devices that may be useful in the operation of the automated teller machine. This may include for example features such as data compression to facilitate the printing of graphics on forms. The middle layer may also include software that deals with particular service or diagnostic functions. It should be understood that the middle layer 58 discussed herein is exemplary and in other embodiments different properties of the middle layer may be provided or alternatively no middle layer may be used.

In exemplary software environment 54 application software 60 is provided. In the exemplary embodiment application software 60 is a hardware independent software application which is suitable for operating ATMs of different manufacturers. Such ATMs may include for example ATMs manufactured by Diebold, Incorporated, NCR Corporation, Fujitsu or Wincor-Nixdorf or other manufacturers. The exemplary application software 60 includes software which is operative to cause the transaction function devices to carry out functions which are required for operation of the auto-

mated teller machine. The application also provides and receives instructions in accordance with the standards that enable the operation of ATM devices and/or the middle layer 58.

Exemplary functions provided by the application may include a browser for the processing of markup language documents. The application may include the functionality of providing the instructions to the other software layers for handling stored value transactions such as moving money between electronic purse devices such as smart cards. The application may include the functionality for delivering the messages to and receiving responses from other software components which causes the processor to carry out the various transactions associated with the ATM machine. These transactions may include the dispense of cash, the receipt of deposits or other functionality provided through the machine. Other aspects of the application may include certain security and communications features and/or features for carrying out the installation of the software, the configuration thereof as well as transaction login and diagnostic features. Other exemplary features may include maintaining a journal of transactions conducted, the capability for monitoring the operation of the ATM remotely. Other functions which may be included in the application software may include certain biometric analysis or reading capabilities as well as capabilities for providing customer relationship management and advertising. Other functions may include aspects associated with imaging of documents such as checks, providing maintenance and testing functions for monitoring operation or for purposes of managing cash which may be dispensed from or received by the machine. It should be understood that these functions supported by the hardware independent software application are exemplary and in other embodiments lesser numbers, greater numbers, other or different functions may be provided.

The exemplary software environment 54 also includes an operating system schematically indicated 62. The operating system may comprise Windows software available from Microsoft® Linux or other suitable operating system software. As represented by devices 64 and 66, other devices in the ATM may be operative to communicate with the software environment and such devices are not operated through the use of service provider software. Such devices may include for example communication devices, and other devices for which operative capability is provided by the functions included in the operating system, or in the middle layer.

It should be understood that the arrangement of software components shown in FIG. 2 is exemplary and in other embodiments other arrangements may be used.

In accordance with a first exemplary method, the development and use of hardware independent software applications for automated teller machines is made generally available to appropriate users at no charge. The distribution of such software is schematically represented in FIG. 3. It should be understood that for purposes of this disclosure "no charge" does not necessarily mean absolutely free, but rather may include an amount charged that is substantially less than the reasonable value of the particular item.

As schematically represented in FIG. 3, in accordance with an exemplary method, application software 60 is offered by an entity to owners of ATMs, developers and others for no charge. For example the entity that is the original developer of the application 60 offers to grant rights to use the application to all owners of ATMs at no charge. Such owners of ATMs are schematically represented 68 and

19

interrelated hardware or software components. This may include for example the service provider software conducting tests which actually cause transaction function devices to operate. In this way the service provider software which is often a close layer to the transaction function devices can verify not only its own proper operation, but also the operation of at least some of the hardware devices. In some embodiments the outputs provided that are indicative of results of one or more tests may include information indicative of a particular device, sensor, module, driver or other hardware or software component in the ATM which did not fulfill one or more tests.

In some embodiments a software component may have the capability to conduct a test of its own functional capabilities independent of any other hardware or software, as well as to conduct at least one test in which the software operates in conjunction with other hardware or software. For example, the service provider software may cause the processor to operate to conduct at least one test where at least one proper response from a transaction function device is simulated. Thereafter if the results of the test of the software indicates the service provider software is functioning properly, another test exercising one or more actual transaction function devices may be conducted, and an output indicative of the results provided responsive to operation of at least one ATM processor. In this way a problem can be more readily identified as involving either the software component or a hardware component.

Alternatively or in addition, software components may be configured to test their own functionality independently, and/or may be configured to test interoperability with one or more other software components. In this way the ATM can provide for example, outputs indicative of test results for each tested component, as well as the functionality that two or more software components (plus perhaps hardware components) provide together. In some embodiments testing capabilities may be included so that additional testing of components can be done so that components can be tested together until a problem area is identified. Such testing can also be done in some embodiments using a plurality of software components that each test operability with another software component to isolate the source of problems. Further, in some embodiments such capabilities may provide servicers with the capabilities for providing work arounds for problems, including the ability to diagnose and provide the remedy of work around remotely from the ATM. Of course other approaches may be used.

As can be appreciated the features of providing verification that software components are authorized to work in the ATM, as well as that software components are authorized to operate or be used together, may or may not be used in ATMs with software that includes diagnostic capabilities like those described. Further in some embodiments, verification features and identifying aspects of software components can be used in determining diagnostic capabilities as well as in determining the authority of an entity attempting to make changes to the machine or its software configuration. Of course the approaches and usage described herein are exemplary and the scope of the invention is not limited thereto.

It should further be understood that although the exemplary forms of the invention have been described with regard to software having a particular architecture and which include applications which may generally be operated in ATM hardware provided by a plurality of manufacturers, the principles of embodiments of the invention may be used in conjunction with other types of ATMs and hardware and software architectures.

20

Thus the new automated banking machine software, system and method of the exemplary forms of the present invention achieve the above stated objectives, eliminate difficulties encountered in the use of prior systems, solve problems and attains the desirable results described herein.

In the foregoing description certain terms have been used for brevity, clarity and understanding, however no unnecessary limitations are to be implied therefrom because such terms are used for descriptive purposes and are intended to be broadly construed. Moreover, the descriptions and illustrations herein are by way of examples and the invention is not limited to the exact details shown and described.

In the following claims any feature described as a means for performing a function shall be construed as encompassing any means known to those skilled in the art to be capable of performing the recited function, and shall not be limited to the structures shown herein or mere equivalents thereof.

Having described the features, discoveries and principles of the invention, the manner in which it is constructed and operated, and the advantages and useful results attained; the new and useful structures, devices, elements, arrangements, parts, combinations, systems, equipment, operations, methods, processes and relationships are set forth in the appended claims.

We claim:

1. A method comprising:

(a) providing an automated teller machine including at least one software verification device;

(b) installing first software on the automated teller machine;

(c) verifying through operation of the at least one verification device that the first software is authorized by an entity to operate the machine;

(d) enabling the automated teller machine to operate to carry out at least one transaction type responsive to the verification in (c).

2. The method according to claim 1 wherein in (c) the entity is associated with a manufacturer of the machine.

3. The method according to claim 1 wherein (c) includes verifying at least one verification feature provided by the entity and included in the first software.

4. The method according to claim 3 and prior to (b) further comprising:

providing the first software to the entity; and

the entity including in the first software the at least one verification feature.

5. The method according to claim 4 wherein the at least one verification feature included in the software by the entity includes at least one digital signature.

6. The method according to claim 5 wherein (c) includes verifying the at least one digital signature.

7. The method according to claim 4 wherein in (b) the first software comprises an automated teller machine application adapted to operate automated teller machines produced by a plurality of different manufacturers.

8. The method according to claim 4 wherein in (b) the first software comprises service provider software adapted to operate only in a type of automated teller machine produced by a manufacturer associated with the entity.

9. The method according to claim 8 and prior to (b) further comprising:

(e) providing the service provider software to a third party;

(f) the third party modifying the service provider software.

21

10. The method according to claim 9 wherein (f) includes modifying the service provider software to support at least one transaction function device not provided in the type of automated teller machine.

11. The method according to claim 3 and prior to (c) providing the first software from a third party to the entity, the entity including in the first software the at least one verification feature, and the entity returning the first software including the verification feature to the third party.

12. The method according to claim 11 and further comprising the third party distributing the first software, wherein in (b) the first software installed is distributed by the third party.

13. The method according to claim 12 wherein in (c) the entity is associated with a manufacturer of the machine, and further comprising:

(d) the entity making the first software available at no charge to a plurality of owners of automated teller machines produced by the manufacturer.

14. The method according to claim 13 and further comprising:

(f) the entity making the source code associated with the software and the right to modify the source code available to third party developers at no charge, on the condition that all modified forms of the software be provided to the entity.

15. The method according to claim 1 and further comprising:

(e) providing the first software to the entity; and wherein (c) comprises communicating data corresponding to at least one identifying feature of the first software with at least one remote computer associated with the entity.

16. The method according to claim 15 wherein in (c) the at least one identifying feature comprises a hash of at least a portion of the first software.

17. The method according to claim 15 wherein in (c) the at least one identifying feature comprises a measured parameter of at least a portion of the first software.

18. The method according to claim 15 and further comprising:

operating the remote computer utilizing the first software provided to the entity in (e) to calculate the data corresponding to the at least one identifying feature.

19. The method according to claim 18 wherein in (b) the first software comprises an automated teller machine software application adapted to operate automated teller machines produced by a plurality of different manufacturers.

20. The method according to claim 18 wherein in (b) the first software comprises service provider software adapted to operate only in automated teller machines produced by a manufacturer associated with the entity.

21. The method according to claim 1 and prior to (d) further comprising:

(e) installing second software in the automated teller machine;

(f) verifying through operation of the at least one verification device that the second software is authorized by the entity to operate in the machine; wherein in (d) the machine is enabled to carry out the at least one transaction type responsive to the verification in both (c) and (f).

22. The method according to claim 21 wherein in (a) the first software comprises application software adapted to operate automated teller machines of a plurality of different manufacturers, and wherein the entity is associated with one of the plurality of different manufacturers.

22

23. The method according to claim 21 wherein in at least one of (c) and (f) at least one verification feature included in at least one of the first software and the second software by the entity, is verified by the at least one software verification device.

24. The method according to claim 23 wherein in (c) the at least one verification device is operative to verify at least one verification feature included in the first software by the entity, and in (f) the at least one verification device is operative to verify at least one verification feature included in the second software by the entity.

25. The method according to claim 21 and prior to (d):

(g) determining through operation of the machine that the first and second software are indicated by the entity to be suitable for operation together; and

(h) enabling the machine to carry out the at least one transaction type responsive to the determination in (g).

26. The method according to claim 25 wherein the determination in (g) is made by the machine responsive to verification features included in the first and second software by the entity.

27. The method according to claim 25 where the determination in (g) is made by the machine through communication with a remote computer associated with the entity.

28. A method comprising:

(a) providing a first software from a third party to an entity

(b) including in the first software at least one verification feature by the entity;

(c) returning the first software including the verification feature to the third party;

(d) providing an automated teller machine including at least one software verification device;

(e) installing the first software on the automated teller machine;

(f) verifying through operation of the at least one verification device that the first software is authorized by the entity to operate the machine, including verifying the at least one verification feature provided by the entity and included in the first software; and

(g) enabling the automated teller machine to operate to carry out at least one transaction type responsive to the verification in (f).

29. A method comprising:

(a) providing a first software to an entity;

(b) providing an automated teller machine including at least one software verification device;

(c) installing first software on the automated teller machine;

(d) verifying through operation of the at least one verification device that the first software is authorized by an entity to operate the machine, including communicating data corresponding to at least one identifying feature of the first software with at least one remote computer associated with the entity;

(e) enabling the automated teller machine to operate to carry out at least one transaction type responsive to the verification in (d).

30. A method comprising:

(a) providing a first software to an entity, wherein the first software comprises an automated teller machine application adapted to operate automated teller machines produced by a plurality of different manufacturers;

(b) including in the first software at least one verification feature by the entity;

23

- (c) providing an automated teller machine including at least one software verification device and a cash dispenser;
 - (d) installing the first software on the automated teller machine; 5
 - (e) verifying through operation of the at least one verification device that the first software is authorized by the entity to operate the machine;
 - (f) enabling the automated teller machine to operate to carry out at least one transaction type responsive to the verification in (e). 10
31. A method comprising:
- (a) providing a service provider software to a third party, wherein the service provider software is adapted to operate only in a type of automated teller machine produced by a manufacturer associated with an entity, 15
 - (b) modifying the service provider software by the third party;
 - (c) providing the service provider software to the entity, 20
 - (d) including in the service provider software at least one verification feature by the entity,
 - (e) providing an automated teller machine including at least one software verification device and a cash dispenser; 25
 - (f) installing the service provider software on the automated teller machine;
 - (g) verifying through operation of the at least one verification device that the service provider software is authorized by the entity to operate the machine; 30
 - (h) enabling the automated teller machine to operate to carry out at least one transaction type responsive to the verification in (g). 35
32. A method comprising:
- (a) providing an automated teller machine including at least one software verification device;
 - (b) installing first software on the automated teller machine, wherein the first software comprises applica-

24

- tion software adapted to operate automated teller machines of a plurality of different manufacturers;
 - (c) verifying through operation of the at least one verification device that the first software is authorized by an entity to operate the machine, wherein the entity is associated with one of the plurality of different manufacturers;
 - (d) installing second software in the automated teller machine;
 - (e) verifying through operation of the at least one verification device that the second software is authorized by the entity to operate in the machine;
 - (f) enabling the automated teller machine to operate to carry out at least one transaction type responsive to the verifications in both (c) and (e).
33. A method comprising:
- (a) providing an automated teller machine including at least one software verification device;
 - (b) installing first software on the automated teller machine;
 - (c) verifying through operation of the at least one verification device that the first software is authorized by an entity to operate the machine;
 - (d) installing second software in the automated teller machine;
 - (e) verifying through operation of the at least one verification device that the second software is authorized by the entity to operate in the machine;
 - (f) verifying through operation of the machine that the first and second software are indicated by the entity to be suitable for operation together; and
 - (g) enabling the automated teller machine to operate to carry out at least one transaction type responsive to the verifications in (c), (e), and (f).

* * * * *