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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
07 September 2018 (07.09.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/158750 A1

(51) International Patent Classification:
G06F 21/44 (2013.01)

(21) International Application Number:
PCT/IB2018/051362

(22) International Filing Date:
03 March 2018 (03.03.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2017900748 03 March 2017 (03.03.2017) AU

(71) Applicant: **GOPC PTY LTD** [AU/AU]; 88 Havelock St, West Perth, Perth, Western Australia 6005 (AU).

(72) Inventors: **SPEAK, Graeme**; 88 Havelock Street, West Perth, Perth, Western Australia 6005 (AU). **RICHARDSON, Neil**; 8 Mills Street, Cannington, Perth, Western Australia 6107 (AU).

(74) Agent: **LAW, Adam**; 26 Glengariff Drive, Floreat, Perth, Western Australia 6014 (AU).

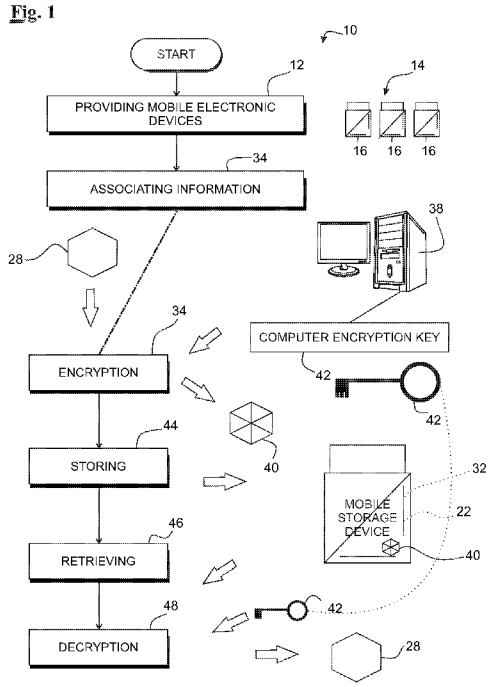
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,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

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

Published:
— *with international search report (Art. 21(3))*
— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

(54) Title: COMPUTING SYSTEMS AND METHODS

Fig. 1



(57) Abstract: In one preferred form of the present invention shown in in Figure 1 there is provided a computer implemented method 10. The method comprises : (A) providing at least one mobile electronics device, each device having a data store comprising a first area and a second area; the second area being distinct from the first area to assist with securing the first area; the first area being a system area and the second area for storing personal information; and (B) in connection with each mobile electronic device: associating personal information with computer identifying information to provide special personal information; storing the special personal information in the second area; and retrieving the personal information by: (i) reading the special personal information from the second area; and (ii) applying the computer identifying information to the special personal information.

WO 2018/158750 A1

COMPUTING SYSTEMS AND METHODS

INCORPORATION BY REFERENCE

[0001] The present application claims priority from Australian Provisional Application 2017900748 entitled 'COMPUTING SYSTEMS AND METHODS' filed 3 March 2017. All parts and elements of Australian Application 2017900748 are hereby fully incorporated by reference for all purposes.

FIELD OF THE INVENTION

[0002] The present invention concerns computing systems and methods. In one particularly preferred form of the present invention there is provided a security device for providing a secure financial interface allowing a user to access his or her bank account.

BACKGROUND TO THE INVENTION

[0003] For a user to access his or her online financial account, the user generally must connect through an HTML browser that is connected to the Internet. The user generally then must enter in a username and a password before the user is provided with access. Examples of financial accounts include bank accounts, asset portfolios, trust accounts, and so forth.

[0004] It is to be recognised that any discussion in the present specification is intended to explain the context of the present invention. It is not to be taken as an admission that the material discussed formed part of the prior art base or relevant general knowledge in any particular country or region.

[0005] It is against this background and the problems and difficulties associated therewith that the inventor has developed the present invention.

SUMMARY OF THE INVENTION

[0006] According to an aspect of embodiments herein described there is provide a computer implemented method comprising: (A) providing at least one mobile electronics device, each device having a data store comprising a first area and a second area; the second area being distinct from the first area to assist with securing the first area; the first area being a system area and the second area for storing personal information; and (B) in connection with each mobile electronic device: associating personal information with computer identifying information to provide special

personal information; storing the special personal information in the second area; and retrieving the personal information by: (i) reading the special personal information from the second area; and (ii) applying the computer identifying information to the special personal information.

[0007] In some embodiments, the first area comprises a locked down system area; the second area comprises an authentication area and the personal information comprises authentication data.

[0008] In some embodiments, in connection with each mobile electronic device: the first area comprises a read-only partition; and the second area comprises a read-write partition.

[0009] In some embodiments, the personal information comprises password, wallet or key data.

[0010] In some embodiments, the personal information comprises personal financial data.

[0011] In some embodiments, the personal information comprises a WIFI network password.

[0012] In some embodiments, each mobile electronic device comprises a dedicated storage device.

[0013] In some embodiments, the dedicated storage device comprises a USB thumb drive.

[0014] In some embodiments, the first area comprises a locked down system area; the second area comprises an authentication area; and the authentication area is no more than 10MB in size.

[0015] In some embodiments, the first area comprises a locked down system area; the second area comprises an authentication area; and the authentication area is no more than 5 MB in size.

[0016] In some embodiments, the first area comprises a locked down system area; the second area comprises an authentication area; and the authentication area is greater than 1MB in size.

[0017] In some embodiments, the first area comprises a locked down system area; the second area comprises an authentication area; and the operating system area is greater than 400MB in size.

[0018] In some embodiments, associating the personal information with the computer identifying information to provide the special personal information comprises encrypting the personal information using the computer identifying information as the encryption password.

[0019] In some embodiments, applying computer identifying information to the special personal information comprises decrypting the special authentication data using the computer identifying information.

[0020] In some embodiments, the personal information comprises a WIFI network password.

[0021] In some embodiments, the first area comprises a locked down operating system area; the second area comprises an authentication area; and the method includes, in connection with each mobile electronic device, booting a computer using the operating system area and, when the computer identifying information corresponds with the computer, automatically logging onto the associated WIFI network using the WIFI password.

[0022] In some embodiments, the first area comprises a locked down operating system area; the second area comprises an authentication area; the operating system area comprises a read-only partition and the authentication area comprises a read-write partition; associating the WIFI network password with the computer identifying information to provide the special authentication data comprises encrypting the WIFI network password using the computer identifying information as the password; and applying computer identifying information to the special authentication data comprises decrypting the special authentication data using the computer identifying information.

[0023] In some embodiments, the computer identifying information is unique to a corresponding host computer such that the personal information of each mobile device is locked to a particular host computer due to the computer identifying information.

[0024] In some embodiments, any changes to the first area are lost when the host computer is powered off or rebooted; and the personal information of the second area is persistent between reboots and power cycles of the host computer.

[0025] In some embodiments, the personal information is encrypted via the Advanced Encryption Standard (AES) with 128 or more bit encryption keys with a cypher block chaining mode of operation.

[0026] In some embodiments, the computer identifying information comprises a unique hardware identifier.

[0027] In some embodiments, the unique hardware identifier comprises a CPU serial number or network MAC address associated with a corresponding computer.

[0028] In some embodiments, the personal information comprises an electronic wallet.

[0029] In some embodiments, the personal information comprises a block-chain private key.

[0030] In some embodiments, the personal information comprises a block-chain private key for electronic currency.

[0031] In some embodiments, the personal information comprises a private key.

[0032] According to an aspect of embodiments herein described there is provide a computer implemented method comprising: (A) providing at least one mobile electronics device, each device having a data store comprising an operating system area and an authentication area; the authentication area being distinct from the operating system area to assist with securing the operating system area; the authentication area for storing authentication data; and (B) in connection with each mobile electronic device: associating authentication data with computer identifying information to provide special authentication data; storing the special authentication data in the authentication area; and retrieving said authentication data by: (i) reading the special authentication data from the authentication area; and (ii) applying the computer identifying information to the special authentication data.

[0033] According to an aspect of embodiments herein described there is provide a computer implemented method comprising the steps of: (A) providing USB devices having a first partition and a second partition; each first partition storing an operating system configured to be loaded upon booting a computer using the USB device; each first partition being a read only partition; each second partition being a read-write partition; (B) in connection with each USB device: encrypting WIFI network password data with computer identifying information that uniquely identifies a computer to provide encrypted WIFI network authentication data; storing the encrypted WIFI network authentication data in the second partition; and retrieving said WIFI network password data by: (i) reading the encrypted WIFI network authentication data from the second partition; and (ii) applying the computer identifying information to the encrypted WIFI network authentication data by using the computer identifying information as a decryption password.

[0034] According to an aspect of embodiments herein described there is provide a computer implemented system comprising: a plurality of USB devices each having a first partition and a second partition; each first partition storing an operating system configured to be loaded upon booting a computer using the USB device; each first partition being a read only partition; each second partition being a read-write partition; each operating system including: (A) an encryption facility for encrypting WIFI network password data with computer identifying information that uniquely identifies a computer to provide encrypted WIFI network authentication data; (B) a storage facility for storing the encrypted WIFI network authentication data in the second partition; and (C) a retrieval facility for retrieving said WIFI network password data by: (i) reading the encrypted WIFI network authentication data from the second partition; and (ii) applying the computer identifying information to the encrypted WIFI network authentication data by using the computer identifying information as a decryption password.

[0035] According to an aspect of embodiments herein described there is provide a storage device comprising: a first area and a second area; the second area being distinct from the first area to assist with securing the first area; the first area being a system area and the second area for storing personal information; the first area including: (A) an associator for associating personal information with computer identifying information to provide special personal information; (B) a storage facility for storing the special personal information data in the second area; and (C) a retrieval facility for retrieving said personal information by: (i) reading the special personal information from the second area; and (ii) applying the computer identifying information to the special personal information.

[0036] According to an aspect of embodiments herein described there is provide a storage device comprising: a first partition and a second partition; the first partition storing an operating system configured to be loaded upon booting a computer using the USB device; each first partition being a read only partition; each second partition being a read-write partition; each operating system including: (A) an encryption facility for encrypting WIFI network password data with computer identifying information that uniquely identifies a computer to provide encrypted WIFI network authentication data; (B) a storage facility for storing the encrypted WIFI network authentication data in the second partition; and (C) a retrieval facility for retrieving said WIFI network password data by: (i) reading the encrypted WIFI network authentication data from the second partition; and (ii) applying the computer identifying information to the encrypted WIFI network authentication

data by using the computer identifying information as a decryption password. According to an aspect of embodiments herein described there is provide a computer implemented method comprising: (A) providing a plurality of mobile electronics devices, each device having a data store comprising a first area; (B) providing an external data store external to the mobile electronics devices; each first area being a system area and the external data store for storing personal information; and (C) in connection with each mobile electronic device: associating personal information with computer identifying information to provide special personal information; storing the special personal information in the external data store; and retrieving the personal information by: (i) reading the special personal information from the external data store; and (ii) applying the computer identifying information to the special personal information.

[0037] In some embodiments, the personal information comprises password, wallet or key data.

[0038] In some embodiments, the personal information comprises personal financial data.

[0039] In some embodiments, associating the personal information with the computer identifying information to provide the special personal information comprises encrypting the personal information using the computer identifying information as the encryption password.

[0040] In some embodiments, applying computer identifying information to the special personal information comprises decrypting the special authentication data using the computer identifying information.

[0041] In some embodiments, each first area comprises a locked down operating system area; the second area comprises an authentication area.

[0042] Preferably the mobile electronic devices each comprise a USB devices having a first partition. Each first partition is provided for storing an operating system configured to be loaded upon booting a computer using the USB device; each first partition being a read only partition.

[0043] In some embodiments personal information is encrypted in the data store via the internet is a state that the encrypted using computer identifying information that identifies the computer allocated to the USB device.

[0044] According to an aspect of embodiments herein described there is provide a computer implemented method comprising: (i) providing users with user accounts; (ii) providing the users

with first virtual machines in association with local electronic devices of the users; (iv) receiving user data from the users where each user is provided with the ability to store data in association with the user account of the user; and (iv) encrypting the user data of each user based on computer identifying information of an associated local electronics device of the user.

[0045] Preferably the computer identifying information of each local electronics device comprises a unique hardware identifier of the local electronics device

[0046] Preferably the method includes storing the unique hardware identifiers the local electronics devices in a data store of encryption keys; and associating the encryption keys with corresponding user accounts.

[0047] Preferably the method includes decrypting the data of each user based on the unique hardware identifier of the associated local electronics device of the user.

[0048] Among a number of other advantages, several preferred embodiments of the present invention are considered to provide:

a) the ability to store personal information on a USB flash drive providing a locked down operating system where the personal information is tied to a particular host computer;

b) the ability to quickly log on to a Wi-Fi network using a USB flash drive that provides a bootable operating system that provides a remote desktop connection to an online financial account;

c) the ability to store at private key on a USB thumb drive that provides a bootable operating system providing a remote desktop connection to an online financial account, where the private key is tied to a particular host computer; and

d) the ability to store a crypto currency private key on a USB thumb drive that provides a bootable operating system providing a remote desktop connection to a financial system, where the private key is tied to a particular host computer.

[0049] It is to be recognised that other aspects, preferred forms and advantages of the present invention will be apparent from the present specification including the detailed description, drawings and claims.

BRIEF DESCRIPTION OF DRAWINGS

[0050] In order to facilitate a better understanding of the present invention, several preferred embodiments will now be described with reference to the accompanying drawings, in which:

Figure 1 provides an illustration of a computer implemented method according to a first preferred embodiment of the present invention.

Figure 2 provides a schematic illustration of a USB flash drive used in the method shown in Figure 1, the USB flash drive providing a further preferred embodiment.

Figure 3 provides an illustration of a computer implemented method according to another preferred embodiment of the present invention.

Figure 4 provides an illustration of the working of the method illustrated in Figure 3.

Figure 5 provides an illustration of a computer implemented method according to another preferred embodiment of the present invention.

Figure 6 provides an illustration of a computer implemented system according to another preferred embodiment of the present invention.

Figure 7 provides an illustration of a USB flash drive device used in the system shown in Figure 6, the USB flash drive providing a further preferred embodiment.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0051] Referring to figure 1 there is shown a computer implemented method 10 according to a first preferred embodiment of the present invention. The computer implemented method 10 is considered to allow for the advantageous storage of personal information in the form of Wi-Fi login passwords and block chain private keys for use in the provision of a remote desktop. The remote desktop provides dedicated access to an online financial account.

[0052] International patent application PCT/AU2015/050758 filed on 1 December 2015 in the name of GOPC Pty Ltd is hereby incorporated by reference for all purposes. The international patent application describes systems and methods that provide a secure banking interface in relation to an online financial account. Various security devices are described that provide a locked down system environment that is directed towards preventing third-party attacks.

[0053] In relation to PCT/AU2015/050758, a minimum operating environment is provided to allow banking operations via secured remote desktop services. The system is locked down to both external parties trying to gain access through the network and to the user. The user only has access to the remote connection facilities to make the connection to a virtual computer that provides access to the online financial account. In one embodiment a USB device is provided whereby the operating system is limited to providing remote protocol functionality that connects to the virtual computer service. The remote desktop is limited to providing access to a banking application running on the remote desktop.

[0054] Referring to figure 1, at block 12 the method 10 includes providing a plurality of mobile electronic devices 14. The mobile electronic devices 14 comprise universal serial bus storage devices 16 (USB devices). The USB devices 16 are each dedicated to the provision of data storage and comprise USB flash drives.

As detailed on Wikipedia: 'A USB flash drive consists of a small printed circuit board carrying the circuit elements and a USB connector, insulated electrically and protected inside a case which can be carried in a pocket or on a key chain, for example. The USB connector may be protected by a removable cap or by retracting into the body of the drive, although it is not likely to be damaged if unprotected. Most flash drives use a standard type-A USB connection allowing connection with a port on a personal computer, but drives for other interfaces also exist. USB flash drives draw power from the computer via the USB connections.

[0055] Referring to figure 2, each device 16 provides a data store 18 comprising a first area 20 and a second area 22. The second area 22 is distinct from the first area 20 to assist with securing the first area 20. The first area 20 of each device 16 comprises a locked down system area 24. The second area 26 comprises an authentication area 26 and is provided for storing personal information 28.

[0056] With each device 16, the first area 20 comprises a read-only partition 30 and the second area 22 comprises a read-write partition 32. By providing the read-only partition 30 the first area 20 can provide a locked down operating system area 24. The read-write partition 32 is utilised as discussed below.

[0057] As would be apparent a partition comprises a region on a storage device that has been formatted so that an operating system can manage information in each region separately. Various

partition types are used by different operating systems. The partitions comprise disk partitions of the dedicate storage devices.

[0058] In connection with the read write partition 32, the method 10 at block 34 includes associating personal information 28 with computer identifying information 38 to provide special personal information 40. In this embodiment, the computer identifying information 38 is used as an encryption key 42.

[0059] At block 44, the method 10 includes storing the special personal information 40 in the read-write partition 32. At block 46, the method 10 includes retrieving the personal information 28 by: (i) reading the special personal information 40 from the second area 22 and (ii) applying the computer identifying information 42 to the special personal information 40. As shown in figure 1 the process of retrieving includes decrypting the special personal information 40 at block 48.

[0060] The personal information 28 comprises authentication data 28. The second area 22 comprises an authentication area 22 for storing the authentication data 28. The authentication data 28 could comprise password, wallet or key data. Examples of password data include WIFI SSID/password pairs for logging into WIFI networks. Examples of wallet data include BITCOIN private keys that are able to be used to transfer electronic currency in relation to a publicly accessible ledger.

[0061] BITCOIN is a crypto currency and payment system based on a peer to peer model where transactions take place between users directly. The BITCOIN blockchain provides a publicly distributed leger where bitcoins comprise units of each transaction. The system is cryptographic requiring the use of keys to validate transactions. Bitcoins are presently created as a reward for computer power that verifies and records bitcoin transaction in the block chain. Users are able to pay for optional transaction fees to miners.

[0062] It is envisaged that the authentication data 28 in other embodiments could comprise a BLOCKCHAIN private key. Keys for providing access to data and information are considered to fall within the expression authentication data 28. In the case of Bitcoin, without a key, a transaction cannot be signed and therefore the currency cannot be spent.

[0063] It is to be appreciated that in other embodiments the personal information could comprise personal financial data including bank account numbers and transactions. Other applications include encrypted wallets of digital currency.

[0064] In one particularly preferred arrangement the personal information 28 comprises a WIFI network password. This relates to the embodiment shown in relation to Figure 3. Figure 3 illustrates a computer implemented method 60 according to another preferred embodiment of the present invention.

[0065] Referring to Figure 3, the method 60 at block 62 provides a number of USB flash drives 65 each having a first partition 66 and a second partition 68. Each first partition 66 comprises a read only partition 66 storing an operating system configured to be loaded upon booting a computer using the USB device. Each second partition 68 comprises a read-write partition 68 for storing authentication data 72. The authentication data 72 comprises WIFI network password data 72.

[0066] The method 60 at block 74, in connection with each USB device 65 includes encrypting WIFI network password data 72 with computer identifying information 76 that uniquely identifies a computer that is associated with the corresponding USB device 65.

[0067] The computer identifying information 76 comprises the computer motherboard serial number of the corresponding computer. The computer motherboard serial number is read by the operating system stored on the first partition 66 during booting of the operating system on the host computer. The hardware motherboard serial number 78 forms the encryption key 78 that is used at block 74. The encryption uses the encryption key 78 to encrypt the WIFI network password data 72 to provide encrypted passwords. Various encryption techniques including AES encryption are able to be readily used in provision of the method 60.

[0068] Block 74 provides encrypted WIFI network authentication data 80. At block 82 the method 60 includes storing the encrypted WIFI network authentication data 80 in the second partition of the corresponding USB device 65. At block 84 the method 10 includes retrieving the WIFI network password data by reading the encrypted WIFI network authentication data 80 from the second partition 68 or the corresponding USB device 65 and applying the encryption key 78 (as a decryption key 78) to the encrypted WIFI network authentication data 80. The computer identifying information 76 is used as a decryption password.

[0069] Each of the USB flash devices 65 is used to store the WIFI password of a WIFI network that the corresponding computer is able to connect to. In this manner users are able to use their USB device 65 to logon to a WIFI network and have the password of the WIFI network saved in the second partition 68 of the corresponding USB device 65. The second partition 68 of each USB device 65 in effect provides an authentication partition 68.

[0070] Each USB device 65 provides a dedicated storage device that stores an operating system in a read only partition and stores authentication data for WIFI networks in an authentication partition. This is performed in the context of the provision of a secured remote desktop for banking operations. As discussed, the locked down system environment provided by the operating system is directed toward preventing third party attacks. The operating system provides no more than is necessary for remote desktop services with authentication to limit the attack surface.

[0071] In one particularly preferred embodiment a custom operating system is limited to providing remote protocol functionality that connects to a virtual computer service. The remote protocol functionality may be a custom remote protocol functionality or one of NX, RDP, ICA. These protocols are distinguished in that they have the ability to provide a remote desktop of some form. In this embodiment, the remote desktop is limited to providing a banking application running on the remote desktop with only the banking application being accessible by the user. On the virtual service a browser is hosted that can access the bank via the Internet. The bank could of course be connected to by VPN or dialup connection.

[0072] Among other things, it is considered that the USB flash devices 65 are distinguished from those described in International patent application PCT/AU2015/050758 by the provision of each USB device having a read-write authentication area where a unique identifier of a corresponding computer is used to encrypt a WIFI password of a WIFI network. In embodiments that relate to BITCOIN the private key does not relate specifically to a network associated with the computer. However, the nature of the types of information are similar in that both provide a key.

[0073] It has been found that an authentication area does not have to be particularly large to store one or more WIFI passwords encrypted using identifiers of computers associated with the corresponding USB device. The authentication area could be between 1 to 4MB for example. In some embodiments, the authentication area is no more than 10MB in size. In other embodiments, the authentication area is no more than 5 MB in size. The size of the partition of the first area

may be greater than 400MB in size. Notably the applicant is not presently aware of any systems providing access to say banking information through a remote desktop by booting a USB device where personal information is associated with the computer identifying information to provide encrypted personal information. Nor is the applicant aware of such systems decrypting special authentication data using the same computer identifying decryption password where the personal information comprises a WIFI network password.

[0074] Figure 4 provides an illustration of the working of the method 60 illustrated in Figure 3. In figure 4 there are provided a number of computers 86 and several WIFI networks 88. A laptop 90 comprises one of the computers 86 and is moved along a path 92. As the laptop moves from a first WIFI network 94 to a second WIFI network 96to a third WIFI network 98 , the user will have to initially enter the password for each network. The motherboard identifier of the laptop computer will however be used to encrypt the various WIFI passwords and store them in the read-write partition of the corresponding USB device. Thus, if the USB is stolen or lost, it will not be able to be used to connect ot the WIFI networks 94, 96 and 98 without the laptop 90. This is considered to be particularly advantageous in the context of USB devices providing locked down operating system that provide remote desktops for banking operations.

[0075] Figure 5 illustrates a method 100 according to a further embodiment of the present invention. The method 100 comprises providing a number of USB devices that can be plugged into a number of computers. The USB devices are associated with one or more computers using a registration method providing access to online bank accounts only if the USB is used to boot those computers. The method 100 advantageously employs the method 60 described above.

[0076] In connection with the USB devices, each USB is used to boot a computer using an operating system partition of the USB device. The operating system obtains a unique identifier from the corresponding computer. The operating system reads encrypted Wi-Fi password information from an authentication partition of the USB device. The Wi-Fi password information is tested by attempting to decrypt the Wi-Fi password information using the unique identifier as a decryption password. If it is determined that the computer identifier is able to decrypt the encrypted Wi-Fi password information, the operating system attempts to log onto the corresponding WIFI network. If the operating system is able to log onto the Wi-Fi network, the operating system commences a Remote Desktop protocol procedure that attempts to provide a Remote Desktop providing dedicated access to a bank account. In the manner described the

method 100 includes booting a computer using the operating system area of a corresponding USB device, when the computer identifying information corresponds with the computer, and then automatically logs onto the associated WIFI network using the WIFI password. The approach of the method 100 is further detailed in figure 5.

[0077] The computer identifying information is unique to a corresponding host computer with the WIFI network information being effectively locked to a particular host computer due to the computer identifying information. In some embodiments, the WIFI network information could comprise sets of WIFI network information each corresponding to a different host computer. A one to one association between the host computer and the USB device is presently preferred in situations requiring high security.

[0078] By virtue of the operating system areas being read only, any changes to the operating system area are always lost when the host computer is powered off or rebooted. Comparatively information stored in the authentication partition is persistent between reboots and power cycles of the host computer.

[0079] In this embodiment, the form of the encryption comprises Advanced Encryption Standard (AES) 256-bit encryption keys with a cypher block chaining mode of operation.

[0080] In one presently preferred embodiment the client software consists of a customised GNU/Linux distribution installed and distributed on a USB stick as a Live USB install. The USB stick is partitioned with: (i) a first partition comprising a bootable, read-only FAT32 partition with Operating System files and the bank access remote desktop client software; and (ii) a second Partition comprising a read/write EXT3 partition for storing Wi-Fi passwords.

[0081] With the first partition any changes to this partition are lost when the host computer is powered off or rebooted. With the second partition passwords are persistent on the USB stick between reboots and power cycles of the host computer.

[0082] In terms of the process: (i) Each user selects a Wi-Fi network SSID; (ii) the User enters a plain text password into the client software; (iii) the software connects to the Wi-Fi SSID with the plain text password; (iv) if there is success the process continues at (v); (iv) if there is failure the process continues at (ii); (v) the plain text password is combined with a unique hardware identifier using an encryption algorithm with the hardware identifier comprising the encryption password to

produce an encrypted password; (vi) the encrypted password is written as a file to the read-write partition; (vi) there is a an eboot/power cycle host computer; (vii) the encrypted password is read from the read-write partition; (viii) the encrypted password and unique hardware identifier are passed to a decryption algorithm that uses the unique hardware identifier as a decryption password; (ix) upon a successful decryption the plain text password is used to connect the SSID; upon failure the process continues at (i). This process is repeated for multiple USB devices.

[0083] In the system, Wi-Fi passwords are encrypted via the Advanced Encryption Standard (AES) with 256bit encryption keys and CBC mode of operation. The size of the encryption key and the mode of operation are predetermined. More specifically, Wi-Fi passwords are stored on a EXT3 file system with of a small size (5-10 MB). Wi-Fi passwords are stored in a separate partition to the Live USB operating system files. The unique hardware identifier (such as CPU serial number, or network MAC address) is used as the cypher when encrypting a Wi-Fi password.

[0084] Advantageously, Wi-Fi passwords persist between reboots of the Live USB system and are locked to a particular host computer. Moving the USB to a different host computer from the one that Wi-Fi password have been saved on does not unlock the plain text version of the encrypted password. Wi-Fi passwords are stored in an AES encrypted form, and not plain text, so are not immediately usable by outside viewers.

[0085] In relation to a computer various unique hardware identifiers may be used other than the motherboard serial number. For example, a CPU serial number or network MAC address associated with a corresponding computer could be used.

[0086] Whilst an embodiment has been described with particular regard to WIFI network passwords, other embodiments may encrypt personal information that is provided in the form of an electronic wallet, a block-chain private key, or other financial information.

[0087] Referring to Figures 6 and 7 there is shown a computer implemented system 200 according to another preferred embodiment of the present invention. The computer implemented system 200 includes: a plurality of USB devices 202 each having a first partition 204 and a second partition 206 (See Figure 7). Each first partition 204 stores an operating system 210 configured to be loaded upon booting a computer using the USB device 202. Each first partition 204 comprises a read only partition. Each second partition 206 comprises a read-write partition. Each operating system includes an encryption facility 212 for encrypting WIFI network password data with computer

identifying information that uniquely identifies a computer to provide encrypted WIFI network authentication data.

[0088] Each operating system 210 includes a storage facility 215 for storing the encrypted WIFI network authentication data in the second partition 206.

[0089] Each operating system 210 further includes a retrieval facility 214 for retrieving said WIFI network password data by: (i) reading the encrypted WIFI network authentication data from the second partition; and (ii) applying the computer identifying information to the encrypted WIFI network authentication data by using the computer identifying information as a decryption password.

[0090] Each USB device provides a further embodiment comprising: a first partition 204 and a second partition 206 having the encryption facility 212, the storage facility 215 and the retrieval facility 214. The operating system can be considered as providing an associator for associating personal information (the WIFI passwords) with computer identifying information to provide special personal information.

[0091] In another embodiment there is provided a method and system. In the embodiment there are provided a plurality of mobile electronics devices in the form of USB storage devices. Each device has a data store comprising a first area.

[0092] The embodiment includes providing an external data store external to the mobile electronics devices. Each first area comprises a system area and in particular an operating system area for running on an authorised host computer.

[0093] The external data store is provided by an external system such as a cloud based system. The external data store is provided for storing personal information in the form of confidential data such as banking account information.

[0094] The embodiment includes: in connection with each mobile electronic device: associating personal information with computer identifying information to provide special personal information. The special personal information is stored in the external data store. The personal information is retrieved by: (i) reading the special personal information from the external data store; and (ii) applying the computer identifying information to the special personal information.

[0095] More particularly each USB device uses computer identifying information determined by the operating system when running on a host computer to decrypt the special personal information which in this example comprises banking account information.

[0096] In other embodiments an system external to each mobile electronics device is used to take the computer identifying information of the host computer when operating system is loaded onto the computer and decrypt the special personal information. This way, the data when stored on the external data store is tied to a computer that is authorised to use the USB device.

[0097] Each operating system is used in provision of a secured remote desktop for banking operations. As discussed, the locked down system environment provided by the operating system is directed toward preventing third party attacks. The operating system provides no more than is necessary for remote desktop services with authentication to limit the attack surface.

[0098] In another embodiment there is provided a method including: (i) providing users with user accounts; (ii) providing the users with first virtual machines in association with local electronic devices of the users; (iii) receiving user data from the users where each user is provided with the ability to store data in association with the user account of the user; and (iii) encrypting the user data of each user based on computer identifying information of an associated local electronics device of the user. The local electronic device of the user is an authorised device and the computer identifying information of the local electronics device is used the encrypt the user data.

[0099] More particularly the computer identifying information of each local electronics device comprises a unique hardware identifier of the local electronics device. The method further includes storing the unique hardware identifiers the local electronics devices in a data store of encryption keys; and associating the encryption keys with corresponding user accounts.

[0100] The method includes decrypting the data of each user based on the unique hardware identifier of the associated local electronics device of the user.

[0101] In this embodiment the user data comprises financial data.

[0102] Referring to Figure 8 there is shown a schematic diagram of a computer system 220 that is configured to provide preferred arrangements of systems and methods described herein. The computer system 220 is provided as a distributed computer environment containing a number of individual computer systems 222 (computers/computing devices) that cooperate to provide the

preferred arrangements. In other embodiments the computer system 220 is provided as a single computing device.

[0103] As shown, a first one of the computing devices 222 includes a memory facility 224. The memory facility 224 includes both 'general memory' and other forms of memory such as virtual memory. The memory facility 224 is operatively connected to a processing facility 226 including at least one processor. The memory facility 224 includes computer information in the form of executable instructions and/or computer data. The memory facility 224 is accessible by the processing facility 226 in implementing the preferred arrangements.

[0104] As shown each of the computing devices 422 includes a system bus facility 228, a data store facility 230, an input interface facility 232 and an output interface facility 234. The data store facility 230 includes computer information in form of executable instructions and/or computer data. The data store facility 230 is operatively connected to the processing facility 226. The data store facility 230 is operatively connected to the memory facility 224. The data store facility 230 is accessible by the processing facility 226 in implementing the preferred arrangements.

[0105] Computer information may be located across a number of devices and be provided in a number of forms. For example the data store facility 230 may include computer information in the form of executable instructions and/or computer data. The computer data information may be provided in the form of encoded data instructions, data signals, data structures, program logic for server side operation, program logic for client side operation, stored webpages and so forth that are accessible by the processing facility 226.

[0106] On one level, input interfaces allow computer data to be received by the computing devices 222. On another level, input interfaces allow computer data to be received from individuals operating one or more computer devices. Output interfaces, on one level, allow for instructions to be sent to computing devices. On another level, output interfaces allow computer data to be sent to individuals. The input and output interface facilities 232, 234 provide input and output interfaces that are operatively associated with the processing facility 226. The input and output facilities 232, 234 allow for communication between the computing devices 222 and individuals.

[0107] The computing devices 222 provide a distributed system in which several devices are in communication over network and other interfaces to collectively provide the preferred

arrangements. Preferably there is provided at least one client device in the system of computing devices 222 where the system is interconnected by a data network.

[0108] The client device may be provided with a client side software product for use in the system which, when used, provides systems and methods where the client device and other computer devices 222 communicate over a public data network. Preferably the software product contains computer information in the form of executable instructions and/or computer data for providing the preferred arrangements.

[0109] Input interfaces associated with keyboards, mice, trackballs, touchpad's, scanners, video cards, audio cards, network cards and the like are known. Output interfaces associated with monitors, printers, speakers, facsimiles, projectors and the like are known. Network interfaces in the form of wired or wireless interfaces for various forms of LANs, WANs and so forth are known. Storage facilities in the form of floppy disks, hard disks, disk cartridges, CD-ROMS, smart card, RAID systems are known. Volatile and non-volatile memory types including RAM, ROM, EEPROM and other data storage types are known. Various transmission facilities such as circuit board material, coaxial cable, fibre optics, wireless facilities and so forth are known.

[0110] It is to be appreciated that systems, components, facilities, interfaces and so forth can be provided in several forms. Systems, components, facilities, interfaces and so forth may be provided as hardware, software or a combination thereof. The present invention may be embodied as an electronics device, computer readable memory, a personal computer and distributed computing environments.

[0111] In addition the present invention may be embodied as: a number of computer executable operations; a number of computer executable components; a set of process operations; a set of systems, facilities or components; a computer readable medium having stored thereon computer executable instructions for performing computer implemented methods and/or providing computer implemented systems; and so forth. In the case of computer executable instructions they preferably encode the systems, components and facilities described herein. For example a computer-readable medium may be encoded with one or more facilities configured to run an application configured to carry out a number of operations forming at least part of the present arrangements. Computer readable mediums preferably participate in the provision of computer executable instructions to one or more processors of one or more computing devices.

[0112] Computer executable instructions are preferably executed by one or more computing devices to cause the one or more computing devices to operate as desired. Preferred data structures are preferably stored on a computer readable medium. The computer executable instructions may form part of an operating system of a computer device for performing at least part of the preferred arrangements. One or more computing devices may preferably implement the preferred arrangements.

[0113] The term computer is to be understood as including all forms of computing device including servers, personal computers, smart phones, digital assistants, electronics devices and distributed computing systems.

[0114] Computer readable mediums and so forth of the type envisaged are preferably intransient. Such computer readable mediums may be operatively associated with computer based transmission facilities for the transfer of computer data. Computer readable mediums may provide data signals. Computer readable mediums preferably include magnetic disks, optical disks and other electric/magnetic and physical storage mediums as may have or find application in the industry.

[0115] Components, systems and tasks may comprise a process involving the provision of executable instructions to perform a process or the execution of executable instructions within say a processor. Applications or other executable instructions may perform method operations in different orders to achieve similar results. It is to be appreciated that the blocks of systems and methods described may be embodied in any suitable arrangement and in any suited order of operation. Computing facilities, modules, interfaces and the like may be provided in distinct, separate, joined, nested or other forms and arrangements. Methods will be apparent from systems described herein and systems will be apparent from methods described herein.

[0116] As would be apparent, various alterations and equivalent forms may be provided without departing from the spirit and scope of the present invention. This includes modifications within the scope of the appended claims along with all modifications, alternative constructions and equivalents.

[0117] There is no intention to limit the present invention to the specific embodiments shown in the drawings. The present invention is to be construed beneficially to the applicant and the invention given its full scope.

[0118] In the present specification, the presence of particular features does not preclude the existence of further features. The words 'comprising', 'including', 'or' and 'having' are to be construed in an inclusive rather than an exclusive sense.

[0119] It is to be recognised that any discussion in the present specification is intended to explain the context of the present invention. It is not to be taken as an admission that the material discussed formed part of the prior art base or relevant general knowledge in any particular country or region.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A computer implemented method comprising: (A) providing at least one mobile electronics device, each device having a data store comprising a first area and a second area; the second area being distinct from the first area to assist with securing the first area; the first area being a system area and the second area for storing personal information; and (B) in connection with each mobile electronic device: associating personal information with computer identifying information to provide special personal information; storing the special personal information in the second area; and retrieving the personal information by: (i) reading the special personal information from the second area; and (ii) applying the computer identifying information to the special personal information.

2. A computer implemented method as claimed in claim 1 wherein the first area comprises a locked down system area; the second area comprises an authentication area and the personal information comprises authentication data.

3. A computer implemented method as claimed in claim 1 or 2 wherein in connection with each mobile electronic device: the first area comprises a read-only partition; and the second area comprises a read-write partition.

4. A computer implemented method as claimed in any one of claims 1 to 3 wherein the personal information comprises password, wallet or key data.

5. A computer implemented method as claimed in any one of claims 1 to 3 wherein the personal information comprises personal financial data.

6. A computer implemented method as claimed in any one of claims 1 to 3 wherein the personal information comprises a WIFI network password.

7. A computer implemented method as claimed in any one of claims 1 to 3 wherein each mobile electronic device comprises a dedicated storage device.

8. A computer implemented method as claimed in claim 7 wherein the dedicated storage device comprises a USB thumb drive.

9. A computer implemented method as claimed in any one of claims 1 to 8 wherein the first area comprises a locked down system area; the second area comprises an authentication area; and the authentication area is no more than 10MB in size.

10. A computer implemented method as claimed in any one of claims 1 to 9 wherein the first area comprises a locked down system area; the second area comprises an authentication area; and the authentication area is no more than 5 MB in size.

11. A computer implemented method as claimed in any one of claims 1 to 10 wherein the first area comprises a locked down system area; the second area comprises an authentication area; and the authentication area is greater than 1MB in size.

12. A computer implemented method as claimed in any one of claims 1 to 11 wherein the first area comprises a locked down system area; the second area comprises an authentication area; and the operating system area is greater than 400MB in size.

13. A computer implemented method as claimed in any one of claims 1 to 12 wherein associating the personal information with the computer identifying information to provide the special personal information comprises encrypting the personal information using the computer identifying information as the encryption password.

14. A computer implemented method as claimed in any one of claims 1 to 13 wherein applying computer identifying information to the special personal information comprises decrypting the special authentication data using the computer identifying information.

15. A computer implemented method as claimed in any one of claims 1 to 14 wherein the personal information comprises a WIFI network password.

16. A computer implemented method as claimed in claim 15 wherein the first area comprises a locked down operating system area; the second area comprises an authentication area; and

the method includes, in connection with each mobile electronic device, booting a computer using the operating system area and, when the computer identifying information corresponds with the computer, automatically logging onto the associated WIFI network using the WIFI password.

17. A computer implemented method as claimed in claim 15 or 16 wherein the first area comprises a locked down operating system area; the second area comprises an authentication area; the operating system area comprises a read-only partition and the authentication area comprises a read-write partition; associating the WIFI network password with the computer identifying information to provide the special authentication data comprises encrypting the WIFI network password using the computer identifying information as the password; and applying computer identifying information to the special authentication data comprises decrypting the special authentication data using the computer identifying information.

18. A computer implemented method as claimed in any one of claims 1 to 17 wherein the computer identifying information is unique to a corresponding host computer such that the personal information of each mobile device is locked to a particular host computer due to the computer identifying information.

19. A computer implemented method as claimed in any one of claims 1 to 18 wherein any changes to the first area are lost when the host computer is powered off or rebooted; and the personal information of the second area is persistent between reboots and power cycles of the host computer.

20. A computer implemented method as claimed in any one of claims 1 to 19 wherein the personal information is encrypted via the Advanced Encryption Standard (AES) with 128 or more bit encryption keys with a cypher block chaining mode of operation.

21. A computer implemented method as claimed in any one of claims 1 to 20 wherein the computer identifying information comprises a unique hardware identifier.

22. A computer implemented method as claimed in claim 21 wherein the unique hardware identifier comprises a CPU serial number or network MAC address associated with a corresponding computer.

23. A computer implemented method as claimed in any one of claims 1 to 22 wherein the personal information comprises an electronic wallet.

24. A computer implemented method as claimed in any one of claims 1 to 23 wherein the personal information comprises a block-chain private key.

25. A computer implemented method as claimed in claim 24 wherein the personal information comprises a block-chain private key for electronic money.

26. A computer implemented method as claimed in any one of claims 1 to 25 wherein the personal information comprises a private key.

27. A computer implemented method comprising: (A) providing at least one mobile electronics device, each device having a data store comprising an operating system area and an authentication area; the authentication area being distinct from the operating system area to assist with securing the operating system area; the authentication area for storing authentication data; and (B) in connection with each mobile electronic device: associating authentication data with computer identifying information to provide special authentication data; storing the special authentication data in the authentication area; and retrieving said authentication data by: (i) reading the special authentication data from the authentication area; and (ii) applying the computer identifying information to the special authentication data.

28. A computer implemented method comprising the steps of: (A) providing USB devices having a first partition and a second partition; each first partition storing an operating system configured to be loaded upon booting a computer using the USB device; each first partition being a read only partition; each second partition being a read-write partition; (B) in connection with each USB device: encrypting WIFI network password data with computer identifying information that uniquely identifies a computer to

provide encrypted WIFI network authentication data; storing the encrypted WIFI network authentication data in the second partition; and retrieving said WIFI network password data by: (i) reading the encrypted WIFI network authentication data from the second partition; and (ii) applying the computer identifying information to the encrypted WIFI network authentication data by using the computer identifying information as a decryption password.

29. A computer implemented system comprising: a plurality of USB devices each having a first partition and a second partition; each first partition storing an operating system configured to be loaded upon booting a computer using the USB device; each first partition being a read only partition; each second partition being a read-write partition; each operating system including: (A) an encryption facility for encrypting WIFI network password data with computer identifying information that uniquely identifies a computer to provide encrypted WIFI network authentication data; (B) a storage facility for storing the encrypted WIFI network authentication data in the second partition; and (C) a retrieval facility for retrieving said WIFI network password data by: (i) reading the encrypted WIFI network authentication data from the second partition; and (ii) applying the computer identifying information to the encrypted WIFI network authentication data by using the computer identifying information as a decryption password.

30. A storage device comprising: a first area and a second area; the second area being distinct from the first area to assist with securing the first area; the first area being a system area and the second area for storing personal information; the first area including: (A) an associator for associating personal information with computer identifying information to provide special personal information; (B) a storage facility for storing the special personal information data in the second area; and (C) a retrieval facility for retrieving said personal information by: (i) reading the special personal information from the second area; and (ii) applying the computer identifying information to the special personal information.

31. A storage device comprising: a first partition and a second partition; the first partition storing an operating system configured to be loaded upon booting a computer using the

USB device; each first partition being a read only partition; each second partition being a read-write partition; each operating system including: (A) an encryption facility for encrypting WIFI network password data with computer identifying information that uniquely identifies a computer to provide encrypted WIFI network authentication data; (B) a storage facility for storing the encrypted WIFI network authentication data in the second partition; and (C) a retrieval facility for retrieving said WIFI network password data by: (i) reading the encrypted WIFI network authentication data from the second partition; and (ii) applying the computer identifying information to the encrypted WIFI network authentication data by using the computer identifying information as a decryption password.

32. A computer implemented method comprising: (A) providing a plurality of mobile electronics devices, each device having a data store comprising a first area; (B) providing an external data store external to the mobile electronics devices; each first area being a system area and the external data store for storing personal information; and (C) in connection with each mobile electronic device: associating personal information with computer identifying information to provide special personal information; storing the special personal information in the external data store; and retrieving the personal information by: (i) reading the special personal information from the external data store; and (ii) applying the computer identifying information to the special personal information.

33. A computer implemented method comprising:

(i) providing users with user accounts;

(ii) providing the users with first virtual machines in association with local electronic devices of the users;

(iii) receiving user data from the users where each user is provided with the ability to store data in association with the user account of the user; and

(iv) encrypting the user data of each user based on computer identifying information of an associated local electronics device of the user.

34. A computer implemented method as claimed in claim 33 wherein the computer identifying information of each local electronics device comprises a unique hardware identifier of the local electronics device

35. A computer implemented method as claimed in claim 33 or 34 wherein the method includes storing the unique hardware identifiers the local electronics devices in a data store of encryption keys; and associating the encryption keys with corresponding user accounts.

36. A computer implemented method as claimed in claim 33, 34 or 35 wherein the method includes decrypting the data of each user based on the unique hardware identifier of the associated local electronics device of the user.

37. A method or system, run via at least one computer processor as claimed in any one of the preceding method or system claims.

38. A memory storing computer program instructions executable by a processor, the computer program instructions including instructions for performing operations comprising:

39. A non-transient computer readable medium having stored thereon computer executable instructions for performing a computer implemented method as claimed in any one of the preceding method claims.

40. A non-transient computer readable medium having stored thereon computer executable instructions encoding a computer implemented system as claimed in any one of the preceding system claims.

41. A non-transient computer-readable medium encoded with one or more facilities configured to run an application configured to carry out a number of operations to provide any one of the preceding method or system claims

42. A non-transient computer implemented method or system as claimed in any one of the preceding claims.

Fig. 1

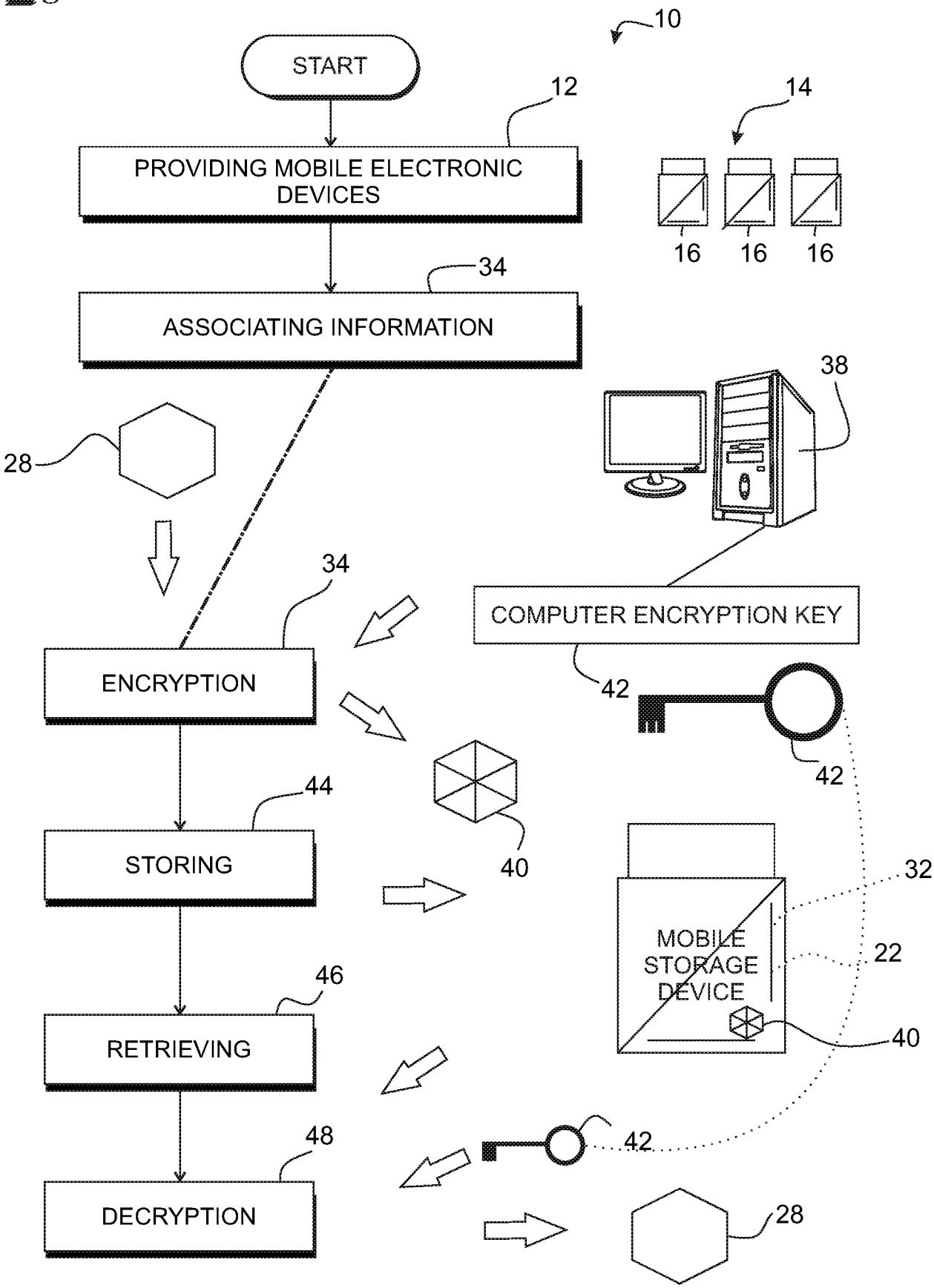

10
START
12
PROVIDING MOBILE ELECTRONIC DEVICES
14
16
16
16
34
ASSOCIATING INFORMATION
38
28
34
COMPUTER ENCRYPTION KEY
ENCRYPTION
42
42
44
40
STORING
32
MOBILE STORAGE DEVICE
22
40
46
RETRIEVING
48
42
DECRYPTION
28

Fig. 2

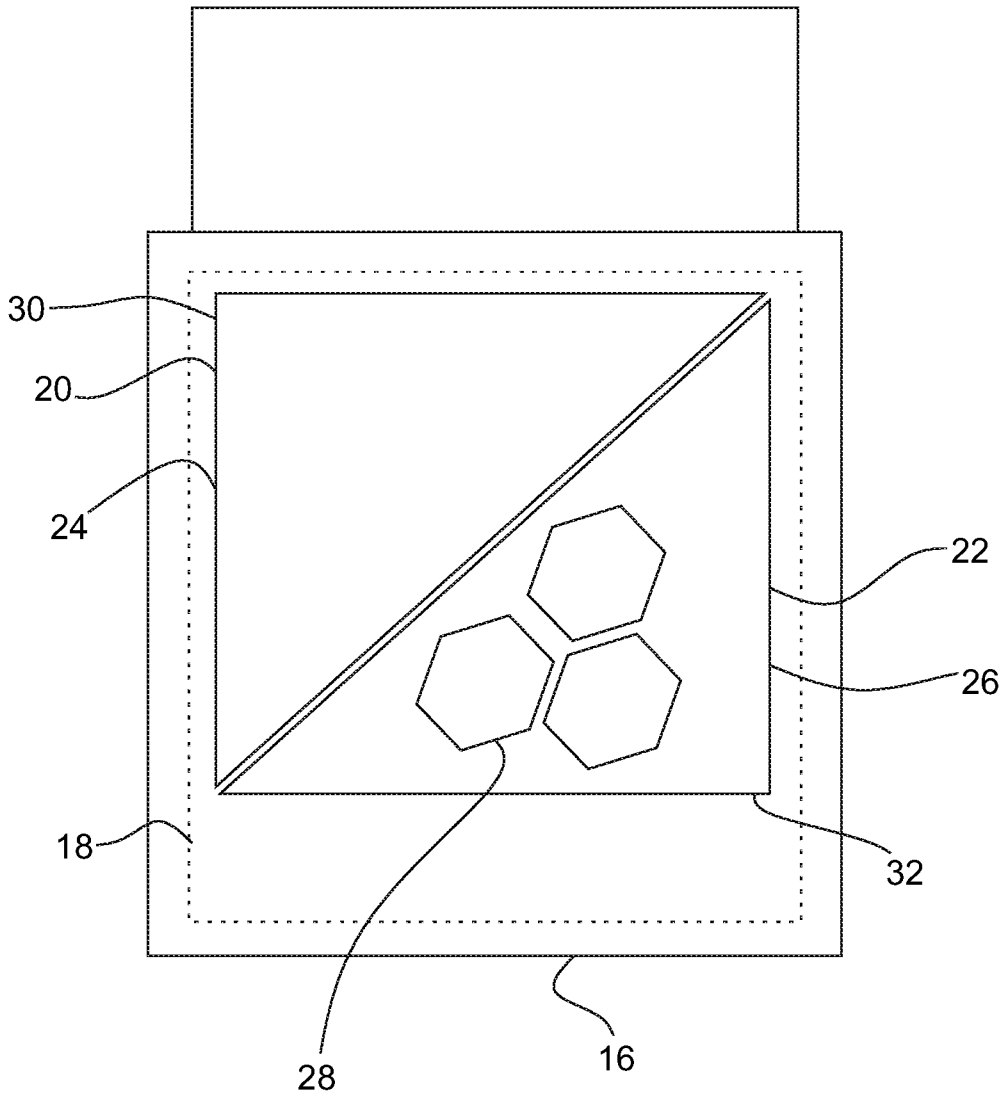


Fig. 3

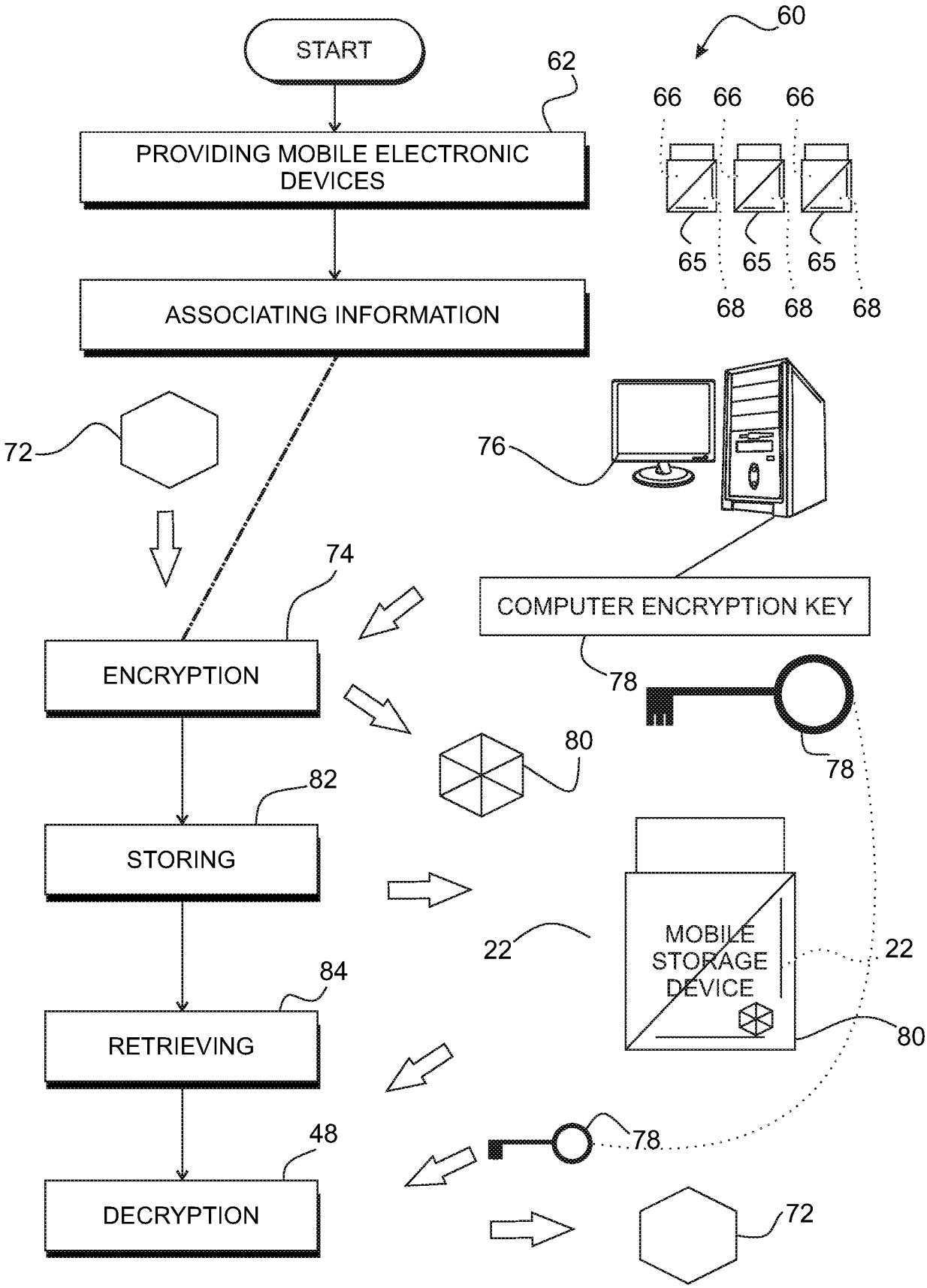

START
62
PROVIDING MOBILE ELECTRONIC DEVICES
ASSOCIATING INFORMATION
60
66
66
66
65
65
65
68
68
68
72
76
74
ENCRYPTION
COMPUTER ENCRYPTION KEY
78
78
80
82
STORING
22
MOBILE STORAGE DEVICE
22
80
84
RETRIEVING
78
48
DECRYPTION
72

Fig. 4

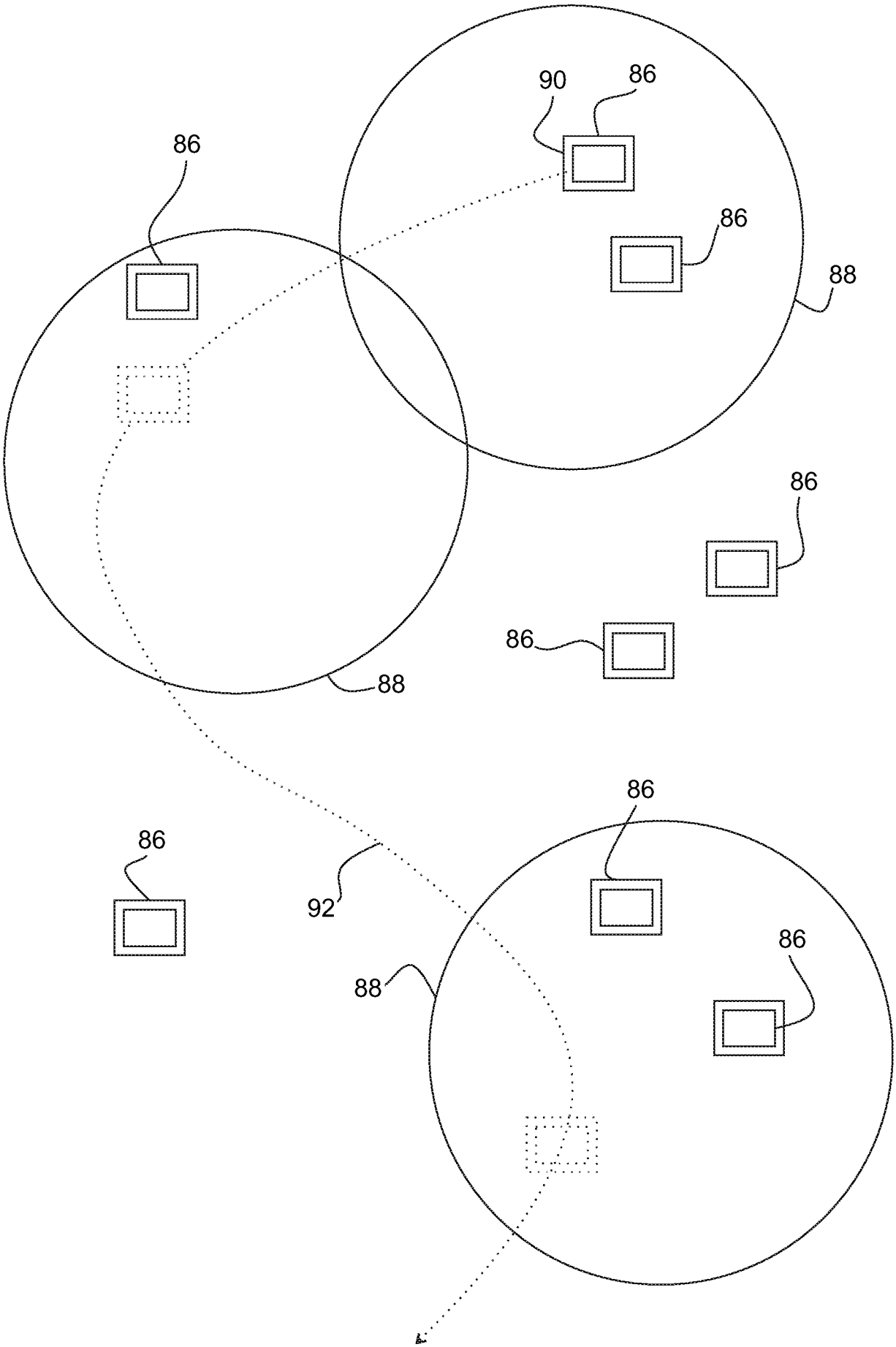


Fig. 5

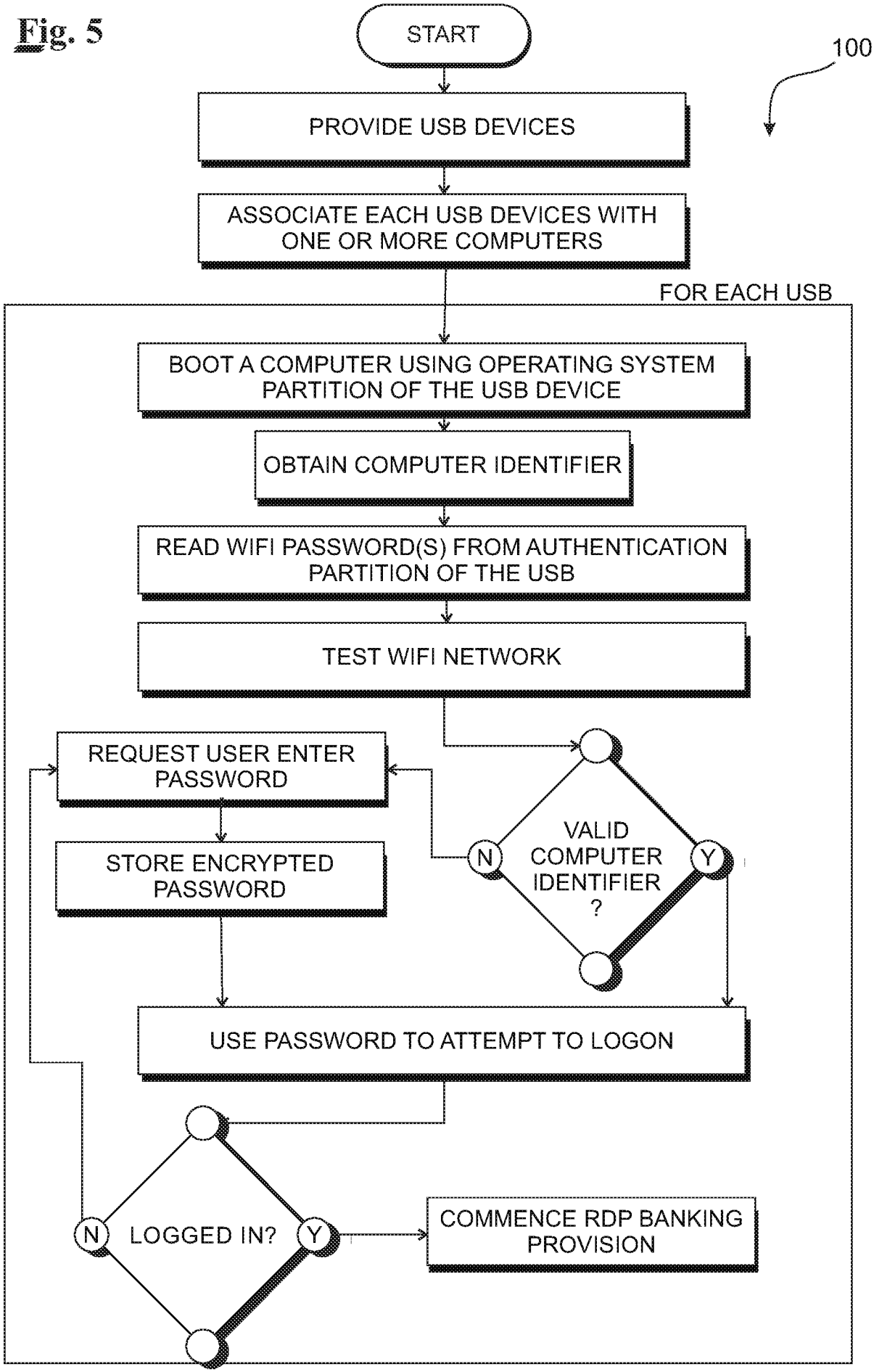

START
100
PROVIDE USB DEVICES
ASSOCIATE EACH USB DEVICES WITH ONE OR MORE COMPUTERS
FOR EACH USB
BOOT A COMPUTER USING OPERATING SYSTEM PARTITION OF THE USB DEVICE
OBTAIN COMPUTER IDENTIFIER
READ WIFI PASSWORD(S) FROM AUTHENTICATION PARTITION OF THE USB
TEST WIFI NETWORK
REQUEST USER ENTER PASSWORD
STORE ENCRYPTED PASSWORD
VALID COMPUTER IDENTIFIER ?
N
Y
USE PASSWORD TO ATTEMPT TO LOGON
LOGGED IN?
N
Y
COMMENCE RDP BANKING PROVISION

Fig. 6

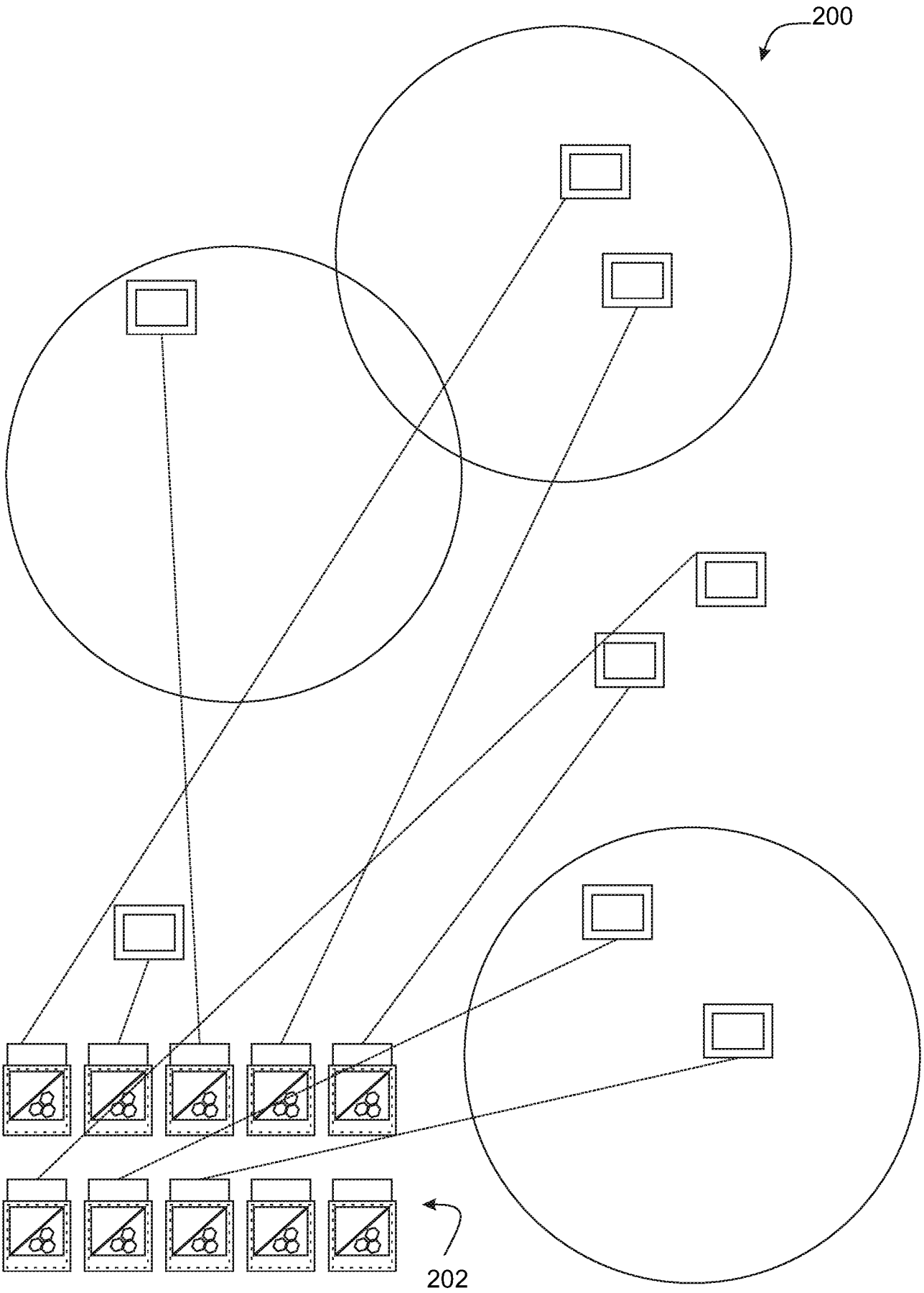
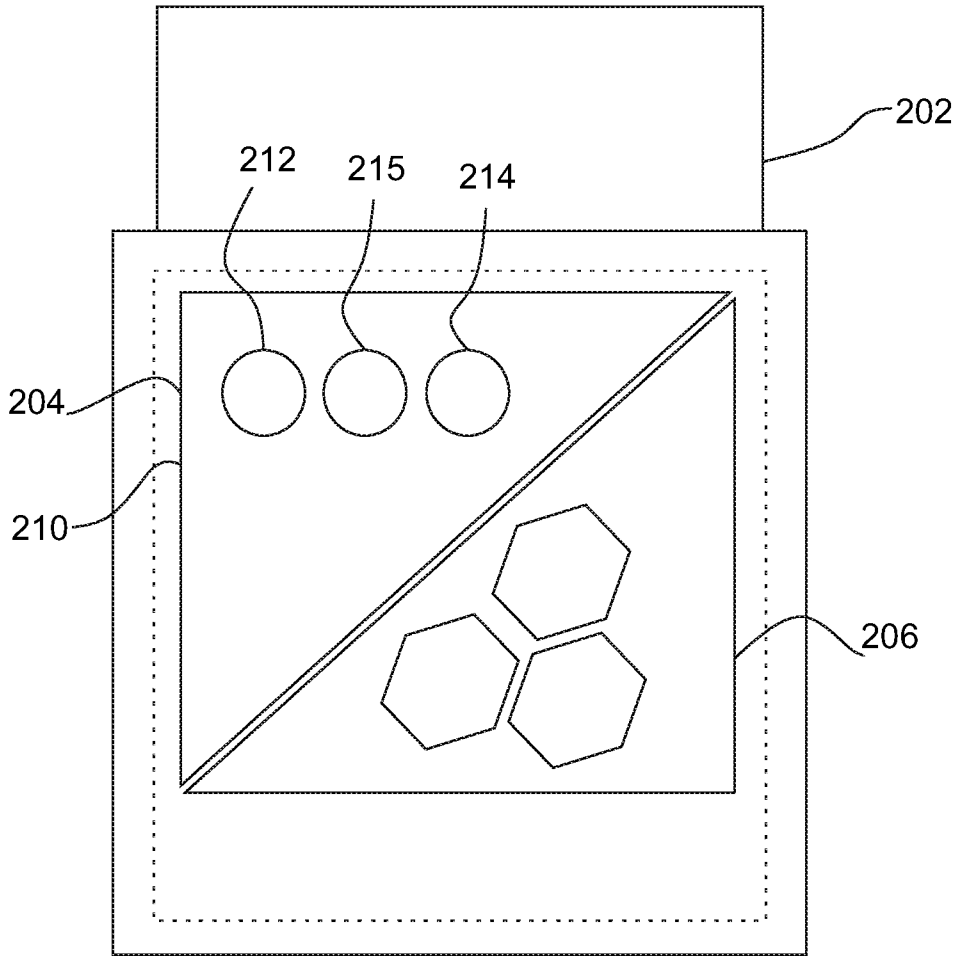


Fig. 7



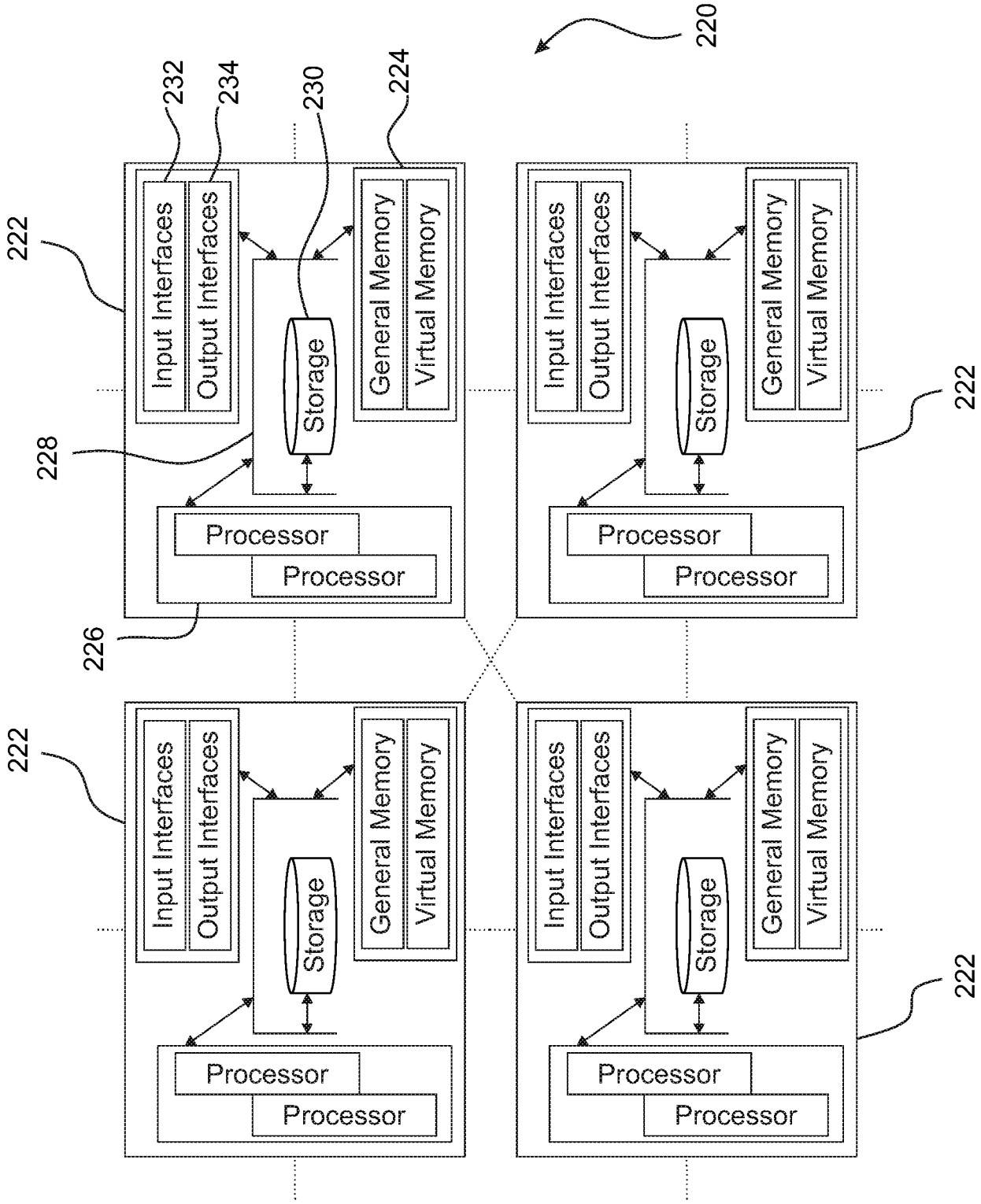

220
222
232
234
230
224
228
226
Input Interfaces
Output Interfaces
Storage
General Memory
Virtual Memory
Processor
Processor

Fig. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2018/051362

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/44 (2013.01)

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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

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

patenw: cpc-ipc g06f21/00, h04l9/00, keywords (disk, drive, storage device, usb, dongle, token, wallet, partition, area, slice, read-only, read-write, write protected, password, passphrase, passcode, pin, key, authentication, challenge, wi-fi, wlan, wireless, serial number, mac address, unique id identifier, uid, identification number, section, segment, second, multi, plural, separate, isolated, usb, dongle, token, wallet, encryption) & like terms; espacenet: opc h04l g6f21 & keywords (encryption key IMEI mac address serial number, guid, partition disk drive) ; Google scholar, keywords (serial number encryption key wifi vault private guid partition hard disk" unique identifier); Google, keywords(linux first boot mac address random); Patentscope; keywords(guid encryption key partition disk drive theft steal); Knoppix.net, keywords(Flash disk); ip australia internal databases: inventor; applicant

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	

[X] Further documents are listed in the continuation of Box C

[X] See patent family annex

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 June 2018	19 June 2018
Name and mailing address of the ISA/AU	**Authorised officer**
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustralia.gov.au	Peter Garay AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. +61262832451

INTERNATIONAL SEARCH REPORT C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		International application No. **PCT/IB2018/051362**
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/0123127 A1 (TEICHER et al.) 24 June 2004 The whole document, especially figs 1, 2, 12, 15, ¶0015, 0020, 0025, 0068-0069, 0071, 0089, 0096	1-32, 37, 39, 40
X	WPSCHULZ: 'Hard drive Installation', Knoppix Documentation Wiki, 15 December 2016, [retrieved from internet on 30 May 2018] <URL: http://knoppix.net/wiki3/index.php?title=Category:Hard_drive_Installation&oldid=9875 > The whole document, especially the sections under headings 'Flash disk install','Persistent memory', 'UNIONFS'	1, 3-8, 15-17, 19, 20, 23-26, 28, 29, 37, 39, 40
A	US 2007/0180515 A1 (DANILAK) 02 August 2007 The whole document	
A	US 2016/0337347 A1 (AIRWATCH LLC) 17 November 2016 The whole document	
A	US 2003/017740 A1 (ARNOLD et al.) 18 September 2003 The whole document	
A	US 2005/0141717 A1 (CROMER et al.) 30 June 2005 The whole document	
A	US 8683232 B2 (YUEN et al.) 25 March 2014 The whole document	
A	'Reading /dev/urandom as early as possible' Stack Overflow forum, 16 October 2015, [retrieved from internet on 5 June 2018] <URL: https://stackoverflow.com/questions/33153010/reading-dev-urandom-as-early-as-possible > The whole document, especially paragraph below first grey code block	
A	ZLATANOV, N., 'Hard Disk Drive and Disk Encryption', Article published on Researchgate, 21 March 2016 [retrieved from internet on 5 June 2018] <URL: https://www.researchgate.net/publication/299282101 > The whole document, especially section 'Disk encryption and Trusted Platform Module'	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2018/051362

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:

because they relate to subject matter not required to be searched by this Authority, namely:

the subject matter listed in Rule 39 on which, under Article 17(2)(a)(i), an international search is not required to be carried out, including

2. ☒ Claims Nos.: 38, 41, 42, **33-36**

because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

See Supplemental Box

3. ☐ Claims Nos:

because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

Supplemental Box

Continuation of **Box II**

Claim **38** is for "A memory storing computer program instructions executable by a processor, the computer program instructions including instructions for performing operations comprising:". There is nothing in the claim to indicate what instructions comprise are in the memory to perform an unspecified operation. This claim is incomplete and does not read not meaningfully.

Claim **41** is for "A non-transient computer-readable medium encoded with one or more facilities configured to run an application configured to carry out a number of operations to provide any one of the preceding method or system claims". As any existing code may be a facility to run an application, this claim is to any code that may be used to carry out what is otherwise claimed, even if not so encoded, in effect claiming any platform that the invention can be implemented on.

Claim **42** is for "A non-transient computer implemented method or system ...". There is nothing to indicate what a non-transient computer implemented method is. Non of the preceding claims are so directed.

Claim **33** and its dependencies (claims **34-36**) feature providing **users** with accounts, where each **user** is provided with the ability to store data in association with the **user** account of the **user**. This claim is therefore by result and not sufficiently disclosed in the description. The fact that a device id is used in some way to carry out encryption/decryption is insufficient information, as it does not define what is to be decrypted. Appended claim 35 has features purporting to clarify the matter, however it does not assist, because it does not define how an association between the keys and the accounts is made.

Furthermore, it is noted that claim 33 features a "first virtual machines in association with local electronic devices of the users", but this "first virtual machine" does not appear to have any functional connection with the rest of the method.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/IB2018/051362**

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

Patent Document/s Cited in Search Report		Patent Family Member/s	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**
US 2004/0123127 A1	24 June 2004	US 2004123127 A1	24 Jun 2004
		US 8745409 B2	03 Jun 2014
		AU 2003282333 A1	09 Jul 2004
		EP 1576762 A1	21 Sep 2005
		EP 1576762 B1	03 Sep 2014
		JP 2006511893 A	06 Apr 2006
		JP 4728120 B2	20 Jul 2011
		WO 2004056032 A1	01 Jul 2004
US 2007/0180515 A1	02 August 2007	US 2007180515 A1	02 Aug 2007
		US 7849510 B2	07 Dec 2010
		US 2008133939 A1	05 Jun 2008
		US 8347115 B2	01 Jan 2013
		US 8386797 B1	26 Feb 2013
		US 2008130901 A1	05 Jun 2008
		US 8392727 B2	05 Mar 2013
US 2016/0337347 A1	17 November 2016	US 2016337347 A1	17 Nov 2016
		AU 2014235160 A1	19 Feb 2015
		AU 2016238935 A1	27 Oct 2016
		EP 2973188 A1	20 Jan 2016
		US 2014282846 A1	18 Sep 2014
		US 9401915 B2	26 Jul 2016
		US 2014282895 A1	18 Sep 2014
		WO 2014151235 A1	25 Sep 2014
US 2003/017740 A1	18 September 2003	US 2003017740 A1	23 Jan 2003
		JP 2003036902 A	07 Feb 2003
US 2005/0141717 A1	30 June 2005	US 2005141717 A1	30 Jun 2005
		US 7421588 B2	02 Sep 2008
US 8683232 B2	25 March 2014	US 2012297205 A1	22 Nov 2012
		US 8683232 B2	25 Mar 2014

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/IB2018/051362**

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

Patent Document/s Cited in Search Report		Patent Family Member/s	
Publication Number	**Publication Date**	**Publication Number**	**Publication Date**

End of Annex

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.