



Industria y Comercio

SUPERINTENDENCIA

Delegatura de propiedad Industrial

División de Nuevas Creaciones

PCT.

SOLICITUD

PATENTE DE INVENCION

21 EXPEDIENTE No. 03-77717

54 TÍTULO Sistema y Método de firmas digitales de
Máquina automática de transacciones

51 CLASIFICACIÓN INTERNACIONAL G06F A160

71 SOLICITANTE DIGBOLD, INCORPORATED

DOMICILIO 5985 Mayfair Road, North Canton, OH
44720 Estados Unidos de América

74 APODERADO Carlos A. Olarte

22 BOGOTÁ, D. C., 05- SEPTIEMBRE 2003

202038

PETITORIO

Industria y Comercio
SUPERINTENDENCIA

03 077717 00

Radicación : 03077717 00000000 Folios: 172
Fecha (AMB): 2003-09-05 15:23:06
E Trámite : 011 PCT-PATENT 379 FASE NACI 411 PRESENTACIÓN
Dependencia: 2020 DIVISION DE NUEVAS CREACIONESFORMULARIO ÚNICO DE SOLICITUD DE PATENTE
PCT
ENTRADA EN FASE NACIONAL

①

SOLICITUD DE :

☒
☐Patente de Invención
Capítulo I.☐
☒Patente de Modelo de Utilidad
Capítulo II.

②

SOLICITANTE
(71)

Nombre: DIEBOLD, INCORPORATED

Dirección: 5995 Mayfair Road, North Canton, OH 44720 Estados Unidos de America.

Nacionalidad o Domicilio:

Lugar de Constitución: North Canton, OH. Estados Unidos de America.

Teléfono:

Fax:

E-Mail

IDENTIFICACION

C.C. ☐ NIT ☐C.E. ☐ Otro ☐Número Cual

③

REPRESENTANTE
O APODERADO

Nombre: CARLOS R. OLARTE

Dirección: World Trade Center Torre C, Calle 100 No. 8A-55 Piso 10.

Teléfono: 6386200

Fax: 6386201

E-Mail: filings@olarteisbeck.com

IDENTIFICACION

C.C. ☒ NIT ☐C.E. ☐ Otro ☐

Número 79.782.747 Bta TP 74.295

④

INVENTOR (ES)
(72)

Nombre: Christopher L. Parmelee; Mark D. Smith.

Dirección: 6140 Triple Crown Drive, edina, OH 44256 US; 1910Hunting Valley, NW, North Canton, OH 44720 US.

Nacionalidad o Domicilio: ESTADOUNIDENSE

⑤

PCT (85)

Solicitud Internacional No. PCT/US02/06826

Fecha Marzo 6, 2002

Publicación Internacional No. WO 02/073341

Fecha Septiembre 19, 2002

⑥

Título (54)

SISTEMA Y MÉTODO DE FIRMAS DIGITALES DE MÁQUINA AUTOMÁTICA DE TRANSACCIONES.

⑦

Clasificación Internacional (51)

G06F 7/60

⑧

Prioridad

SI ☒ NO ☐

(33) País de Origen

US

US

(32) Fecha

Marzo 7, 2001

Noviembre 29, 2001

(31) Número de Solicitud

60/273.996

60/319.015

⑨

Comprobante de pago No. 61667

Fecha 090103

Instrucciones para el diligenciamiento del presente formulario, ver reverso de esta página

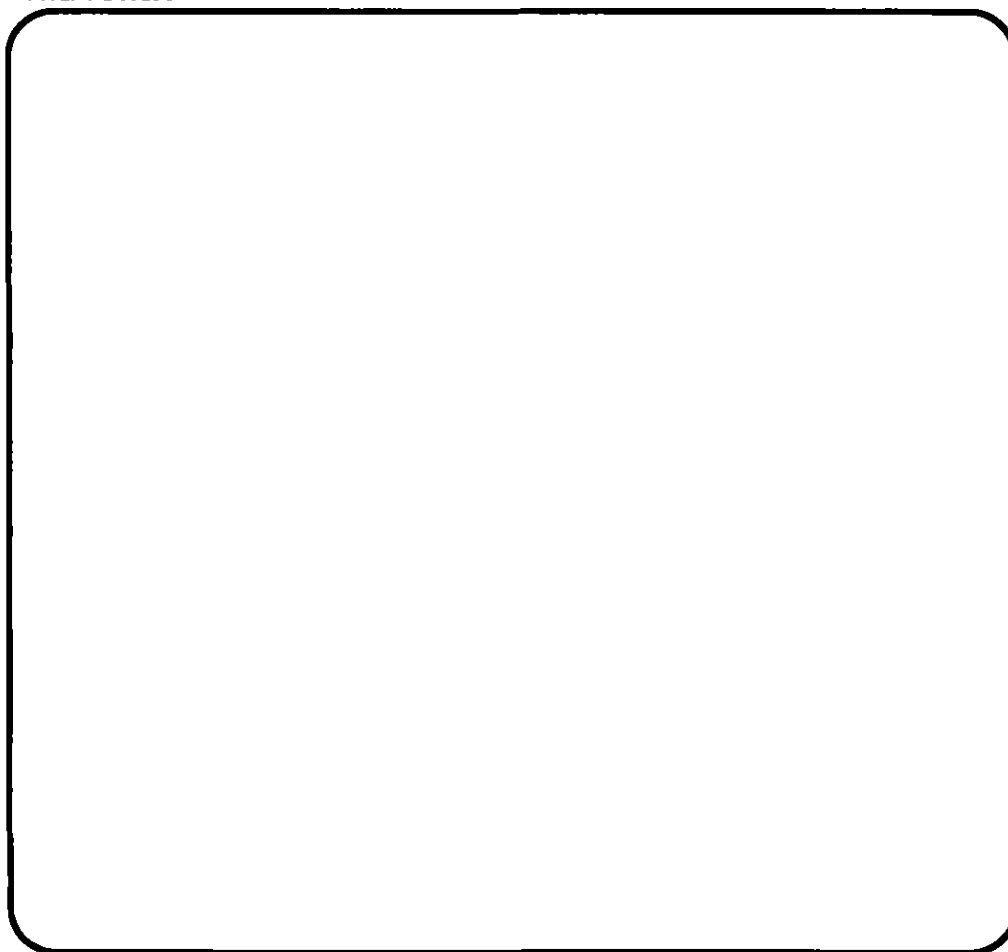
10

ANEXOS

- ☒ Comprobante de pago de la tasa de presentación de la solicitud
- ☐ Documento que acredite la existencia y representación legal cuando el solicitante sea persona jurídica
- ☒ Poderes, si fuere el caso
- ☐ Documento de cesión del inventor al solicitante o a su causante
- ☐ Declaraciones
- ☒ Copia de la solicitud internacional. (Resumen, descripción, reivindicaciones, dibujos)
- ☒ Traducción de la solicitud internacional al castellano. (Resumen, descripción, reivindicaciones, dibujos)
- ☒ Copia del examen preliminar internacional efectuado por la Autoridad Internacional de Examen preliminar (IPEA)
- ☐ Traducción del examen preliminar internacional efectuado por la IPEA
- ☐ De ser el caso, copia del contrato de acceso
- ☐ De ser el caso, documento que acredite la licencia o autorización de uso de conocimientos tradicionales de las comunidades indígenas
- ☐ De ser el caso, certificado de depósito del material biológico
- ☐ Arte final 12 x 12
- ☒ De ser el caso, información sobre otras solicitudes de patente o títulos obtenidos en el extranjero por el mismo titular o su causante, relacionadas parcial o totalmente con la invención de esta solicitud
- ☐ De ser el caso, modificaciones efectuadas a la solicitud internacional.
- ☒ Otras: BUSQUEDA INTERNACIONAL

11

FIGURA CARACTERISTICA



12

Solicita la concesión de la patente,

NOMBRE: CARLOS R. OLARTE

FIRMA:

C.C. 74.782.747 de Btá T.P. 74.295

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
19 September 2002 (19.09.2002)

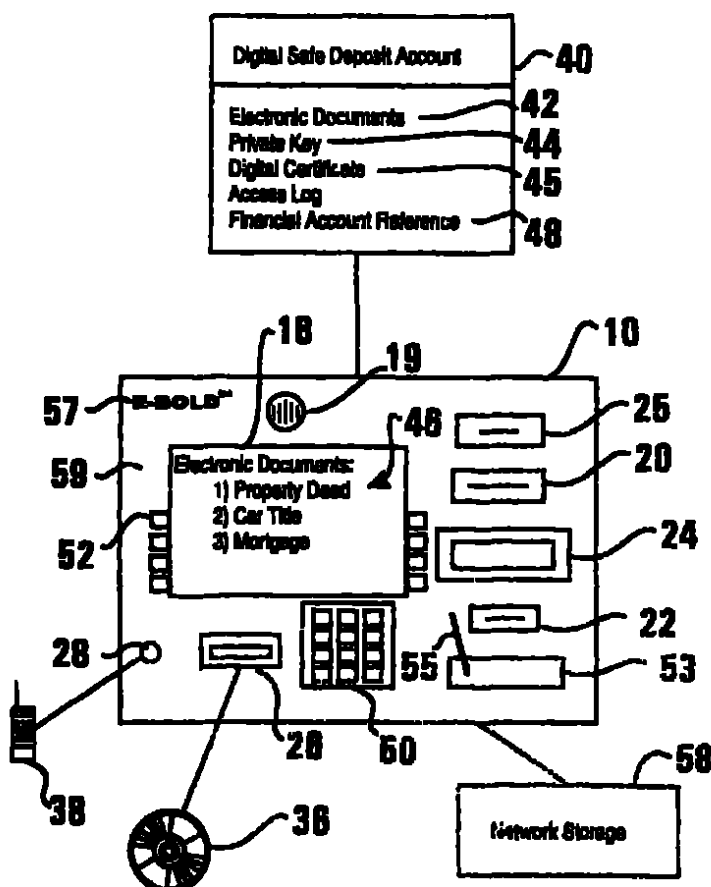
PCT

(10) International Publication Number
WO 02/073341 A2

- (51) International Patent Classification: G06F (72) Inventors: PARMELEE, Christopher L.; 6140 Triple Crown Drive, Medina, OH 44256 (US); SMITH, Mark D.; 1910 Hunting Valley, NW, North Canton, OH 44720 (US).
- (21) International Application Number: PCT/US02/06826
- (22) International Filing Date: 6 March 2002 (06.03.2002) (74) Agent: JOCKE, Ralph E.; 231 South Broadway, Medina, OH 44256 (US).
- (25) Filing Language: English (81) Designated States (national): BR, CA, CN, CO, IN, MX, PL, RU, ZA.
- (26) Publication Language: English (84) Designated States (regional): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- (30) Priority Data: 60/273,996 7 March 2001 (07.03.2001) US
60/319,015 29 November 2001 (29.11.2001) US
- (71) Applicant: DIEBOLD, INCORPORATED [US/US]; 5995 Mayfair Road, North Canton, OH 44720 (US).
- Published:
-- without international search report and to be republished upon receipt of that report

[Continued on next page]

(54) Title: AUTOMATED TRANSACTION MACHINE: DIGITAL SIGNATURE SYSTEM AND METHOD



(57) Abstract: An automated transaction machine such as an ATM (10) is provided. The ATM is operative to digitally sign electronic documents (42). The ATM may be in operative connection with a storage server (32). The storage server is operative responsive to the ATM to maintain electronic documents (42) in a data store (34) in association with the user's digital safe deposit account (40) and/or a financial account (48) such as checking, savings, debit, or credit account. The storage server is further operative to store a private key (44) of a user in association with the user's digital safe deposit account and/or financial account. The ATM is operative to cause electronic documents to be signed using the private key associated with the user. The ATM is further operative to output the electronic document on a display device (18) of the ATM where the user may view and edit the electronic document.

WO 02/073341 A2

**AUTOMATED TRANSACTION MACHINE
DIGITAL SIGNATURE SYSTEM AND METHOD**

TECHNICAL FIELD

5 This invention relates to automated transaction machines. Specifically this invention relates to an automated transaction machine system and method that is capable of digitally signing electronic documents.

BACKGROUND ART

10 As an increasing number of individuals own or have access to personal computers, more and more individuals are generating electronic documents. Examples of electronic documents include electronically filed tax returns, contracts for goods or services ordered online through the internet, e-mail, word processing documents, or any other type of document that has a digital
15 form. Some electronic documents are of a type that the individuals involved in generating, sending or receiving such documents might prefer to have the documents maintained as secure and confidential for long periods of time.

 Unfortunately, many personal computers have insecure configurations. With the increasing popularity of the Internet, many personal computers are
20 vulnerable to being accessed remotely by hackers on the Internet. Further, many home personal computers are not configured with passwords and as a result anyone with physical access to the personal computer such as a friend, a child care giver, or a relative may accidentally or intentionally gain access to sensitive electronic documents. Although cryptography software exists to
25 encrypt private electronic documents, many individuals do not have the technical skill to install and configure encryption software correctly on their personal computers. Consequently, there exists a need for a system and method of protecting personal electronic documents which can be more easily used by individuals.

30

Electronic documents belonging to individuals are often stored on a hard drive of a personal computer. For example, consumer tax software typically generates electronic tax return documents which are stored on a hard drive. Word processors often store electronic document files in a common directory on a hard drive. E-mail received by and sent from a personal computer is also often stored on a hard drive. Unfortunately, over time personal computers may encounter software and/or hardware problems which destroy computer files stored on a hard drive. Unless the individual proactively and regularly performs backups of computer files located on the hard drive of their personal computer, important, difficult to replace, personal electronic documents may be lost due to a hardware or software problem. Even if the documents are backed-up on removable media such as a tape, portable disk or CD, the portable media itself may become corrupted, unreadable, obsolete, or lost. As a result, there exists a need for a system and method of storing important personal electronic documents which can preserve the integrity of the documents for long periods of time.

With the enactment of electronic signature laws at the state and federal levels, individuals are likely to encounter more opportunities to generate and electronically sign electronic documents. Many electronic signature systems use public key encryption methods to generate and validate electronic signatures. When signing an electronic document an individual uses a secret private key to generate a digital signature for the electronic document. Such a private key is generally associated with a public key. Another party may use the public key to authenticate the electronic document and digital signature. Such public keys are often distributed as part of a digital certificate which is digitally signed by a trusted third party certificate authority.

Although the digital certificate and public key may be publicly disclosed to the world, the private key must remain a secret to prevent forgeries. When a person wishes to digitally sign a document, the user must employ a computer program which has access to the private key. As with

6
[Handwritten signature]

encryption software, many individuals do not have the technical skill to successfully install and use digital signature programs on their personal computers. Consequently there exists a need for a system and method of digitally signing electronic documents which can be easily employed by individuals.

In general, when a digital signature program belongs to a person using the program, that person may have reasonable assurance that the person's private key will be kept a secret by the program. In addition the person has reasonable assurance that the electronic document being signed corresponds to the electronic document that was read and reviewed by the person. Unfortunately, if the digital signing program belongs to an untrusted party, the individual has very little assurance that a private key inputted by the individual will remain a secret and/or that the electronic document that was read and reviewed by the individual is the actual document being digitally signed. As a result there exists a need for a system and method of protecting the confidentiality of private keys used to digitally sign electronic documents. There also exists a need to provide a system and method of digitally signing electronic documents which provides additional assurance to individuals that the process is a safe substitute for signing paper documents.

DISCLOSURE OF INVENTION

It is an object of an exemplary form of the present invention to provide a system and method which can be easily employed by individuals for protecting electronic documents.

It is a further object of an exemplary form of the present invention to provide a system and method of storing electronic documents which can preserve the integrity and confidentiality of the electronic documents for long periods of time.

It is a further object of an exemplary form of the present invention to provide a system and method which can be easily employed by individuals for

7 ~~10/20~~

digitally signing electronic documents.

It is a further object of an exemplary form of the present invention to provide a system and method of protecting the confidentiality of private keys used to digitally sign electronic documents.

5 It is a further object of an exemplary form of the present invention to provide a system and method of digitally signing electronic documents which provides further assurance to individuals that digital signing of electronic documents is a safe substitute for signing paper documents.

10 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 may be accomplished in an exemplary embodiment by a system and method of storing and digitally signing electronic documents with automated transaction machines. An example of an
15 automated transaction machine which may be used by individuals or users with exemplary embodiments includes 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 receipt of deposits, the transfer of funds between accounts, the
20 payment of bills and account balance inquiries. The type of banking transactions a customer can carry out are determined by the capabilities of the particular machine and the programming of the institution operating the machine. Other types of automated transaction machines may allow customers to charge against accounts or to transfer funds. Other types of automated
25 transaction machines may print or dispense items of value such as coupons, tickets, wagering slips, vouchers, checks, food stamps, money orders, scrip or travelers checks. For purposes of this disclosure references to an ATM, an automated transaction machine, or an automated banking machine shall encompass any device which carries out transactions including transfers of
30 value.

An exemplary embodiment of the ATM may include at least one output device such as a display screen, audio system, and printer. The ATM may also include at least one input device such as a touch screen, function keys, keypad, keyboard, and/or card reader. The ATM may further include devices such as a dispenser mechanism for sheets of currency, a receipt printer mechanism, a card reader/writer, a depository mechanism and other transaction function devices that are used by the machine in carrying out transactions including transfers of value.

The ATM may include or be in operative connection with at least one computer. The computer may be in operative connection with the output devices and the input devices, as well as with the transaction function devices in the machine. The computer may include software components and programs that are executed therein. In an exemplary embodiment, at least one software component may be operative to cause the computer to provide a user interface through the display device or other output device of the machine, which enables users to store and retrieve electronic documents from a digital safe deposit box or account associated with the user. In one exemplary embodiment a digital safe deposit account includes an amount of file storage space maintained by a storage server in operative connection with the ATM. The exemplary ATM is operative to communicate with the storage server and cause the storage server to maintain electronic documents which are stored in association with the user's digital safe deposit account. In one exemplary embodiment, the ATM is operative to have the storage server store, retrieve, copy, and delete electronic documents stored in the user's digital safe deposit account. In addition the exemplary storage server is configured with operative hardware, software, and backup technology to preserve the integrity of the electronic files for long periods of time. Exemplary embodiments of the storage server are also operative to encrypt the electronic documents such that only authorized individuals may access the electronic documents.

Exemplary embodiments of the ATM may enable a user to retrieve an electronic document from an external source and store the retrieved document in the user's digital safe deposit account. External sources for example may include a portable storage medium such as a CD, a portable computing device such as a mobile phone, and/or a network accessible storage location. In exemplary embodiments, the ATM includes a portable storage medium reading device that is operative to read electronic documents from a portable storage medium. Examples of portable storage medium reading devices for use with exemplary embodiments include portable hard drive readers such as an Iomega Jaz® drive; magneto optical drives such as an Iomega Zip® drive; flash memory drives for writing to flash memory devices such as CompactFlash and Sony Memory Stick®; PC Cards Interfaces; CD drives, DVD drives; Mini-CD drives; smart cards; floppy disk drives; and digital tape drives.

The exemplary ATM may further enable users to view and/or listen to the contents of electronic documents through an output device of the machine. The exemplary ATM for example, may include document output software components which may be operative to cause the computer of the ATM to output corresponding visual representations of the electronic documents through a display device of the ATM. Examples of document output software components which may be operatively used with exemplary embodiments include an Adobe® PDF viewer, HTML or XML browser, a word processor, or any other software application which is operative to read or access an electronic document and output a visual representation of the accessed electronic document. The exemplary ATM may further include document output software components that are operative to output audible representations of the electronic documents through an audio device of the ATM. For example, electronic documents may include text which is both displayed through a display screen and converted into audible speech which is outputted through speakers of the ATM. Also, the ATM may further be

40
02/08

7

operative to print a visual representation of the electronic document through a printer device.

5 In an alternative exemplary embodiment, users may have access to electronic documents stored in the digital safe deposit account through a public network such as the Internet. In one exemplary embodiment, the present invention may enable users to choose to add Internet access to their digital safe deposit account in addition to ATM access to their digital safe deposit account. Users may or may not enable Internet access depending on the sensitivity and type of electronic documents stored in the digital safe deposit account.

10 An exemplary ATM may be operative to digitally sign electronic documents. In one exemplary embodiment, the ATM may include digital signature software components which are operative to sign electronic documents using public key cryptography algorithms and protocols, or other digital signature algorithm and protocol. For example, the exemplary digital signature software may be operative to sign electronic documents using a private key associated with the user. In one exemplary embodiment the private key may be stored by a storage server in association with a digital safe deposit account of the user. After authenticating the user, the exemplary ATM may be operative to cause an electronic document to be digitally signed using the private key securely stored by the storage server. Once an electronic document has been caused to be signed by the exemplary ATM, the ATM may be operative to send the signed electronic document to a location of the user's choosing such as the digital safe deposit account associated with the user or an external source such as a portable storage medium, portable computing device and/or network accessible storage location.

20 In some exemplary embodiments, the exemplary ATM may be operative to sign electronic documents with a private key of a user that is stored on an external source such as a portable computing device. For example, the private key of the user may be securely stored on a smart card.

30

An exemplary embodiment of the ATM may include a smart card reader which is operative to communicate with the smart card for purposes of signing an electronic document.

5 The exemplary storage server or an external source such as a smart card, may require a password or biometric data from the ATM prior to enabling a digital signature to be generated using the private key of the user. The exemplary ATM may include input devices such as a keypad or a biometric reading device which a user may use to input a required password such as a PIN, or biometric data.

10 In one exemplary embodiment, the ATM may be operative to retrieve the private key from the storage server or an external device for purposes of generating the digital signature with the ATM. In some exemplary embodiments, the system may be configured such that the ATM does not require that the private key be retrieved by the ATM. In this exemplary
15 embodiment, the ATM is operative to generate a one-way hash of the electronic document such as a message digest, cryptographic checksum, message integrity check, or manipulation detection code. The one-way hash may then be forwarded to the storage server, smart card, or other secure external source which has secure access to the private key. The storage server,
20 smart card, or other secure external source may then generate a digital signature responsive to the one-way hash, private key and the appropriate encryption or digital signature algorithm. The storage server, smart card, or other secure external source may then return the digital signature to the ATM. The ATM may then attach the digital signature to the electronic document
25 prior to storage in the digital safe deposit account or prior to sending the electronic document to an external source.

In an exemplary embodiment, the ATM may forward the electronic document to the storage server, smart card, or other external source. In this
30 embodiment the storage server, smart card, or other external source is operative to generate the digest and the corresponding digital signature from

12
12/12

the received electronic document and then forward the digital signature and/or electronic document back to the ATM. It is to be understood that exemplary embodiments encompass the use of any digital signature algorithm and key management system which is operative to enable an ATM to securely sign electronic documents. Examples of cryptographic algorithms which may be used with the present exemplary invention include RSA and DSA.

In some exemplary embodiments, the digital safe deposit account and/or a user's private key may be associated with a banking or other financial account of the user such as a checking account, savings account, debit account and/or credit account. A user may access the digital safe deposit account and/or digital signature features of the exemplary ATM by inserting an ATM card, bank card, credit card, or any other card which is associated with the user's financial account. After a user inputs a corresponding password such as a PIN or biometric information into an input device of the ATM, the exemplary ATM may be operative to enable the user to select transaction functions of the ATM such as the dispensing of cash, transfers, deposits, bill payment, and balance inquiry. In addition the exemplary ATM may be operative to enable the user to display and digitally sign electronic documents with a private key associated with the user's financial account. Further, the exemplary ATM may be operative to enable the user to access and maintain electronic documents stored in a digital safe deposit account which is associated with the user's financial account.

In embodiments where a user's digital safe deposit account and/or private key is not associated with a financial account card, a user may be issued a digital safe deposit account card with machine readable indicia thereon which corresponds to the user's digital safe deposit account. ATMs of exemplary embodiments may be operative to enable a user to access his/her digital safe deposit account and sign electronic documents responsive to reading the machine readable indicia from the digital safe deposit account card.

13
0018

In addition, the exemplary ATM may be operative to enable a user to generate private and public keys for digitally signing electronic documents. Also, the exemplary ATM may be operative to enable a user to acquire and/or purchase a digital certificate such as an X.509 certificate using the ATM. The exemplary ATM may be in operative connection with a certificate authority and may be operative to send the certificate authority sufficient information to enable the certificate authority to generate and issue the certificate to the user. Such digital certificates may be used to authenticate the user's digital signature created using the exemplary ATM. The exemplary ATM may be operative to store the digital certificate in the user's digital safe deposit account and/or in association with the user's financial account. As with other electronic documents, the exemplary ATM may be operative to send the digital certificate to an external source of the user's choosing. When signing an electronic document, the exemplary ATM may be operative to associate the digital certificate with the signed electronic document. Other parties may use the digital certificate to authenticate the digital signature of the electronic document. In this described exemplary embodiment, the ATM may be operative to cause the costs associated with purchasing a digital certificate to be charged against the financial account of the user or another party. If the user already has a digital signature, an exemplary embodiment may be operative to retrieve the digital certificate from an external source selected by the user. The exemplary ATM may be operative to associate a retrieved digital certificate with electronic documents being signed by the ATM. The exemplary ATM may further be operative to have the exemplary storage server store the retrieved digital certificate in the digital safe deposit account of the user and/or in association with a financial account of the user.

As discussed previously, the exemplary ATM may be operative to read the electronic document and output through a display device of the ATM a visual representation of the electronic document. In addition, the exemplary ATM may further be operative to enable a user to input through an input

14
100

device of the ATM, information into the electronic document. For example, an electronic document such as a contract may include fields for entering the names of the contracting parties, a description of the goods, and an amount of consideration being paid for the goods. The exemplary ATM may be
5 operative to enable a user to input or select text, numbers, and other information for incorporation into the electronic document prior to signing the document. In addition exemplary embodiments of the ATM may be operative to access a data store of user information. Such a data store may be used to retrieve information for automatically populating input fields of an electronic
10 document being viewed and edited by the ATM.

BRIEF DESCRIPTION OF DRAWINGS

Figure 1 is a schematic view representative of a first exemplary embodiment of an ATM.

15 Figure 2 is a schematic view representative of an exemplary embodiment of a system for storing and digitally signing electronic documents with an ATM.

Figures 3-8 are schematic views representative of exemplary embodiments of user interface screens of an ATM.

20 Figures 9-14 are schematic views representative of exemplary embodiments of ATM systems for digitally signing documents.

Figure 15 shows a schematic view of a document signing system of a further exemplary embodiment.

25 Figure 16 shows a top plan view of an exemplary embodiment of a portable machine that is operative to digitally sign electronic documents.

Figure 17 shows steps for an exemplary embodiment of a method for signing electronic documents.

Figure 18 shows a schematic view of a document signing system of a further exemplary embodiment.

30

15
16

Figure 19 shows an exemplary embodiment of a user interface screen of an ATM.

BEST MODES FOR CARRYING OUT INVENTION

5 Referring now to the drawings and particularly to Figure 1, there is shown therein a schematic view of an exemplary automated transaction machine, ATM 10 of an exemplary embodiment. The ATM 10 may include at least one computer processor 12 and a plurality of software components 11. The computer processor 12 may be operative responsive to the software

10 components 11 to control the operation of the ATM. In the exemplary embodiment the computer processor 12 may be operatively programmed to enable the ATM to perform at least one of the following functions: at least one banking transaction such as the dispensing of cash; the storage and retrieval of electronic documents; and/or the digital signing of electronic documents.

15 To perform these functions the ATM may further include in operative connection with the computer processor 12, at least one output device 14 such as a display device 18, at least one input device 16, and a card reader 20 which also serves as an input device. In some embodiments, the ATM may also include in operative connection with the computer processor 12, one or more

20 transaction function devices. Transaction function devices may include for example a cash dispenser 24, a depositor 22, a receipt printer 25 and other devices. The ATM 10 may further be operative to communicate with at least one financial transaction processing computer or system which is operative to carry out financial transfers and authorizations, which in this example is host banking system 30. ATM 10 also may be enabled to communicate with at

25 least one storage server 32. In the exemplary embodiment the storage server 32 may be in operative communication with at least one data store 34. Also in an exemplary embodiment, the ATM 10 may be operative to communicate with the at least one storage server 32 through communication with the host

30 banking system 30.

16
02/02/02

In one exemplary embodiment the storage server may be responsive to a plurality of ATMs 10 to securely store and maintain a plurality of electronic documents 42 in digital safe deposit boxes or accounts 40. Such digital safe deposit accounts may correspond to individual file storage locations on the data store 34. The electronic documents 42 may include for example digital representations of physical documents, word processing documents, HTML files, XML files, other markup language documents, Acrobat® PDF files, spreadsheet files, digital certificates, image files, sound files, audio visual files, source code files, application specific storage files, electronic voting ballots, or any other type of digital file which is operative to store information in a computer readable format. A user may establish one or more digital safe deposit accounts 40 and use an ATM 10 to store and maintain electronic documents 42 in association with his/her digital safe deposit account.

The exemplary embodiment of ATM 10 may be operative to display the viewable contents of an electronic document on the display device 18 and enable a user to digitally sign the electronic document. In many digital signature algorithms, the signer must use secret information such as a private key to generate the digital signature. In one exemplary embodiment, a user's private key 44, may be stored in a user's digital safe deposit account or stored in association with a user's digital safe deposit account 40. In exemplary embodiments, a user's private key 44 may further be stored in association with a user's financial account such as a credit card account, debit card account, checking account, savings account or any other financial account of the user. In addition, as will be further discussed below, exemplary embodiments of the ATM 10 and/or storage server 32 may be operative to digitally sign electronic documents using the private key 44 associated with the user's digital safe deposit account 40 and/or a financial account.

It should be understood that the ATM 10 is an exemplary embodiment and in other embodiments automated transaction machines may include other or additional devices and may operate in other types of systems. For example,

17

embodiments may include in operative connection with the computer processor 12, a data store including a storage device drive 26, and a communication port 28 which serves as an input/output device. The storage device drive 26 serves as a data store and enables the computer processor to read and/or write electronic documents to an external source 56 such as portable storage medium 36. The communication port 28 enables the computer processor to read and/or write electronic documents to external sources 56 such as a portable computing device 38 or a network accessible storage location 58.

Figure 2 schematically shows an exemplary embodiment of the ATM 10 that may be operative to store and maintain electronic documents 42 in a digital safe deposit account 40. The exemplary embodiment of the ATM 10 may include a display device 18 such as a CRT monitor or LCD display. The display device may be operative responsive to the computer processor to output user interface indicia 46. The user interface indicia may include instructional outputs for operating the ATM as well as content indicia which are representative of lists of electronic documents that may be accessed by the ATM 10 or portions of an electronic document which are operative to be viewed on the display device 18. Some exemplary embodiments may further include other output devices 14 such as a sound system 19 that is operative to output audio content that corresponds to an electronic document. For example when an electronic document includes audio information such as an MP3 file, an ATM 10 may be operatively programmed to cause the sound system to output sound in response to the MP3 file. In addition, if the electronic document includes language information such as text, an exemplary embodiment may include a speech synthesizer device or software that is operative to read the language information to a user by outputting spoken words through the sound system of the ATM 10.

The exemplary embodiment of the ATM 10 may also include at least one input device 16 such as a keypad 50 or selection buttons 52. The input

18
18/02/02

15

device(s) such as a keypad 50 and selection buttons 52 may enable users to enter operational inputs such as a personal identification number (PIN) corresponding to an account, an amount of cash to withdraw, or a selection of a particular electronic document to view, store and/or digitally sign. Some
5 exemplary embodiments of the ATM 10 may further include a biometric reading input device 54 such as a fingerprint reader, iris scanner, retina scanner, voice recognition device, facial recognition reader or other device which is operative to enable a user to input user identifying biometric information. Such identifying biometric information may be used by an
10 exemplary embodiment of the ATM 10 to further authenticate a user prior to enabling the user to perform transaction functions, access a digital safe deposit account, and/or digitally sign an electronic document.

In exemplary embodiments, the ATM may include other or additional types of input devices for entering information, such as a touch screen device,
15 a speech recognition system, a track ball, and/or a digitizing signature pad 53. The digitizing signature pad 53 is operative to produce a digital representation or scan of a handwritten signature drawn on the pad 53 with a pen or an inkless stylus 55. Such a digitized scan of the handwritten signature may be captured by the ATM 10 and integrated into electronic documents that are
20 digitally signed by the ATM.

As discussed previously, the ATM 10 may include a card reader 20. The card reader 20 may be operative to read indicia corresponding to account information or other information from a user's card. The card may be a bank card, credit card, debit card, gas card, merchant card, smart card, or other
25 medium that is operative to store account data and/or other information which may be used to identify a user or their accounts. Such account data may include an account number of a checking, savings, debit, credit, or other banking or financial account. Such account data may further include data representative of a digital safe deposit account of the user.

30

19

In one exemplary embodiment, a digital safe deposit account, a private key 44, and/or a digital certificate 45 may be associated with a financial account 48 of the user. When the user uses the exemplary ATM 10 with a card associated with the financial account 48, the exemplary ATM may be operative to automatically provide the user with access to the user's associated digital safe deposit account 40, private key 44, and/or digital certificate. For example, when a user inserts a credit or debit card in the card reader 20, the exemplary ATM may be operative to read the credit or debit account number from the card. This number may be used by the ATM to access the financial account through communication with the host banking system 30. In one exemplary embodiment, the private key of the user may be directly associated with the financial account of the user and the ATM is operative through communication with the host banking system to cause an electronic document to be digitally signed responsive to the private key associated with the financial account. In some embodiments, the user's digital safe deposit account 40 may be associated with the user's financial account 48 and the ATM may be operative to receive access to the digital safe deposit account 40 through communication with the host banking system.

An exemplary embodiment of the ATM 10 may be operative to dispense a selected amount of cash to the user from the cash dispenser 24, and to debit a banking or financial account through communication with a financial transaction computer such as the host banking system 30. The exemplary ATM 10 may be configured to debit user fees from a financial account of the user for storing, viewing, and digitally signing electronic documents with the ATM. The ATM may further be configured to debit user fees from a financial account of a further party or entity which may be associated with the electronic document being viewed, stored, and/or digitally signed by the ATM.

The exemplary embodiment of the ATM 10 may include a storage device drive 26 such as a CD drive which is operative to accept a portable

70

storage medium 36 such as a read-only, write-once or rewriteable CD. The exemplary embodiment of the ATM 10 is operative to cause the storage device drive 26 to read electronic documents from the portable storage medium 36. The read electronic documents may be viewed on the display screen 18 of the ATM 10 and/or transferred to a digital safe deposit account 40. In addition the exemplary ATM may further be operative to retrieve electronic documents stored in the digital safe deposit account 40, view them on the display device 18 and/or cause the storage device drive 26 to record the electronic document to the portable storage medium 36. Examples of other types of storage device drives that may be used with embodiments include portable hard drive readers such as an Iomega Jaz® drive; magneto optical drives such as an Iomega Zip® drive; flash memory drives for writing to flash memory devices such as CompactFlash and Sony Memory Stick®; DVD drives, Mini-CD drives, and digital tape drives.

Some embodiments may include one or more communication ports 28 that are operative to retrieve and record electronic documents to a portable computing device such as a mobile phone 38 or a network accessible storage location 58 associated with a customer selected or inputted URL, e-mail address, or other network address. Examples of suitable communication ports 18 may include a Universal Serial Bus (USB) port, a serial RS-232 port, parallel port, an infrared (IR) port, a radio frequency (RF) port such as Bluetooth, an IEEE-1394 port, or a network port such as a wired Ethernet or wireless Ethernet (IEEE-802.11x) connection. Examples of other types of portable computing devices that may be accessed with embodiments of the ATM 10 include a portable computer such as a notebook computer and a personal digital assistant (PDA).

The exemplary embodiment of the ATM 10 may further include a fascia 59 through which the one or more of the input devices, display devices, and transaction function devices are accessible to a user. The ATM 10 may further include a visible indicia 57 adjacent the fascia 59 of the ATM, visible

21

on the display screen or otherwise communicated to a user of the machine.

The visible indicia 57 may include a logo, design, or text that serves as a source indicator mark for a digital signature service or network. Such a mark may correspond to a service mark of the entity that operates the servers, data stores, host systems, and/or network through which the ATM 10 communicates to produce electronic signatures for an electronic document displayed by the ATM 10. Such indicia may be visually similar to indicia on a card of the user, so that the user can quickly determine that the ATM is capable of digitally signing documents using the card of the user. Such indicia may also serve to confirm to the user that the ATM is associated with a third party and independent digital signature service or network that can be trusted to accurately display the electronic document and to securely digitally sign the electronic document for the user.

Figures 3-8 show examples of user interface screens of an exemplary embodiment of the ATM 10. Figure 3 shows an example of a user interface screen 100 which ATM 10 may be operative to cause to be output through the display device 18. In one exemplary embodiment user interface screen 100 may be displayed after a user activates the ATM 10 by placing a card into card reader 20 and inputting a PIN into the keypad 50. User interface screen 100 may include a plurality of user selectable functions 102 which include the option of withdrawing cash 104 from the cash dispenser 24; the option of depositing a check 106 with the depositor 22; the option of transferring value between accounts 108; and the option of viewing an electronic document 110 with display device 18. Each of these selectable functions 102 may be adjacent a different selection button 52, which when pressed are operative to cause the ATM 10 to proceed with the corresponding function 102.

In one exemplary embodiment, when a user selects the option to view an electronic document 110, the exemplary ATM 10 may be operative to cause the user interface screen 120 shown in Figure 4 to be output through the display device 18. Here the user interface screen 120 may include a plurality

22

of selection functions 122 which correspond to different sources for retrieving electronic documents to view. In the presently described example, selection functions 122 may include the option to select electronic documents from a digital safe deposit account 124; the options 126-130 for selecting electronic documents from the external sources of a zip disk, local network which may include portable computing devices such as the user's PDA, and a secure internet/intranet site.

In response to a user selecting one of these electronic document sources, an exemplary embodiment of ATM 10 may be operative to cause the output of the user interface screen 140 shown in Figure 5. The user interface screen 140 may include a listing of electronic documents 142 that the ATM 10 has determined are present at the electronic document source selected with user interface screen 120. In response to a user selecting one of the listed electronic documents 142, an exemplary embodiment of the ATM 10 may be operative to cause the selected electronic document to be viewed through the display screen 18. Figure 6 is representative of an example of a user interface screen 160 which includes indicia representative of a selected automobile loan electronic document 162.

Exemplary embodiments of the ATM 10 may further include functionality for enabling the user to edit the displayed electronic document 162. For example in one exemplary embodiment, the ATM 10 may include software components for displaying through the output device 18 electronic documents which include HTML, DHTML, XML, Active X, .Net objects, plugins, Java script, and/or Java applets associated with the electronic document. Such features may generate input or selection fields on the display device, which can be completed or modified by operating the input devices of the ATM 10.

To further aid a user with the completion of fields in an electronic document, an exemplary ATM may further be operative to retrieve relevant information for completing input fields of an electronic document from a data

23

store of stored user information. The stored user information may be associated with the user's financial account and/or digital safe deposit account. The exemplary ATM may use the stored user information to automatically complete input fields of an electronic document. For example, the electronic document may include an input field labeled "ship_to_address." The stored user information may include address information which is associated with the description "ship_to_address." The exemplary ATM may be operative to retrieve matching user information from the data store and insert the matching user information in the input fields of the electronic document. When the user manually inputs information into an electronic document, exemplary embodiments of the ATM may further be operative to store the inputted information in the digital safe deposit account or other data store for later use with completing similarly labeled fields.

Once a user has completed reviewing and/or editing an electronic document, the exemplary embodiment of the ATM 10 may be operative to display a further user interface screen 170 as shown in Figure 7. User interface screen 170 may include a plurality of selectable functions 172 including the option to review the electronic document 174; the option to digitally sign the electronic document 176; the option to send the electronic document to another location 178; and the option of deleting the electronic document 180. In the described embodiment of ATM 10, the option to delete an electronic document 180 may be generally available when viewing an electronic document located in the user's digital safe deposit account.

When a user selects the option to digitally sign an electronic document 176, the exemplary embodiment of the ATM 10 may be operative to have a digital signature generated and attached to either the original or a copy of the electronic document. Exemplary embodiments may be operatively programmed to generate a digital signature using any digital signature algorithm and protocol. Examples of digital signature cryptography algorithms available for use with the present invention may include RSA and

100
94

DSA. In the exemplary embodiment an electronic document may be signed using a private key associated with the user. The digital signature may be verified at a later time by using a public key of the user which corresponds to the private key. Such a public key may be retrieved from a digital certificate of the user. In exemplary embodiments, the ATM may be operative to cause the digital certificate associated with the user to be attached to the electronic document when the electronic document is digitally signed. Also the ATM may be operative to cause the digital certificate associated with the certificate authority that signed the user's digital certificate to be attached to the electronic document.

For a digital signature to correspond to a legally binding signature of the user, the user may need to show his/her manifestation of intent to use a digital signature as a legally binding electronic signature. As a result, exemplary embodiments of the ATM 10 may provide additional user interface screens which require a user to affirmatively show such a manifestation of intent to create a legally binding electronic signature. For example, as shown in Figure 19, the ATM may output a user interface screen 182 which prompts the user to make an affirmative confirming input with an input device, that represents the intent of the user to create a legally binding electronic signature.

Some exemplary embodiments of the ATM 10 may cause a declaration to be attached to the electronic document that includes a statement that the user has affirmatively shown his intent to create a legally binding electronic signature with the generation of the digital signature. The ATM 10 may further cause such a statement and/or the entire electronic document to be digitally signed or digitally notarized by a further entity which affirms that the user provided an input to the ATM which represents the user's intent to create a legally binding electronic signature. The declaration and/or the electronic document may also be associated with a digital time stamp representative of the time the intent of the user was shown and/or when the digital signature was

25

created. Such a digital time stamp may be obtained by the ATM communicating with a digital time stamping server.

In some exemplary embodiments, the ATM 10 may prompt the user to hand write his/her signature on a digitizing signature pad. The ATM 10 may generate a digitized representation or scan of the handwritten signature in the form of a bitmap or vector drawing. The digitized representation of the written signature may then be incorporated into the electronic document by the ATM. A displayed or printed view of the electronic document may then include a visual representation of the customer's written signature.

When a user selects the option of sending an electronic document to another location 178, one exemplary embodiment of the ATM 10 may be operative to generate the user interface screen 190 as shown in Figure 8. User interface screen 190 may include a plurality of selection functions which correspond to different locations 192 to send a copy of the original or signed electronic document. In the presently described example, the selection functions 192 may include the option to send the electronic document to the digital safe deposit account 194, the options 196-200 to send the electronic document to the external sources of a zip disk, local network, and a secure internet/intranet site.

In one exemplary embodiment, the digital safe deposit account is associated with the private key of the user. In such embodiments the exemplary ATM 10 may include further user interface screens which enable a user to generate a private and public key set which may be associated with and/or stored in the user's digital safe deposit account. The private key may be used by the exemplary embodiment to sign electronic documents for the user.

Referring back to Figure 1, exemplary embodiments of the ATM 10 may further be in operative connection with a certificate authority 60. The exemplary ATM 10 may be operative to communicate with a certificate authority for purposes of creating a digital certificate such as an X.509 certificate which may be attached to the electronic document for purposes of

26

23

authenticating the digital signature created by a user. The exemplary ATM 10 may be operative to send the certificate authority information which identifies the user and a copy of the user's public key. In response, the certificate authority may be operative to generate and return a signed digital certificate which includes the identifying information and the user's public key. The digital certificate may then be attached to the electronic document by the ATM 10, stored in association with or in the user's digital safe deposit account and/or sent to an external source selected by the user. The ATM 10 may also receive a copy of the digital certificate associated with the certificate authority that issued and signed the user's digital certificate. Such a digital certificate of the certificate authority may also be attached to the electronic document, stored in association with or in the user's digital safe deposit account and/or sent to an external source selected by the user.

Figures 9-14 are schematic views of a plurality of different embodiments. Figure 9 shows an exemplary embodiment of an ATM 300 that may be operative to communicate with one exemplary embodiment of a storage server 302. Here the storage server may be operative to securely store private keys 304 associated with a plurality of different users. The exemplary private keys may be stored in association with digital safe deposit accounts and/or financial accounts such as a checking or savings account. In this described embodiment the ATM 300 may be operative to send an electronic document 306 associated with a user using the ATM 300 to the storage server 302. The storage server includes digital signature software 308 which may be operative to generate a digital signature 310 for the electronic document 306 using the private key 304 associated with the user. The storage server may then attach the digital signature to the electronic document and return the signed electronic document to the ATM 300 or the storage server may only send the digital signature 310 to the ATM 300. The exemplary ATM 300 may then attach the digital signature 310 to the electronic document 306 and

30

27

forward the signed electronic document to a selected destination location chosen by the user.

In the exemplary embodiment, the digital signature software may include the RSA algorithm. However in some exemplary embodiments, the digital signature software may include other or additional digital signature software/hardware. In embodiments where the server includes more than one type of digital signature software/hardware, the exemplary ATM 300 may be operatively programmed to enable users to select the type of digital signature they would like the ATM to generate for the electronic document.

Figure 10 shows an exemplary embodiment of an ATM 320 that may be operative to communicate with an exemplary embodiment of a storage server 322. Here the storage server 322 may also be operative to securely store private keys 324 associated with a plurality of different users. However, in this described embodiment, rather than sending the storage server 322 a complete copy of the electronic document 326, the exemplary ATM 320 may be operative to generate and send the storage server 322 a one-way hash 332 of the electronic document 326. The exemplary ATM 320 may include one or more one-way hash algorithms 334 which correspond to the digital signature protocols which the user wishes to use for signing his electronic document. For example, for generating digital signatures, exemplary one-way hash algorithm 334 of ATM 320 may include the one-way hash functions MD5 or SHA.

Here the storage server 322 may include one or more encryption and/or digital signing algorithms 328 such as RSA which are operative to generate a digital signature 330 for the electronic document 326 using the one-way hash 332 and the private key 324 associated with the user. The storage server may then return the digital signature 330 to the ATM 320 and the ATM 320 may attach the digital signature 330 to the electronic document 326.

Figure 11 shows an exemplary embodiment of an ATM 340 that may be operative to communicate with an alternative exemplary embodiment of a

28

25

storage server 342. Here the storage server 342 may also be operative to securely store private keys 344 associated with a plurality of different users. However, in this described embodiment, the storage server 342 may be operative to securely send a private key of a user to the ATM 340. The
5 exemplary ATM 340 may include digital signature software 348 which is operative to cause the ATM 340 to generate a digital signature 350 for an electronic document 346 of the user operating the ATM 340.

Figure 12 shows an exemplary embodiment of an ATM 400 that may be operative to communicate with a portable computing device 402 associated with a user such as a smart card, PDA, or mobile phone. Here the portable
10 computing device 402 may include at least one private key 404 associated with the user. In this described embodiment, after the user has viewed an electronic document 406 associated with the user, the ATM 400 may be operative to send the electronic document 406 to the portable computing device 402. The
15 exemplary portable computing device may include digital signature software 408 which is operative to generate a digital signature 410 for the electronic document 406 using the private key 404 stored on the portable computing device. The portable computing device 402 may then attach the digital
signature 410 to the electronic document 406 and return the signed electronic
20 document to the ATM 400 or the portable computing device may only send the digital signature 410 to the ATM 400. The exemplary ATM 400 may then attach the digital signature 410 to the electronic document 406 and forward the signed electronic document to a selected destination location chosen by the user.

Figure 13 shows an exemplary embodiment of an ATM 420 that may be operative to communicate with a portable computing device 422. Here the
25 portable computing device 422 may also include at least one private key 424 of the user. However, in this described embodiment, rather than sending the portable computing device 422 a complete copy of the electronic document 426, the exemplary ATM 420 may be operative to generate and send the
30

29

portable computing device 422 a one-way hash 432 of the electronic document 426. The exemplary ATM 420 may include one or more software components with one-way hash algorithms 434 that correspond to the digital signature protocols which the user wishes to use for signing his electronic document 426. Using the one-way hash algorithms 434, the ATM 420 may be operative to produce a one-way hash 432 of the electronic document 426 and forward the one-way hash 432 to the portable computing device 422.

The exemplary portable computing device 422 may include one or more encryption and/or digital signing algorithms 428 which are operative to generate a digital signature 430 for the electronic document 426 using the one-way hash 432 and the private key 424 associated with the user. The portable computing device 422 may then return the digital signature 430 to the ATM 420 and the ATM 420 may attach the digital signature 430 to the electronic document 426.

Figure 14 shows an exemplary embodiment of an ATM 440 that may be operative to communicate with an exemplary portable computing device 442. Here, the portable computing device 442 may include at least one private key 444 of the user. However, in this described embodiment, the portable computing device 442 may be operative to securely send the private key 444 of a user to the ATM 440. The exemplary ATM 440 may include digital signature software 448 which is operative to cause the ATM 440 to generate a digital signature 450 for an electronic document 446 of the user operating the ATM 440.

Referring back to Figure 1, the exemplary storage server 32 may be operative to maintain an access log 62 in association with the digital safe deposit account 40 and/or the financial account 48 of the user. The exemplary storage server 32 may be operative to store in the access log 62 a record of each attempted access of a user's digital safe deposit account 40 and/or use of the private key 44. If an imposter gains access to a user's digital safe deposit account and/or private key, the exemplary access log may be used to determine

90

when and where the unauthorized access occurred. The exemplary access log may further include a record of which electronic document was signed by the system. The record for example may include the one-way hash of the electronic document. If an imposter uses the present exemplary system to

5 digitally sign an electronic document, the access log may be reviewed to determine what document may have been forged.

Some exemplary embodiments of the ATM may be operative to encrypt electronic documents stored in the digital safe deposit account using a symmetrical encryption algorithm such as DES and a secret key. The

10 exemplary ATM may be operative to enable a user to generate a secret key for encrypting electronic documents from a password or from biometric information inputted by the user into the ATM. To decrypt the electronic documents, the exemplary ATM may be operative to regenerate the secret key by prompting the user to re-enter the password and/or biometric data.

15 In addition to causing an electronic document to be signed, an alternative exemplary embodiment of an ATM may be operative to digitally sign, notarize and/or cosign an electronic document using a private key associated with the ATM, storage server, digital signature service/ network, or a third party. For example, in addition to enabling a user to digitally sign an

20 electronic document using his private key, the exemplary ATM may also cause the electronic document to be further digitally signed using a further private key not associated with the private key of the user. Such a further private key may be associated with an authorized notary public, a digital signature service, or another party to a transaction which is associated with the electronic

25 document. The exemplary ATM may further attach the digital certificate associated with the further private key to the signed electronic document. Such a digital certificate can be used to verify the authenticity of the second digital signature. Also the digital certificates associated with the certificate authorities which issued and signed either or both of the user's digital

31

certificate and a digital certificate of the notary public or other party may also be attached to the electronic document.

In an exemplary embodiment, the ATM may be operative to attach a digital time stamp to the electronic document by including the current date and time in the electronic document prior to the electronic document being digitally signed by the user of the ATM. In some exemplary embodiments, the ATM may be operative to cause an electronic document to be digitally time stamped by a document time stamping entity or server. For example, the exemplary ATM may send a one-way hash of the electronic document to a time stamping entity. That time stamping entity would be operative to attach time data representative of the date, time and time zone at which the time stamping entity received the one-way hash. The time stamping entity may then digitally sign the one-way hash and time data with a private key of the time stamping entity to form a digital time stamp. This digital time stamp may then be returned to the ATM along with a digital certificate of the time stamping entity. The ATM may then attach the digital time stamp and the digital certificate of the time stamping entity to the electronic document. In some embodiments, the digital time stamping entity may correspond to the same entity, service, or network that is operative to produce the digital signature for the user of the ATM.

Figure 15 shows an example of a document signing system of one exemplary embodiment. Here the system 500 may include at least one ATM 510 that is operative to display and digitally sign electronic documents. The ATM 510 may further be operative to communicate with one or more servers 508 including servers associated with a financial transaction processing system, host banking system, document processing system, or a digital signature service or network.

In addition the ATM 510 may be operative to receive electronic documents from at least one personal computer (PC) 512 or other computing devices through a wired or wireless network 516. In this described

192

29

embodiment, ATM 510 may include or be in operative connection with a shared or externally accessible network drive 514 that is operative to store incoming and outgoing electronic documents. Such a shared network drive may be segregated into one or more locations such as an "in-box" and an "out-box" storage area.

The PC 512 may selectively be given permission to access the shared network drive 514 or a portion of the shared network drive such as an "in-box" associated with the ATM 510. Electronic documents created by the PC 512 may then be saved, exported and/or sent to the shared network drive 514 of the ATM 510. A user operating the ATM 510 may select commands of the ATM which cause the ATM to display and digitally sign electronic documents stored in the shared network drive 514. Digitally signed versions of the electronic document may then be saved, exported, or sent to the shared network drive 514 or a portion of the shared network drive such as an "out-box" of the shared network drive 514. The PC 512 or another computing device may then retrieval the signed document from the shared network drive 514. The ATM 510 may also be in operative connection with a printer 518 and may include selectable options for printing the digitally signed electronic document to the printer.

Exemplary embodiments of the ATM 510 may include transaction function devices such as a cash dispenser and a depository device which enable the ATM to perform other types of transaction functions such as the dispense of cash and the deposit of checks. However, some exemplary embodiments of the ATM 510 may be configured in a different form such as a portable form which does not dispense cash or receive deposited checks. An example of such a portable form of an ATM is shown in Figure 16. Here the exemplary embodiment of the portable ATM 520 may include a magnetic swipe card reader 522 or other card reader, a display screen 524, and a digitizing signature pad 526. The exemplary ATM 520 may further include function keys 528 for providing inputs to the ATM. Further exemplary

33

embodiments of the display screen 524 may include a touch screen for providing inputs to the ATM and a communication device 527 such as a wireless or wired network interface.

Referring back to Figure 15, the exemplary embodiment of the ATM 510 may be used by organizations which wish to offer users the ability to safely and securely digitally sign electronic documents. Such organizations may include banks, mortgage companies, title companies, S&Ls, insurance companies, car dealerships, leasing companies, universities, hospitals, government agencies, or any other organization that generates documents which require signatures by their customers. The exemplary ATM 510 provides the customers or clients of the organization or other users with a convenient method to view and digitally sign electronic documents.

Figure 17 shows exemplary steps involved with the operation of the system 500. Here the method steps are described with respect to a car dealership; however, it is to be understood that the exemplary steps may also apply to any organization, entity, group or individual that wishes to have users digitally sign electronic documents. The method may begin in step 600 with a finance manager or other member of the organization preparing electronic documents which correspond to a car loan. Such an electronic document may include a word processing document, an Acrobat® PDF document, eXtensible Markup Language (XML) document, or any other type of document which may electronically represent a car loan.

In an exemplary embodiment, the electronic document may conform to a standardized loan format. Such a format may include standardized XML tags which describe information about the Lender, Lendee, and terms of the loan. Such tags may include for example the names and addresses of the parties, the loan amount, the loan duration, the interest rate and any other term or category of information that may be part of the loan. Once the document is created, the finance manager in step 602 may save the electronic document to a storage location that is accessible to the ATM. For example, the finance

34

manager may save the electronic document to the "in-box" associated with the ATM.

In busy organizations which may process loan applications concurrently, multiple ATMs may be available for saving the electronic document. In such cases, the shared network drive may be associated with the name or identification of the particular ATM which is operative to access the electronic document from the shared network drive. Once the electronic document is saved to the storage location, the finance manager may direct the customer to begin using the particular ATM which is operative to retrieve the electronic document.

Once the customer has access to the ATM, the customer may follow the instructions displayed through the display screen of the ATM. If the customer already has a digital safe deposit account, digital certificate, and/or private key associated with a financial account, the customer may be prompted by the ATM to insert or swipe a card that is associated with the digital safe deposit account, digital certificate, and/or private key. For example if the customer has a checking account or a credit card which is associated with a digital safe deposit account, the customer may in step 604 insert or swipe his/her checking ATM card or credit card within the card reader of the ATM.

In response, the ATM may be operative to read the financial account number associated with the card in step 606 with the card reader and request that the customer input a PIN. In step 608 the customer may input a PIN through a keypad or through a touch screen which may be configured to display a visual representation of a keypad. In one exemplary embodiment, the PIN may correspond to the 4 digit PIN associated with the customer's financial account. In other exemplary embodiments, the PIN may correspond to a different password stored in association with the customer's digital safe deposit account, digital certificate, and/or private key. Such a password may include four or more digits and/or alphanumeric characters. In other

195

embodiments the ATM may prompt the user to provide biometric data as a password through use of a biometric reading device of the ATM.

For ATMs that are operative to perform many different types of transaction functions, the ATM may display a user interface screen similar to screen 100 of Figure 3 after the customer inputs a PIN. As discussed previously, user interface screen 100 may include selectable functions 102 for withdrawing cash, depositing a check, transferring value between accounts, and viewing an electronic document. For ATMs such as the portable ATM 520 of Figure 16, the ATM may immediately retrieve the electronic document stored in the "in-box" associated with the ATM and display a user interface screen similar to screen 160 of Figure 6. If more than one electronic document is present in the "in-box" the ATM may display a listing of available electronic documents to choose from. In each case the exemplary ATMs may be operative to retrieve an electronic document in step 610 from the storage location and display a visual representation of the document in step 612.

The customer may read through the document being displayed and make any necessary inputs of information that the electronic document may require. For example, the electronic document may include clauses which require a customer to affirmatively agree thereto. Such clauses may include user interface elements such as a checkbox, entry fields, and/or drop down list boxes which can be checked/unchecked, edited, and/or selected with the input devices of the ATM.

Once the document has been reviewed and updated with any necessary customer supplied information, in step 614 the customer may provide an input representative of a command to digitally sign the electronic document. In response, the ATM may in step 616 prompt the customer to provide a further input that is representative of a confirmation by the customer that the digital signature is intended to be the customer's legally binding signature. For ATMs that include a digitizing signature pad, this confirming input may include having the customer draw his/her handwritten signature on the

10/2/02
36

digitizing signature pad. The digital scan of the handwritten signature may then be integrated into the electronic document prior to digitally signing the document.

5 In response to receiving a confirming input, the ATM in step 618 may cause the electronic document to be digitally signed using a private key associated with the financial account read from the customer's card. Once the document has been digitally signed it may be associated with one or more digital certificates including the digital certificate associated with the financial account. Such a digital certificate includes the customer's public key which
10 can be used to verify the digital signature on the electronic document. In other embodiments, the electronic document may include a serial number and/or a reference to an entity, address or URL where the customer's digital certificate may be retrieved to verify the digital signature. In some embodiments, the digital certificate of the certificate authority which issued and signed the user's
15 digital certificate may be associated with the electronic document.

Once the electronic document has been digitally signed, the ATM in step 620 is operative to send the signed electronic document to one or more specified output addresses. Such a specified output address may include the original storage location where the ATM retrieved the unsigned electronic
20 document. Such a specified output address may include a portion of shared network drive which corresponds to an electronic "out box." Such a specified output address may correspond to a network address, e-mail address, data base, URL, or any other external storage location or communication system which is operative to receive an electronic document. For example, in one
25 exemplary embodiment the specified output address may include a URL of a document processing server. For example, if the electronic document corresponds to a car loan, the specified output address may be a document processing server of a bank that is lending money to the customer to buy the car.

37

Such a document processing server may verify the digital signature of the electronic document. If the signature is valid, the document processing server may parse the XML tags of the electronic document to determine the name and address of the party and the terms of the loan. Such information may then be integrated into the loan processing system of the bank to establish a loan account and to initiate processes necessary to collect payments from the customer. In other exemplary embodiments, the specified output address may correspond to a loan processing system that is operative to securitize the loan for resale to another bank or other entity. In other exemplary embodiments, the specified output address may correspond to any system that is operative to store and/or process the signed electronic document.

In one exemplary embodiment the specified output address may be a configurable parameter within the ATM. In other exemplary embodiments, the specified output address may be determined by the ATM from a parameter of the electronic document. For example, the electronic document may include an XML tag which includes an address for the specified output address. In exemplary embodiments where the customer's financial account is associated with a digital safe deposit account, the ATM may further cause a copy of the signed electronic document to be stored in the customer's digital safe deposit account which may be associated with the customer's financial account.

In the exemplary embodiment, the ATM in step 622 may cause a digital signature processing fee to be assessed to a party associated with the electronic document. The exemplary ATM is operative to cause a financial transaction processing system such as a host banking system or other server to record information associated with the processing fee in a database, log, or journal for immediate or delayed settlement. In an exemplary embodiment, the processing fee may be charged to the financial account associated with the customer's card. In other exemplary embodiments, the processing fee may be charged to an account associated with the organization that prepared the

unsigned electronic document. For example, the ATM may include a configuration parameter that corresponds to a financial account that may be assessed processing fees. In the case of a car dealership for example, the configuration parameter may include an account number associated with the car dealership or the bank providing the loan. In step 622 the ATM or the digital signature service or network servers associated with the ATM may communicate with a financial transaction processing system such as a host banking system to charge the processing fees to the account. In an exemplary embodiment, the electronic document may include an account number that is to be assessed the processing fees. For example the electronic document may include an XML tag for a fee processing account.

Also in some exemplary embodiments, the ATM may contact a financial transaction processing system such as a host banking system or other server to authorize the assessing of the processing fee to an account prior to digitally signing the document in step 618 or prior to sending the signed electronic document to a specified output address in step 620. If the account does not have sufficient funds to pay for the processing fee or otherwise is not able to accept a charge of a processing fee, the ATM may be operative to cancel the signing of the electronic document. The ATM may then output a visual message through the display screen of the ATM that indicates that the electronic document cannot be digitally signed.

The specified output address may correspond to a storage location that is accessible to the organization which created the unsigned document. For example, with reference to a car dealership, the specified output address may include the network drive which is accessible to the finance manager. The manager may then cause the electronic document to be printed out so that a hard copy view of the electronic document may be given to the customer. In other embodiments, the ATM may be in operative connection with a printer and may include a selectable option for printing out a hard copy of the electronic document.

39

In some exemplary embodiments where the electronic document was previously signed by one or more further parties, the ATM may include the step of validating the signature of the further party prior to enabling a user to digitally sign the electronic document. In the case of a car dealership for example, the finance manager may digitally sign the car loan prior to the ATM accessing the electronic document. The digital signature of the car dealership may be verified by the ATM prior to enabling the user to digitally sign the car loan. In such cases the electronic document may include the digital certificate associated with the further parties such as the car dealership. The electronic document may also include the digital certificates of the certificate authorities which signed the digital certificates of the further parties.

In the previously described embodiment, a financial account card of the customer was previously associated with the customer's digital safe deposit account, digital certificate, and/or private key. The exemplary embodiment may include a method for providing financial account cards with the ability to digitally sign electronic documents at an ATM. For example, a credit card issuer such as a bank may have a plurality of credit card accounts. As the credit card business tends to be highly competitive, adding a digital signing capability to the credit cards of the bank's customers may provide an additional incentive for the customer to carry and use the bank's issued credit cards.

This described embodiment of the method may include the bank or other entity creating individual digital certificates, public/private key pairs, and/or digital safe deposit accounts for a plurality of pre-existing financial accounts such as credit card accounts or other financial accounts. Such individual digital certificates, public/private key pairs, and/or digital safe deposit accounts may be stored in association with each of the financial accounts on one or more servers operated by the bank or a digital signature service or network.

Figure 18 shows a schematic view of an exemplary embodiment of a system 700 that may be operative to carry out this described method. Here the system 700 includes a plurality of banks 702, 704, or other financial organizations. Each of the banks includes a plurality of financial accounts 706, 708 such as credit card accounts. For each of these accounts, the banks may have a digital signature service or network entity 710 manage a digital certificate, public/private key pair, and/or digital safe deposit account in one or more storage servers 712.

The exemplary embodiment of the digital signature service or network 710 includes or is in operative communication with a host system 714. The host system is operative to provide a plurality of ATMs 716 with access to the services of the digital signature network 710. Such services may include for example the digital signing of electronic documents and the storage of electronic documents in digital safe deposit accounts. As discussed previously, customers of the banks 702, 704 may use their credit cards or other cards associated with financial accounts to cause an ATM to digitally sign electronic documents. The processing fees acquired from the signing of electronic documents may be transferred or assessed to at least one of the entities that operates the digital signature network and the banks or other card issuers. In one exemplary embodiment, the processing fees may be split between the entity that operates the digital signature network and the banks or other card issuers.

To advertise that the financial accounts of the customers may be used to digitally sign electronic documents, the described exemplary method may include marking or branding the cards issued by the bank with a logo, design, or mark which indicates that the card may be used to digitally sign electronic documents. Such a logo may be a source indicator mark such as a trademark/service mark for the digital signature network 710. In addition, to enable a customer to more easily locate the ATMs 716 which may be used to sign electronic documents, the ATMs 716 may include or output a matching

41
02/07

logo. For banks or other entities with a large number of preexisting financial accounts such as credit cards, the exemplary embodiment of the presently described method may include mailing replacement credit cards to the customers which include a mark such as a logo which indicates that the card may be used to digitally sign electronic documents. In one exemplary embodiment, the customers may use the PIN previously associated with their financial account to access an ATM for purposes of digitally signing an electronic document. In other exemplary embodiments, the bank may supply the user with a separate password for use with accessing the services of the digital signature network.

In some exemplary embodiments, the ATM may be operative to cause a new digital certificate to be created for a user for use with signing an electronic document. For example, if the user does not have a previously issued digital certificate, public/private key pair and/or digital safe deposit account associated with a smart card, portable computing device, financial account, credit card, and/or digital safe deposit account, the exemplary ATM may be operative to provide the user with a digital certificate, public/private key pair, and/or digital safe deposit account. In some exemplary embodiments, the ATM may enable the user to forward the newly created digital certificate to a smart card, portable storage medium, portable computing device, networked storage location, or other user selectable storage location or address for use in signing electronic documents in the future through the exemplary ATM or other digital signature software and devices. As will be discussed below, in some exemplary embodiments the ATM may enable a user to associate the newly created digital certificate, public/private key pair, and/or digital safe deposit account with a card selected by the user or issued to the user by the digital signature network.

As with regard to the fees associated with the signing of electronic documents, fees may also be caused to be assessed by the ATM for the creation of a digital certificate, a public/private key pair, and/or a digital safe

42

deposit account. As discussed previously, such fees may be accessed to a financial account of the user, a financial account stored in association with the ATM, or a financial account associated with the electronic document intended to be signed. For example, as in the previously discussed scenario of signing electronic documents related to car loans, the ATM may be operative to cause the fees associated with the creation of the digital certificate to be associated with the entity supplying the electronic documents such as the car dealership or financial institution issuing the loan.

The described exemplary embodiment of the ATM may prompt the user to enter through an input device of the ATM information about the user which is to be integrated into and/or associated with the digital certificate. Such information may include the name, address, and birth date of the user. The information may also include the user's social security number, passport number, driver's license number, national identification number, student number, or any other unique number associated with the user. The information provided for generating the digital certificate may also include a user provided password or other number for use with creating or accessing public/private key pairs, the public key thereof being integrated into the digital certificate.

To expedite the input of information into the ATM for generating the digital certificate, the ATM may be operative to retrieve user specific information for the digital certificate from an electronic document intended to be digitally signed using the ATM. For example, in the previous example scenario of a user signing loan documents for a car, the finance manager or other employee of the car dealership may input the user's name, address, social security number, birth date, drivers license number, and/or other user specific information into the electronic document that corresponds to the loan. Such information may be stored as XML data or another computer accessible format within or in association with the electronic document. Prior to the ATM enabling the user to sign the electronic document, the ATM may access the

43

user specific information associated with the electronic document. The information accessed from the electronic document in addition to any information requested to be inputted directly into the ATM by the user, may be caused to be integrated into a digital certificate by the ATM. In some

5 exemplary embodiments, the ATM may output the user specific information through an output device of the ATM. The ATM may prompt the user to verify the accuracy of the information prior to causing digital certificate to be created.

In an exemplary embodiment, the ATM may cause the user specific

10 information to be forwarded to a certificate authority which is operative to issue a signed digital certificate for the user. In some embodiments, the ATM may forward the user specific information to the previously discussed digital signature network, storage server, and/or other server which is operative to format the digital certificate and/or interface with the certificate authority to

15 issue the digital certificate.

In an exemplary embodiment, the digital signature network may further be operative to authenticate the provided user specific information by contacting a credit reporting service 720 or other database of user information to compare and validate the provided user specific information. If the user

20 specific information is invalid, inconsistent, or is otherwise suspect, the exemplary digital signature network may return a message to the ATM which is representative of a denial to generate a digital certificate for the user. Such a message may indicate the reasons for the denial.

Exemplary embodiments of the ATM may further acquire additional

25 information from the user requesting the digital certificate including a biometric input, such as a fingerprint scan, a digital image of the user's face, iris scan, hand scan, or any other input which may be representative of the identity of the user. Such information may be integrated into or associated with the digital certificate. Such information may also be used to validate the

30 identity of the user prior to creating the digital certificate.

44
02/02

In some exemplary embodiments, the ATM may further prompt the user to input a card, such as a credit card, smart card, drivers license, national identification card, or any other unique card which can be accessed by the card reader of the ATM to retrieve user specific information. Such user specific information may include an account number or other number stored on the card which can be forwarded to the digital signature network, financial transaction processing system such as a host banking system, or other server to be used to authenticate the identity of the user. In some exemplary embodiments, the ATM may further prompt the user to input through an input device of the ATM, a secret password or PIN associated with the card. The ATM may be operative to validate the inputted secret password or PIN through communication with the digital signature network, host banking system, or the card itself.

In some exemplary embodiments, the ATM may prompt the user to provide an input that indicates whether the user would like the newly created digital certificate, public/private key pairs and/or digital safe deposit account to be associated with a pre-existing financial account of the user such as a credit card or a bank card. In such cases, the exemplary ATM may prompt the user to insert or swipe the desired card through the card reader of the ATM. The account number read from the card may be forwarded to the digital signature network and be stored in association with the user's newly created digital certificate, public/private key pairs, and/or digital safe deposit account. The digital signature network may further notify the financial institution associated with the card, that the consumer has associated a digital certificate, public/private key pairs and/or digital safe deposit account with the account number of the card. The financial institution may then issue a new card to the user, which includes the mark or logo of the digital signature network.

Exemplary embodiments of the ATM may also prompt the user, as to whether the user would like the newly created digital certificate, public/private key pairs and/or digital safe deposit account to be associated with other

45

cards/numbers uniquely associated with the user. Such cards for example may include the user's social security card, drivers license card, national identification card, and student ID card. In such cases, the exemplary ATM may prompt the user to insert or swipe the card with the desired unique
5 number stored thereon through the card reader of the ATM. The unique number read from the card may be forwarded to the digital signature network and be stored in association with the user's newly created digital certificate, public/private key pairs, and/or digital safe deposit account.

In some embodiments, where the newly created digital certificate, public/private key pairs, and/or digital safe deposit account is not associated
10 with a financial account or other unique card/number of the user, the digital signature network may be operative to issue the user a digital signature card for use with signing future electronic documents and for accessing electronic documents stored in the user's digital safe deposit account. The digital
15 signature card may include stored thereon a unique account number associated with the newly created digital certificate, public/private key pairs, and/or digital safe deposit account. In one exemplary embodiment, the ATM may include a card issuing device which is operative to output the digital signature card directly to the user once the digital certificate is created. In further
20 exemplary embodiments, the digital signature network may initiate the production of a digital signature card which is mailed to the address of the user.

Once the digital certificate, public/private key pair, and/or digital safe deposit account is created, the exemplary ATM may proceed to prompt the
25 user through the process of signing the electronic document using the private key associated with the newly created digital certificate.

In exemplary embodiments, where the user associates a financial account or other card/number with a newly created digital certificate or where a digital signature card is issued to the user, the ATM may prompt the user to input
30 through an input device of the ATM, a secret password or PIN to be

46

associated with the card for purposes of using the card in the future to sign electronic documents and/or for accessing electronic documents stored in the newly created digital safe deposit account. In the future, the user may use his/her credit card, digital signature card, or other card associated with the newly created digital certificate, public/private key pair, and/or digital safe deposit account to sign other electronic documents at the same ATM or other exemplary ATM connected to the exemplary digital signature network. As discussed previously exemplary embodiments of the ATM may prompt the user to enter the password or PIN associated with the card prior to enabling the user to sign electronic documents and/or access electronic documents for a digital safe deposit account with the ATM.

As shown in Figure 18, the exemplary embodiment of the digital signature network may further be in communication with a public network such as the Internet 718 to enable user to access their digital certificate, public/private key pair, and/or digital safe deposit account from a home computer or other computing device. The digital signature network may further provide services over the Internet such as digitally signing electronic documents and/or storing electronic documents in a digital safe deposit account associated with a financial account. For example, in one exemplary embodiment, the digital signature network may include a web server which enables a user to enter his/her financial account number or other card/number and PIN or other password through a browser of a PC or other computing device. If the entered information is valid, the exemplary digital signature network may enable the user to sign an electronic document using the private key associated with the inputted financial account number or other card/numbers. The web server may further enable Internet users to manage electronic documents that are stored in the storage servers of the digital signature network 710, such as viewing, copying, deleting, and forwarding the documents to other locations and addresses.

47
02/02

Computer software used in operating the automated transaction machines of the present invention and connected computers, computer processors, and servers may be loaded from articles of various types into the respective computers. Such computer software may be included on and loaded
5 from one or more articles such as diskettes, compact disks, or DVDs. Such software may also be included on articles such as hard disk drives, tapes, read-only memory devices, or memory cards. 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 automated
10 transaction machines and associated digital signature services, networks and servers and systems in accordance with embodiments described herein.

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

Thus the new automated transaction machine digital signature system and method achieves one or more of the above stated objectives, eliminates
20 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 used for descriptive purposes and
25 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
30 to those skilled in the art to be capable of performing the recited function, and

148
07/2002

45

shall not be limited to the features and structures shown herein 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.

- 5 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 and relationships are set forth in the appended claims.

CLAIMS

We claim:

1. An apparatus comprising:

5 an ATM, wherein the ATM includes:

 at least one computer processor;

10 at least one input device in operative connection with the
 computer processor; and

 at least one display device in operative connection with the
 computer processor, wherein the computer processor is
 operative to output a visual representation of at least one
15 electronic document through the display device responsive to at
 least one first input through the at least one input device, and
 wherein the computer processor is operative to cause the at
 least one electronic document to be digitally signed with a
 private key responsive to at least one second input through the
20 at least one input device.

2. The apparatus according to claim 1, wherein the computer
processor is operative to cause a message to be output through the display
device which prompts a user to enter through the at least one input device a
25 confirming input which is representative of a confirmation that a digital
 signing of the electronic document is intended to be a legally binding
 signature, wherein the at least one second input includes the confirming input.

3. The apparatus according to claim 1, wherein the ATM further
30 includes a cash dispenser device in operative connection with the computer

50
/ 50

c

47

processor, wherein the computer processor is operative to cause the cash dispenser to dispense currency responsive to at least one third input through the at least one input device.

5 4. The apparatus according to claim 2, wherein the ATM further includes a digitizing signature pad in operative connection with the computer processor, wherein the computer processor is operative to receive at least one hand written signature scan through the digitizing signature pad, wherein the computer processor is operative to include the hand written signature scan
10 with the electronic document.

5. The apparatus according to claim 3, wherein the ATM further includes a card reader in operative connection with the computer processor, wherein the computer processor is operative to cause the card reader to read at
15 least one account number from a card, wherein the computer processor is operative to cause a remote server to access the private key responsive to the at least one account number read from the card.

6. The apparatus according to claim 5, wherein the account number
20 includes a financial account number associated with a financial account.

7. The apparatus according to claim 6, wherein computer processor is operative to cause the electronic document to be digitally time stamped.

25 8. The apparatus according to claim 7, wherein the ATM includes a fascia, wherein the at least one display device and the at least one input device are accessible to the user through the fascia, wherein further comprising a visible indicia adjacent the fascia, wherein the visible indicia is representative of source indicator mark for a digital signature service.
30

51
6000

9. The apparatus according to claim 5, wherein the ATM further includes at least one communication port in operative connection with the computer processor, wherein the computer processor is operative to communicate with at least external source through the communication port,
5 wherein the computer processor is operative to retrieve the electronic document from the at least one external source.

10. The apparatus according to claim 9, wherein the computer processor is operative to send a digitally signed copy of the electronic
10 document to the at least one external source.

11. The apparatus according to claim 9, wherein the at least one external source includes a network accessible storage location.

12. The apparatus according to claim 9, wherein the at least one
15 external source includes portable computing device.

13. The apparatus according to claim 2, wherein the computer processor is operative responsive to the at least one second input to attach a
20 statement to the electronic document which indicates that the user confirmed that the digital signing of the electronic document is intended to represent a legally binding electronic signature of the user.

14. The apparatus according to claim 13, wherein the computer
25 processor is operative to cause at least the statement to be digitally signed with a further private key.

15. The apparatus according to claim 3, wherein the ATM further includes a storage device drive in operative connection with the computer
30 processor, wherein the computer processor is operative to read and write to a

S2
~~2/20~~

49

portable storage medium placed in operative connection with the storage device drive, wherein the computer processor is operative to retrieve the electronic document from the portable storage medium.

5 16. The apparatus according to claim 15, wherein the computer processor is operative to store a digitally signed copy of the electronic document on the portable storage medium.

10 17. The apparatus according to claim 3, further comprising at least one server located remotely from the ATM, wherein the computer processor is operative to communicate with the at least one server, wherein the at least one server is operative to generate a digital signature responsive to the private key.

15 18. The apparatus according to claim 17, wherein the computer processor is operative to send the electronic document to the at least one server, wherein the at least one server is further operative to generate the digital signature responsive to the electronic document.

20 19. The apparatus according to claim 17, wherein the computer processor is operative to generate and send a one-way hash of the electronic document to the at least one server, wherein the at least one server is further operative to generate the digital signature responsive to the one-way hash, wherein the computer processor is operative to receive the digital signature from the at least one server, wherein the computer processor is operative to
25 attach the digital signature to the electronic document.

30 20. The apparatus according to claim 3, wherein the computer processor is operative to communicate with at least one server located remotely from the ATM, wherein the computer processor is operative to retrieve the private key from the at least one server, wherein the computer



processor is operative to generate a digital signature responsive to the electronic document and the private key.

5 21. The apparatus according to claim 3, wherein the computer processor is operative to communicate with at least one portable computing device, wherein the at least one portable computing device includes the private key, wherein the at least one portable computing device is operative to generate a digital signature responsive to the private key.

10 22. The apparatus according to claim 21, wherein the computer processor is operative to send the electronic document to the at least one portable computing device, wherein the at least one portable computing device is further operative to generate the digital signature responsive to the electronic document.

15 23. The apparatus according to claim 21, wherein the computer processor is operative to generate and send a one-way hash of the electronic document to the at least one portable computing device, wherein the at least portable computing device is further operative to generate the digital signature
20 responsive to the one-way hash, wherein the computer processor is operative to receive the digital signature from the portable computing device, wherein the computer processor is operative to attach the digital signature to the electronic document.

25 24. The apparatus according to claim 3, wherein the computer processor is operative to communicate with at least one portable computing device, wherein the computer processor is operative to retrieve the private key from the at least one portable computing device, wherein the computer
30 processor is operative to generate a digital signature responsive to the electronic document and the private key.

25. The apparatus according to claim 3, wherein the ATM further includes a smart card reader in operative connection with the computer processor, wherein the computer processor is operative to communicate with at least one smart card through the smart card reader, wherein the private key is stored on the smart card., wherein the smart card is operative to generate a digital signature responsive to the private key.

26. The apparatus according to claim 25, wherein the computer processor is operative to send the electronic document to the smart card, wherein the smart card is further operative to generate the digital signature responsive to the electronic document.

27. The apparatus according to claim 25, wherein the computer processor is operative to generate and send a one-way hash of the electronic document to the smart card, wherein the smart card is further operative to generate the digital signature responsive to the one-way hash, wherein the computer processor is operative to receive the digital signature from the smart card, wherein the computer processor is operative to attach the digital signature to the electronic document.

28. The apparatus according to claim 3, wherein the ATM further includes a smart card reader in operative connection with the computer processor, wherein the computer processor is operative to communicate with at least one smart card through the smart card reader, wherein the private key is stored on the smart card., wherein the computer processor is operative to retrieve the private key from the smart card, wherein the computer processor is operative to generate a digital signature responsive to the electronic document and the private key.

55
01/20**29. An automated transaction machine comprising:**

at least one computer processor;

5 at least one display device in operative connection with the computer processor, wherein the computer processor is operative to output a visual representation of an electronic document through the display device;

10 a card reader in operative connection with the computer processor, wherein the computer processor is operative to cause the card reader to read indicia corresponding to at least one account number from a card; and

15 at least one input device in operative connection with the computer processor, wherein the computer processor is operative to output a message through the display device which prompts a user to enter a confirming input through the at least one input device which is representative of a confirmation that a digital signing of the electronic
20 document is intended to be a legally binding signature, wherein the computer processor is operative to cause the electronic document to be digitally signed with a private key associated with the account number responsive to the confirming input.

25 30. The apparatus according to claim 29, further comprising a digitizing signature pad in operative connection with the computer processor, wherein the computer processor is operative to receive at least one hand written signature scan through the digitizing signature pad, wherein the computer processor is operative to include the hand written signature scan
30

56

53

with the electronic document prior to the electronic document being digitally signed.

5 31. The apparatus according to claim 29, further comprising a cash dispenser in operative connection with the computer processor, wherein the computer processor is operative to cause the cash dispenser to dispense cash responsive to at least one further input received through the at least one input device.

10 32. The apparatus according to claim 29, wherein the computer processor is operative to access at least one digital safe deposit account located remotely from the automated transaction machine, wherein the private key is stored in association with the digital safe deposit account, wherein the account number is associated with digital safe deposit account.

15 33. The apparatus according to claim 32, wherein the computer processor is operative to access at least one storage server, wherein the at least one storage server is in operative connection with at least one data store, wherein the at least one data store includes the private key stored in
20 association with the digital safe deposit account.

25 34. The apparatus according to claim 33, wherein the computer processor is operative to cause the storage server to store the electronic document in the at least one data store in association with the digital safe deposit account.

30 35. The apparatus according to claim 29, wherein the account number includes a financial account number associated with a financial account.

57

36. The apparatus according to claim 35, wherein the computer processor is operative to communicate the financial account number to at least one remote server, wherein the remote server is operative to access the private key responsive to the financial account number.

5

37. The apparatus according to claim 36 wherein the computer processor is operative to cause the remote server to produce a digital signature for the electronic document responsive to the private key, wherein the computer processor is operative to receive the digital signature from the remote server and attach the digital signature to the electronic document.

10

38. The apparatus according to claim 37, wherein the computer processor is operative to attach a digital certificate to the electronic document, wherein the digital certificate includes a public key that is operative to validate the digital signature.

15

39. The apparatus according to claim 29, wherein the computer processor is operative to cause the private key and a matching public key to be produced, wherein the computer processor is in operative communication with a certificate authority, wherein the computer processor is operative to cause the certificate authority to generate a digital certificate that includes the public key.

20

40. The apparatus according to claim 39, wherein the computer processor is operative to attach the digital certificate to the electronic document.

25

41. The apparatus according to claim 40, wherein the computer processor is operative to cause the private key and the digital certificate to be stored in association with a digital safe deposit account.

30

58

55

42. The apparatus according to claim 41, wherein the computer processor is operative to cause a remote server to establish the digital safe deposit account.

5 43. The apparatus according to claim 42, wherein the computer processor is operative to cause the remote server to associate the digital safe deposit account with a financial account associated with the account number.

10 44. The apparatus according to claim 29, wherein the computer processor is operative to cause the private key to be produced, wherein the computer processor is operative to cause the private key to be remotely stored in association with the account number.

15 45. The apparatus according to claim 44, wherein the account number corresponds to a financial account number.

20 46. The apparatus according to claim 29, wherein the computer processor is operative to communicate with a financial transaction processing system, wherein the computer processor is operative to cause the electronic document to be digitally signed responsive to communication with the financial transaction processing system.

25 47. The apparatus according to claim 29, wherein the computer processor is operative to cause the electronic document to be further digitally signed with a further private key.

30 48. The apparatus according to claim 47, wherein the further private key is associated with a notary public.

49. The apparatus according to claim 29, wherein computer processor is operative to cause the electronic document to be digitally time stamped.

50. The apparatus according to claim 29, wherein prior to causing the electronic document to be digitally signed, the computer processor is operative to modify the electronic document responsive to at least one further input through the at least one input device.

51. A method comprising:

- a) accessing an electronic document with an ATM;
- b) displaying the electronic document through a display screen of the ATM;
- c) prompting a user to enter at least one first input representative of a confirmation that a digital signature for the electronic document is intended to correspond to a legally binding signature;
- d) receiving the at least one first input through at least one input device of the ATM;
- e) producing the digital signature for the electronic document responsive to the at least one first input; and
- f) attaching the digital signature to the electronic document.

52. The method according to claim 51, wherein after step (b) further comprising:

57

g) capturing a handwritten signature scan through a digitizing signature pad of the ATM; and

h) attaching the handwritten signature scan to the electronic document.

5

53. The method according to claim 51, wherein further comprising:

g) receiving at least one second input through the at least one input device;

10

h) causing a cash dispenser of the ATM to dispense cash responsive to the at least one second input.

54. The method according to claim 51, wherein prior to step (e) further comprising:

15

g) reading a financial account number from a card through operation of a card reader of the ATM;

h) causing a private key associated with the financial account number to be accessed from a remote server; and

20

wherein in step (e) the digital signature is caused to be generated responsive to the private key associated with the financial account number.

25

55. The method according to claim 51, further comprising:

g) producing a digital time stamp for the electronic document; and

h) attaching the digital time stamp to the electronic document.

30

56. Computer readable media bearing instructions which are operative to cause at least one computer in the ATM to cause the ATM to carry out the method steps recited in claim 51.

5

57. A method comprising:

- 10
- a) reading a financial account number from a card through operation of a card reader device;
- b) sending the financial account number read from the card to a server associated with a digital signature network, wherein the server is operative to cause a private key stored in association with a financial account to be accessed responsive to correlating the financial account number read from the card with the financial account; and
- 15
- c) causing an electronic document to be digitally signed responsive to the private key associated with the financial account.
- 20

58. The method according to claim 57, further comprising:

- 25
- d) accessing a digital safe deposit account that corresponds to the financial account number; and
- e) causing the electronic document to be stored in a remote data store in association with the digital safe deposit account.
- 30

02/062

59

59. The method according to claim 57, further comprising:

d) receiving the electronic document from the remote data store;
and

5

e) sending the electronic document to an external storage location
other than the remote data store.

60. The method according to claim 57, wherein prior to step (c) further
comprising:

10

d) outputting a visual representation of the electronic document
through a display device of an automated transaction machine
including a cash dispenser, wherein the automated transaction
machine includes the card reader device.

15

61. The method according to claim 60, wherein prior to step (c) further
comprising:

20

e) enabling a user to modify the content of the electronic
document through at least one input to at least one input device
of the automated transaction machine.

62. The method according to claim 60, wherein prior to step (c) further
comprising:

25

e) capturing a handwritten signature scan through a digitizing
signature pad of the automated transaction machine; and

30

- f) attaching the handwritten signature scan to the electronic document.

5 63. The method according to claim 57, wherein prior to step (c) further comprising:

- e) prompting a user to enter at least one input representative of a confirmation that the digital signature is intended to correspond to a legally binding signature; and
- 10 wherein step (c) is performed responsive to receiving the at least one input.

64. The method according to claim 63, wherein after step (e) further comprising:

- 15 f) receiving the at least one input through at least one input device of an automated transaction machine, wherein the automated transaction machine includes the card reader device; and
- 20 g) causing a record of the at least one input to be stored in association with the financial account number.

65. The method according to claim 57, wherein in step (a) the financial account number corresponds to a credit card number.

25 66. The method according to claim 57, wherein prior to step (c) further comprising:

- d) receiving at least one input through at least one input device of an automated transaction machine, wherein the automated
- 30

64
~~64~~

61

transaction machine includes the card reader device; and

- e) sending the server associated with the digital signature network information corresponding to the received at least one input, wherein the server is operative to cause access to the private key to be permitted responsive to a determination that the received input corresponds to a password associated with the private key.

67. The method according to claim 66, wherein in step (d) the at least one input corresponds to biometric data received through a biometric reading device of the automated transaction machine.

68. The method according to claim 66, wherein in step (d) the at least one input corresponds to a PIN of the financial account, wherein the PIN is entered through a keypad of the automated transaction machine.

69. The method according to claim 57, further comprising:

d) causing the electronic document to be digitally time stamped.

70. Computer readable media bearing instructions which are operative to cause at least one computer in the automated transaction machine to cause the automated transaction machine to carry out the method steps recited in claim 57.

71. A method comprising:

a) accessing an electronic document with an automated transaction machine;

65
~~62~~

62

- 5 b) causing a digital certificate to be produced, wherein the digital certificate includes information associated with the identity of a user of the automated transaction machine, wherein the digital certificate includes a public key that corresponds to a private key;
- c) displaying a visual representation of the electronic document through a display screen of the automated transaction machine;
- 10 d) prompting a user to enter at least one input representative of a confirmation that a digital signature for the electronic document is intended to correspond to a legally binding signature;
- e) receiving the at least one input through at least one input device
- 15 of the automated transaction machine;
- f) causing the digital signature for the electronic document to be produced responsive to the at least one input and the private key; and
- 20 g) causing the digital signature and digital certificate to be attached to the electronic document.

25 72. The method according to claim 71, wherein prior to step (b) further comprising:

- h) retrieving at least a portion of the information associated with the identity of the user from the electronic document.

30

66
[Signature]

63

73. The method according to claim 72, further comprising:

- h) causing a digital safe deposit account to be established for the user in a remote data store, including storing the digital certificate and the private key in association with the digital safe deposit account.

74. The method according to claim 73, further comprising:

- i) causing a digitally signed copy of the electronic document to be stored in association with the digital safe deposit account.

75. The method according to claim 71, wherein in step (a) the electronic document is accessed from a network accessible storage location.

76. The method according to claim 71, further comprising:

- h) sending a digitally signed copy of the electronic document to a network accessible storage location.

77. The method according to claim 71, further comprising:

- h) sending a digitally signed copy of the electronic document to a network address specified by the electronic document.

78. The method according to claim 71, further comprising:

- h) sending a digitally signed copy of the electronic document to a network address specified by the automated transaction machine.

67 76 77

79. The method according to claim 71, further comprising:

- h) causing a digital signature processing fee to be assessed to an account specified in the electronic document through communication with a financial transaction processing system.

80. The method according to claim 71, further comprising:

- h) causing a digital signature processing fee to be assessed to an account specified by the automated transaction machine through communication with a financial transaction processing system.

81. The method according to claim 71, further comprising:

- h) causing a digital time stamp to be created for the electronic document; and
- i) causing the digital time stamp to be attached to the electronic document.

82. The method according to claims 71, wherein the automated transaction machine includes a cash dispenser.

83. Computer readable media bearing instructions which are operative to cause at least one computer in the automated transaction machine to cause the automated transaction machine to carry out the method steps recited in claim 71.

68
68

65

84. An apparatus comprising:

at least one computer processor; and

5 at least one data store in operative connection with the computer processor, wherein the at least one data store includes a plurality of digital safe deposit accounts stored therein, wherein each of the digital safe deposit accounts is associated with at least one private key, wherein the computer processor is operative to communicate with a
10 plurality of ATMs, wherein the computer processor is operative responsive to at least one of the ATMs to cause a digital signature to be produced for an electronic document responsive to the private key associated with one of the digital safe deposit accounts.

15 85. The apparatus according to claim 84 wherein the computer processor is operative to receive the electronic document from the at least one ATM, wherein the computer processor is operative to store the electronic document in the data store in association with the one digital safe deposit account.

20 86. The apparatus according to claim 85 wherein the computer processor is operative to retrieve the electronic document from the data store and send the electronic document to any one of the plurality of ATMs.

25 87. The apparatus according to claim 85 wherein the computer processor is operative to encrypt and decrypt the electronic document stored in the at least one data store responsive to a secret key received from the at least one ATM.

30

88. The apparatus according to claim 84 wherein each digital safe deposit account is associated with a financial account number, wherein the computer processor is operative to access the private key associated with the one digital safe deposit account responsive to a message received from the at least one ATM which includes a financial account number that corresponds to the financial account number associated with the one digital safe deposit account.

89. The apparatus according to claim 88, wherein the at least one financial account number corresponds to a credit card number.

90. The apparatus according to claim 84 wherein each digital safe deposit account is associated with at least one digital certificate, wherein the computer processor is operative to cause the digital signature and at least one of the digital certificates associated with the one digital safe deposit account to be attached to the electronic document.

91. The apparatus according to claim 84 wherein the computer processor is operative to maintain and store in the at least one data store, an access log in association with each digital safe deposit account.

92. The apparatus according to claim 84 wherein the at least one ATM includes a cash dispenser, wherein the computer processor is operative through communication with a financial transaction processing system to cause a dispense of cash from the cash dispenser to be authorized.

93. The apparatus according to claim 84 wherein the computer processor is operative to cause a new digital safe deposit account to be created in the data store responsive to communication from the at least one ATM.

70
10/2/05

67

94. The apparatus according to claim 93 wherein the computer processor is operative to cause a new private key and a corresponding public key to be produced responsive to communication from the at least one ATM, wherein the computer processor is operative to store the private key in association with the new digital safe deposit account.

95. The apparatus according to claim 94 wherein the computer processor is operative to cause a digital certificate to be generated and stored in association with the new digital safe deposit account, wherein the digital certificate includes the public key.

96. The apparatus according to claim 95 wherein the computer processor is operative to receive a financial account number from the at least one ATM, wherein the computer processor is operative to store the financial account number in association with the new digital safe deposit account.

97. The apparatus according to claim 96 wherein the computer processor is operative to receive a password input from the at least one ATM, wherein the computer processor is operative to store the password input in association with the new digital safe deposit account.

98. The apparatus according to claim 84 wherein the computer processor is operative to receive a one-way hash of the electronic document from the at least one ATM, wherein the computer processor is operative to cause the digital signature to be generated responsive to the one-way hash and the private key.

99. The apparatus according to claim 84 wherein the computer processor is operative to cause a second digital signature to be produced for

41
0000

the electronic document responsive to a private key that is not associated with the one digital safe deposit account.

5 100. The apparatus according to claim 84 wherein the computer processor is operative to cause a digital signature processing fee to be assessed to a financial account in response to causing the digital signature to be produced for the electronic document.

10 101. The apparatus according to claim 100 wherein the computer processor is operative to receive information about the financial account from the at least one ATM.

15 102. The apparatus according to claim 84 wherein the computer processor is operative to cause a digital time stamp to be produced and attached to the electronic document.

103. A method comprising:

- 20 a) receiving a financial account number from an automated transaction machine;
- b) accessing a private key associated with the financial account number; and
- 25 c) enabling an electronic document displayed by the automated transaction machine to be digitally signed with the private key.

30 104. The method according to claim 103, wherein prior to step (c) further comprising:

72
0000

69

d) receiving a password from the automated transaction machine;
and

5

e) verifying that the password corresponds to a valid password
previously associated with the financial account number.

105. The method according to claim 103, further comprising:

10

d) accessing a digital certificate previously associated with the
financial account number, wherein the digital certificate
includes a public key that corresponds to the private key,
wherein the public key is capable of being used to validate the
digital signature; and

15

e) enabling the digital certificate to be associated with the
electronic document.

106. The method according to claim 103, further comprising:

20

d) storing a digitally signed copy of the electronic document in a
digital safe deposit account in association with the financial
account number.

107. The method according to claim 103, further comprising:

25

d) receiving a second financial account number from the
automated transaction machine; and

30

e) assessing a processing fee associated with the digital signing of
the electronic document to a financial account associated with
the second financial account number.

73
[Handwritten signature]

108. The method according to claim 103, further comprising:

- d) enabling the electronic document to be digitally time stamped.

5

109. The method according to claim 103, further comprising:

- d) dispensing cash from the automated transaction machine.

110. A method comprising:

10

- a) receiving a request from an automated transaction machine to digitally sign an electronic document visually displayed by the automated transaction machine, wherein the request includes an account number that is associated with a digital safe deposit account;

15

- b) accessing a private key associated with the digital safe deposit account responsive to the account number; and

20

- c) producing a digital signature for the electronic document responsive to the private key; and

- d) causing the digital signature to be attached to the electronic document.

25

111. The method according to claim 110, further comprising:

- e) storing a digitally signed copy of the electronic document in a data store in association with the digital safe deposit account.

30

74

112. The method according to claim 110, wherein in step (a) the account number corresponds to a financial account number.

113. The method according to claim 110 and further comprising:

5

e) dispensing cash from the automated transaction machine.

114. A method comprising:

10

a) receiving a request at an ATM to digitally sign an electronic document visually displayed by the ATM;

b) causing a digital signature and a digital time stamp to be produced for the electronic document; and

15

c) causing the digital signature and the digital time stamp to be attached to the electronic document.

115. The method according to claim 114 and further comprising:

20

d) dispensing cash from the ATM.

116. A method comprising:

25

a) producing a plurality of digital certificates for a plurality of individual customers, wherein each individual customer is associated with an account;

30

b) associating the accounts of the individual customers with the corresponding digital certificates of the individual customers;

75
[Handwritten signature]

- 5 c) producing at least one card for each of the individual customers, wherein each card includes a first visible indicia thereon which corresponds to a source indicator mark for a digital signature service, wherein each card includes machine readable data corresponding to an account number associated with the account of the individual customer;
- d) sending the cards to the individual customers; and
- 10 e) enabling each individual customer to digitally sign an electronic document using any one of a plurality of automated transaction machines and one of the cards, wherein each automated transaction machine is operative to display a visual representation of the electronic document through a display device of the automated transaction machine, wherein each
- 15 automated transaction machine is operative to cause the electronic document to be digitally signed through communication with the digital signature service, wherein the communication includes the account number read from the card
- 20 by the automated transaction machine.

117. The method according to claim 116, wherein in step (e) each of the machines includes a second visible indicia which corresponds to a source indicator mark for the digital signature service.

118. The method according to claim 117, wherein in step (e) the second indicia is displayed adjacent a fascia of the automated transaction machines, wherein the first indicia and the second indicia are visually similar.

76
~~11/20/01~~

119. The method according to claim 116, wherein in step (a) each digital certificate includes a public key that corresponds to a private key, wherein in step (c) the digital signature service is operative to cause the electronic document to be digitally signed responsive to the private key that
5 corresponds to the public key of the digital certificate which is associated with the account of the individual customer using the machine.

120. The method according to claim 116, wherein in step (e) the digital signature service is operative to access a private key associated with the account number read from the card, wherein the digital signature service is
10 operative cause the electronic document to be digitally signed responsive to the private key.

121. The method according to claim 116, wherein in step (c) the cards
15 correspond to financial account cards, wherein the accounts correspond to financial accounts.

122. The method according to claim 121, wherein in step (e) the automated transaction machines are operative to cause processing fees to be
20 assessed for the digital signing of electronic documents, and further comprising:

f) enabling an entity that manages the financial accounts for the individual customers to receive at least a portion of the
25 processing fees.

123. The method according to claim 116, wherein in step (e) the automated transaction machines include digitizing signature pads, wherein the automated transaction machines are operative to include handwritten signature
30 data captured with the digitizing signature pads in the electronic documents.

77
02/02

124. The method according to claim 116, wherein at least some of the automated transaction machines include cash dispensers, wherein the automated transaction machines that include cash dispensers are further operative to dispense cash.

5

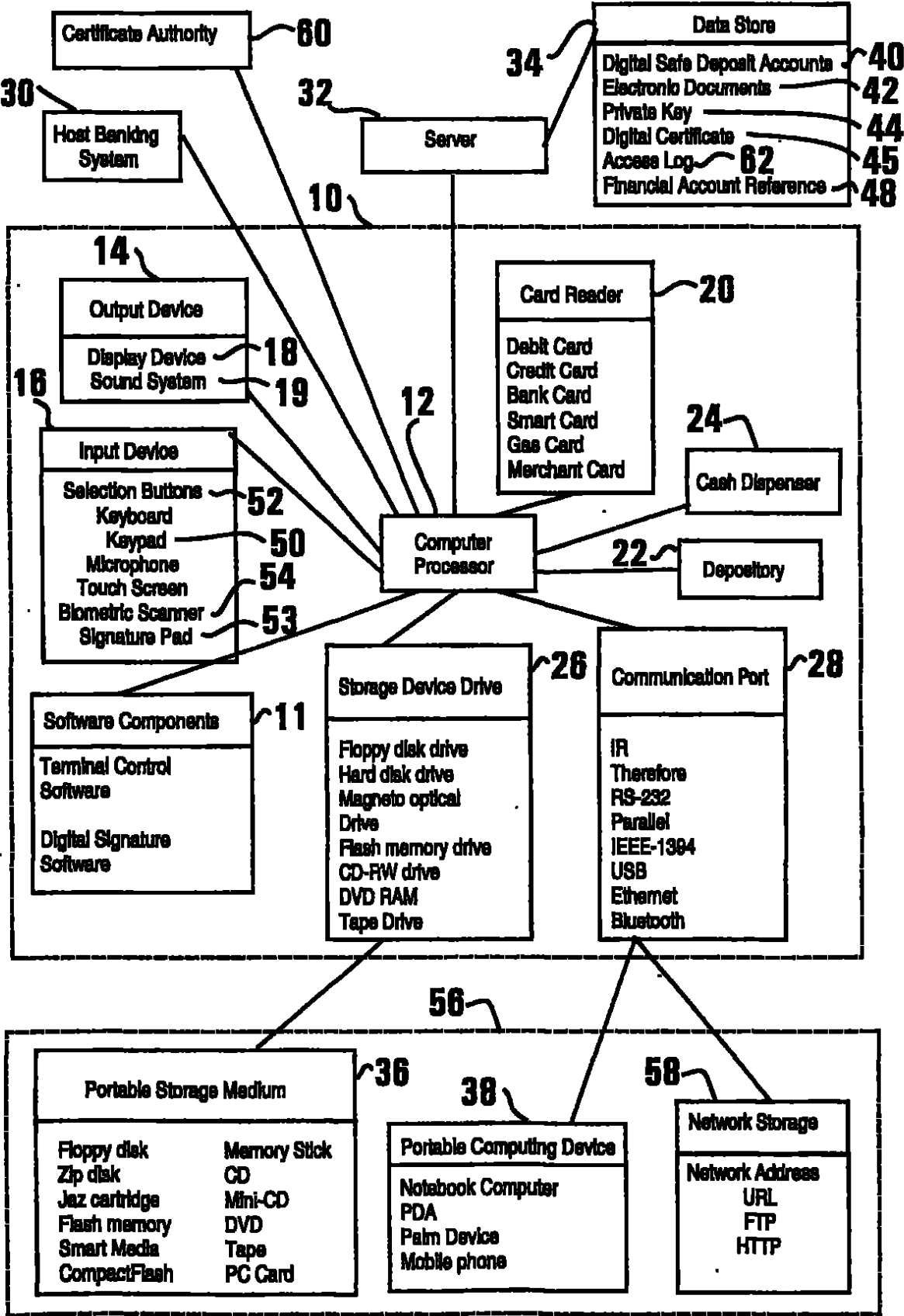
125. The method according to claim 124, wherein in step (c) the cards correspond to bank cards, wherein the accounts correspond to banking accounts, and wherein the automated transaction machines include cash dispensers, and wherein the automated transaction machines are further operative to dispense cash withdrawn from the banking accounts.

10

126. The method according to claim 116, wherein in step (a) the accounts correspond to digital safe deposit accounts, wherein in step (c) the cards correspond to digital safe deposit account cards.

15

78
~~100~~



79
[Handwritten signature]

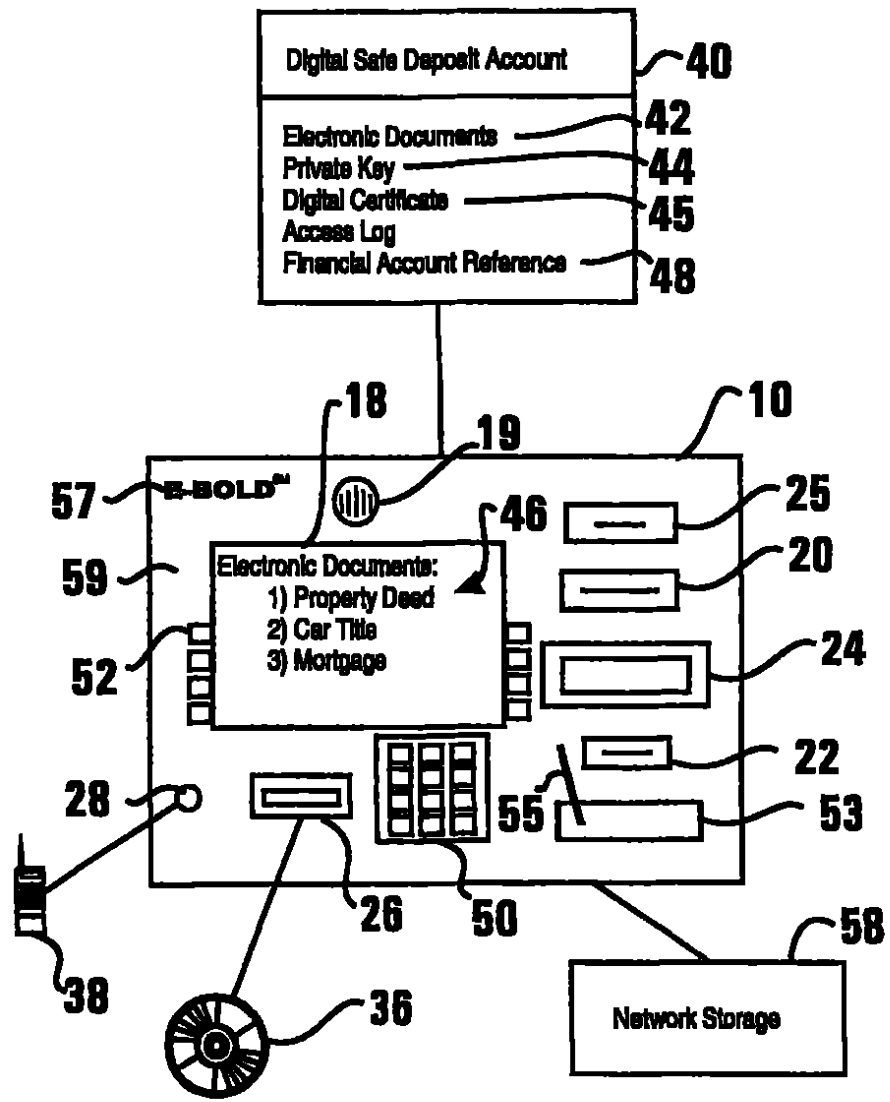


FIG. 2

80

3/11

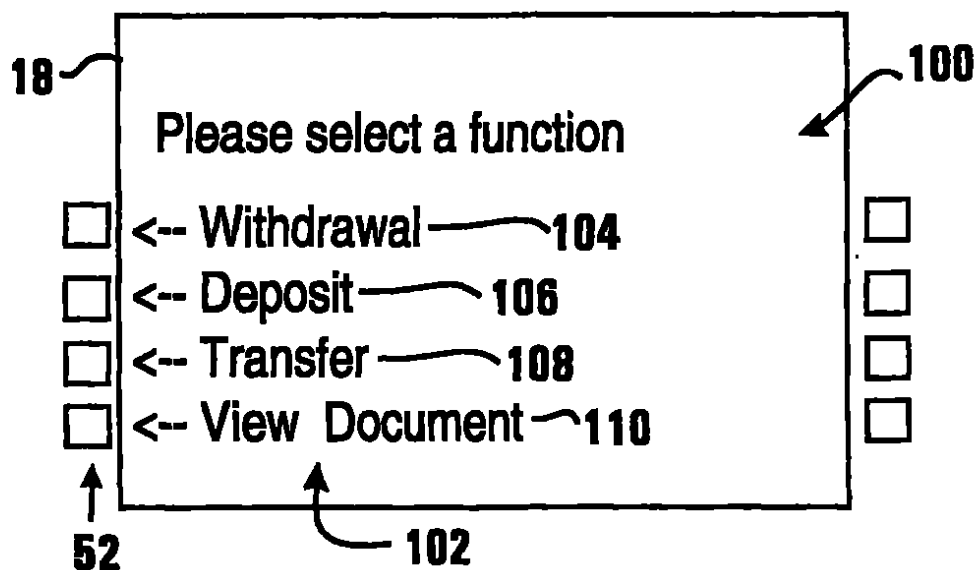


FIG. 3

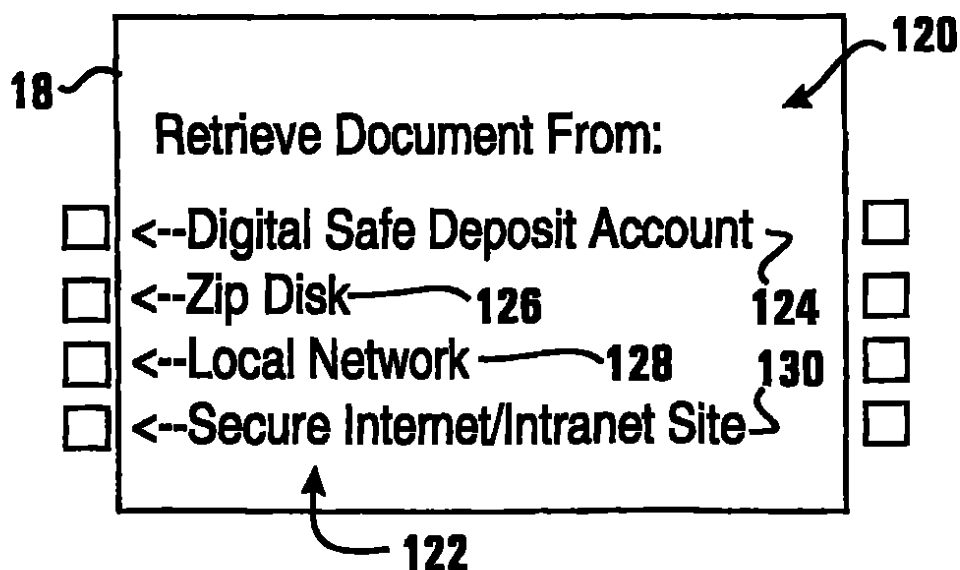


FIG. 4

81
[Handwritten signature]

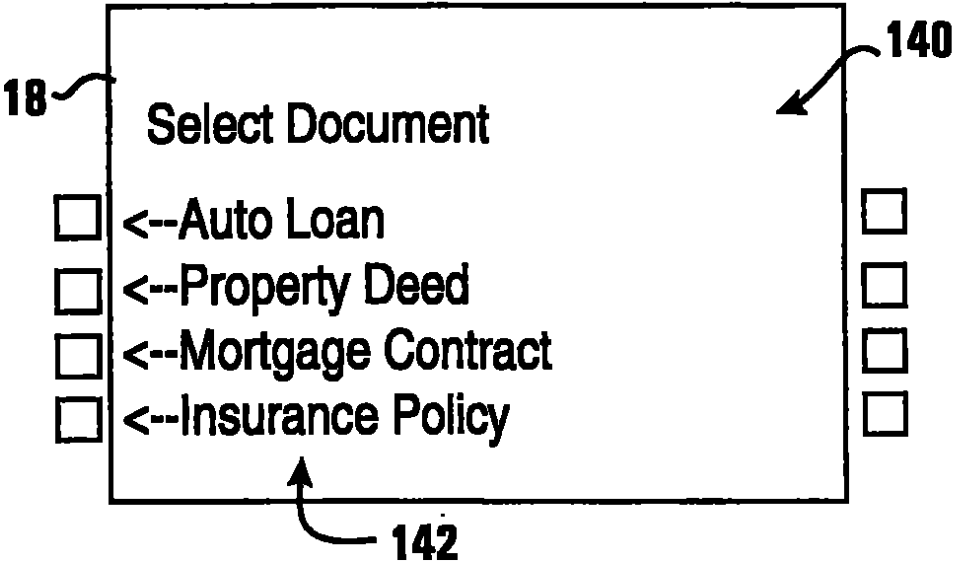


FIG. 5

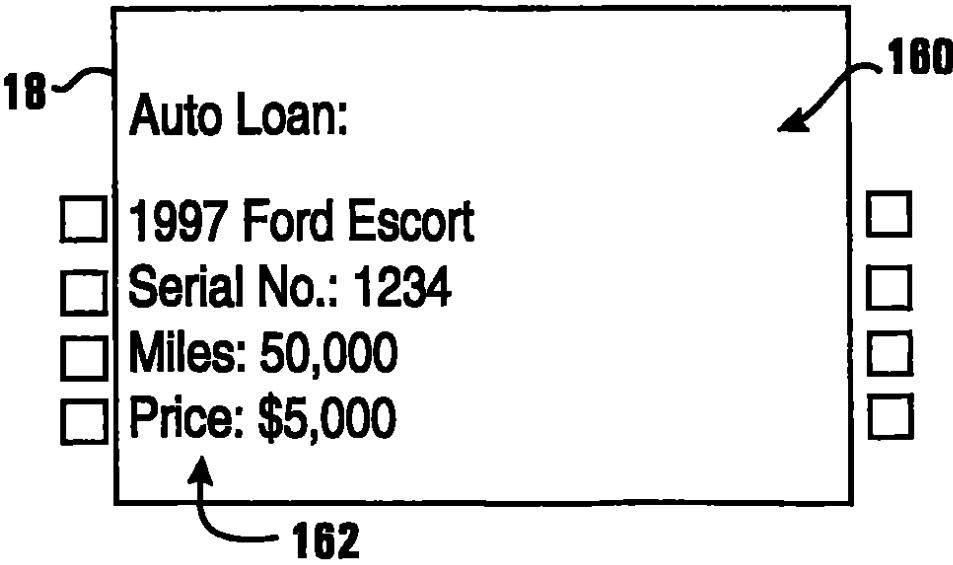


FIG. 6

82
~~82~~

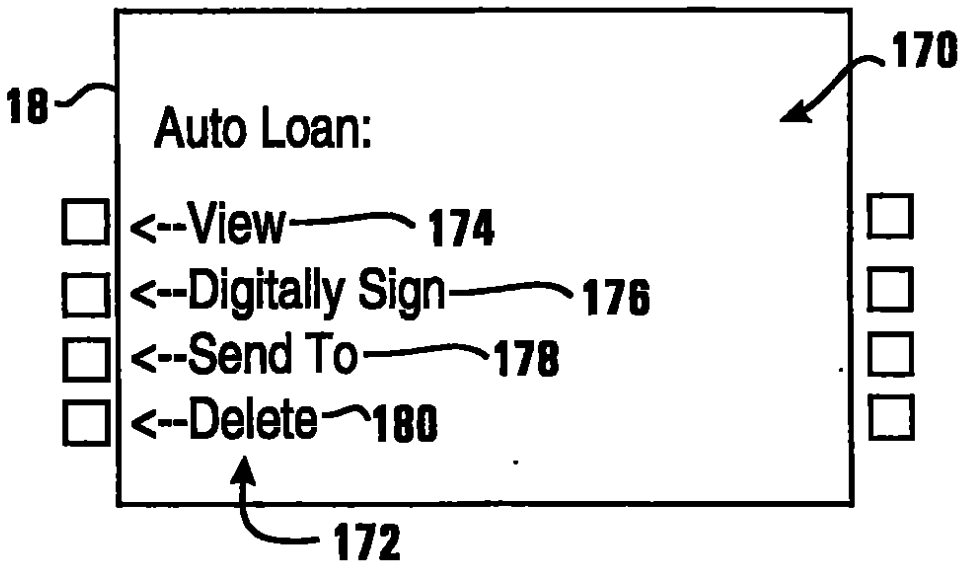


FIG. 7

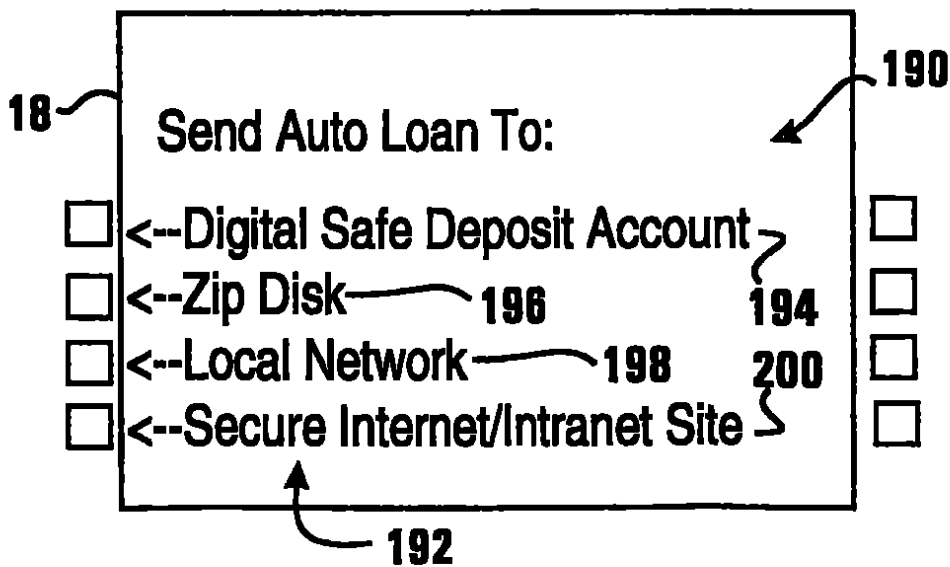


FIG. 8

83
0000

FIG. 9

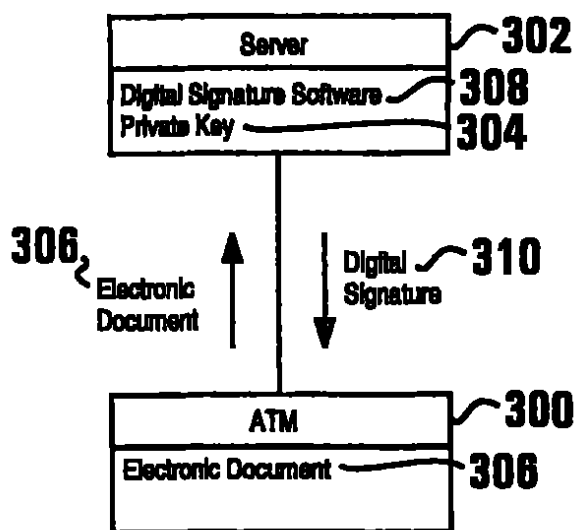


FIG. 10

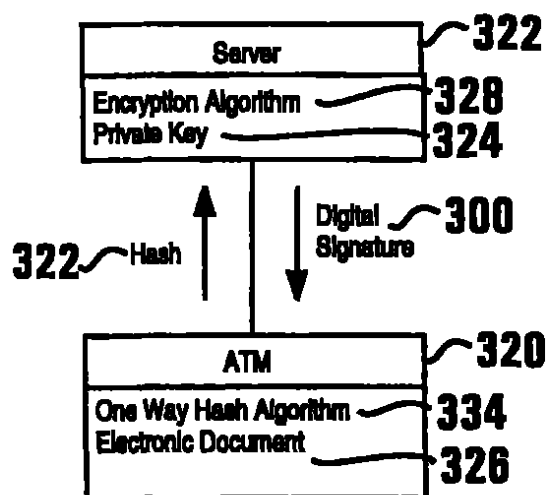
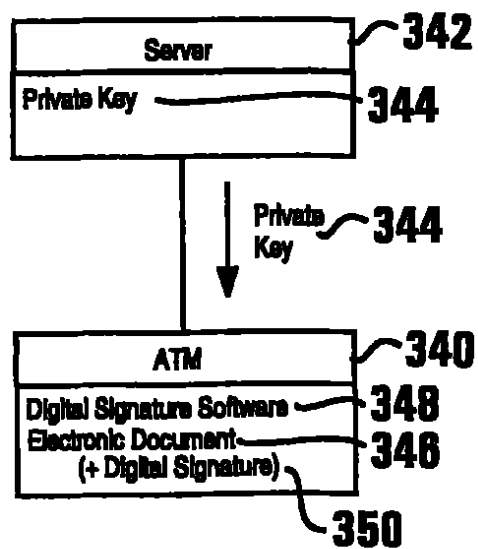


FIG. 11



84
2/2002

FIG. 12

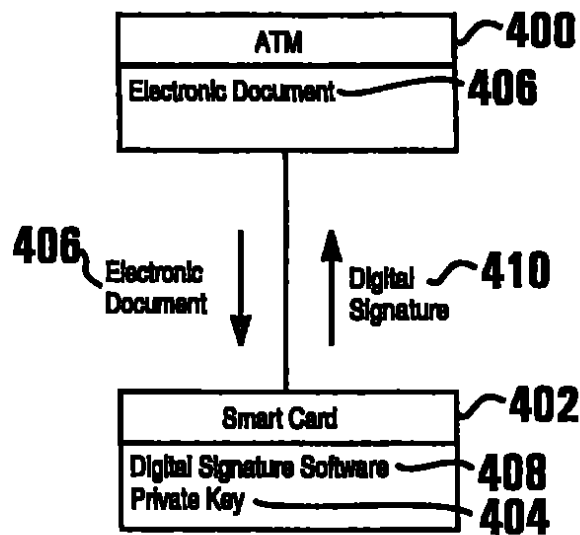


FIG. 13

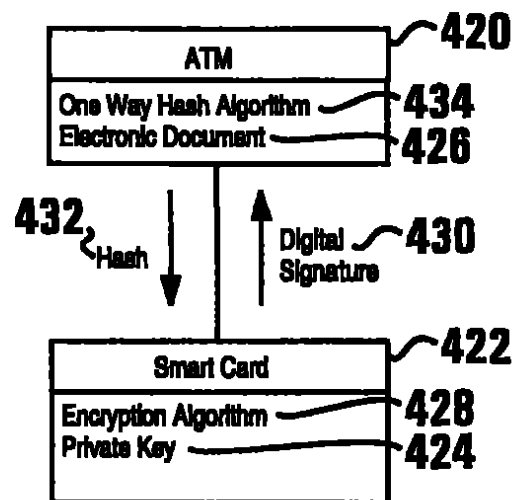
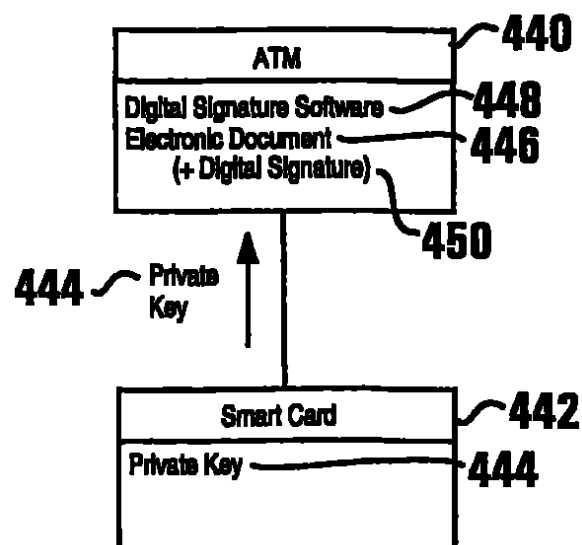


FIG. 14



85
02/073341

8/11

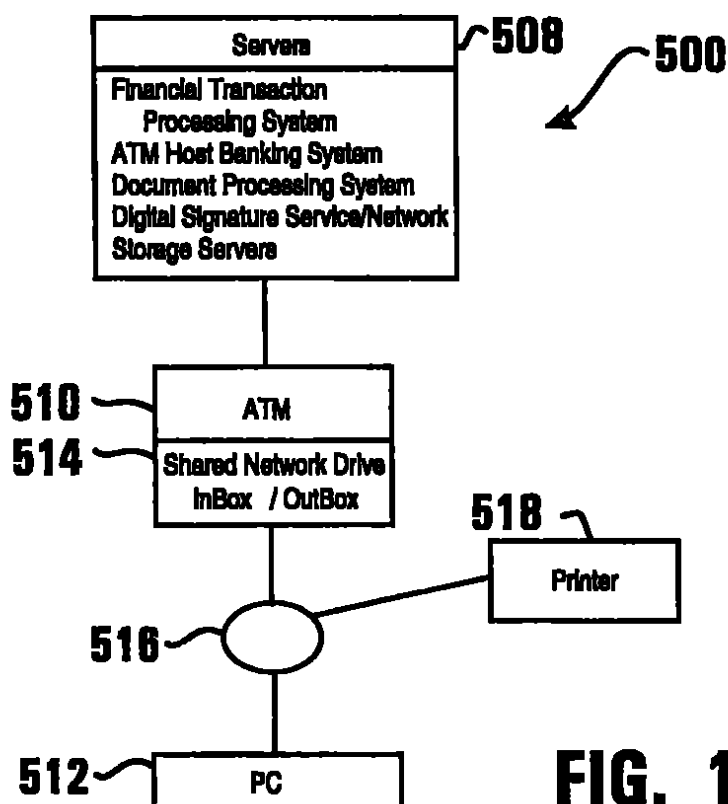


FIG. 15

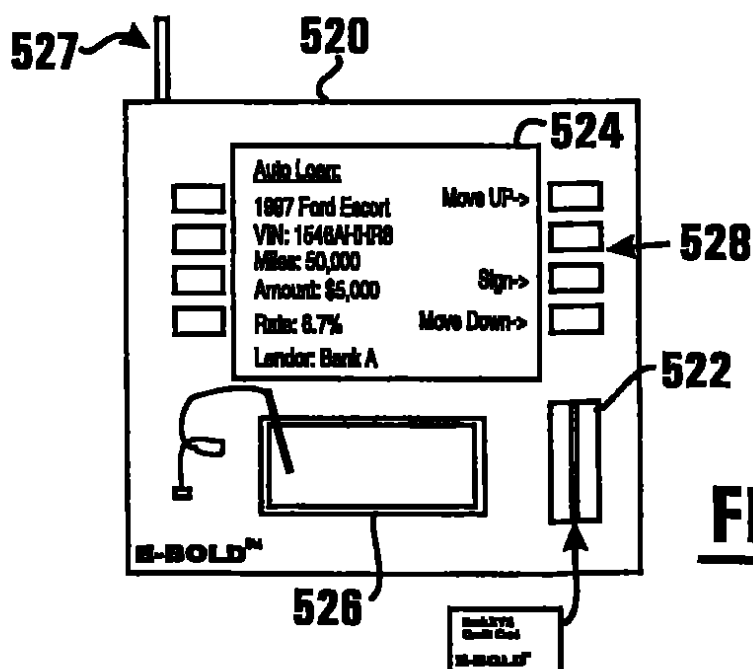
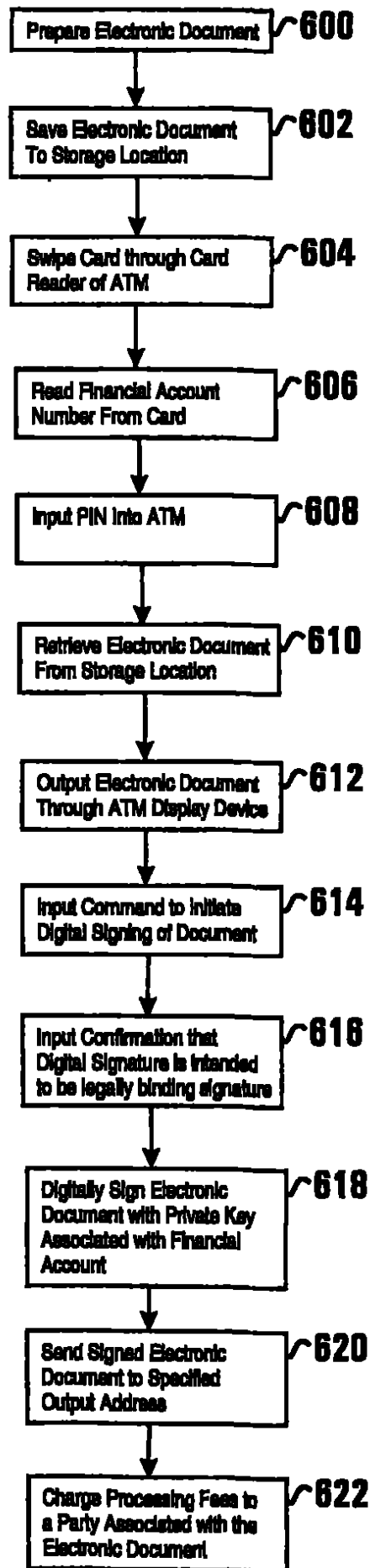


FIG. 16

86
9/11

9/11

FIG. 17

87
[Handwritten signature]

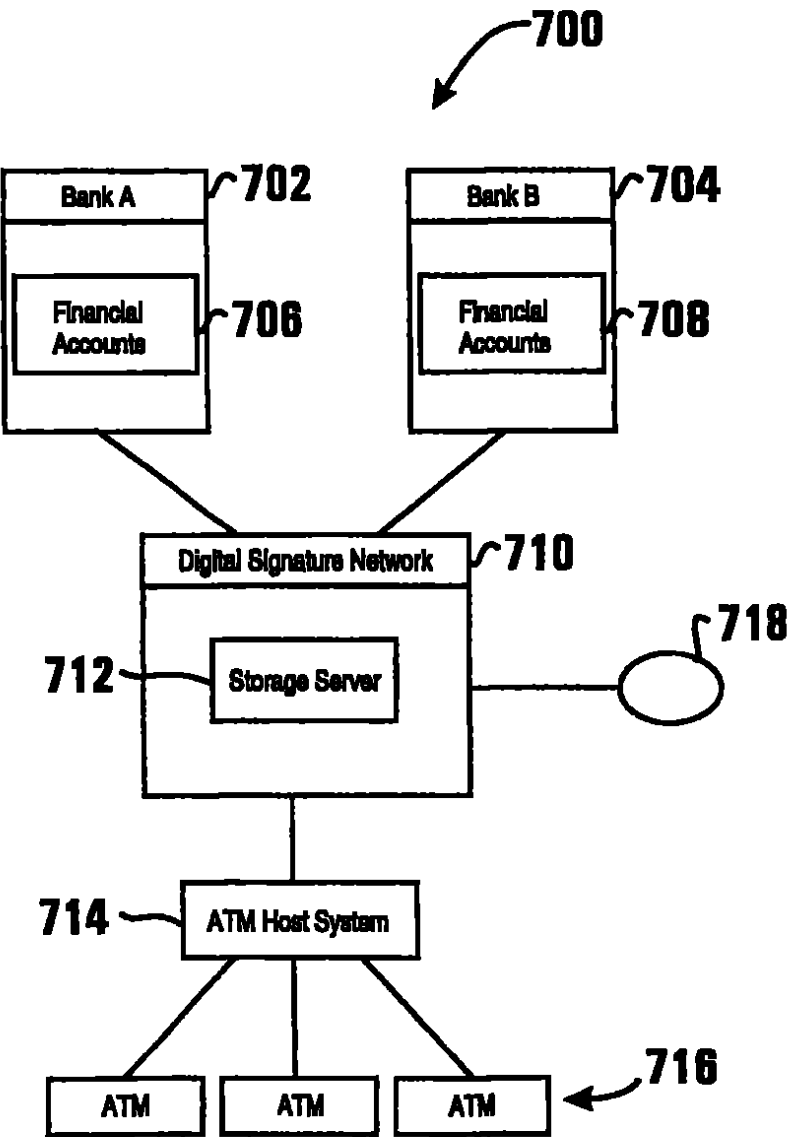


FIG. 18

18

Auto Loan:

182

☐ I confirm that the digital signing of this document is intended to create my legally binding electronic signature.

☐ <-- YES NO--> ☐

☐

☐

FIG. 19

SISTEMA Y MÉTODO DE FIRMAS DIGITALES DE MÁQUINA AUTOMÁTICA DE TRANSACCIONES

5

CAMPO TÉCNICO

Este invento se relaciona con máquinas automáticas de transacciones. Específicamente este invento se relaciona con un sistema y método de máquina automática de transacciones que es capaz de firmar digitalmente documentos electrónicos.

10

ESTADO DE LA TÉCNICA DE FUNDAMENTO

Puesto que un número creciente de individuos posee o tiene acceso a computadores personales, más y más individuos están generando documentos electrónicos. Ejemplos de documentos electrónicos incluyen declaraciones de renta presentadas electrónicamente, contratos para bienes o servicios ordenados en línea a través de Internet, correo electrónico, documentos de procesamiento de texto, o cualquier otro tipo de documento que tenga una forma digital. Algunos documentos electrónicos son de cierto tipo tal que los individuos involucrados en la generación, envío o recepción de tales documentos pueden preferir mantener los documentos bajo seguridad y confidencialidad durante largos períodos de tiempo.

20

Desafortunadamente, muchos computadores personales tienen configuraciones inseguras. Con la creciente popularidad de la Internet, muchos computadores personales son vulnerables a ser accedidos remotamente por hackers en la Internet. Además, muchos computadores personales del hogar no están configurados con contraseñas y como resultado cualquiera con acceso físico al computador personal tal como un amigo, niñera, o familiar puede accidental o intencionalmente tener acceso a documentos electrónicos importantes y sensibles. Aunque existe software de criptografía para encriptar documentos electrónicos privados, muchos individuos no tienen la capacidad técnica para instalar y configurar software de encriptación adecuadamente en sus computadores personales. Por

25

30

consiguiente, existe la necesidad de un sistema y método para proteger documentos electrónicos personales los cuales pueden ser fácilmente utilizados por terceros.

obers 90

Los documentos electrónicos que pertenecen a individuos a menudo son almacenados en la unidad de disco duro del computador personal. Por ejemplo, el software

5 tributario personal típicamente genera documentos electrónicos de declaraciones tributarias

los cuales son almacenados en la unidad de disco duro. Los procesadores de texto a menudo

2 almacenan archivos de documentos electrónicos en un directorio común sobre una unidad

de disco duro. El correo electrónico recibido y enviado desde un computador personal

también es almacenado en el disco duro. Desafortunadamente, con el paso del tiempo los

10 computadores personales pueden encontrar problemas de software y/o hardware los cuales

destruyen los archivos del computador almacenados en la unidad de disco duro. A menos

que el individuo proactiva y regularmente realice copias de seguridad de los archivos del

computador localizados en la unidad de disco duro de su computador personal, documentos

15 electrónicos personales, importantes, difíciles de reemplazar se pueden perder debido a un

problema de hardware o software. Aún si los documentos han sido copiados sobre medios

removibles tales como una cinta, disco portátil o CD, el mismo medio portátil se puede

dañar, volver ilegible, obsoleto, o se puede perder. Como resultado, existe la necesidad de

un método y sistema para almacenar documentos electrónicos personales importantes que

puedan preservar la integridad de los documentos durante largos periodos de tiempo.

20 Con la aprobación de leyes sobre firmas digitales a niveles estatales y federales, los individuos probablemente encuentran más oportunidades para generar y firmar

electrónicamente documentos electrónicos. Muchos sistemas de firmas electrónicas utilizan métodos de encriptación de claves públicas para generar y validar firmas electrónicas.

Cuando se firma un documento electrónico un individuo utiliza una clave privada secreta

25 para generar una firma digital para el documento electrónico. Tal clave privada

generalmente está asociada con una clave pública. Otro individuo puede utilizar la clave

pública para autenticar el documento electrónico y la firma digital. Tales claves públicas a

menudo son distribuidas como parte de un certificado digital el cual es digitalmente

firmado por una autoridad certificadora confiable externa.

Aunque el certificado digital y la clave pública pueden ser públicamente divulgados al mundo, la clave privada debe permanecer secreta para evitar adulteraciones. Cuando una persona desea firmar digitalmente un documento, el usuario debe emplear un programa de computador el cual tiene acceso a la clave privada. Como con el software de encriptación, muchos individuos no tienen la capacidad técnica para instalar y utilizar adecuadamente los programas de firmas digitales sobre sus computadores personales. Por consiguiente existe la necesidad de un método y sistema para firmar digitalmente documentos electrónicos los cuales puedan ser fácilmente empleados por individuos.

En general, cuando un programa de firmas digitales pertenece a la persona que utiliza el programa, la persona puede tener seguridad razonable que la clave privada de la persona permanecerá secreta por parte del programa. Además la persona tiene seguridad razonable que el documento electrónico firmado corresponde al documento electrónico que fue leído y revisado por la persona. Desafortunadamente, si el programa de firmas digitales pertenece a una parte no confiable, el individuo tiene muy poca seguridad que la clave privada proporcionada por el individuo permanecerá secreta y/o que el documento electrónico que fue leído y revisado por el individuo es el documento actual siendo digitalmente firmado. Como resultado existe la necesidad de un sistema y método para proteger la confidencialidad de claves privadas utilizadas para firmar digitalmente documentos electrónicos. También existe la necesidad de proporcionar un sistema y método para firmar digitalmente documentos electrónicos que suministre seguridad adicional a individuos que el proceso es un sustituto seguro de firmar documentos físicos.

DIVULGACIÓN DEL INVENTO

Un objetivo de una forma de ejemplo del presente invento es proporcionar un sistema y método que puedan ser fácilmente empleados por individuos para proteger documentos electrónicos.

Un objetivo adicional de una forma de ejemplo del presente invento es proporcionar un sistema y método para almacenar documentos electrónicos los cuales puedan preservar

92
~~92~~

la integridad y confidencialidad de los documentos electrónicos durante largos periodos de tiempo.

5 Un objetivo adicional de una forma de ejemplo del presente invento es proporcionar un sistema y método los cuales puede ser fácilmente empleados por individuos para firmar de manera digital documentos electrónicos.

Un objetivo adicional de una forma de ejemplo del presente invento es proporcionar un sistema y método para proteger la confidencialidad de claves privadas utilizadas para firmar de manera digital documentos electrónicos.

10 Un objetivo adicional de una forma de ejemplo del presente invento es proporcionar un sistema y método para firmar de manera digital documentos electrónicos los cuales proporcionen seguridad adicional a individuos que la firma digital de documentos electrónicos es un sustituto seguro de firmar de documentos físicos.

15 Objetivos adicionales de formas de ejemplo del presente invento serán hechos manifiestos en la siguiente sección Mejores Modos para Llevar a Cabo el Invento y las reivindicaciones adjuntas.

Los objetivos anteriores pueden ser alcanzados en la realización de ejemplo por un sistema y método de almacenamiento y firma digital de documentos electrónicos con máquinas automáticas de transacciones. Un ejemplo de una máquina automática transacciones la cual puede ser utilizada por individuos o usuarios con realizaciones de ejemplo incluye un cajero automático ("ATM"). Los cajeros automáticos permiten a los consumidores realizar transacciones bancarias. Transacciones bancarias comunes que pueden ser realizadas con los cajeros automáticos incluyen la dispensación de efectivo, recepción de consignaciones, transferencia de fondos entre cuentas, el pago de servicios y la solicitud de saldos. El tipo de transacciones bancarias que un cliente puede realizar es determinado por las capacidades de la máquina particular y la programación de la institución que opera la máquina. Otros tipos de máquinas automáticas de transacciones pueden permitir a los clientes debitar cuentas o transferir fondos. Otros tipos de máquinas automáticas de transacciones pueden imprimir o dispensar ítems de valor tales como cupones, boletos, cupones de juego o apuestas, comprobantes, cheques, estampillas para alimentos, giros postales, vales o cheques de viajero. Para propósitos de esta divulgación

las referencias a un cajero automático, una máquina automática transacciones, o una máquina automática de banca incluirán cualquier dispositivo que realice transacciones incluyendo transferencias de valor.

Una realización de ejemplo del cajero automático puede incluir al menos un dispositivo de salida tal como una pantalla, sistema de audio, e impresora. El cajero automático puede también incluir al menos un dispositivo de entrada tal como una pantalla táctil, teclas de función, teclado, y/o lector de tarjetas. El cajero automático puede además incluir dispositivos tal como un mecanismo dispensador para billetes, un mecanismo de impresión de recibos, un lector/transcriptor de tarjetas, un mecanismo para consignaciones y otros dispositivos de función de transacciones que son utilizados por la máquina para realizar transacciones incluyendo transferencias de valor.

El cajero automático puede incluir o estar en conexión operativa con al menos un computador. El computador puede estar en conexión operativa con los dispositivos de salida y los dispositivos de entrada, así como también con los dispositivos de función de transacciones en la máquina. El computador puede incluir componentes de software y programas que son ejecutados en el mismo. En la realización de ejemplo, al menos un componente de software puede ser operativo para hacer que el computador proporcione una interfase de usuario a través del dispositivo de pantalla u otro dispositivo de salida de la máquina, la cual permite a los usuarios almacenar y recuperar documentos electrónicos a partir de una caja fuerte digital o cuenta asociada con el usuario con el usuario. En una realización de ejemplo una cuenta de depósito seguro digital incluye una cantidad de espacio de almacenamiento de archivos mantenido en un servidor de almacenamiento en conexión operativa con el cajero automático. El cajero automático de ejemplo es operativo para comunicarse con el servidor de almacenamiento y hacer que el servidor de almacenamiento mantenga documentos electrónicos los cuales son almacenados en asociación con la cuenta de depósito seguro digital del usuario. En una realización de ejemplo, el cajero automático es operativo para hacer que el servidor de almacenamiento almacene, recupere, copie, y elimine documentos electrónicos almacenados en la cuenta de depósito seguro digital del usuario. Además el servidor de almacenamiento de ejemplo es configurado con hardware operativo, software, y tecnología de copia de seguridad para

preservar la integridad de los archivos electrónicos durante largos periodos de tiempo. Realizaciones de ejemplo del servidor de almacenamiento también son operativas para encriptar los documentos electrónicos tal que solamente individuos autorizados puedan tener acceso a los documentos electrónicos.

Realizaciones de ejemplo del cajero automático pueden permitir a un usuario recuperar un documento electrónico desde una fuente externa y almacenar el documento recuperado en la cuenta de depósito seguro digital del usuario. Fuentes externas por ejemplo pueden incluir un medio de almacenamiento portátil tal como un CD, un dispositivo de cómputo portátil tal como un teléfono celular, y/o una ubicación de almacenamiento accesible por red. En realizaciones de ejemplo, el cajero automático incluye un dispositivo de lectura de medio de almacenamiento portátil que es operativo para leer documentos electrónicos desde un medio de almacenamiento portátil. Ejemplos de dispositivos de lectura de medios portátiles de almacenamiento para utilizar con realizaciones de ejemplo incluyen lectores portátiles de unidades de disco duro tales como la unidad Iomega Jaz®; unidades magneto ópticas tales como una unidad Iomega Zip®; unidades de memoria las para escribir en dispositivos de memoria las tales como CompactFlash y Sony Memory Stick®; PC Cards Interfaces; unidades de CD, unidades de DVD; unidades mini-CD; tarjetas inteligentes; unidades de disquete; y unidades de cinta digital.

El cajero automático de ejemplo puede además permitir a los usuarios leer y/o escuchar el contenido de documentos electrónicos a través de un dispositivo de salida de la máquina. El cajero automático de ejemplo por ejemplo, puede incluir componentes de software de salida de documentos los cuales pueden ser operativos para hacer que el computador del cajero automático saque representaciones visuales correspondientes de los documentos electrónicos a través de un dispositivo de pantalla del cajero automático. Ejemplos de componentes de software de salida de documentos los cuales pueden ser operativamente utilizados con realizaciones de ejemplo incluyen un lector Adobe® PDF, navegador HTML o XML, un procesador de texto, o cualquier otra aplicación de software que es operativa para leer o acceder un documento electrónico y sacar una representación visual del documento electrónico accesado. El cajero automático de ejemplo puede además

95
[Handwritten signature]

incluir componentes de software de salida de documentos que son operativos para sacar representaciones audibles de los documentos electrónicos a través de un dispositivo de audio del cajero automático. Por ejemplo, los documentos electrónicos pueden incluir texto en cual es presentado a través de una pantalla o convertido en lenguaje audible el cual es sacado a través de los parlantes del cajero automático. También, el cajero automático puede además ser operativo para imprimir una representación visual del documento electrónico a través de un dispositivo de impresora.

En una realización de ejemplo alternativa, los usuarios pueden tener acceso a los documentos electrónicos almacenados en la cuenta de depósito seguro digital a través de una red pública tal como la Internet. En una realización de ejemplo, el presente invento puede permitir a los usuarios elegir agregar acceso de Internet a su cuenta de depósito seguro digital además de acceso de cajero automático a sus cuentas de depósito de seguro digital. Los usuarios pueden o no permitir acceso de Internet dependiendo de la sensibilidad y tipo de documentos electrónicos almacenados en la cuenta de depósito seguro digital.

Un cajero automático de ejemplo puede ser operativo para firmar de manera digital documentos electrónicos. En una realización de ejemplo, el cajero automático puede incluir componentes de software de firmas digitales los cuales son operativos para firmar documentos electrónicos utilizando algoritmos y protocolos de criptografía de claves públicas, u otro algoritmo y protocolo de firmas digitales. Por ejemplo, el software de firmas digitales de ejemplo puede ser operativo para firmar documentos electrónicos utilizando una clave privada asociada con el usuario. En una realización de ejemplo la clave privada puede ser almacenada mediante un servidor de almacenamiento en asociación con una cuenta de depósito seguro digital del usuario. Después de autenticar el usuario, el cajero automático de ejemplo puede ser operativo para hacer que un documento electrónico sea digitalmente firmado utilizando la clave privada almacenada de manera segura por el servidor de almacenamiento. Una vez un documento electrónico se ha hecho firmar por el cajero automático de ejemplo, el cajero automático puede ser operativo para enviar el documento electrónico firmado hacia una ubicación de elección del usuario tal como una cuenta de depósito seguro digital asociada con el usuario o una fuente externa tal como un

96
212

medio de almacenamiento portátil, dispositivo de cómputo portátil y/o ubicación de almacenamiento accesible por red.

En algunas realizaciones de ejemplo, el cajero automático de ejemplo puede ser operativo para firmar documentos electrónicos con una clave privada de un usuario que es almacenada en una fuente externa tal como un dispositivo de cómputo portátil. Por ejemplo, la clave privada del usuario puede ser almacenada de manera segura sobre una tarjeta inteligente. Una realización de ejemplo del cajero automático puede incluir un lector de tarjetas inteligentes el cual es operativo para comunicarse con la tarjeta inteligente para propósitos de firmar un documento electrónico.

El servidor de almacenamiento de ejemplo o una fuente externa tal como una tarjeta inteligente, puede requerir una contraseña o datos biométricos desde el cajero automático antes de permitir que la firma digital sea generada utilizando la clave privada del usuario. El cajero automático de ejemplo puede incluir dispositivos de entrada tales como un teclado o un dispositivo de lectura biométrico el cual puede ser utilizado por el usuario para entrar una contraseña requerida tal como un PIN (número de identificación personal), o datos biométricos.

En una realización de ejemplo, el cajero automático puede ser operativo para recuperar la clave privada desde el servidor de almacenamiento o un dispositivo externo para propósitos de generar la firma digital con el cajero automático. En algunas realizaciones de ejemplo, el sistema puede ser configurado tal que el cajero automático no requiere que la clave privada sea recuperada por el cajero automático. En esta realización de ejemplo, el cajero automático es operativo para generar un hash unidireccional del documento electrónico tal como un mensaje digest, suma de comprobación criptográfica, verificación de integridad de mensaje, o código detector de manipulación. El hash unidireccional puede entonces ser transmitido hacia el servidor de almacenamiento, tarjeta inteligente, u otra fuente externa segura la cual tiene acceso seguro a la clave privada. El servidor de almacenamiento, tarjeta inteligente, u otra fuente externa segura puede entonces generar una firma digital en respuesta al hash unidireccional, clave privada y la encriptación apropiada o algoritmo de firmas digitales. El servidor de almacenamiento, tarjeta inteligente, o fuente externa segura puede luego retornar la firma digital al cajero

automático. El cajero automático puede luego anexar la firma digital al documento electrónico antes de almacenar en la cuenta de depósito seguro digital o antes de enviar el documento electrónico a una fuente externa.

5 En una realización de ejemplo, el cajero automático puede transmitir el documento electrónico hacia el servidor de almacenamiento, tarjeta inteligente, u otra fuente externa. En esta realización el servidor de almacenamiento, tarjeta inteligente, u otra fuente externa es operativo para generar el digest y la correspondiente firma digital desde el documento electrónico recibido y luego transmitir la firma digital y/o documento electrónico de vuelta al cajero automático. Se debe entender que las realizaciones de ejemplo incluyen el uso de
10 cualquier algoritmo de firmas digitales y sistema de administración de claves el cual es operativo para permitir al cajero automático firmar documentos electrónicos de manera segura. Ejemplos de algoritmos criptográficos que pueden ser utilizados en el presente invento incluyen RSA y DSA.

15 En algunas realizaciones de ejemplo, la cuenta de depósito seguro digital y/o la clave privada del usuario pueden estar asociadas con una cuenta bancaria u otra cuenta bancaria del usuario tal como una cuenta corriente, cuenta de ahorros, cuenta debito y/o cuenta crédito. Un usuario puede tener acceso a la cuenta de depósito seguro digital y/o características de la firma digital del cajero automático de ejemplo al insertar una tarjeta de cajero automático, tarjeta bancaria, tarjeta de crédito, o cualquier otra tarjeta que esté
20 asociada con la cuenta bancaria del usuario. Después que un usuario entra una contraseña correspondiente tal como un PIN o información biométrica en el dispositivo de entrada del cajero automático, el cajero automático de ejemplo puede ser operativo para permitir al usuario seleccionar las funciones de transacción del cajero automático tal como la dispensación efectivo, transferencias, consignaciones, pago de servicios, y solicitud de
25 saldos. Además el cajero automático de ejemplo puede ser operativo para permitir al usuario desplegar y firmar de manera digital documentos electrónicos con una clave privada asociada con la cuenta bancaria del usuario. Además, el cajero automático de ejemplo puede ser operativo para permitir al usuario acceder y mantener documentos electrónicos almacenados en una cuenta de depósito seguro digital la cual está asociada con
30 la cuenta bancaria del usuario.

98
~~99~~

En realizaciones donde una cuenta de depósito seguro digital y/o clave privada de usuario no están asociadas con una tarjeta de cuenta bancaria, se puede expedir al usuario una tarjeta de cuenta de depósito seguro digital con indicios legibles de máquina sobre la misma que corresponden a la cuenta de depósito seguro digital del usuario. Los cajeros
5 automáticos de las realizaciones de ejemplo puede ser operativos para permitir al usuario acceder su cuenta de depósito seguro digital y firmar documentos electrónicos en respuesta a la lectura de indicios legibles de máquina desde la tarjeta de cuenta de depósito seguro digital.

Además, el cajero automático de ejemplo puede ser operativo para permitir a un
10 usuario generar claves públicas y privadas para firma digital de documentos electrónicos. También, el cajero automático de ejemplo puede ser operado para permitir al usuario adquirir y/o comprar un certificado digital tal como un certificados X.509 utilizando el cajero automático. El cajero automático de ejemplo puede estar en conexión operativa con una autoridad certificadora y puede ser operativo para enviar a la autoridad certificadora
15 suficiente información para permitir a la autoridad certificadora generar y expedir el certificado al usuario. Tales certificados digitales pueden ser utilizados para autenticar la firma digital del usuario, creada utilizando el cajero automático de ejemplo. El cajero automático de ejemplo puede ser operativo para almacenar el certificado digital en la cuenta de depósito seguro digital del usuario y/o en asociación con la cuenta bancaria del
20 usuario. Como con otros documentos electrónicos, el cajero automático de ejemplo puede ser operativo para enviar el certificado digital a una fuente externa de elección del usuario. Al firmar un documento electrónico, el cajero automático de ejemplo puede ser operativo para asociar el certificado digital con el documento electrónico firmado. Otros individuos pueden utilizar el certificado digital para autenticar la firma digital del documento
25 electrónico. En esta realización de ejemplo descrita, el cajero automático puede ser operativo para hacer los costos asociados con la compra de un certificado digital sean cobrados a la cuenta bancaria del usuario u otro individuos. Si el usuario ya tiene una firma digital, una realización de ejemplo puede ser operativa para recuperar el certificado digital desde una fuente externa seleccionada por el usuario. El cajero automático de ejemplo
30 puede ser operativo para asociar un certificado digital recuperado con documentos

99
1000

electrónicos firmados por el cajero automático. El cajero automático de ejemplo puede además ser operativo para hacer que el servidor de almacenamiento de ejemplo almacene y recupere el certificado digital en la cuenta de depósito seguro digital del usuario y/o en asociación con una cuenta bancaria del usuario.

- 5 Como se discutió anteriormente, el cajero automático de ejemplo puede ser operativo para leer el documento electrónico y sacar a través de un dispositivo de pantalla del cajero automático una representación visual del documento electrónico. Además, el cajero automático de ejemplo puede ser operativo para permitir al usuario entrar a través de un dispositivo de entrada del cajero automático información en el documento electrónico.
- 10 Por ejemplo, un documento electrónico tal como un contrato puede incluir campos para entrar los nombres de las partes contractuales, una descripción de los bienes, y una cantidad de consideración pagada por los bienes. El cajero automático de ejemplo puede ser operativo para permitir al usuario entrar o seleccionar textos, números, y otra información para incorporación en el documento electrónico antes de firmar el documento. Además las
- 15 realizaciones de ejemplo del cajero automático pueden ser operativas para acceder un almacenamiento de datos de información de usuario. Tal almacenamiento de datos puede ser utilizado para recuperar información para llenar automáticamente campos de entrada de un documento electrónico leído y editado por el cajero automático.

Handwritten notes and signatures on the right margin, including a signature and the text "C. J. S. 2".

20 **BREVE DESCRIPCIÓN DE LAS ILUSTRACIONES**

La figura 1 es una vista esquemática representativa de una primera realización de ejemplo de un cajero automático.

- 25 La figura 2 es una vista esquemática representativa de una realización de ejemplo de un sistema para almacenar y firmar de manera digital documentos electrónicos con un cajero automático.

Las figuras 3-8 son vistas esquemáticas representativas de realizaciones de ejemplo de pantallas de interfase de usuario de un cajero automático.

- 30 Las figuras 9-14 son vistas esquemáticas representativas de realizaciones de ejemplo de sistemas de cajeros automáticos para firmar de manera digital documentos.

100
~~100~~

La figura 15 muestra una vista esquemática de un sistema de firma de documentos de una realización de ejemplo adicional.

La figura 16 muestra una vista de plano superior de una realización de ejemplo de una máquina portátil que es operativa para firmar digitalmente documentos electrónicos.

5 La figura 17 muestra los pasos para una realización de ejemplo de un método para firmar documentos electrónicos.

La figura 18 muestra una vista esquemática de un sistema de firma documentos de una realización de ejemplo adicional.

10 La figura 19 muestra una realización de ejemplo de una pantalla de interfase de usuario de un cajero automático.

MEJORES MODOS PARA LLEVAR A CABO EL INVENTO

Con referencia ahora a las ilustraciones y particularmente a la figura 1, se muestra allí una vista esquemática de una máquina automática de transacciones de ejemplo, cajero automático 10 de una realización de ejemplo. El cajero automático 10 puede incluir al menos un procesador de computador 12 y una pluralidad de componentes de software 11. El procesador de computador 12 puede ser operativo en respuesta a componentes de software 11 para controlar la operación del cajero automático. En la realización de ejemplo el procesador de computador 12 puede ser operativamente programado para permitir al cajero automático realizar al menos una las siguientes funciones al menos una transacción bancaria tal como la dispensación de efectivo; el almacenamiento y recuperación de documentos electrónicos; y/o la firma digital de documentos electrónicos.

Para realizar estas funciones el cajero automático puede además incluir en conexión operativa con el procesador de computador 12, al menos un dispositivo de salida 14 tal como un dispositivo de pantalla 18, al menos un dispositivo de entrada 16, y un lector de tarjetas 20 el cual también puede servir como un dispositivo de entrada. En algunas realizaciones, el cajero automático también puede incluir en conexión operativa con el procesador de computador 12, uno o más dispositivos de función de transacciones. Los dispositivos de función de transacciones pueden incluir por ejemplo un dispensador de efectivo 24, un mecanismo de consignaciones 22, una impresora de recibos 25 y otros

mas.

101
~~101~~

dispositivos. El cajero automático 10 puede además ser operativo para comunicarse con al menos un sistema o computador de procesamiento de transacciones financieras el cual es operativo para realizar transferencias financieras y autorizaciones, el cual en este ejemplo es una red bancaria local 30. El cajero automático 10 también puede comunicarse con al menos un servidor de almacenamiento 32. En la realización de ejemplo el servidor de almacenamiento 32 puede estar en comunicación operativa con al menos un almacenamiento de datos 34. También en una realización de ejemplo, el cajero automático 10 puede ser operativo para comunicarse con al menos un servidor de almacenamiento 32 a través de comunicación con la red bancaria local 30.

10 En una realización de ejemplo el servidor de comunicación puede responder a una pluralidad de cajeros automáticos para almacenar de manera segura y mantener una pluralidad de documentos electrónicos 42 en cuentas o cajas de depósito seguro digitales 40. Tales cuentas de depósitos seguros digitales pueden corresponder a ubicaciones de almacenamiento de archivos individuales sobre el almacenamiento de datos 34. Los documentos electrónicos 42 pueden incluir por ejemplo representaciones digitales de documentos físicos, documentos de procesamiento de texto, archivos HTLM, archivos XML, otros documentos de lenguaje markup, archivos de Acrobat® PDF, archivos de hoja de cálculo, certificados digitales, archivos de imágenes, archivos de sonido, archivos audiovisuales, archivos de código fuente, archivos de almacenamiento específicos a aplicaciones, balotas electorales electrónicas, o cualquier otro tipo de archivo digital el cual es operativo para almacenar información en un formato legible de computador. Un usuario puede establecer una o más cuentas digitales de depósito seguro 40 y utilizar un cajero automático 10 para almacenar y mantener documentos electrónicos 42 en asociación con su cuenta de depósito seguro digital.

25 La realización de ejemplo del cajero automático 10 puede ser operativa para presentar el contenido legible de un documento electrónico sobre el dispositivo de pantalla 18 y permitir a un usuario firmar digitalmente el documento electrónico. En muchos algoritmos de firmas digitales, el signatario debe utilizar información secreta tal como una clave privada para generar la firma digital. En una realización de ejemplo, una clave privada de usuario 44, puede ser almacenada en una cuenta de depósito seguro digital de

102
01/22/20

usuario o almacenada en asociación con una cuenta de depósito seguro digital 40 del usuario. En realizaciones de ejemplo, una tecla privada de usuario 44 puede además ser almacenada en asociación con una cuenta bancaria de usuario tal como una cuenta de tarjeta de crédito, cuenta de tarjeta de débito, cuenta corriente, cuenta de ahorros o cualquier otra cuenta bancaria del usuario. Además, como se discutirá adicionalmente más adelante, las realizaciones de ejemplo del cajero automático 10 y/o servidor de almacenamiento 32 puede ser operativa para firmar digitalmente documentos electrónicos utilizando la clave privada 44 asociada con la cuenta de depósito seguro digital 40 y/o una cuenta bancaria.

10 Se debe entender que el cajero automático 10 es una realización de ejemplo y en otras realizaciones máquinas automáticas de transacciones pueden incluir otros dispositivos y pueden operar en otros tipos de sistemas. Por ejemplo, las realizaciones pueden incluir en conexión operativa con el procesador de computador 12, un almacenamiento de datos que incluye una unidad de dispositivo de almacenamiento 26, y un puerto de comunicaciones 28 el cual sirve como un dispositivo de entrada/salida. La unidad de dispositivo de almacenamiento 26 sirve como un almacenamiento de datos y permite al procesador de computador leer y/o escribir documentos electrónicos hacia una fuente externa 56 tal como un medio de almacenamiento portátil 36. El puerto de comunicaciones 28 permite al procesador de computador leer y/o escribir documentos electrónicos a fuentes externas 56 tal como un dispositivo de cómputo portátil 38 o una ubicación de almacenamiento accesible por red 58.

La figura 2 esquemáticamente muestra una realización de ejemplo del cajero automático 10 que puede ser operativo para almacenar y mantener documentos electrónicos 42 en una cuenta de depósito seguro digital 40. La realización de ejemplo del cajero automático 10 puede incluir un dispositivo de pantalla 18 tal como un monitor CRT o una pantalla LCD. El dispositivo de pantalla puede ser operativo en respuesta al procesador de computador para sacar indicios de interfase de usuario 46. Los indicios de interfase de usuario pueden incluir salidas de instrucción para operar el cajero automático así como también indicios de contenido los cuales son representativos de listas de documentos electrónicos que puede ser accedidos por el cajero automático 10 o partes de un documento

electrónico las cuales son operativas para ser leídas en el dispositivo de pantalla 18.

Algunas realizaciones de ejemplo pueden además incluir otros dispositivos de salida 14 tales como un sistema de sonido 19 que es operativo para reproducir contenidos de audio que corresponden a un documento electrónico. Por ejemplo cuando un documento

5 electrónico incluye información de audio tal como un archivo MP3, un cajero automático 10 puede ser operativamente programado para hacer que el sistema de sonido reproduzca sonido en respuesta al archivo MP3. Además, si el documento electrónico incluye información de lenguaje tal como texto, una realización de ejemplo puede incluir un dispositivo sintetizador de lenguaje o software que es operativo para leer información de

10 lenguaje a un usuario al reproducir lenguaje hablado a través del sistema de sonido del cajero automático 10.

La realización de ejemplo del cajero automático 10 también puede incluir al menos un dispositivo de entrada 16 tal como un teclado 50 o botones de selección 52. El dispositivo de entrada tal como un teclado 50 y botones de selección 52 pueden permitir a

15 usuarios proporcionar entradas operacionales tal como un número de identificación personal (PIN) que corresponde a una cuenta, una cantidad de efectivo para retirar, una selección de un documento electrónico particular para leer, almacenar y/o firmar digitalmente. Algunas realizaciones de ejemplo del cajero automático 10 pueden además incluir un dispositivo de entrada de lectura biométrica 54 tal como un lector de huellas

20 digitales, escáner de iris, escáner de retina, dispositivo de reconocimiento de voz, lector de reconocimiento facial u otro dispositivo el cual es operativo para permitir al usuario proporcionar información biométrica de identificación de usuario. Tal información biométrica de identificación puede ser utilizada por una realización del ejemplo del cajero automático 10 para autenticar adicionalmente un usuario antes de permitir al usuario

25 realizar funciones de transacción, acceder una cuenta de depósito seguro digital, y/o firmar digitalmente un documento electrónico.

En realizaciones de ejemplo, el cajero automático puede incluir otros tipos de dispositivos de entrada para proporcionar información, tales como un dispositivo de pantalla táctil, un sistema de reconocimiento de voz, una bola de ratón, y/o un tablero

30 digitalizador de firmas 53. El tablero digitalizador de firmas 53 es operativo para producir

una representación o escaneo digital de una firma escrita a mano sobre el tablero 53 con un bolígrafo o estilógrafo sin tinta 55. Tal escaneo digitalizado de la firma escrita a mano puede ser capturado por el cajero automático 10 e integrado en los documentos electrónicos que están digitalmente firmados por el cajero automático.

- 5 Como se discutió anteriormente, el cajero automático 10 puede incluir un lector de tarjetas 20. El lector de tarjetas 20 puede ser operativo para leer indicios que corresponden a la información de cuenta u otra información desde una tarjeta de usuario. La tarjeta puede ser una tarjeta bancaria, tarjeta de crédito, tarjeta débito, tarjeta de crédito para combustible, tarjeta de crédito comercial, tarjeta inteligente, u otro medio que es operativo para
- 10 almacenar datos de cuenta y/o otra información la cual puede ser utilizada para identificar un usuario o sus cuentas. Tales datos de cuenta pueden incluir un número de cuenta de una cuenta corriente, cuenta de ahorros, cuenta débito, cuenta crédito, u otra cuenta bancaria o financiera. Tales datos de cuenta pueden además incluir datos representativos de una cuenta de depósito seguro digital del usuario.
- 15 En una realización de ejemplo, una cuenta de depósito seguro digital, una clave privada 44, y/o un certificado digital 45 pueden estar asociados con una cuenta bancaria 48 del usuario. Cuando el usuario utiliza el cajero automático 10 de ejemplo con una tarjeta asociada con la cuenta bancaria 48, el cajero automático de ejemplo puede ser operativo para proporcionar automáticamente al usuario acceso a la cuenta de depósito seguro digital .
- 20 40 asociada al usuario, la clave privada 44, y/o el certificado digital. Por ejemplo, cuando un usuario inserta una tarjeta de crédito o débito en el lector de tarjetas 20, el cajero automático de ejemplo puede ser operativo para leer el número de cuenta crédito o débito de la tarjeta. Este número puede ser utilizado por el cajero automático para acceder la cuenta bancaria a través de comunicación con la red bancaria local 30. En una realización
- 25 de ejemplo, la clave privada del usuario puede estar directamente asociada con la cuenta bancaria del usuario y el cajero automático es operativo través de comunicación con la red bancaria local para hacer que un documento electrónico sea digitalmente firmado en respuesta a la clave privada asociada con la cuenta bancaria. En algunas realizaciones, la cuenta de depósito seguro digital 40 del usuario de puede estar asociada con la cuenta

bancaria 48 del usuario y el cajero automático puede ser operativo para recibir acceso a la cuenta de depósito seguro digital 40 a través de comunicación con la red bancaria local.

Una realización de ejemplo del cajero automático 10 puede ser operativa para dispensar una cantidad seleccionada de efectivo al usuario desde el dispensador de efectivo

5 24, y para debilitar una cuenta bancaria o financiera a través de comunicación con un computador de transacciones financieras tal como la red bancaria local 30. El cajero automático de ejemplo 10 puede ser configurado para debilitar cargos de usuario de una cuenta bancaria del usuario para almacenar, leer, y firmar digitalmente documentos electrónicos con el cajero automático. El cajero automático puede además ser configurado
10 para debitar cargos de usuario desde una cuenta bancaria de una tercera parte o entidad la cual puede estar asociada con el documento electrónico siendo leído, almacenado, y/o digitalmente firmado por el cajero automático.

La realización de ejemplo del cajero automático 10 puede incluir una unidad de dispositivo de almacenamiento 26 tal como una unidad de CD la cual es operativa para
15 aceptar un medio de almacenamiento portátil 36 tal como un CD de lectura solamente, de solo una escritura o un CD reutilizable. La realización de ejemplo del cajero automático 10 es operativa para hacer que la unidad de dispositivo de almacenamiento 26 lea documentos electrónicos desde el medio de almacenamiento portátil 36. Los documentos electrónicos leídos pueden ser leídos sobre la pantalla 18 del cajero automático 10 y/o transferidos hacia
20 una cuenta de depósito seguro digital 40. Además el cajero automático de ejemplo puede ser adicionalmente operativo para recuperar documentos electrónicos almacenados en la cuenta de depósito seguro digital 40, leer éstos sobre la pantalla 18 y/o hacer que el la unidad de dispositivo de almacenamiento 26 grave el documento electrónico en el medio de almacenamiento portátil 36. Ejemplos de otros tipos de unidades de dispositivo de
25 almacenamiento que pueden ser utilizados con realizaciones incluyen lectores de unidades de disco duro portátiles tal como una unidad Iomega Jaz®; unidades magneto ópticas tal como una unidad Iomega Zip®; unidades de memoria flash para escribir en dispositivos de memoria flash tales como CompactFlash y Sony Memory Stick®; unidades DVD, unidades Mini-CD, y unidades de cinta digital.

Algunas realizaciones pueden incluir uno más puertos de comunicación 28 que son operativos para recuperar y grabar documentos electrónicos en un dispositivo de cómputo portátil tal como un teléfono celular 38 o una ubicación de almacenamiento accesible por red 58 asociada con un URL seleccionado o ingresado por el cliente, dirección de correo electrónico, u otra dirección de red. Ejemplos de puertos de comunicación apropiados 18 pueden incluir un puerto de Bus Serial Universal (USB), puerto serial RS-232, puerto paralelo, puerto infrarrojo (IR), un puerto de radiofrecuencia (RF) tal como Bluetooth, un puerto IEEE-1394, o un puerto de red tal como una conexión Ethernet cableada o Ethernet inalámbrica (IEEE-802.11x). Ejemplos de otros tipos de dispositivos de cómputo portátiles que pueden ser accedidos con realizaciones del cajero automático 10 incluyen un computador portátil y un asistente digital personal (PDA).

La realización de ejemplo del cajero automático 10 puede además incluir una cara frontal del cajero automático 59 a través de la cual uno o más dispositivos de entrada, dispositivos de pantalla, y dispositivos de función de transacciones son accesibles a un usuario. El cajero automático 10 puede además incluir indicios visibles 57 adyacentes a la cara frontal 59 del cajero automático, visibles sobre la pantalla o de otra manera comunicados a un usuario de la máquina. Los indicios visibles 57 pueden incluir un logotipo, diseño, o texto que sirve como una marca indicadora de fuente para una red o servicio de firmas digitales. Tal marca corresponde a una marca de servicio de la entidad que opera los servidores, almacenamiento de datos, sistemas hospederos, y/o red a través de los cuales el cajero automático 10 se comunica para producir las firmas electrónicas para un documento presentado en la pantalla del cajero automático 10. Tales indicios pueden ser visualmente similares a los indicios sobre una tarjeta del usuario, de manera que el usuario puede rápidamente determinar que el cajero automático es capaz de firmar digitalmente documentos utilizando la tarjeta del usuario. Tales indicios también pueden servir para confirmar al usuario que el cajero automático está asociado con una tercera parte y red o servicio de firmas digitales independiente que puede ser de confianza para presentar en la pantalla con exactitud el documento electrónico y para firmar digitalmente de manera segura el documento electrónico para el usuario.

104
Q212

Las figuras 3-8 muestran ejemplos de pantallas de interfase de usuario de una realización de ejemplo del cajero automático 10. La figura 3 muestra un ejemplo de una pantalla de interfase de usuario 100 la cual el cajero automático puede ser operativo para presentar a través del dispositivo de pantalla 18. En una realización de ejemplo la pantalla de interfase de usuario 100 puede ser presentada por pantalla después que un usuario activa el cajero automático 10 colocando una tarjeta en el lector de tarjetas 20 y entrando un PIN en el teclado 50. La pantalla de interfase de usuario 100 puede incluir una pluralidad de funciones elegibles por el usuario 102 las cuales incluyen la opción de retirar efectivo 104 desde el dispensador de efectivo 24; la opción de consignar un cheque 106 con el mecanismo de consignación 22; la opción de transferir valor entre las cuentas 108; y la opción de leer un documento electrónico 110 con el dispositivo de pantalla 18. Cada una de estas funciones elegibles 102 pueden estar adyacentes a un botón de selección diferente 52, los cuales cuando se presionan son operativos para hacer que el cajero automático 10 proceda con la correspondiente función 102.

En una realización de ejemplo, cuando un usuario selecciona la opción para leer el documento electrónico 110, el cajero automático de ejemplo 10 puede ser operativo para hacer que la pantalla de interfase de usuario 120 mostrada en figura 4 sea sacada a través del dispositivo de pantalla 18. Aquí la pantalla de interfase usuario 120 puede incluir una pluralidad de funciones de selección 122 las cuales corresponden a diferentes fuentes para recuperar documentos electrónicos para leer. En el presente ejemplo descrito, las funciones de selección 122 pueden incluir la opción para seleccionar documentos electrónicos desde una cuenta de depósito seguro digital 124; las opciones 126-130 para seleccionar documentos electrónicos desde las fuentes externas de un disco zip, red local la cual puede incluir dispositivos de cómputo portátiles tales como el PDA del usuario, y un sitio seguro de Internet/Intranet.

En respuesta a un usuario seleccionando una de éstas fuentes de documentos electrónicos, una realización de ejemplo del cajero automático 10 puede ser operativa para producir la salida de la pantalla de interfase de usuario 140 mostrada en la figura 5. La pantalla de interfase usuario 140 puede incluir una lista de documentos electrónicos 142 que el cajero automático 10 ha determinado están presentes en la fuente de documentos

electrónicos seleccionada con la pantalla de interfase de usuario 120. En respuesta a un usuario seleccionando uno de los documentos electrónicos listados 142, una realización de ejemplo del cajero automático 10 puede ser operativa para hacer que el documento electrónico seleccionado sea leído a través de la pantalla 18. La figura 6 es representativa de un ejemplo de una pantalla de interfase de usuario 160 la cual incluye indicios representativos de un documento electrónico seleccionado de crédito de automóviles 162.

Las realizaciones de ejemplo del cajero automático 10 puede además incluir funcionalidad para permitir al usuario editar el documento electrónico presentado en pantalla 162. Por ejemplo en una realización de ejemplo, el cajero automático 10 puede incluir componentes de software para presentar a través del dispositivo de salida 18 documentos electrónicos que incluyen HTML, DHTML, XML, Active X, objetos .Net, plugins, Java Script, y/o applets Java asociados con el documento electrónico. Tales características pueden generar campos de entrada o selección sobre el dispositivo de pantalla, los cuales pueden ser llenados o modificados operando los dispositivos de entrada del cajero automático 10.

Con el fin de colaborarle más al usuario al llenar los campos de un documento electrónico, un cajero automático de ejemplo puede además ser operativo para recuperar información relevante para llenar los campos de entrada de un documento electrónico desde un almacenamiento de datos de información de usuario almacenada. La información de usuario almacenada puede estar asociada con la cuenta bancaria del usuario y/o cuenta de depósito seguro digital. El cajero automático de ejemplo puede utilizar la información de usuario almacenada para llenar automáticamente campos de entrada de un documento electrónico. Por ejemplo, el documento electrónico puede incluir un campo de entrada rotulado "enviar _a _la _dirección." *La información de usuario almacenada puede incluir información de dirección la cual está asociada con la descripción "enviar _a _la _dirección."* El cajero automático de ejemplo puede ser operativo para recuperar información de usuario correspondiente desde el almacenamiento de datos e insertar la información de usuario correspondiente en los campos de entrada del documento electrónico. Cuando el usuario entra manualmente información en el documento electrónico, las realizaciones de ejemplo del cajero automático pueden además ser

109
109

operativas para almacenar ésta información en la cuenta de depósito seguro digital u otro almacenamiento de datos para posterior uso para llenar de manera similares campos rotulados.

Una vez que el usuario ha terminado de revisar y/o editar un documento electrónico, la realización de ejemplo del cajero automático 10 puede ser operativa para desplegar una pantalla de interfase de usuario adicional 170 tal como se muestra en la figura 7. La pantalla de interfase de usuario 170 puede incluir una pluralidad de funciones elegibles 162 incluyendo la opción de revisar el documento electrónico 174; la opción para firmar digitalmente el documento electrónico 176; la opción para enviar el documento electrónico a otra ubicación 178; y la opción para eliminar el documento electrónico 180. En la realización descrita del cajero automático 10, la opción para eliminar el documento electrónico 180 puede generalmente estar disponible cuando se lee un documento electrónico localizado en la cuenta de depósito seguro digital del usuario.

Cuando un usuario selecciona la opción de firmar digitalmente un documento electrónico 176, la realización de ejemplo del cajero automático 10 puede ser operativa para generar una firma digital y anexar ésta al original o a una copia del documento electrónico. Realizaciones de ejemplo pueden ser operativamente programadas para generar una firma digital utilizando cualquier algoritmo y protocolo de firmas digitales. Ejemplos de algoritmos de criptografía de firmas digitales disponibles para utilizar con el presente invento pueden incluir RSA y DSA. En la realización de ejemplo un documento electrónico puede ser firmado utilizando una clave privada asociada con el usuario. La firma digital puede ser verificada luego mediante el uso de una clave pública del usuario la cual corresponde a la clave privada. Tal clave pública puede ser recuperada desde un certificado digital del usuario. En realizaciones de ejemplo, el cajero automático puede ser operativo para hacer que el certificado digital asociado con el usuario sea anexado al documento electrónico cuando el documento electrónico es firmado digitalmente. También el cajero automático puede ser operativo para hacer que el certificado digital asociado con la autoridad certificadora que firmó el certificado digital del usuario sea anexado al documento electrónico.

110
11/11/15

Para que una firma digital corresponda a una firma del usuario legalmente valedera, el usuario puede necesitar mostrar su manifestación de intención para utilizar una firma digital como una firma electrónica legalmente valedera. Como resultado, las realizaciones de ejemplo del cajero automático 10 pueden proporcionar pantallas de interfase de usuario adicionales que requieren que un usuario muestre afirmativamente tal manifestación de intención para crear una firma electrónica legalmente valedera. Por ejemplo, como se muestra en la figura 19, el cajero automático puede sacar una pantalla de interfase de usuario 182 la cual pide al usuario hacer una entrada de confirmación afirmativa con un dispositivo de entrada, que represente la intención del usuario para crear una firma electrónica legalmente valedera.

Algunas realizaciones de ejemplo del cajero automático 10 pueden hacer que una declaración sea anexada al documento electrónico la cual incluye una afirmación con respecto a que el usuario ha mostrado afirmativamente su intención para crear una firma electrónica legalmente valedera con la generación de la firma digital. El cajero automático 10 puede además hacer que tal declaración y/o todo el documento electrónico sea digitalmente firmado o notariado mediante una entidad externa la cual afirme que el usuario proporcionó una entrada al cajero automático la cual representa la intención del usuario para crear una firma electrónica legalmente valedera. La declaración y/o el documento electrónico también pueden estar asociados con un sello digital de fecha y hora representativo del momento en que la intención del usuario fue mostrada y/o cuando la firma digital fue creada. Tal sello digital de fecha y hora puede ser obtenido por el cajero automático mediante comunicación con un servidor de sellos digitales de fecha y hora.

En algunas realizaciones de ejemplo, el cajero automático 10 puede solicitar al usuario la realización de la firma a mano sobre un tablero digitalizador de firmas. El cajero automático puede generar una representación digitalizada o escaneo de la firma hecha a mano en la forma de un mapa de bits o dibujo vectorial. La representación digitalizada de la firma escrita puede luego ser incorporada en el documento electrónico mediante el cajero automático. Una vista impresa o presentada en pantalla del documento electrónico puede luego incluir una representación visual de la firma escrita del cliente.

111
111
111

Cuando un usuario selecciona la opción de enviar un documento electrónico hacia otra ubicación 178, una realización de ejemplo del cajero automático 10 puede ser operativa para generar la pantalla de interfase de usuario 190 tal como se muestra en la figura 8. La pantalla de interfase de usuario 190 puede incluir una pluralidad de funciones de selección que corresponden a las diferentes ubicaciones 192 para enviar una copia del original o el documento electrónico firmado. En el ejemplo actualmente descrito, las funciones de selección 192 pueden incluir la opción de enviar el documento electrónico a la cuenta de depósito seguro digital 194, las opciones 196-200 para enviar el documento electrónico hacia fuentes externas de un disco zip, red local, y un sitio seguro de Internet/Intranet.

En una realización de ejemplo, la cuenta de depósito seguro digital está asociada con la clave privada del usuario. En tales realizaciones el cajero automático de ejemplo 10 puede incluir además pantallas de interfase de usuario que permiten al usuario generar un grupo de claves privadas y públicas las cuales pueden estar asociadas con la cuenta de depósito seguro digital del usuario y/o almacenadas en la misma. La clave privada puede ser utilizada por la realización de ejemplo para firmar documentos electrónicos para el usuario.

Con referencia a la figura 1, las realizaciones de ejemplo del cajero automático 10 pueden además estar en conexión operativa con una autoridad certificadora 60. El cajero automático 10 puede ser operativo para comunicarse con una autoridad certificadora para propósitos de generar un certificado digital tal como un certificado X.509 el cual puede ser anexado al documento electrónico para propósitos de autenticar la firma digital creada por el usuario. El cajero automático de ejemplo 10 puede ser operativo para enviar a la autoridad certificadora información que identifica al usuario y una copia de la clave pública. En respuesta, la autoridad certificadora puede ser operativa para generar y devolver un certificado digital firmado el cual incluye la información de identificación y la clave pública del usuario. El certificado digital puede luego ser anexado al documento electrónico por el cajero automático 10, almacenado en asociación con o en la cuenta de depósito seguro digital del usuario y/o enviado hacia una fuente externa seleccionada por el usuario. El cajero automático 10 también puede recibir una copia del certificado digital asociado con la autoridad certificadora que expidió y firmó el certificado digital del usuario. Tal

112
~~112~~

certificado digital de la autoridad certificadora también puede ser anexado al documento electrónico, almacenado en asociación con o en la cuenta de depósito seguro digital del usuario y/o enviado a una fuente externa seleccionada por el usuario.

Las figuras 9-14 son vistas esquemáticas de una pluralidad de diferentes realizaciones. La figura 9 muestra una realización de ejemplo de un cajero automático 300 que puede ser operativo para comunicarse con una realización de ejemplo de un servidor de almacenamiento 302. Aquí el servidor de almacenamiento puede ser operativo para almacenar de forma segura claves privadas 304 asociadas con una pluralidad de diferentes usuarios. Las claves privadas de ejemplo pueden ser almacenadas en asociación con cuentas de depósito seguro digital y/o cuentas bancarias tal como una cuenta corriente o cuenta de ahorros. En esta realización descrita el cajero automático 300 puede ser operativo para enviar un documento electrónico 306 asociado con un usuario utilizando el cajero automático 300 hacia el servidor de almacenamiento 302. El servidor de almacenamiento incluye software de firmas digitales 308 el cual puede ser operativo para generar una firma digital 310 para el documento electrónico 306 utilizando la clave privada 304 asociada con un usuario. El servidor de almacenamiento puede luego anexar la firma digital al documento electrónico y devolver el documento electrónico firmado al cajero automático 300 o el servidor de almacenamiento puede solamente enviar la firma digital 310 al cajero automático 300. El cajero automático de ejemplo 300 puede luego anexar la firma digital 310 al documento electrónico 306 y transmitir el documento electrónico firmado hacia una ubicación de destino seleccionada elegida por el usuario.

En la realización de ejemplo, el software de firmas digitales puede incluir un algoritmo RSA. Sin embargo en algunas realizaciones de ejemplo, el software de firmas digitales puede incluir otro software/hardware de firmas digitales adicional. En realizaciones donde el servidor incluye más de un tipo de software/hardware de firmas digitales, el cajero automático de ejemplo 300 puede ser operativamente programado para permitir a los usuarios seleccionar el tipo de firma digital que ellos prefieren que el cajero automático genere para el documento electrónico.

La figura 10 muestra una realización de ejemplo de un cajero automático 320 que puede ser operativo para comunicarse con una realización de ejemplo de un servidor de

113
11/11/08

almacenamiento 322. Aquí el servidor de almacenamiento 322 también puede ser operativo para almacenar de forma segura claves privadas 324 asociadas con una pluralidad de diferentes usuarios. Sin embargo, en esta realización descrita, más que enviar al servidor de almacenamiento 322 una copia completa del documento electrónico 326, el cajero

5 automático de ejemplo 320 puede ser operativo para generar y enviar al servidor de almacenamiento 322 un hash unidireccional 332 del documento electrónico 326. El cajero automático de ejemplo 320 puede incluir uno o más algoritmos de hash unidireccional 334 que corresponden a los protocolos de firmas digitales que el usuario desea utilizar para firmar sus documentos electrónicos. Por ejemplo, para generar firmas digitales, el algoritmo
10 de hash unidireccional de ejemplo 334 del cajero automático 320 puede incluir funciones de hash unidireccionales MD5 o SHA.

Aquí el servidor de almacenamiento 322 puede incluir uno o más algoritmos de encriptación y/o firmas digitales 328 tal como RSA los cuales son operativos para generar una firma digital 330 para el documento electrónico 326 utilizando el hash unidireccional
15 332 y la clave privada 324 asociada con el usuario. El servidor de almacenamiento puede luego devolver la firma digital 330 al cajero automático 320 y el cajero automático 320 puede anexar la firma digital 330 al documento electrónico 326.

La figura 11 muestra una realización de ejemplo de un cajero automático 340 que puede ser operativo para comunicarse con una realización de ejemplo alternativa de un
20 servidor de almacenamiento 342. Aquí el servidor de almacenamiento 342 puede ser operativo para almacenar de manera segura claves privadas 344 asociadas con una pluralidad de diferentes usuarios. Sin embargo, en esta realización descrita, el servidor de almacenamiento 342 puede ser operativo para enviar de manera segura una clave privada de un usuario al cajero automático 340. El cajero automático 340 de ejemplo puede incluir
25 un software de firmas digitales 348 el cual es operativo para hacer que el cajero automático 340 genere una firma digital 300 para un documento electrónico 346 del usuario operando el cajero automático 340.

La figura 12 muestra una realización de ejemplo de un cajero automático 400 que puede ser operativo para comunicarse con un dispositivo de cómputo portátil 402 asociado
30 con un usuario tal como una tarjeta inteligente, PDA, o teléfono celular. Aquí el dispositivo

114
~~114~~

de cómputo portátil 402 puede incluir al menos una clave privada 404 asociada con el usuario. En esta realización descrita, después que el usuario ha leído un documento electrónico 406 asociado con el usuario, el cajero automático 400 puede ser operativo para enviar el documento electrónico 406 hacia el dispositivo de cómputo portátil 402. El

5 dispositivo de cómputo portátil de ejemplo puede incluir software de firmas digitales 408 el cual es operativo para generar una firma digital 410 para el documento electrónico 406 utilizando la clave privada 404 almacenada en el dispositivo de cómputo portátil. El dispositivo de cómputo portátil 402 puede luego anexar la firma digital 410 al documento electrónico 406 y devolver el documento electrónico firmado al cajero automático 400 o el
10 dispositivo de cómputo portátil puede solamente enviar la firma digital 410 al cajero automático 400. El cajero automático 400 de ejemplo puede luego anexar la firma digital 410 al documento electrónico 406 y transmitir el documento electrónico firmado hacia una ubicación de destino seleccionada elegida por el usuario.

La figura 13 muestra una realización de ejemplo de un cajero automático 420 que
15 puede ser operativo para comunicarse con un dispositivo de cómputo portátil 422. Aquí el dispositivo de cómputo portátil 422 también puede incluir al menos una clave privada 424 del usuario. Sin embargo en esta realización descrita, más que el envío al dispositivo de cómputo portátil 422 de una copia completa de un documento electrónico 426, el cajero automático de ejemplo 420 puede ser operativo para generar y enviar al dispositivo de
20 cómputo portátil 422 un hash unidireccional 432 del documento electrónico 426. El cajero automático de ejemplo 420 puede incluir uno o más componentes de software con algoritmos de hash unidireccional 432 que corresponden a los protocolos de firmas digitales que el usuario desea utilizar para firmar su documento electrónico 426. Utilizando los algoritmos de hash unidireccional 432, el cajero automático 420 puede ser operativo para
25 producir un hash unidireccional 432 del documento electrónico 426 y transmitir el hash unidireccional 432 hacia el dispositivo de cómputo portátil 422.

El dispositivo de cómputo portátil de ejemplo 422 puede incluir uno o más algoritmos de encriptación y/o de firmas digitales 428 los cuales son operativos para generar una firma digital 430 para el documento electrónico 426 utilizando el hash
30 unidireccional 432 y la clave privada 424 asociada con el usuario. El dispositivo de

115
11/11/11

cómputo portátil 422 puede luego devolver la firma digital 430 hacia el cajero automático 420 y el cajero automático 420 puede anexar la firma digital 430 al documento electrónico 426.

5 La figura 14 muestra una realización de ejemplo de un cajero automático 440 que puede ser operativo para comunicarse con un dispositivo de cómputo portátil de ejemplo 442. Aquí, el dispositivo de cómputo portátil 442 puede incluir al menos una clave privada 444 del usuario. Sin embargo, en esta realización descrita, el dispositivo de cómputo portátil 442 puede ser operativo para enviar de manera segura la clave privada 444 del usuario hacia el cajero automático 440. El cajero automático 440 de ejemplo puede incluir software de firmas digitales 448 el cual es operativo para hacer que el cajero automático 10 440 genere una firma digital 450 para un documento electrónico 446 del usuario que opera el cajero automático 440.

Con referencia a la figura 1, el servidor de almacenamiento de ejemplo 32 puede ser operativo para mantener un registro de acceso 62 en asociación con la cuenta de depósito seguro digital 40 y/o la cuenta bancaria 48 del usuario. El servidor de almacenamiento de 15 ejemplo 32 puede ser operativo para almacenar en el registro de acceso 62 un registro de cada acceso intentado de una cuenta de depósito seguro digital del usuario 40 y/o utilización de la clave privada 44. Si un impostor logra acceso a la cuenta de depósito seguro digital de un usuario y/o clave privada, el registro de acceso de ejemplo puede ser utilizado para determinar cuándo y dónde ocurrió el acceso no autorizado. El registro de 20 acceso de ejemplo puede además incluir un registro de cual documento electrónico fue firmado por el sistema. El registro por ejemplo puede incluir el hash unidireccional del documento electrónico. Si un impostor utiliza el presente sistema de ejemplo para firmar digitalmente un documento electrónico, el registro de acceso puede ser utilizado para 25 determinar cual documento puede haber sido adulterado.

Algunas realizaciones de ejemplo del cajero automático pueden ser operativas para encriptar documentos electrónicos almacenados en la cuenta de depósito seguro digital utilizando un algoritmo de encriptación simétrica tal como DES y una clave secreta. El cajero automático de ejemplo puede ser operativo para permitir a un usuario generar una 30 clave secreta para la encriptación de documentos electrónicos a partir de una contraseña o a

H6
02/02/02

partir de información biométrica proporcionada por el usuario al cajero automático. Para descryptar el documento electrónico, el cajero automático de ejemplo puede ser operativo para generar nuevamente la clave secreta solicitando al usuario nuevamente la entrada de la contraseña y/o datos biométricos.

5 Además para hacer que un documento electrónico sea firmado, una realización de ejemplo alternativa de un cajero automático puede ser operativa para firmar, notarizar y/o servir como consignatario un documento electrónico utilizando una clave privada asociada con el cajero automático, servidor de almacenamiento, servicio/red de firmas digitales, o un tercero. Por ejemplo, además de permitir que el usuario firme digitalmente un documento

10 electrónico utilizando su clave privada, el cajero automático de ejemplo también puede hacer que el documento electrónico sea además digitalmente firmado utilizando una clave privada adicional no asociada con la clave privada del usuario. Tal clave privada adicional puede estar asociada con un notario público autorizado, servicio de firmas digitales, u otra parte para una transacción la cual está asociada con el documento electrónico. El cajero

15 automático de ejemplo puede además anexar el certificado digital asociado con la clave privada adicional al documento electrónico firmado. Tal certificado digital puede ser utilizado para verificar la autenticidad de la segunda firma digital. También los certificados digitales asociados con las autoridades certificadoras que expiden y firman el certificado digital del usuario y/o un certificado digital del notario público u otra parte también pueden

20 ser anexados al documento electrónico.

En una realización de ejemplo, el cajero automático puede ser operativo para anexar un sello digital de fecha y hora al documento electrónico mediante la inclusión de la fecha y hora en el documento electrónico antes que el documento electrónico sea digitalmente firmado por el usuario del cajero automático. En algunas realizaciones de ejemplo, el cajero

25 automático puede ser operativo para hacer que a un documento electrónico se anexe un sello digital de fecha y hora mediante un servidor o entidad de sellado digital con fecha y hora de documentos. Por ejemplo, el cajero automático de ejemplo puede enviar un hash unidireccional del documento electrónico hacia una entidad de sellado digital con fecha y hora. La entidad de sellado digital con fecha y hora sería operativa para anexar datos de

30 horarios representativos de la fecha, hora y huso horario en que la entidad de sellado con

117
~~117~~

fecha y hora recibió el hash unidireccional. La entidad de sellado con fecha y hora puede luego firmar digitalmente el hash unidireccional y los datos de horarios con una clave privada de la entidad de sellado de fecha y hora para formar un sello digital de fecha y hora y este sello de fecha y hora puede luego ser devuelto al cajero automático junto con un

5 certificado digital de la entidad de sellado digital con fecha y hora. El cajero automático puede luego anexar el sello digital de fecha y hora y el certificado digital de la entidad de sellado digital con fecha y hora al documento electrónico. En algunas realizaciones, la entidad de sellado digital con fecha y hora puede corresponder a la misma entidad, servicio, o red que es operativa para producir la firma digital para el usuario del cajero automático.

10 La figura 15 muestra un ejemplo de un sistema de firma de documentos de una realización de ejemplo. Aquí el sistema 500 puede incluir al menos un cajero automático 500 que es operativo para presentar por pantalla y firmar de manera digital documentos electrónicos. El cajero automático 510 puede además ser operativo para comunicarse con uno o más servidores 508 incluyendo servidores asociados con un sistema de

15 procesamiento de transacciones financieras, red bancaria local, sistema de procesamiento de documentos, una red o servicio de firmas digitales.

Además el cajero automático 510 puede ser operativo para recibir documentos electrónicos desde al menos un computador personal 512 u otros dispositivos de cómputo a través de una red alambica o inalámbrica 516. En esta realización descrita, el cajero

20 automático 510 puede incluir o estar en conexión operativa con una unidad de red compartida o externamente accesible 514 la cual es operativa para almacenar documentos electrónicos entrantes y salientes. Tal unidad de red compartida puede ser segregada hacia una o más ubicaciones tal como un área de almacenamiento de ingreso y egreso.

Selectivamente se puede dar permiso al computador personal 512 para accesar la

25 unidad de red compartida 514 o una parte de la unidad de red compartida tal como un "ingreso" asociado con el cajero automático 510. Los documentos electrónicos creados por el computador personal 512 pueden luego ser guardados, exportados y/o enviados hacia la unidad de red compartida 514 del cajero automático 510. Un usuario que opera el cajero automático 510 puede seleccionar comandos del cajero automático los cuales hacen que el

30 cajero automático presente por pantalla y firme de manera digital documentos electrónicos

118
11/18

almacenados en la unidad de red compartida 514. Las versiones digitalmente firmadas del documento electrónico pueden luego ser guardadas, exportadas, o enviadas hacia la unidad de red compartida 514 o una parte de la unidad de red compartida tal como un "egreso" de la unidad de red compartida 514. El computador personal 512 u otros dispositivos de
5 cómputo pueden luego recuperar el documento firmado desde la unidad de red compartida 514. El cajero automático 510 también puede estar en conexión operativa con una impresora 518 y puede incluir opciones elegibles para imprimir el documento electrónico digitalmente firmado en la impresora.

Las realizaciones de ejemplo del cajero automático 510 puede incluir dispositivos
10 de funciones de transacciones tales como un dispensador de efectivo y un dispositivo para consignaciones los cuales permiten que el cajero automático realice otros tipos de funciones de transacciones tales como la dispensación de efectivo y la consignación de cheques. Sin embargo, algunas realizaciones de ejemplo del cajero automático 510 pueden ser configuradas en una forma diferente tal como una forma portátil la cual no dispensa
15 efectivo o recibe cheques depositados. Un ejemplo de tal forma portátil de un cajero automático es mostrado en la figura 16. Aquí la realización de ejemplo del cajero automático portátil 520 puede incluir un lector de tarjetas de banda magnética 52 u otro lector de tarjetas, una pantalla 524, y un tablero digitalizador de firmas 526. El cajero automático 520 puede además incluir teclas de función 528 para proporcionar
20 entradas al cajero automático. Realizaciones de ejemplo adicionales de la pantalla 524 pueden incluir una pantalla táctil para proporcionar entradas al cajero automático y un dispositivo de comunicación 527 tal como una interfase de red alambica o inalámbrica.

Con referencia a la figura 15, la realización de ejemplo del cajero automático 510 puede ser utilizada por organizaciones que deseen ofrecer a los usuarios la capacidad para
25 firmar de manera digital con seguridad documentos electrónicos. Tales organizaciones pueden incluir bancos, compañías hipotecarias, inmobiliarias, S&Ls, compañías de seguros, concesionarios de vehículos, compañías arrendatarias, universidades, hospitales, agencias gubernamentales, o cualquier otra organización que genere documentos los cuales requieren firmas de sus clientes. El cajero automático 510 de ejemplo proporciona a los

419
~~419~~

consumidores o clientes de la organización u otros usuarios un método conveniente para leer y firmar digitalmente documentos electrónicos.

La figura 17 muestra los pasos de ejemplo involucrados en la operación del sistema 500. Aquí los pasos del método son descritos con respecto un concesionario de vehículos; sin embargo, se debe entender que los pasos de ejemplo también se pueden cualquier a cualquier organización, entidad, grupo o individuo que desee que los usuarios firmen de manera digital documentos electrónicos. El método puede comenzar en el paso 600 con un gerente financiero u otros miembros de la organización preparando documentos electrónicos que corresponden a un crédito para vehículo. Tal documento electrónico pueden incluir un documento de procesamiento de texto, un documento Acrobat® PDF, documento de Lenguaje Markup eXtensible, o cualquier otro tipo de documento el cual puede representar electrónicamente un crédito para vehículo.

En una realización de ejemplo, el documento electrónico puede ajustarse a un formato de crédito estandarizado. Tal formato puede incluir etiquetas XML estandarizadas que describen la información acerca del Prestamista, receptor del crédito, y los términos de crédito. Tales etiquetas pueden incluir por ejemplo los nombres y direcciones de las partes, el monto del crédito, la duración del crédito, la tasa de interés y cualquier otro término o categoría de información que pueda ser parte del crédito. Una vez el documento es creado, el gerente financiero en el paso 602 puede guardar el documento electrónico en una ubicación de almacenamiento que es accesible al cajero automático. Por ejemplo, el gerente financiero puede guardar el documento electrónico en el ingreso asociado con un cajero automático.

En organizaciones grandes las cuales pueden procesar dos solicitudes de crédito concurrentemente, múltiples cajeros automáticos pueden estar disponibles para guardar el documento electrónico. En tales casos, la unidad de red compartida puede estar asociada con el nombre o identificación del cajero automático particular el cual es operativo para acceder el documento electrónico desde la unidad de red compartida. Una vez el documento electrónico es guardado en la ubicación de almacenamiento, el gerente de finanzas puede indicar al cliente para comenzar a utilizar el cajero automático particular el cual es operativo para recuperar el documento electrónico.

120
~~120~~

Una vez el cliente tiene acceso al cajero automático, el cliente puede seguir las instrucciones presentadas a través del dispositivo de pantalla del cajero automático. Si el cliente tiene una cuenta de depósito seguro digital, certificado digital, y/o clave privada asociadas con una cuenta bancaria, el cajero automático puede solicitar al cliente insertar o

5 deslizar una tarjeta que esté asociada con una cuenta de depósito seguro digital, certificado digital, y/o clave privada. Por ejemplo si el cliente tiene una tarjeta de cuenta corriente o tarjeta de crédito la cual está asociada con una cuenta de depósito seguro digital, el cliente puede en el paso 604 insertar o deslizar su tarjeta de cuenta corriente o tarjeta de crédito dentro del lector de tarjetas del cajero automático.

10 En respuesta, el cajero automático puede ser operativo para leer el número de cuenta bancaria asociado con la tarjeta en el paso 606 con el lector de tarjetas y solicitar que el cliente entre un PIN. En el paso 608 el cliente puede entrar un PIN a través de un teclado o a través de una pantalla táctil la cual puede ser configurada para desplegar una

15 representación visual de un teclado. En la realización de ejemplo, el PIN puede corresponder a un PIN de cuatro dígitos asociado con la cuenta bancaria del cliente. En otras realizaciones de ejemplo, el PIN puede corresponder a una contraseña diferente almacenada en asociación con la cuenta de depósito seguro digital del cliente, certificado digital, y/o clave privada. Tal contraseña puede incluir cuatro más dígitos y/o caracteres numéricos. En otras realizaciones el cajero automático puede solicitar al usuario

20 proporcionar datos biométricos como una contraseña a través del uso del dispositivo lector biométrico del cajero automático.

Para cajeros automáticos que son operativos para realizar muchos tipos diferentes de funciones de transacciones, el cajero automático puede presentar una pantalla de interfase de usuario similar a la pantalla 100 de la figura 3 después que el cliente ha proporcionado

25 un PIN. Como se discutió anteriormente, la pantalla de interfase de usuario 100 puede incluir funciones elegibles 102 para retirar efectivo, consignar un cheque, transferir fondos entre cuentas, y leer un documento electrónico. Para cajeros automáticos tales como el cajero automático portátil 520 de la figura 16, el cajero automático puede recuperar inmediatamente el documento electrónico almacenado en el ingreso asociado con el cajero

30 automático y presentar una pantalla de interfase de usuario similar a la pantalla 160 de la

12/10/12

figura 6. Si más de un documento electrónico está presente en el ingreso el cajero automático puede presentar por pantalla un listado de documentos electrónicos a elegir. En cada caso los cajeros automáticos de ejemplo pueden ser operativos para recuperar un documento electrónico en el paso 610 desde la ubicación de almacenamiento y presentar por pantalla una representación visual del documento en el paso 612.

El cliente puede leer a través del documento presentado y hacer cualquier entrada necesaria de información que el documento electrónico puede requerir. Por ejemplo, el documento electrónico puede incluir cláusulas que requieren ser aprobadas por el cliente. Tales cláusulas pueden incluir elementos de interfase de usuario tal como, campos de entrada, y/o listados que pueden ser marcados o desmarcados, editados, y/o seleccionados con los dispositivos de entrada del cajero automático.

Una vez el documento ha sido revisado y actualizado con información necesaria suministrada por el cliente, en el paso 614 el cliente puede proporcionar una entrada representativa de un comando para firmar digitalmente el documento electrónico. En respuesta, el cajero automático puede en el paso 616 solicitar al cliente el suministro de una entrada adicional que es representativa de una confirmación por parte del cliente sobre que la firma digital pretende ser la firma legalmente valedera del cliente. Para cajeros automáticos que incluyen un tablero digitalizador de firmas, ésta entrada de confirmación puede incluir la realización por parte del cliente de la firma a mano sobre el tablero digitalizador de firmas. El escaneo digital de la firma a mano puede luego ser integrado en el documento electrónico antes del firmar digitalmente el documento.

En respuesta a la recepción de entrada de confirmación, el cajero automático en el paso 618 puede hacer que el documento electrónico sea digitalmente firmado utilizando una clave privada asociada con la cuenta bancaria leída desde la tarjeta del cliente. Una vez el documento ha sido digitalmente firmado este puede ser asociado con uno o más certificados digitales incluyendo el certificado digital asociado con la cuenta bancaria. Tal certificado digital incluye la clave pública del cliente la cual puede ser utilizada para verificar la firma digital sobre el documento electrónico. En otras realizaciones, el documento electrónico puede incluir un número de serie y/o una referencia a una entidad, dirección o URL donde el certificado digital del cliente puede ser recuperado para verificar la firma digital. En

algunas realizaciones, el certificado digital de la autoridad certificadora la cual expide y firma los certificados digitales de usuarios puede ser asociado con el documento electrónico.

Una vez el documento electrónico ha sido digitalmente firmado, el cajero automático en el paso 620 es operativo para enviar el documento electrónico firmado a una o más direcciones de salida especificadas. Tal dirección de salida especificada puede incluir la ubicación de almacenamiento original donde el cajero automático recuperó el documento electrónico no firmado. Tal dirección de salida especificada puede incluir una parte de la unidad de red compartida que corresponde a un egreso electrónico. Tal dirección de salida especificada puede corresponder a una dirección de red, una dirección electrónica, base de datos, URL, o cualquier otra ubicación de almacenamiento externo o sistema de comunicación el cual es operativo para recibir un documento electrónico. Por ejemplo, en la realización de ejemplo la dirección de salida especificada puede incluir un URL de un servidor de procesamiento de documentos. Por ejemplo si el documento electrónico corresponde a un crédito para vehículo, la dirección de salida especificada puede ser un servidor de procesamiento de documentos del banco que está prestando el dinero al cliente para comprar el vehículo.

Tal servidor de procesamiento de documentos puede verificar la firma digital del documento electrónico. Si la firma es válida, el servidor de procesamiento de documentos puede analizar sintácticamente las etiquetas XML del documento electrónico para determinar el nombre y la dirección del individuo y los términos del crédito. Tal información puede luego ser integrada en el sistema de procesamiento de créditos del banco para establecer una cuenta de crédito y para iniciar los procesos necesarios para recolectar pagos por parte del cliente. En otras realizaciones de ejemplo, la dirección de salida especificada puede corresponder a un sistema de procesamiento de créditos que es operativo para titularizar el crédito para liberación a otro banco u otra entidad. En otras realizaciones de ejemplo, la dirección de salida especificada puede corresponder a cualquier sistema que es operativo para almacenar y/o procesar el documento electrónico firmado.

En una realización de ejemplo la dirección de salida especificada puede ser un parámetro configurable dentro del cajero automático. En otras realizaciones de ejemplo, la

dirección de salida especificada puede ser determinada por el cajero automático a partir de un parámetro del documento electrónico. Por ejemplo, el documento electrónico puede incluir una etiqueta XML la cual incluye una dirección para la dirección de salida especificada. En realizaciones de ejemplo donde la cuenta bancaria del cliente está asociada con la cuenta de depósito seguro digital, el cajero automático puede además hacer que una copia del documento electrónico firmado sea almacenada en la cuenta de depósito seguro digital del cliente la cual puede ser asociada con la cuenta bancaria del cliente.

En la realización de ejemplo, el cajero automático en el paso 622 puede hacer que un cargo de procesamiento de firmas digitales sea cobrado a un individuo asociado con el documento electrónico. El cajero automático de ejemplo es operativo para hacer que un sistema de procesamiento de transacciones financieras tal como una red bancaria local u otro servidor registre información asociada con el cargo de procesamiento en una base de datos, registro, o diario para establecimiento inmediato o posterior. En una realización de ejemplo, el cargo de procesamiento puede ser cobrado a la cuenta bancaria asociada con la tarjeta del cliente. En otras realizaciones de ejemplo, el cargo de procesamiento puede ser cobrado a una cuenta asociada con la organización que preparó el documento electrónico sin firmar. Por ejemplo, el cajero automático puede incluir un parámetro de configuración que corresponde a una cuenta bancaria que puede ser grabada con los cargos de procesamiento. En el caso del concesionario de vehículos por ejemplo, el parámetro de configuración puede incluir un número de cuenta asociado con el concesionario de vehículos o el banco que proporciona el crédito. En el paso 622 el cajero automático o los servidores de red o servicio de firmas digitales asociados con el cajero automático pueden comunicarse con un sistema de procesamiento de transacciones financieras tal como una red bancaria local para cobrar los cargos de procesamiento a la cuenta. En una realización de ejemplo, el documento electrónico puede incluir un número de cuenta a la cual serán cobrados los cargos de procesamiento. Por ejemplo el documento electrónico puede incluir una etiqueta para una cuenta de procesamiento de cargos.

También en algunas realizaciones de ejemplo, el cajero automático puede contactar un sistema de procesamiento de transacciones financieras tal como una red bancaria local u otro servidor para autorizar el cobro del cargo de procesamiento a una cuenta antes de-

124
10/16/20

firmar digitalmente el documento en el paso 618 o antes de enviar del documento electrónico firmado a una dirección de salida especificada en el paso 620. Si la cuenta no tiene fondos suficientes para pagar el cargo de procesamiento o de otra manera no puede aceptar el cobro de un cargo de procesamiento, el cajero automático puede ser operativo para cancelar la firma del documento electrónico. El cajero automático puede luego sacar un mensaje visual a través de la pantalla del cajero automático que indica que el documento electrónico no puede ser digitalmente firmado.

La dirección de salida especificada puede corresponder a una ubicación de almacenamiento que es accesible a la organización que creó el documento sin firmar. Por ejemplo, con referencia a un concesionario de vehículos, la dirección de salida especificada puede incluir la unidad de red que es accesible al gerente financiero. El gerente puede entonces hacer que el documento electrónico sea impreso de manera que una copia física del documento electrónico pueda ser proporcionada al cliente. En otras realizaciones, el cajero automático puede estar en conexión operativa con una impresora y puede incluir una opción elegible para imprimir una copia física del documento electrónico.

En algunas realizaciones de ejemplo donde el documento electrónico fue previamente firmado por uno o más individuos adicionales, el cajero automático puede incluir el paso de validación de la firma del individuo adicional antes de permitir al usuario firmar digitalmente el documento electrónico. En el caso de un concesionario de vehículos por ejemplo, el gerente financiero puede firmar digitalmente el crédito de vehículo antes que el cajero automático acceda al documento electrónico. La firma digital del concesionario de vehículos puede ser verificada por el cajero automático antes del permitir al usuario firmar digitalmente el crédito de vehículo. En tales casos el documento electrónico puede incluir el certificado digital asociado con los individuos adicionales tales como el concesionario de vehículos. El documento electrónico también puede incluir certificados digitales de las autoridades certificadoras las cuales firmaron los certificados digitales de los individuos adicionales.

En la realización anteriormente descrita, una tarjeta de cuenta bancaria del cliente fue anteriormente asociada con la cuenta de depósito seguro digital del cliente, certificado digital, y/o clave privada. La realización de ejemplo puede incluir un método para

proporcionar tarjetas de cuenta bancarias con la capacidad para firmar digitalmente documentos electrónicos en un cajero automático. Por ejemplo, el emisor de tarjetas de crédito tal como un banco puede tener una pluralidad de cuentas de tarjetas de crédito. Al volverse el mercado de tarjetas de crédito más competitivo, agregar una capacidad de firma digital a las tarjetas de crédito de los clientes de un banco puede proporcionar un incentivo adicional para que el cliente porte y utilice las tarjetas de crédito expedidas por el banco.

Esta realización descrita del método puede incluir la creación por parte del banco u otra entidad de certificados digitales individuales, pares de claves públicas/privadas, y/o cuentas de depósito seguro digital para una pluralidad de cuentas bancarias pre-existentes tales como cuentas de tarjetas de crédito u otras cuentas bancarias. Tales certificados digitales individuales, pares de claves públicas /privadas, y/o cuentas de depósito seguro digital pueden ser almacenadas en asociación con cada una de las cuentas bancarias sobre uno o más servidores operados por el banco o un una red o servicio de firmas digitales.

La figura 18 muestra una vista esquemática de una realización de ejemplo de un sistema 700 que puede ser operativo para realizar este método descrito. Aquí el sistema 700 incluye una pluralidad de bancos 702, 704, u otras organizaciones financieras. Cada uno de los bancos incluye una pluralidad de cuentas bancarias 706, 708 tal como cuentas de tarjetas de crédito. Para cada una de estas cuentas, los bancos pueden tener una entidad de red 710 o de servicio de firmas digitales 710 para administrar un certificado digital, par de claves públicas privadas, y/o cuenta de depósito seguro digital en uno o más servidores de almacenamiento 712.

La realización de ejemplo del servicio o red de firmas digitales 710 incluye o está en comunicación operativa con un sistema hospedero 714. El sistema hospedero es operativo para proporcionar a una pluralidad de cajeros automáticos 716 acceso a los servicios de la red de firmas digitales 710. Tales servicios pueden incluir por ejemplo la firma digital de documentos electrónicos y el almacenamiento de documentos electrónicos en cuentas de depósito seguro digital. Como se discutió anteriormente, los clientes de los bancos 702, 704 pueden utilizar sus tarjetas de crédito u otras tarjetas asociadas con cuentas bancarias para hacer que un cajero automático firme digitalmente documentos electrónicos. Los cargos de procesamiento adquiridos a partir de la firma documentos electrónicos pueden ser

126
02/08/00

transferidos o cobrados a al menos una de las entidades que ópera la red de firmas digitales y los bancos u otros emisores de tarjetas. En una realización de ejemplo, los cargos de procesamiento pueden ser divididos entre la entidad que opera la red de firmas digitales y los bancos u otros emisores de tarjetas.

- 5 Para anunciar que las cuentas bancarias de los clientes pueden ser utilizadas para firmar digitalmente documentos electrónicos, el método de ejemplo descrito puede incluir la marcación de las tarjetas emitidas por el banco con un logotipo, diseño, o marca que indique que la tarjeta puede ser utilizada para firmar documentos electrónicos. Tal logotipo puede ser una marca indicadora de fuente tal como una marca comercial/de
- 10 servicios para la red de firmas digitales 710. Además, para permitir a un usuario localizar más fácilmente los cajeros automáticos 716 que pueden ser utilizados para firmar los documentos electrónicos, los cajeros automáticos 716 pueden incluir o sacar un logotipo de correspondencia. Para bancos u otras entidades con un gran número de cuentas bancarias preexistentes tales como tarjetas de crédito, la realización de ejemplo del método
- 15 actualmente descrito puede incluir el envío por correo de tarjetas de crédito de reemplazo a los clientes las cuales incluyen una marca tal como un logotipo el cual indica que la tarjeta puede ser utilizada para firmar digitalmente documentos electrónicos. En una realización de ejemplo, los clientes pueden utilizar el PIN anteriormente asociado con su cuenta bancaria para acceder un cajero automático para propósitos de firmar digitalmente un documento
- 20 electrónico. En otras realizaciones de ejemplo, el banco puede suministrar al usuario una contraseña separada para utilizar para tener acceso a los servicios de la red de firmas digitales.

- En algunas realizaciones de ejemplo, el cajero automático puede ser operativo para hacer que un nuevo certificado digital sea creado para un usuario para firmar un documento
- 25 electrónico. Por ejemplo, si el usuario no tiene un certificado digital anteriormente expedido, par de claves públicas/privadas y/o cuenta de depósito seguro digital asociada con una tarjeta inteligente, dispositivo de cómputo portátil, cuenta bancaria, tarjeta de crédito, y/o cuenta de depósito seguro digital, el cajero automático de ejemplo puede ser operativo para proporcionar al usuario un certificado digital, par de claves
- 30 públicas/privadas, y/o cuenta de depósito seguro digital. En algunas realizaciones de

ejemplo, el cajero automático puede permitir al usuario transmitir el certificado digital recién creado hacia la tarjeta inteligente, medio de almacenamiento portátil, dispositivo de cómputo portátil, ubicación de almacenamiento en red, u otra ubicación de almacenamiento seleccionada por usuario o dirección para utilizar en la firma de documentos electrónicos en el futuro por medio del cajero automático de ejemplo u otro software y dispositivo de firmas digitales. Como se discutirá más adelante, en algunas realizaciones de ejemplo el cajero automático puede permitir al usuario asociar el certificado digital recientemente creado, par de claves públicas privadas, y/o cuenta depósito seguro digital con una tarjeta seleccionada por usuario o emitida al usuario por la red de firmas digitales.

10 Como con respecto a los productos asociados con la firma de documentos electrónicos, los cargos también pueden ser cobrados por el cajero automático por la creación de un certificado digital, un par de claves públicas/privadas, y/o una cuenta de depósito seguro digital. Como se discutió anteriormente, tales cargos de pueden ser cobrados a una cuenta bancaria del usuario, una cuenta bancaria almacenada en asociación con el cajero automático, una cuenta bancaria asociada con el documento electrónico que se pretende firmar. Por ejemplo, como en el escenario discutido anteriormente para la firma de documentos electrónicos relacionados con créditos para vehículos, el cajero automático puede ser operativo para hacer que los cargos asociados con la creación del certificado digital sean asociados con la entidad que proporciona los documentos electrónicos tal como el concesionario de vehículos o la institución financiera que emite el crédito.

La realización de ejemplo descrita del cajero automático puede solicitar al usuario entrar a través del dispositivo de entrada del cajero automático información acerca del usuario la cual será integrada y/o asociada con el certificado digital. Tal información puede incluir el nombre, dirección, y fecha de nacimiento del usuario. La información de puede incluir el número de seguridad social del usuario, número de pasaporte, número de licencia de conducción del usuario, número de identificación nacional, número de estudiante, o cualquier otro número único asociado con el usuario. La información proporcionada para la generación del certificado digital también puede incluir una contraseña proporcionada por el usuario u otro número para utilizar con la creación o acceso a pares de claves públicas/privadas, la clave pública siendo integrada al certificado digital.

Para facilitar la entrada de información en el cajero automático para la generación del certificado digital, el cajero automático puede ser operativo para recuperar información específica al usuario para el certificado digital a partir de un documento electrónico que se pretende sea firmado digitalmente utilizando el cajero automático. Por ejemplo, en el

5 escenario de ejemplo anterior del usuario firmando los documentos de crédito para vehículo, el gerente financiero o empleado del concesionario de vehículos puede entrar el nombre del usuario, dirección, número de seguro social, fecha de nacimiento, número de licencia de conducción, y/o otra información específica al usuario en el documento electrónico que corresponde al crédito. Tal información puede ser almacenada como datos

10 XML u otro formato accesible de computador dentro o en asociación con el documento electrónico. Antes que el cajero automático permita al usuario firmar el documento electrónico, el cajero automático puede acceder la información específica del usuario asociada con el documento electrónico. La información accedida a partir del documento electrónico además de cualquier otra información solicitada para ser proporcionada

15 directamente al cajero automático por el usuario, puede ser integrada en el certificado digital por el cajero automático. En algunas realizaciones de ejemplo, el cajero automático puede sacar la información específica del usuario a través del dispositivo de salida del cajero automático. El cajero automático puede solicitar al usuario verificar la exactitud de la información antes de la creación de certificado digital.

20 En una realización de ejemplo, el cajero automático puede hacer que la información específica del usuario sea transmitida a una autoridad certificadora la cual es operativa para emitir un certificado digital firmado para el usuario. En algunas realizaciones, el cajero automático puede transmitir la información específica del usuario hacia la red de firmas digitales discutida anteriormente, servidor de almacenamiento, y/o otro servidor el cual es

25 operativo para dar formato al certificado digital y/o interfase con la autoridad certificadora para emitir el certificado digital.

En una realización de ejemplo, la red de firmas digitales puede ser operativa para autenticar la información proporcionada específica al usuario mediante contacto con los servicios de reporte de créditos 720 o cualquier otra base de datos o información de usuario

30 para comparar y validar la información proporcionada específica al usuario. Si la

información específica al usuario es inválida, inconsistente, o de otra manera sospechosa, la red de firmas digitales de ejemplo puede devolver un mensaje al cajero automático el cual es representativo de un rechazo para generar un certificado digital para el usuario. Tal mensaje puede indicar las razones para el rechazo.

- 5 Las realizaciones de ejemplo del cajero automático pueden además adquirir información adicional del usuario que solicita el certificado digital incluyendo una entrada biométrica, tal como un escaneo de huellas digitales, una imagen digital de la cara del usuario, escaneo de iris, de escaneo de manos, o cualquier otra entrada que pueda ser representativa de la identidad del usuario. Tal información puede ser integrada o asociada
- 10 con un certificado digital. Tal información también puede ser utilizada para validar la identidad del usuario antes de crear el certificado digital.

- En algunas realizaciones de ejemplo, el cajero automático puede además solicitar al usuario entrar una tarjeta, tal como una tarjeta de crédito, tarjeta inteligente, licencia de conducción, tarjeta de identificación nacional, o cualquier otra tarjeta única la cual pueda
- 15 ser accesada por el lector de tarjetas del cajero automático para recuperar información específica del usuario. Tal información específica del usuario puede incluir un número de cuenta u otro número almacenado en una tarjeta el cual puede ser transmitido hacia la red de firmas digitales, sistema de procesamiento de transacciones financieras tal como la red bancaria local, u otro servidor para ser utilizado para autenticar la identidad del usuario. En
- 20 algunas realizaciones de ejemplo, el cajero automático puede además solicitar al usuario la entrada a través del dispositivo de entrada del cajero automático, de una contraseña secreta o PIN a través de comunicación con la red de firmas digitales, red bancaria local, o la tarjeta misma.

- En algunas realizaciones de ejemplo, el cajero automático puede solicitar al usuario
- 25 proporcionar una entrada que indique si el usuario desea que el certificado digital recién creado, pares de claves públicas/privadas y/o cuenta de depósito seguro digital sean asociados con una cuenta bancaria preexistente del usuario tal como una tarjeta de crédito o tarjeta bancaria. En tales casos, el cajero automático de ejemplo puede solicitar al usuario la inserción de la tarjeta deseada en el lector de tarjetas del cajero automático. El número de
- 30 cuenta leído de la tarjeta puede ser transmitido a la red de firmas digitales y ser almacenado

en asociación con un certificado digital recién creado, pares de claves públicas/privadas, y/o cuenta de depósito de seguro digital del usuario. La red de firmas digitales puede además notificar a la institución financiera asociada con la tarjeta, que el usuario ha asociado un certificado digital, pares de claves públicas/privadas y/o cuenta de depósito seguro digital con el número de cuenta de la tarjeta. La institución financiera puede luego emitir una nueva tarjeta al usuario, la cual incluye la marca o logotipo de la red de firmas digitales.

Las realizaciones de ejemplo el cajero automático también puede solicitar al usuario confirmación acerca de si el usuario desea que el certificado digital recién creado, pares de claves públicas/privadas y/o cuenta de depósito seguro digital sean asociados con otros números de tarjetas únicamente asociados con el usuario. Tales tarjetas por ejemplo pueden incluir la tarjeta de seguridad social del usuario, la tarjeta de licencia de conducción, la tarjeta de identificación nacional, y una tarjeta de identificación de estudiante. En tales casos, el cajero automático de ejemplo puede pedir al usuario que inserte la tarjeta con el número único deseado almacenado sobre la misma a través del lector de tarjetas del cajero automático. El número único leído desde la tarjeta puede ser transmitido hacia la red de firmas digitales y ser almacenado en asociación con el certificado digital recién creado, pares de claves públicas/privadas, y/o cuenta de depósito seguro digital del usuario.

En algunas realizaciones, donde el certificado digital recién creado, los pares de claves públicas/privadas, y/o cuenta de depósito seguro digital no están asociados con una cuenta bancaria u otro número/tarjeta únicos del usuario, la red de firmas digitales puede ser operativa para emitir al usuario una tarjeta de firmas digitales para utilizar para la firma futura de documentos electrónicos y para acceder documentos electrónicos almacenados en la cuenta de depósito seguro digital del usuario. La tarjeta de firmas digitales puede incluir almacenado sobre la misma un único número de cuenta asociado con un certificado digital recién creado, pares de claves públicas privadas, y/o cuenta de depósito seguro digital. En una realización de ejemplo, el cajero automático puede incluir un dispositivo emisor de tarjetas el cual es operativo para sacar la tarjeta de firmas digitales directamente al usuario una vez el certificado digital es creado. En realizaciones de ejemplo adicionales, la red de

431
00000

firmas digitales puede iniciar la producción de una tarjeta de firmas digitales la cual es enviada por correo a la dirección del usuario.

Una vez el certificado digital, par de claves públicas/ privadas, y/o la cuenta de depósito seguro digital son creados, el cajero automático de ejemplo puede proceder para solicitar al usuario a través del proceso de la firma del documento electrónico la utilización de la clave privada asociada con el certificado digital recién creado. En realizaciones de ejemplo, donde el usuario asocia una cuenta bancaria u otro número/tarjeta con el certificado digital recién creado o donde una tarjeta de firmas digitales es emitida al usuario, el cajero automático puede solicitar al usuario entrar a través del dispositivo de entrada del cajero automático, una contraseña secreta o PIN para ser asociado con la tarjeta para propósitos de utilizar la tarjeta en el futuro para firmar documentos electrónicos. Para acceder documentos electrónicos almacenados en la cuenta de depósito seguro digital recién creado. En el futuro, el usuario puede utilizar su tarjeta de crédito, tarjeta de firmas digitales, u otra tarjeta asociada con el certificado digital recién creado, par de claves públicas/privadas, y/o cuenta de depósito seguro digital para firmar otros documentos electrónicos en el mismo cajero automático u otro cajero automático de ejemplo conectado a la red de firmas digitales de ejemplo. Como se discutió anteriormente las realizaciones de ejemplo del cajero automático pueden solicitar al usuario la entrada de la contraseña o PIN asociado con la tarjeta antes de permitir al usuario la firma de documentos electrónicos y/o acceder documentos electrónicos para una cuenta de depósito seguro digital con el cajero automático.

Como se muestra en la figura 18, la realización de ejemplo de la red de firmas digitales puede además estar en comunicación con una red pública tal como la Internet 718 para permitir al usuario acceder su certificado digital, par de claves públicas/privadas, y/o cuenta de depósito seguro digital desde el computador de hogar u otro dispositivo de cómputo. La red de firmas digitales puede además proporcionar servicios en la Internet tal como la firma digital de documentos electrónicos y/o almacenamiento de documentos electrónicos en una cuenta de depósito seguro digital asociada con una cuenta bancaria. Por ejemplo, en una realización de ejemplo, la red de firmas digitales puede incluir un servidor de Internet el cual permite al usuario entrar su número de cuenta bancaria u otro

número/tarjeta y PIN u otra contraseña a través de un navegador de un computador personal u otro dispositivo de cómputo. Si la información proporcionada es válida, la red de firmas digitales de ejemplo puede permitir al usuario firmar un documento electrónico utilizando la clave privada asociada con el número de cuenta bancaria proporcionada u otros
5 números/tarjeta. El servidor de Internet puede además permitir a usuarios de Internet administrar documentos electrónicos que están almacenados en los servidores de almacenamiento de la red de firmas digitales 710, tal administración comprende la lectura, copia, eliminación, y transmisión de documentos a otras ubicaciones y direcciones.

El software de computador utilizado para operar las máquinas automáticas
10 transacciones del presente invento y computadores conectados, procesadores de computador, y servidores puede ser cargado desde dispositivos de varios tipos en los computadores respectivos. Tal software de computador puede ser incluido y cargado desde uno o más dispositivos tales como disquetes, discos compactos, o DVDs. Tal software también puede ser incluido en dispositivos tales como unidades de disco duro, cintas,
15 dispositivos de memoria de sólo lectura, o tarjetas de memoria. Otros dispositivos que incluyen datos representativos de las instrucciones para operar los computadores en la manera descrita en la presente son apropiados para utilizar para lograr la operación de las máquinas automáticas transacciones y servicios de firmas digitales asociados, redes y servidores y sistemas según las realizaciones descritas en la presente.

20 Las realizaciones de ejemplo de las máquinas automáticas de banca y sistemas descritos en la presente han sido descritas con referencia a componentes de software, funciones y características particulares. Otras realizaciones del invento pueden incluir otros componentes de software diferentes, algoritmos de firmas digitales, y componentes de criptografía los cuales proporcionan funcionalidad similar.

25 El nuevo sistema y método de firmas digitales de máquinas automáticas de transacciones logra uno o más de los objetivos anteriormente declarados, elimina las dificultades encontradas en el uso de dispositivos y sistemas anteriores, resuelve problemas y consigue los resultados deseados descritos en la presente.

En la anterior descripción ciertos términos han sido utilizados por brevedad,
30 claridad y entendimiento, sin embargo limitaciones necesarias serán implicadas a partir de

la misma puesto que tales términos son utilizados para propósitos descriptivos y tienen la intención de ser ampliamente interpretados. Además, las descripciones e ilustraciones en la presente son la manera de ejemplos y el invento no está limitado a detalles exactos mostrados y descritos.

- 5 En los siguientes reivindicaciones cualquier característica descrita como un medio para realizar una función será interpretada como incluyendo cualquier medio conocido por aquellos con experiencia en el estado de la técnica para ser capaz de realizar la función citada, y no será limitada a las características y estructuras mostradas en la presente o meros equivalentes de las mismas. La descripción de la realización de ejemplo incluida en el
- 10 Resumen el cual es incluido en la presente no se considera que limite el invento a las características descritas en la presente.

- Habiendo descrito las características, descubrimientos y principios del invento, la manera en los cuales éste es construido y operado, y las ventajas y resultados útiles logrados; las estructuras, dispositivos, elementos, disposiciones, partes, combinaciones,
- 15 sistemas, equipo, operaciones, métodos y relaciones nuevas y útiles son divulgados en las reivindicaciones anexas.

REIVINDICACIONES

1. Un aparato que comprende
un cajero automático, en donde el cajero automático incluye:
al menos un procesador de computador;

Al menos un dispositivo de entrada en conexión operativa con el procesador de computador, y

Al menos un dispositivo de pantalla en conexión operativa con el procesador de computador, en donde el procesador de computador es operativo para aceptar una representación visual de al menos un documento electrónico a través del dispositivo de pantalla en respuesta a por lo menos una primera entrada a través de al menos un dispositivo de entrada, y en donde el procesador de computador es operativo para hacer que al menos un documento electrónico sea firmado digitalmente con una clave privada en respuesta a por lo menos una segunda entrada a través de al menos un dispositivo de entrada.

2. El aparato según la reivindicación 1, en donde el procesador de computador es operativo para hacer que un mensaje sea sacado a través del dispositivo de pantalla el cual solicita al usuario entrar a través del al menos un dispositivo de entrada, una entrada de confirmación la cual es representativa de una confirmación que una firma digital del documento electrónico pretende ser una firma legalmente valedera, en donde al menos una segunda entrada incluye la entrada de confirmación.

3. El aparato según la reivindicación 1, en donde el cajero automático además incluye un dispositivo dispensador de efectivo en conexión operativa con el procesador de computador, en donde el procesador de computador es operativo para hacer que el dispensador de efectivo dispense dinero en respuesta a por lo menos una tercera entrada a través del al menos un dispositivo de entrada.

4. El aparato según la reivindicación 2, en donde el cajero automático además incluye un tablero digitalizador de firmas en conexión operativa con el procesador de computador, en donde el procesador de computador es operativo para recibir al menos un escaneo de firma escrita a mano a través del tablero digitalizador de firmas, en donde el procesador de computador es operativo para incluir el escaneo de la firma escrita a mano con el documento electrónico.

5. El aparato según la reivindicación 3, en donde el cajero automático además incluye un lector de tarjetas en conexión operativa con el procesador de computador, en donde el procesador de computador es operativo para hacer que lector de tarjetas lea al menos un número de cuenta desde una tarjeta, en donde el procesador de computador es operativo para hacer que un servidor remoto acceda a la clave privada en respuesta a al menos un número de cuenta leído desde la tarjeta.

6. El aparato según la reivindicación 5, en donde el número de cuenta incluye un número de cuenta bancaria asociada con una cuenta bancaria.

7. El aparato según la reivindicación 6, en donde el procesador de computador es operativo para hacer que el documento electrónico sea sellado digitalmente con fecha y hora.

8. El aparato según la reivindicación 7, en donde el cajero automático incluye una cara frontal, en donde al menos un dispositivo de pantalla y al menos un dispositivo de entrada son accesibles al usuario a través de la cara frontal, en donde además comprende indicios visibles adyacentes a la cara frontal del ATM, en donde los indicios visibles son representativos de una marca indicadora de fuente para un servicio de firmas digitales.

9. El aparato según la reivindicación 5, en donde el cajero automático además incluye al menos un puerto de comunicación en conexión operativa con el procesador de

computador, en donde el procesador de computador es operativo para comunicarse con al menos una fuente externa a través del puerto de comunicación, en donde el procesador de computador es operativo para recuperar el documento electrónico desde hace menos una fuente externa.

5 10. El aparato según la reivindicación 9, en donde el procesador de computador es operativo para enviar una copia digitalmente firmada del documento electrónico hacia al menos una fuente externa.

10 11. El aparato según la reivindicación 9, en donde al menos una fuente externa incluye una ubicación de almacenamiento accesible por red.

12. El aparato según la reivindicación 9, en donde al menos una fuente externa incluye un dispositivo de cómputo portátil.

15 13. El aparato según la reivindicación 2, en donde el procesador de computador es operativo en respuesta al menos una segunda entrada para anexar una declaración al documento electrónico la cual indica que el usuario confirmó que la firma digital del documento electrónico pretende representar una firma electrónica legalmente valedera del usuario.

20 14. El aparato según la reivindicación 13, en donde el procesador de computador es operativo para hacer que al menos la declaración sea digitalmente firmada con una clave privada adicional.

25 15. El aparato según la reivindicación 3, en donde el cajero automático además incluye una unidad de dispositivo de almacenamiento en conexión operativa con el procesador de computador, en donde el procesador de computador es operativo para leer y escribir en un medio de almacenamiento portátil colocado en conexión operativa con la 30 unidad de dispositivo de almacenamiento, en donde el procesador de computador es

operativo para recuperar el documento electrónico desde el medio de almacenamiento portátil.

5 16. El aparato según la reivindicación 15, en donde el procesador de computador es operativo para almacenar una copia digitalmente firmada del documento electrónico sobre un medio de almacenamiento portátil.

10 17. El aparato según la reivindicación 3, que comprende además al menos un servidor remotamente localizado al cajero automático, en donde el procesador de computador es operativo para comunicarse con al menos un servidor, en donde al menos un servidor es operativo para generar una firma digital en respuesta a la clave privada.

15 18. El aparato según la reivindicación 17, en donde el procesador de computador es operativo para enviar el documento electrónico a al menos un servidor, en donde al menos un servidor es además operativo para generar la firma digital en respuesta al documento electrónico.

20 19. El aparato según la reivindicación 17, en donde el procesador de computador es operativo para generar y enviar un hash unidireccional del documento electrónico hacia al menos un servidor, en donde al menos un servidor es además operativo para generar la firma digital en respuesta al hash unidireccional, en donde el procesador de computador es operativo para recibir la firma digital desde al menos un servidor, en donde el procesador de computador es operativo para anexar la firma digital al documento electrónico.

25 20. El aparato según la reivindicación 3, en donde el procesador de computador es operativo para comunicarse con al menos un servidor localizado remotamente al cajero automático, en donde el procesador de computador es operativo para recuperar la clave privada desde al menos un servidor, en donde el procesador de computador es operativo para generar una firma digital en respuesta al documento electrónico y la clave privada.

30

21. El aparato según la reivindicación 3, en donde el procesador de computador es operativo para comunicarse con al menos un dispositivo de cómputo portátil, en donde al menos un dispositivo de cómputo portátil incluye la clave privada, en donde al menos un dispositivo de cómputo portátil es operativo para generar una firma digital en respuesta a la clave privada.

22. El aparato según la reivindicación 21, en donde el procesador de computador es operativo para enviar el documento electrónico a al menos un dispositivo de cómputo portátil, en donde al menos un dispositivo de cómputo portátil es además operativo para generar la firma digital en respuesta al documento electrónico.

23. El aparato según la reivindicación 21, en donde el procesador de computador es operativo para generar y enviar un hash direccional del documento electrónico a al menos un dispositivo de cómputo portátil, en donde al menos el dispositivo de cómputo portátil es operativo además para generar la firma digital en respuesta al hash unidireccional, en donde el procesador de computador es operativo para recibir la firma digital desde el dispositivo de cómputo portátil, en donde el procesador de computador es operativo para anexar la firma digital al documento electrónico.

24. El aparato según la reivindicación 3, en donde el procesador de computador es operativo para comunicarse con al menos un dispositivo de cómputo portátil, en donde el procesador de computador es operativo para recuperar la clave privada desde el dispositivo de cómputo portátil, en donde el procesador de computador es operativo para generar una firma digital en respuesta al documento electrónico y la clave privada.

25. El aparato según la reivindicación 3, en donde el cajero automático además incluye un lector de tarjetas inteligentes en conexión operativa con el procesador de computador, en donde el procesador de computador es operativo para comunicarse con al menos una tarjeta inteligente a través del lector de tarjetas, en donde la clave privada es

almacenada sobre la tarjeta inteligente, en donde la tarjeta inteligente es operativa para generar una firma digital en respuesta a la clave privada.

26. El aparato según la reivindicación 25, en donde el procesador de computador es operativo para enviar el documento electrónico hacia la tarjeta inteligente, en donde la tarjeta inteligente es además operativa para generar la firma digital en respuesta al documento electrónico.

27. El aparato según la reivindicación 25, en donde el procesador de computador es operativo para generar y enviar una elección unidireccional del documento electrónico a la tarjeta inteligente, en donde la tarjeta inteligente es además operativa para generar la firma digital en respuesta al hash unidireccional, en donde el procesador de computador es operativo para recibir la firma digital desde la tarjeta inteligente, en donde el procesador de computador es operativo para anexar la firma digital al documento electrónico.

28. El aparato según la reivindicación 3, en donde cajero automático además incluye un lector de tarjetas inteligentes en conexión operativa con el procesador de computador, en donde el procesador de computador es operativo para comunicarse con al menos una tarjeta inteligente a través del lector de tarjetas inteligentes, en donde la clave privada es almacenada sobre la tarjeta inteligente, en donde el procesador de computador es operativo para recuperar la clave privada desde la tarjeta inteligente, en donde el procesador de computador es operativo para generar una firma digital en respuesta al documento electrónico y la clave privada.

29. Una máquina automática de transacciones que comprende:

Al menos un procesador de computador;

al menos un dispositivo de pantalla en conexión operativa con el procesador de computador, en donde el procesador de computador es operativo para sacar una

Fcorat

140
representación visual de un documento electrónico a través del dispositivo de pantalla;

5 un lector de tarjetas en conexión operativa con el procesador de computador, en donde el procesador de computador es operativo para ser que el lector de tarjetas lea indicios correspondientes a al menos un número de cuenta desde una tarjeta; y

10 al menos un dispositivo de entrada en conexión operativa con el procesador de computador, en donde el procesador de computador es operativo para sacar un mensaje a través del dispositivo de pantalla el cual solicita al usuario proporcionar una entrada de confirmación a través de al menos un dispositivo de entrada la cual es representativa de una confirmación que una firma digital del documento electrónico pretende ser una firma legalmente valedera, en donde el procesador de computador es operativo para hacer que el documento electrónico sea digitalmente
15 firmado con una clave privada asociada con el número de cuenta en respuesta a la entrada de confirmación.

20 30. El aparato según la reivindicación 29 que comprende además un tablero digitalizador de firmas en conexión operativa con el procesador de computador, en donde el procesador de computador es operativo para recibir al menos un escaneo de la firma escrita a mano a través del tablero digitalizador de firmas, en donde el procesador de computador es operativo para incluir el escaneo de la firma escrita a mano con el documento electrónico antes que el documento electrónico es firmado digitalmente.

25 31. El aparato según la reivindicación 29, que comprende además un dispensador de efectivo en conexión operativa con el procesador de computador, en donde el procesador de computador es operativo para hacer que el dispensador de efectivo dispense efectivo en respuesta a al menos una entrada adicional recibida a través de menos un dispositivo entrada.
30

147

32. El aparato según la reivindicación 29, en donde el procesador de computador es operativo para acceder al menos una cuenta de depósito seguro digital localizada remotamente a la máquina automática de transacciones, en donde la clave privada es almacenada en asociación con la cuenta de depósito seguro digital, en donde el número de cuenta es asociado con la cuenta de depósito seguro digital.

33. El aparato según la reivindicación 32, en donde el procesador de computador es operativo para acceder al menos un servidor de almacenamiento, en donde al menos un servidor de almacenamiento está en conexión operativa con al menos un almacenamiento de datos, en donde al menos un almacenamiento de datos incluye la clave privada almacenada en asociación con la cuenta de depósito seguro digital.

34. El aparato según la reivindicación 33, en donde el procesador de computador es operativo para hacer que el servidor de almacenamiento almacene el documento electrónico en al menos un almacenamiento de datos en asociación con la cuenta de depósito seguro digital.

35. El aparato según la reivindicación 29, en donde el número de cuenta incluye un número de cuenta bancaria asociado con una cuenta bancaria.

36. El aparato según la reivindicación 35, en donde el procesador de computador es operativo para comunicar el número de cuenta bancaria a al menos un servidor remoto, en donde el servidor remoto es operativo para acceder la clave privada en respuesta al número de cuenta bancaria.

37. El aparato según la reivindicación 36, en donde el procesador de computador es operativo para hacer que servidor remoto produzca una firma digital para el documento electrónico en respuesta a la clave privada, en donde el procesador de computador es operativo para recibir la firma digital desde el servidor remoto y para anexar la firma digital al documento electrónico.

38. El aparato según la reivindicación 37, en donde el procesador de computador es operativo para anexar un certificado digital al documento electrónico, en donde el certificado digital incluye la clave pública que es operativa para validar la firma digital.

5

39. El aparato según la reivindicación 29, en donde el procesador de computador es operativo para hacer que la clave privada y una clave pública correspondiente sean producidas, en donde el procesador de computador está en comunicación operativa con autoridades certificadoras, en donde el procesador de computador es operativo para hacer que la autoridad certificadora genere un certificado digital que incluye la clave pública.

10

40. El aparato según la reivindicación 39, en donde el procesador de computador es operativo para anexar el certificado digital al documento electrónico.

41. El aparato según la reivindicación 40, en donde el procesador de computador es operativo para hacer la clave privada y el certificado digital sean almacenados en asociación con la cuenta de depósito seguro digital.

15

42. El aparato según la reivindicación 41, en donde el procesador de computador es operativo para hacer un servidor remoto establezca la cuenta de depósito seguro digital.

20

43. El aparato según la reivindicación 42, en donde el procesador de computador es operativo para hacer que el servidor remoto asocie la cuenta de depósito seguro digital con una cuenta bancaria asociada con el número de cuenta.

25

44. El aparato según la reivindicación 29, en donde el procesador de computador es operativo para hacer que la clave privada sea producida, en donde el procesador de computador es operativo para hacer que la clave privada sea remotamente almacenada en asociación con el número de cuenta.

30

45. El aparato según la reivindicación 44, en donde el número de cuento corresponde a un número de cuenta bancaria.

5 46. El aparato según la reivindicación 29, en donde el procesador de computador es operativo para comunicarse con un sistema de procesamiento de transacciones financieras, en donde el procesador de computador es operativo para hacer que el documento electrónico sea digitalmente firmado en respuesta a comunicación con el sistema de procesamiento de transacciones financieras.

10 47. El aparato según la reivindicación 29, en donde el procesador de computador es operativo para hacer que el documento electrónico sea digitalmente firmado con una clave privada adicional.

15 48. El aparato según la reivindicación 47, en donde la clave privada adicional es asociada con un notario público.

49. El aparato según la reivindicación 29, en donde el procesador de computador es operativo para hacer que el documento electrónico sea sellado digitalmente con fecha y hora.

20 50. El aparato según la reivindicación 29, en donde antes de hacer que el documento electrónico sea digitalmente firmado, el procesador de computador es operativo para modificar el documento electrónico en respuesta a al menos una entrada adicional a través de al menos un dispositivo de entrada.

25 51. Un método que comprende:

- a) accesar un documento electrónico con un cajero automático;
- b) presentar el documento electrónico a través de una pantalla del cajero automático;
- c) solicitar al usuario el suministro de al menos una primera entrada
representativa de una confirmación que una firma digital para el

30

Ad que para fue
Sec-cla to
Proc-1
1/15/10
(e)

144
~~144~~

documento electrónico pretende corresponder a una firma legalmente valedera;

- d) recibir al menos una primera entrada a través de al menos un dispositivo de entrada del cajero automático;
- e) producir la firma digital para el documento electrónico en respuesta a al menos una primera entrada; y
- f) anexar la firma digital al documento electrónico.

52. El método según la reivindicación 51, en donde después del paso (b) además comprende:

- g) capturar un escaneo de una firma escrita mano a través de un tablero digitalizador de firmas del cajero automático; y
- h) anexar el escaneo de la firma escrita a mano al documento electrónico.

53. El método según la reivindicación 51, en donde además comprende:

g) recepción de al menos una segunda entrada a través de al menos un dispositivo de entrada;

h) hacer que el dispensador de efectivo del cajero automático dispense efectivo en respuesta a al menos una segunda entrada.

54. El método según la reivindicación 51, en donde antes del paso (e) además comprende:

g) leer un número de cuenta bancaria desde una tarjeta a través de operación de un lector de tarjetas del cajero automático;

h) hacer que una clave privada asociada con el número de cuenta bancaria sea accedida desde un servidor remoto; y

en donde en el paso (e) la firma digital es generada en respuesta a la clave privada asociada con el número de cuenta bancaria.

55. El método según la reivindicación 51, que comprende además:

g) producir un sello digital de fecha y hora para el documento electrónico; y

5 h) anexar el sello digital de fecha y hora al documento electrónico.

56. Medios legibles de computador que llevan instrucciones las cuales son operativas para hacer que al menos un computador en el cajero automático haga que el cajero automático realice los pasos del método citado en la reivindicación 51.

no se admite

10

57. Un método que comprende:

vide pte. para pte.

a) leer un número de cuenta bancaria desde una tarjeta a través de operación de un dispositivo lector de tarjetas;

dec-19
pr-10
15e)

15

b) enviar el número de la cuenta bancaria leído desde la tarjeta hacia un servidor asociado con una red de firmas digitales, en donde el servidor es operativo para hacer que una clave privada almacenada en asociación con una cuenta bancaria sea accedida en respuesta a correlación entre el número de cuenta bancaria leído de la tarjeta y la cuenta bancaria; y

20

c) hacer que el documento electrónico sea digitalmente firmado en respuesta a la clave privada asociada con la cuenta bancaria.

58. El método según la reivindicación 57, que comprende además:

25

d) acceder una cuenta de depósito seguro digital que corresponde al número de la cuenta bancaria; y

e) hacer que el documento electrónico sea almacenado en almacenamiento de datos remoto en asociación con la cuenta de depósito seguro digital.

30

↑

59. El método según la reivindicación 57, que comprende además:

d) recibir el documento electrónico desde el almacenamiento de datos remoto; y

e) enviar el documento electrónico hacia una ubicación de almacenamiento externo diferente al almacenamiento de datos remoto.

60. El método según la reivindicación 57, en donde antes del paso (c) además comprende:

d) sacar una representación visual del documento electrónico a través de un dispositivo de pantalla de una máquina automática de transacciones incluyendo un dispensador de efectivo, en donde la máquina automática de transacciones incluye el dispositivo lector de tarjetas.

61. El método según la reivindicación 60, en donde antes del paso (c) además comprende:

e) permitir al usuario modificar el contenido del documento electrónico a través de al menos una entrada a al menos un dispositivo de entrada de la máquina automática transacciones.

62. El método según la reivindicación 60, en donde antes del paso (c) además comprende:

e) capturar un escaneo de una firma escrita a mano a través de un tablero digitalizador de firmas de una máquina automática transacciones; y

f) a anexar el escaneo de la firma escrita a mano al documento electrónico.

63. El método según la reivindicación 57, en donde antes del paso una (c) además comprende:

e) solicitar al usuario proporcionar al menos una entrada representativa de una confirmación que la firma digital pretende corresponder a una firma legalmente valedera; y
en donde el paso (c) es realizado en respuesta a la recepción de al menos una entrada.

5

64. El método según la reivindicación 63, en donde después del paso (e) además comprende:

10

f) recibir al menos una entrada a través de al menos un dispositivo de entrada de una máquina automática de transacciones, en donde la máquina automática transacciones incluye un dispositivo lector de tarjetas; y

g) hacer que un registro de al menos una entrada sea almacenado en asociación con el número de cuenta bancaria.

15

65. El método según la reivindicación 57, en donde en el paso (a) el número de cuenta bancaria corresponde a un número de tarjeta de crédito.

66. El método según la reivindicación 57, en donde antes del paso (c) además comprende:

20

d) recibir al menos una entrada a través de al menos un dispositivo de entrada de una máquina automática de transacciones, en donde la máquina automática de transacciones incluye el dispositivo lector de tarjetas; y

25

e) enviar al servidor asociado con la red de firmas digitales la información correspondiente a la entrada recibida, en donde el servidor es operativo para hacer que el acceso a la clave privada sea permitido en respuesta a una determinación que la entrada recibida corresponde a la contraseña asociada con la clave privada.

448

67. El método según la reivindicación 66, en donde en el paso (d) al menos una entrada corresponde a datos biométricos recibidos a través de un dispositivo de lectura biométrica de la máquina automática transacciones.

5 68. El método según la reivindicación 66, en donde en el paso (d) al menos una entrada corresponde a un PIN de una cuenta bancaria, en donde el PIN es ingresado a través de un teclado de la máquina automática de transacciones.

69. El método según la reivindicación 57, que además comprende:

10

d) hacer que el documento electrónico sea sellado digitalmente con fecha y hora.

70. Medios legibles de computador que llevan instrucciones las cuales son operativas para hacer que al menos un computador en la máquina automática de transacciones haga que la

15 máquina automática de transacciones realice los pasos del método citados en la reivindicación 57.

71. Un método que comprende:

20

a) accesar un documento electrónico con una máquina automática de transacciones;

b) hacer que han certificado digital se ha producido, en donde el certificado digital incluye información asociada con la identidad de usuario de la máquina automática transacciones, en donde el certificado digital incluye una clave pública que

25 corresponde a una clave privada;

c) Desplegar una representación visual del documento electrónico a través de una pantalla de la máquina automática de transacciones;

Se-cia
m-cto
15 el
f)

149
~~149~~

d) Solicitar al usuario proporcionar al menos una entrada representativa de una confirmación que una firma digital para el documento electrónico pretende corresponder a una firma legalmente valedera;

5 e) Recibir al menos una entrada a través de al menos un dispositivo de entrada de la máquina automática de transacciones;

f) Hacer que la firma digital para el documento electrónico sea producida en respuesta a la entrada y la clave privada; y

10

g) Hacer que la firma digital y el certificado digital sean anexados al documento electrónico.

72. El método según la reivindicación 71, en donde antes del paso (b) además comprende:

15

h) recuperar al menos una parte de la información asociada con la identidad del usuario desde el documento electrónico.

73. El método según la reivindicación 72, que además comprende:

20

h) hacer que una cuenta de depósito seguro digital sea establecida para el usuario en un almacenamiento de datos remoto, incluyendo almacenamiento del certificado digital y la clave privada en asociación con la cuenta de depósito seguro digital.

25

74. El método según la reivindicación 73, que comprende además:

i) hacer que una copia firmada digitalmente del documento electrónico sea almacenada en asociación con la cuenta de depósito seguro digital.

150

75. El método según la reivindicación 71, en donde en el paso (a) el documento electrónico es accedido desde una ubicación de almacenamiento accesible por red.

5

76. El método según la reivindicación 71, que además comprende:

h) enviar una copia digitalmente firmada del documento electrónico a una ubicación de almacenamiento accesible por red.

10

77. El método según la reivindicación 71, que comprende además:

h) enviar una copia digitalmente firmada del documento electrónico a una dirección de red especificada por el documento electrónico.

15

78. El método según la reivindicación 71, que comprende además:

g) enviar una copia digitalmente firmada del documento electrónico a una dirección de red especificada por la máquina automática transacciones.

20

79. El método según la reivindicación 71, que comprende además:

h) hacer que un cargo de procesamiento de firmas digitales sea cobrado a una cuenta especificada en el documento electrónico a través de comunicación con el sistema de procesamiento de transacciones financieras.

25

80. El método según la reivindicación 71, que comprende además:

h) hacer que un cargo de procesamiento de firmas digitales sea cobrado a una cuenta especificada por la máquina automática transacciones a través de comunicación con un sistema de procesamiento de transacciones financieras.

30

15/ ~~15/~~
81. El método según la reivindicación 71, que comprende además:

h) hacer que un sello digital de fecha y hora sea creada para el documento electrónico; y

5 i) hacer que el sello digital de fecha y hora sea anexada al documento electrónico.

82. El método según la reivindicación 71, en donde la máquina automática de transacciones incluye un dispensador de efectivo.

10 83. Medios legibles de computador con instrucciones que son operativas para hacer que al menos un computador en la máquina automática transacciones haga que la máquina automática transacciones realice los pasos del método citado en la reivindicación 71.

84. Un aparato que comprende:

15

al menos un procesador de computador; y

20

Al menos un almacenamiento de datos en conexión operativa con el procesador de computador, en donde el almacenamiento de datos incluye una pluralidad de cuentas de depósito seguro digital almacenadas en el mismo, en donde cada una de las cuentas de depósito seguro digital está asociada con al menos una clave privada, en donde el procesador de computador es operativo para comunicarse con una pluralidad de cajeros automáticos, en donde el procesador de computador es operativo en respuesta al menos uno de los cajeros automáticos para hacer que una firma digital sea producida para un documento electrónico en respuesta a la clave privada asociada con una de las cuentas de depósito seguro digital.

25

85. El aparato según la reivindicación 84 en donde el procesador de computador es operativo para recibir el documento electrónico desde al menos un cajero automático, en

no
de
modo
red. A.
en
fórmulas
uso

donde el procesador de computador es operativo para almacenar el documento electrónico en el almacenamiento de datos en asociación con una cuenta de depósito seguro digital.

5 86. El aparato según la reivindicación 85 en donde el procesador de computador es operativo para recuperar el documento electrónico desde el almacenamiento de datos y enviar el documento electrónico hacia uno de la pluralidad de cajeros automáticos.

10 87. El aparato según la reivindicación 85 en donde el procesador de computador es operativo para encriptar y desencriptar el documento electrónico almacenado en al menos un almacenamiento de datos en respuesta a una clave privada recibida desde al menos un cajero automático.

15 88. El aparato según la reivindicación 84 en donde cada cuenta de depósito seguro digital está asociada con el número de cuenta bancaria, en donde el procesador de computador es operativo para acceder la clave privada asociada con una cuenta de depósito seguro digital en respuesta a un mensaje recibido desde al menos un cajero automático el cual incluye un número de cuenta bancaria que corresponde al número de cuenta bancaria asociado con la cuenta depósito seguro digital.

20 89. El aparato según la reivindicación 88, en donde al menos un número de cuenta bancaria corresponde a un número de tarjeta de crédito.

25 90. El aparato según la reivindicación 84 en donde cada cuenta de depósito seguro digital está asociada con al menos un certificado digital, en donde el procesador de computador es operativo para hacer que la firma digital y al menos uno de los certificados digitales asociados con la cuenta de depósito seguro digital sean anexados al documento electrónico.

30 91. El aparato según la reivindicación 84 en donde el procesador de computador es operativo para mantener y almacenar en al menos un almacenamiento de datos, un registro de acceso en asociación con cada cuenta de depósito seguro digital.

92. El aparato según la reivindicación 84 en donde al menos un cajero automático incluye un dispensador de efectivo, en donde el procesador de computador es operativo a través de comunicación como el sistema de procesamiento de transacciones financieras para hacer
5 que una dispensación de efectivo desde el dispensador de efectivo sea autorizada.

93. El aparato según la reivindicación 84 en donde el procesador de computador es operativo para hacer que una nueva cuenta de depósito seguro digital sea creada en el almacenamiento de datos en respuesta a comunicación desde al menos un cajero
10 automático.

94. El aparato según la reivindicación 93 en donde el procesador de computador es operativo para hacer que una nueva clave privada y una clave pública correspondiente sean producidas en respuesta a comunicación desde al menos un cajero automático, en donde el
15 procesador de computador es operativo para almacenar la clave privada en asociación con la nueva cuenta de depósito seguro digital.

95. El aparato según la reivindicación 94 en donde el procesador de computador es operativo para hacer que un certificado digital sea generado y almacenado en asociación
20 con la nueva cuenta de depósito seguro digital, en donde el certificado digital incluye la clave pública.

96. El aparato según la reivindicación 95 en donde el procesador de computador es operativo para recibir un número de cuenta bancaria desde al menos un cajero automático,
25 en donde el procesador de computador es operativo para almacenar el número de cuenta bancaria en asociación con la nueva cuenta de depósito seguro digital.

97. El aparato según la reivindicación 96 en donde el procesador de computador es operativo para recibir una entrada de contraseña desde al menos un cajero automático, en

154
donde el procesador de computador es operativo para almacenar la entrada de contraseña en asociación con la nueva cuenta de depósito seguro digital.

5 98. El documento según la reivindicación 84 en donde el procesador de computador es operativo para recibir un hash unidireccional del documento electrónico desde al menos un cajero automático, en donde el procesador de computador es operativo para hacer que la firma digital sea generada en respuesta al hash unidireccional y la clave privada.

10 99. El aparato según la reivindicación 84 en donde el procesador de computador es operativo para hacer que una segunda firma digital sea producida para el documento electrónico en respuesta a la clave privada que no está asociada con una cuenta de depósito seguro digital.

15 100. El aparato según la reivindicación 84 en donde el procesador de computador es operativo para hacer que un cargo de procesamiento de firma digital sea cobrado a una cuenta bancaria en respuesta a la generación de una firma digital para el documento electrónico.

20 101. El aparato según la reivindicación 100 en donde el procesador de computador es operativo para recibir información acerca de la cuenta bancaria desde al menos un cajero automático.

25 102. El aparato según la reivindicación 84 en donde el procesador de computador es operativo para hacer que un sello digital de fecha y hora sea producida y anexada al documento electrónico.

30 103. Un método que comprende:

- a) recibir un número de cuenta bancaria desde una máquina automática de transacciones;

ser-cep
prod-to
1rel, f1

155
~~155~~

b) acceder una clave privada asociada con el número de cuenta bancaria; y

c) Permitir que un documento electrónico presentado por pantalla por la máquina automática transacciones sea digitalmente firmado con la clave privada.

5

104. El método según la reivindicación 103, en donde antes del paso (c) además comprende:

d) recibir una contraseña desde la máquina automática transacciones; y

10

e) verificar que la contraseña corresponde a una contraseña válida anteriormente asociada con el número de cuenta bancaria.

105. El método según la reivindicación 103, que comprende además:

15

d) acceder un certificado digital anteriormente asociado con el número de cuenta bancaria, en donde el certificado digital incluye una clave pública que corresponde a la clave privada, en donde la clave pública puede ser utilizada para validar la firma digital; y

20

e) permitir que el certificado digital sea asociado con el documento electrónico.

106. El método según la reivindicación 103, que además comprende:

25

d) almacenar en una copia digitalmente firmada del documento electrónico en una cuenta de depósito seguro digital en asociación con el número de cuenta bancaria.

107. El método según la reivindicación 103, que comprende además:

d) recibir un segundo número de cuenta bancaria desde la máquina automática de transacciones; y

5 e) cobrar un cargo de procesamiento asociado con la firma digital del documento electrónico a una cuenta bancaria asociada con un segundo número de cuenta bancaria.

108. El método según la reivindicación 103, que comprende además:

10 d) permitir que el documento electrónico sea sellado digitalmente con fecha y hora.

109. El método según la reivindicación 103, que además comprende:

d) dispensación de efectivo desde la máquina automática de transacciones.

15 110. Un método que comprende:

20 a) recibir una solicitud de la máquina automática de transacciones para firmar digitalmente un archivo electrónico visualmente presentado en pantalla por la máquina automática transacciones, en donde la solicitud incluye un número de cuenta que está asociado con una cuenta de depósito seguro digital;

b) acceder una clave privada asociada con la cuenta de depósito seguro digital en respuesta al número de cuenta; y

25 c) Producir una firma digital por el documento electrónico en respuesta de la clave privada; y

d) Hacer que la firma digital sea anexada al documento electrónico

30 111. El método según la reivindicación 110, que además comprende:

De acuerdo con
Se - cio
pro. Jo
15 el, 11

457
~~1110~~

- e) almacenar una copia digitalmente firmada del documento electrónico en un almacenamiento de datos en asociación con la cuenta de depósito seguro digital.

5 112. El método según la reivindicación 110, en donde en el paso (a) el número de cuenta corresponde a un número de cuenta bancaria.

113. El método según la reivindicación 110 y que además comprende:

- f) dispensar efectivo desde la máquina automática transacciones.

10

114. Un método que comprende:

- a) recibir una solicitud en un cajero automático para firmar digitalmente un documento electrónico visualmente presentado por cajero automático;
- 15 b) hacer que una firma digital y un sello digital de fecha y hora sean producidas para el documento electrónico; y
- c) Hacer que la firma digital y el sello digital de fecha y hora sean anexadas al
20 documento electrónico.

115. El método según la reivindicación 114 y que además comprende:

- d) dispensar efectivo desde el cajero automático.

25

116. Un método que comprende:

- a) producir una pluralidad de certificados digitales para una pluralidad de clientes individuales, en donde cada cliente individual está asociado con una cuenta;

30

158

- b) asociar las cuentas de los clientes individuales con los correspondientes certificados digitales de los clientes individuales;
- 5 c) producir al menos una tarjeta para cada cliente individual, en donde la tarjeta incluye un primer indicio visible sobre la misma el cual corresponde a una marca indicadora de fuente para un servicio de firmas digitales, en donde cada tarjeta incluye datos legibles de máquina que corresponden a un número de cuenta asociado con la cuenta del cliente individual;
- 10 d) enviar las tarjetas a los clientes individuales; y
- e) permitir a cada cliente individual firmar digitalmente un documento electrónico utilizando una de una pluralidad de máquinas automáticas de transacciones y una de las tarjetas, en donde cada máquina automática de transacciones es operativa para sacar por pantalla una representación visual del documento electrónico a través de un dispositivo de pantalla de la máquina automática de transacciones, en donde cada máquina automática de transacciones es operativa para hacer que el documento electrónico sea digitalmente firmado a través de comunicación con el servicio de firmas digitales, en donde la comunicación incluye el número de cuenta leído desde la tarjeta por la máquina automática de transacciones.
- 15
- 20

117. El método según la reivindicación 116,
en donde en el paso (e) cada una de las máquinas incluye un segundo indicio visible el cual corresponde a una marca indicadora de fuente para el servicio de firmas digitales.

25 118. El método según la reivindicación 117,
en donde en el paso (e) el segundo indicio es sacado en pantalla adyacente a la cara frontal del cajero automático en donde el primer indicio y el segundo indicio son visualmente similares.

159
~~159~~

119. El método según la reivindicación 116, en donde en el paso (a) cada certificado digital incluye una clave pública que corresponde a una clave privada, en donde en el paso (c) el servicio de firmas digitales es operativo para hacer que el documento electrónico sea digitalmente firmado en respuesta a la clave privada que corresponde a la clave pública del certificado digital el cual está asociado con la cuenta del cliente individual que utiliza la máquina.

120. En el método según la reivindicación 116, en donde en el paso (e) el servicio de firmas digitales es operativo para acceder una clave privada asociada con el número de cuenta leído desde la tarjeta, en donde el servicio de firmas digitales es operativo para hacer que el documento electrónico sea digitalmente firmado en respuesta a la clave privada.

121. El método según la reivindicación 116, en donde en el paso (c) las tarjetas corresponden a tarjetas de cuentas bancarias, en donde las cuentas corresponden a cuentas bancarias.

122. El método según la reivindicación 121, en donde en el paso (e) las máquinas automáticas de transacciones son operativas para hacer que los cargos de procesamiento sean cobrados por la firma digital de documentos electrónicos, y que además comprende:

- e) permitir que la entidad y que maneja las cuentas bancarias para los clientes individuales reciba al menos una parte de los cargos de procesamiento.

123. El método según la reivindicación 116, en donde en el paso (e) las máquinas automáticas de transacciones incluyen tableros digitalizadores de firmas, en donde las máquinas automáticas de transacciones son operativas para incluir datos de firmas escritas a mano capturadas con los tableros digitalizadores de firmas en los documentos electrónicos.

124. El método según la reivindicación 116, en donde al menos algunas de las máquinas automáticas de transacciones incluyen dispensadores de efectivo, en donde las máquinas

160 160

automáticas de transacciones que incluyen dispensadores de efectivo son además operativas para dispensar efectivo.

5 125. El método según la reivindicación 124, en donde en el paso (c) las tarjetas corresponden a tarjetas bancarias, en donde las cuentas corresponden a cuentas bancarias, y en donde las máquinas automáticas de transacciones incluyen dispensadores de efectivo, y en donde las máquinas automáticas de transacciones son además operativas para dispensar efectivo retirado de las cuentas bancarias.

10 126. El método según la reivindicación 116, en donde en el paso (a) la cuentas corresponden a cuentas de deposito seguro digital, en donde en el paso (c) las tarjetas corresponden a las tarjetas de cuentas de deposito seguro digital.

RESUMEN

Una máquina automática de transacciones como un cajero automático (ATM) (10) es suministrado. El ATM es operativo para digitalmente firmar documentos electrónicos (42). El ATM puede estar en conexión operativa con un servidor de almacenamiento (32). El servidor de almacenamiento responde operativamente al ATM para mantener documentos electrónicos (42) en un almacén de datos (34) en asocio con la cuenta de depósito (40) digitalmente segura y/o cuenta bancaria (48) tal como una cuenta corriente, de ahorros, débito, o de crédito. El servidor de almacenamiento adicionalmente es operativo para almacenar una clave privada (44) de un usuario es asocio con la cuenta de depósito /o bancaria digitalmente segura. El ATM es operativo para causar que documentos electrónicos sean firmados usando la clave privada asociada con el usuario. El ATM adicionalmente es operativo para dar salida al documento electrónico en un dispositivo de pantalla (18) del ATM donde le usuario podrá leer y editar el documento electrónico.

(19) World Intellectual Property Organization
International Bureau



162
162

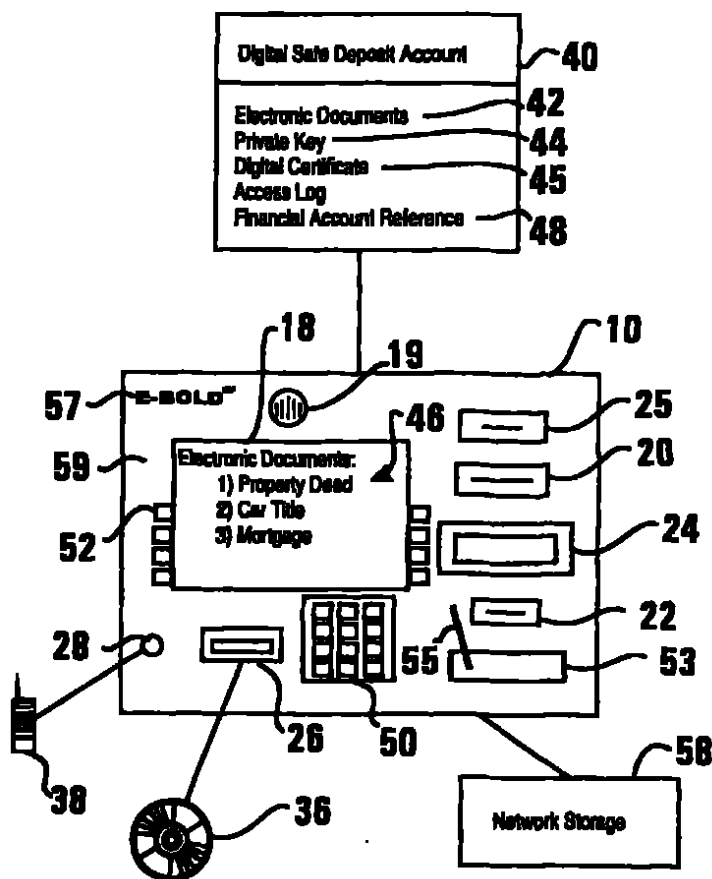
(43) International Publication Date
19 September 2002 (19.09.2002)

PCT

(10) International Publication Number
WO 02/073341 A3

- (51) International Patent Classification⁷: G06F 17/60 (74) Agent: JOCKE, Ralph E.; 231 South Broadway, Medina, OH 44256 (US).
- (21) International Application Number: PCT/US02/06826
- (22) International Filing Date: 6 March 2002 (06.03.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/273,996 7 March 2001 (07.03.2001) US
60/319,015 29 November 2001 (29.11.2001) US
- (31) Designated States (national): BR, CA, CN, CO, IN, MX, PL, RU, ZA.
- (34) Designated States (regional): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- (38) Published:
-- with international search report
- (71) Applicant: DIEBOLD, INCORPORATED [US/US]; 5995 Mayfair Road, North Canton, OH 44720 (US).
- (72) Inventors: PARMELEE, Christopher L.; 6140 Triple Crown Drive, Medina, OH 44256 (US). SMITH, Mark D.; 1910 Hunting Valley, NW, North Canton, OH 44720 (US).
- (88) Date of publication of the international search report: 10 April 2003
- For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: AUTOMATED TRANSACTION MACHINE: DIGITAL SIGNATURE SYSTEM AND METHOD



(57) Abstract: An automated transaction machine such as an ATM (10) is provided. The ATM is operative to digitally sign electronic documents (42). The ATM may be in operative connection with a storage server (32). The storage server is operative responsive to the ATM to maintain electronic documents (42) in a data store (34) in association with the user's digital safe deposit account (40) and/or a financial account (48) such as checking, savings, debt, or credit account. The storage server is further operative to store a private key (44) of a user in association with the user's digital safe deposit account and/or financial account. The ATM is operative to cause electronic documents to be signed using the private key associated with the user. The ATM is further operative to output the electronic document on a display device (18) of the ATM where the user may view and edit the electronic document.

WO 02/073341 A3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US02/06826

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G 06 F 17/60

US CL : 705/57

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/57

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,085,976 A (SEHR) 11 July 2000 (11.07.2000); column 1, line 5 to column 2, line 60.	1-24, 29-31, 35-40, 44-57, 59-72, 75-89, 91, 92, 98, 100-109, 112-125
Y	US 5,453,601 A (ROSEN) 26 september 1995 (26.09.1995). column 2 lines 16-23.	25-28
Y	US 5,920,640, A (SALA'TINO et al.) 06 July 1999 (06.07.1999); column 1, line 5 to column 4, line 50.	32-34, 41-43, 58, 73-74, 90, 93-97, 99, 110, 111, 126
Y	US 6,253,322 B1 (SUSAKI et al.) 26 June 2001 (26.06.2001) column 2, lines 27-41.	32-34, 41-43, 58, 73-74, 90, 93-97, 99, 110, 111, 126

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claims) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"A" document number of the same patent family

Date of the actual completion of the international search

29 September 2002 (29.09.2002)

Date of mailing of the international search report

30 DEC 2002

Name and mailing address of the ISA/US

Commissioner of Patents and Trademarks

Box PCT

Washington, D.C. 20231

Facsimile No. (703)305-3230

Authorized officer

James T. Hume

Telephone No. 703.305.3900

PATENT COOPERATION TREATY

INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:
RALPH E. JOCKE
231 SOUTH BROADWAY
MEDINA, OH 44256

PCT

**NOTIFICATION OF TRANSMITTAL OF
INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

(PCT Rule 71.1)

Date of Mailing
(day/month/year)

19 AUG 2003

Applicant's or agent's file reference

D-1154PCT

IMPORTANT NOTIFICATION

International application No.

International filing date (day/month/year)

Priority date (day/month/year)

PCT/US02/06826

06 March 2002 (06.03.2002)

07 March 2001 (07.03.2001)

Applicant

DIEBOLD, INCORPORATED

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the International preliminary examination report and its annexes, if any, established on the international application.
2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.
3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. REMINDER

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/US

Consolidated Patent and Trademark
Box PCT
Washington, D.C. 20531

Authorized officer

James F. Farnham

465
02/16/03

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference D-1154PCT	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/US02/06826	International filing date (day/month/year) 06 March 2002 (06.03.2002)	Priority date (day/month/year) 07 March 2001 (07.03.2001)
International Patent Classification (IPC) or national classification and IPC IPC(7): G 06 F 17/60 and US Cl.: 705/57		
Applicant DIBBOLD, INCORPORATED		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 3 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 3 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of report with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 07 March 2002 (07.03.2002) Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Tel. 1-800-595-6000	Date of completion of this report 17 March 2003 (17.03.2003) [Signature] Telephone No. 202 706 7000
--	--

166
0222

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/US02/06826

I. Basis of the report

1. With regard to the elements of the international application:*

- ☒ the international application as originally filed.
- ☒ the description:
 pages 1-45 as originally filed
 pages NONE, filed with the demand
 pages NONE, filed with the letter of _____
- ☒ the claims:
 pages 46-74, as originally filed
 pages NONE, as amended (together with any statement) under Article 19
 pages NONE, filed with the demand
 pages NONE, filed with the letter of _____
- ☒ the drawings:
 pages 1-11, as originally filed
 pages NONE, filed with the demand
 pages NONE, filed with the letter of _____
- ☐ the sequence listing part of the description:
 pages NONE, as originally filed
 pages NONE, filed with the demand
 pages NONE, filed with the letter of _____

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in printed form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages NONE
- ☐ the claims, Nos. NONE
- ☐ the drawings, sheets/fig NONE

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

The Examiner's attention is drawn to the fact that any amendments to the international application under Article 14 are referred to in the Supplemental Box. Any amendments to the international application must be referred to under item 1 and entered in this report.

167
[Signature]

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US02/06826

V. Reasoned statement under Rule 66.2(a)(II) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. STATEMENT

Novelty (N)	Claims 1-126	YES
	Claims NONE	NO
Inventive Step (IS)	Claims 1-126	YES
	Claims NONE	NO
Industrial Applicability (IA)	Claims 1-126	YES
	Claims NONE	NO

2. CITATIONS AND EXPLANATIONS

Claims 1-126 meet the criteria set out in PCT Article 33(2)-(3), because the prior art of record does not teach or fairly suggest a digitalizing signature pad.

NEW CITATIONS

168

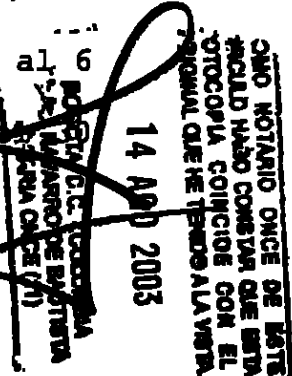
TRADUCCION OFICIAL No. 03-358

Efectuada el día 11 de agosto de 2003, de un documento escrito en Inglés, al cual para su identificación se le estampa el sello de María del Pilar Iglesias, Traductora e Intérprete Oficial según consta en la Resolución No. 819 del 15 de abril de 1971 expedida por el Ministerio de Justicia de la República de Colombia.

Autenticaciones notariales y subsiguientes correspondientes a un Poder otorgado por **Diebold, Incorporated** a **Carlos R. Iarte y/o Ana María Frieri**, documento éste que fue firmado por Warren W. Dettinger el 23 de julio de 2003, viene en Español y en él se explica que el objeto principal del mismo es tramitar, obtener y defender Patentes, Modelos de Utilidad y Diseños Industriales.

La firma y cargo de Warren W. Dettinger como Vicepresidente y Asesor General de Diebold Incorporated fueron debidamente certificados por el Notario Público Michael E. Lindroos según consta en la correspondiente Certificación Notarial expedida el 23 de julio de 2003 por el mencionado Notario, quien para ello tuvo a la vista la Escritura de Constitución y Estatutos de la Compañía actualizados al 28 de febrero de 1989; el Código de Reglamentaciones del Estado de Ohio modificado al 6 de abril de 1981; y la Resolución de Junta Directiva del 1 de enero de 1991.

M. P. Iglesias
María del Pilar Iglesias
TRADUCTORA E
INTERPRETE OFICIAL
Resolución No. 819 de 1971



169

APOSTILLA

(Convención de La Haya del 5 de octubre de 1961)

1. País: Estados Unidos de América

El presente documento público

2. Fue firmado por Michael E. Lindroos
3. Que actuó en su calidad de Notario Público de Ohio
4. Lleva el sello del Notario Público arriba citado

Se certificó:

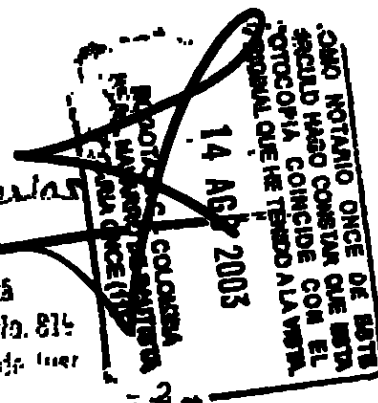
5. En Columbus, Ohio
6. El 31 de julio de 2003
7. Por parte del Secretario de Estado de Ohio
8. Bajo el Número 136082
9. Aparece el Sello de la Secretaría de Estado de Ohio
10. Firmado por J. Keneth Blackwell, Secretario de Estado

Este Certificado atestigua solamente la autenticidad de la firma del funcionario que firmó el documento, la capacidad en que actuó, y cuando sea apropiado, la autenticidad del sello estampado en el documento. Esta certificación no implica que el contenido del documento sea correcto o que cuente con la aprobación de este despacho.

Es traducción fiel y completa efectuada por:

María del Pilar Iglesias
María del Pilar Iglesias
C.C. 41.339.183 de Bogotá

María del Pilar Iglesias
María del Pilar Iglesias
C. C. 41.339.183 de Bogotá
Intérprete Oficial según Resolución No. 814
de 7 de Julio de 1971 del Poder Judicial de la Unión



OLARTE RAISBECK

LARTE RAISBECK & FRIERI, LTDA.
LEGAL & PROFESSIONAL SERVICES

WORLD TRADE CENTER — TORRE C
CALLE 100 No. 8A-55 Piso 10
BOGOTÁ, COLOMBIA
TELEPHONE +57-1 638-6200
FAX +57-1 638-6201

www.olarteraisbeck.com

Power of Attorney

The undersigned,

domiciled in

5995 Mayfair Road, North Canton, OH 44720 U.S.

by means of these presents hereby grants to **Carlos R. Olarte and/or Ana María Frieri** full and sufficient Power of Attorney to file, prosecute, obtain, defend and enforce any and all of the company's Patents, Utility Models and Industrial Designs in the Republic of Colombia, to which end it empowers them to take all steps necessary before any administrative or judicial authority of any class for the objects stated, to file petitions, appeals, replies and oppositions, pay taxes and annuities, request testimonies, receive documents and securities, abandon applications and collect refunds. Sufficient power is hereby granted to receive notifications on behalf of the Company, to confer powers on those who are to represent the company judicially and extrajudicially, to answer in court in the matter of all claims and demands that may be presented in connection with the objects stated, giving them likewise power to substitute these presents and revoke such substitutions.

El suscrito,

Diebold, Incorporated

domiciliado en

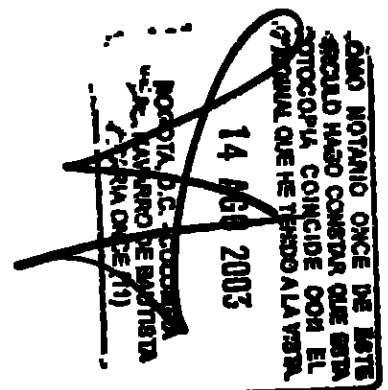
5995 Mayfair Road, North Canton, OH 44720 U.S.

por medio del presente otorga a **Carlos R. Olarte y/o Ana María Frieri** poder especial, amplio y suficiente para presentar, tramitar, obtener, defender y hacer respetar todas y cualquiera de Patentes, Modelos de Utilidad y Diseños Industriales de la compañía en la República de Colombia, a cuyo efecto los faculta para dar todos los pasos necesarios ante cualquier autoridad administrativa o judicial de cualquier jerarquía para cumplir con lo encomendado, elevar solicitudes, apelaciones, respuestas y oposiciones, pagar impuestos y anualidades, solicitar testimonios, recibir documentos y valores, desistir y percibir. Se concede poder bastante para recibir notificaciones a nombre de la compañía, otorgar poderes a quienes vayan a representar a la compañía judicial y extrajudicialmente, responder en juicio a todas las reclamaciones o demandas que por motivo de lo encomendado se presentaren, dándoles asimismo facultad para sustituir el presente y revocar dichas sustituciones.

Signature/Firma:

Date/Fecha: July 23, 2003

City/Country/Ciudad,País: North Canton, U.S.



OLARTE RAISBECK

OLARTE RAISBECK & FRIERI, LTDA.
LEGAL & PROFESSIONAL SERVICES

WORLD TRADE CENTER — TORRE C
CALLE 100 No. 8A-55 PISO 10
BOGOTÁ, COLOMBIA
TELEPHONE: +57-1 638-6200
FAX: +57-1 638-6201

www.olarteraisbeck.com

Notarial Certification

On this date,

July 23, 2003

The undersigned Notary Public certifies:

1. That

Warren W. Dettinger

of legal age and domiciled in

5237 Birkdale Street NW, Canton, OH 44708. USA

Signed the foregoing document.

2. That the grantor has executed the foregoing document as V.P. and General Counsel of Diebold, Incorporated.

3. That Diebold, Incorporated, having its principal place of business located in 5995 Mayfair Road, North Canton, OH 44720 U.S.

is duly incorporated, is currently in existence, and that the purposes for which the Power of Attorney is granted are within the scope of its corporate purposes.

4. That the grantor has the authority to execute the Power of Attorney and that his/her representation is legal.

5. The foundation for my certifications contained in points 2, 3 and 4 was the exhibition of the following authentic document(s):

Amended and Restated Articles of Incorporation dated February 28, 1989; State of Ohio and Amended Code of Regulations dated April 6, 1981, State of Ohio; and Resolution of Board of Directors dated January 30, 1991.

Certificación Notarial

En esta fecha,

el Notario Público suscrito certifica:

1. Que

mayor de edad y domiciliado

suscribió el documento que antecede.

2. Que el otorgante ha suscrito el referido documento en su carácter de de

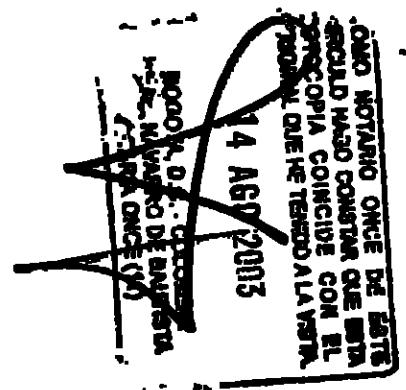
4. Que

con sede principal ubicada en

está legalmente constituida, que tiene existencia legal vigente y que los propósitos para los cuales se otorga el poder se encuentra dentro de los que comprenden su objeto social.

4. Que el otorgante tiene la representación para suscribir el poder, y que ésta es legítima.

5. El fundamento de mis certificaciones contenidas en los puntos 2, 3 y 4 fue la exhibición de los (del) siguiente(s) documento(s) auténtico(s):



APOSTILLE

(Convention de la Haye du 5 octobre 1961)

1. Country: United States of America

This public document

2. has been signed by MICHAEL E. LINDROOS
3. acting in the capacity of Attorney at Law, Notary Public, State of Ohio
4. bears the seal/stamp of Notary Public, State of Ohio

CERTIFIED

5. at Columbus, Ohio
6. July 31, 2003
7. by the Secretary of State of Ohio.
8. No. 136082
9. Seal/Stamp:

10. Signature:



J. Kenneth Blackwell
J. Kenneth Blackwell
Secretary of State of Ohio

This certification certifies only the authenticity of the signature of the official who signed the document, the capacity in which that official acted, and where appropriate, the identity of the seal or stamp which the document bears. This certification does not imply that the contents of the document(s) are correct, nor that they have the approval of this office.

14 AGO 2003
OF DC - COLUMBIA
DE NOTARIES
ONCE (11)
ONCE NOTARIO ONCE DE ESTE
SEALADO NASO CONSTAR QUE ESTA
FOTOCOPIA CORRESPONDE COM-IL
ORIGINAL QUE SE TENDOS A LA VISTA

173

OLARTE RAISBECK

LARTE RAISBECK & FRIERI, LTDA.
LEGAL & PROFESSIONAL SERVICES

WORLD TRADE CENTER — TORRE C
CALLE 100 No. 8A-55 Piso 10
BOGOTA, COLOMBIA
TELEPHONE +57-1 638-6200
FAX +57-1 638-6201

www.olarteraisbeck.com

NOTARY PUBLIC (Signature):

County of Stark)

State of Ohio)

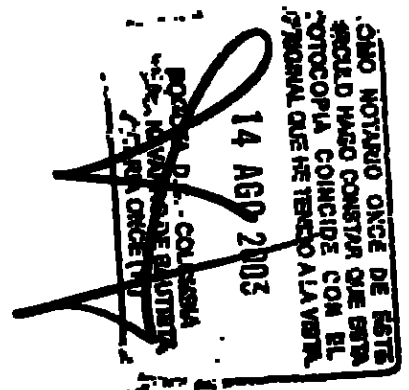
Michael E. Lindroos

Subscribed and sworn to before me this 23rd day of July, 2003

Michael E. Lindroos

Notary Public

MICHAEL E. LINDROOS
ATTORNEY-AT-LAW
NOTARY PUBLIC - STATE OF OHIO
MY COMMISSION HAS NO EXPIRATION DATE
SEC. 147.03 R.C.



174

Radicacion : 03077717 00000000
Fecha (AMB): 2003-09-05 15:23:06
Tramite : 011 PCT-PATENT 379 FASE INCI 411 PRESENTAC
Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

Folios: 172

NIT : 800176089-2

RECIBO OFICIAL DE CAJA : 03 - 61,687
FECHA : SEPTIEMBRE 1 DE 2003

***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PGO	Vr. PAGO
FREDERICK TORRES	CONSIGNACION	BANCO POPULAR	050-00110-6	14578066	29/08/2003	3,870,000.00

***** CONCEPTO *****

CANT. RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1 50005-01-01 SOLICITUDES	1 TRAMITES DE SOL. DE PATENTE DE IN	400,000.00
	TOTAL :	\$ 400,000.00

SON: CUATROCIENTOS MIL PESOS

RESPONSABLE : 

RECIBO DE CAJA APLICADO AL EXPEDIENTE No. _____

Radicacion : 03077717 00000000

Folios: 172

Fecha (MM): 2003-09-05 15:23:06

Tramite : 011 PCT-PATENT 379 FASE NACI 411 PRESENTAC

Dependencia: 2020 DIVISION DE NUEVAS CREACIONES

REQUISITOS NECESARIOS PARA PRESENTACION Y AGILIZACION DEL TRAMITE

	USUARIO	RADICADOR
PATENTE DE INVENCION ✓ MODELO DE UTILIDAD	()	()
- Indicación de que se solicita la concesión de una patente.	☒	()
- Datos de identificación del solicitante o de la persona que se presenta la solicitud.	☒	()
- Descripción de la invención.	☒	()
- Dibujos de ser estos pertinentes.	☒	()
- Comprobante de Pago de las tasas establecidas.		
COMPLETA () INCOMPLETA ()		
DISEÑO INDUSTRIAL ()		
- Indicación de que se solicita el registro de Diseño Industrial	()	()
- Datos de identificación del solicitante o de la persona que presenta la solicitud.	()	()
- Representación gráfica y fotográfica del Diseño Industrial o muestra del Material que incorpora el diseño.	()	()
- Comprobante de pago de las tasas establecidas	()	()
COMPLETA () INCOMPLETA ()		
ESQUEMA DE TRAZADO ()		
- Indicación de que solicita el registro de un Esquema de trazado.	()	()
- Datos de identificación del solicitante o de la persona que presenta La solicitud.	()	()
- Representación gráfica del esquema de trazado	()	()
- Comprobante de pago de las tasas establecidas.	()	()
COMPLETA () INCOMPLETA ()		

Firma Responsable:

Andrea Rosse

Fecha:



2020
Bogotá, D.C.,

Doctor:
CARLOS R. OLARTE
Apoderado
DIEBOLD INCORPORATED

Oficio N° **08442**

ASUNTO:	Radicación N°	03-77717
	Solicitud internacional	PCT/US2002/08826
	Fecha inicio fase nacional	07/10/2003
	Trámite	011
	Evento	379
	Actuación	430
	Folios	001

Como resultado del examen de forma, realizado con fundamento en el artículo 38 de la Decisión 486 de la Comisión de la Comunidad Andina, artículo 27 del Tratado de Cooperación en Materia de Patentes (PCT), regla 51 bis del Reglamento y Circular Única de la Superintendencia de Industria y Comercio, se le comunica que:

- ☐ La solicitud no contiene los dibujos. (Art. 26-d) Decisión 486 y numeral 5.2.5, capítulo quinto del título décimo de la Circular Única de la SIC).
- ☐ La solicitud no contiene la copia del documento en que consta la cesión del derecho a la patente del inventor al solicitante o a su causante. (Art. 26-k) Decisión 486).

En cumplimiento de lo dispuesto por el artículo 39 de la Decisión 486, se le requiere para que dentro del término de dos meses siguientes a la fecha de notificación del presente oficio, complete los requisitos anteriormente enunciados. En caso de no dar cumplimiento al presente requerimiento, la solicitud se considerará abandonada y perderá su prelación.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Única N° 10 de 2001.

ALIX CARMENZA CESPEDES DE VERGEL
Jefe de la División de Nuevas Creaciones.

El anterior requerimiento fue notificado por fijación en lista de fecha 10 OCT. 2003.