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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 June 2016 (30.06.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/101009 A1

(51) International Patent Classification:
G06F 21/10 (2013.01) *G06Q 20/04* (2012.01)
G06F 21/30 (2013.01) *G06Q 20/36* (2012.01)

(21) International Application Number:
PCT/AU2015/000759

(22) International Filing Date:
21 December 2015 (21.12.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2014905206 22 December 2014 (22.12.2014) AU

(71) Applicant: **IN4MA PTY LTD** [AU/AU]; c/- Houlihan², Level 1, 70 Doncaster Road, Balwyn North, Victoria 3104 (AU).

(72) Inventor: **HASAN, Bashar, Mahmoud, Sadi**; c/- Houlihan², Level 1, 70 Doncaster Road, Balwyn North, Victoria 3104 (AU).

(74) Agent: **WARDEN-HUTTON, Paul, David**; Houlihan2, Level 1, 70 Doncaster Road, Balwyn, North Victoria 3104 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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,

[Continued on next page]

(54) Title: UNLOCKING OF A COMPUTER READABLE MEDIUM OR OF AN ELECTRONIC PROCESS USING A COMPUTER READABLE MEDIUM

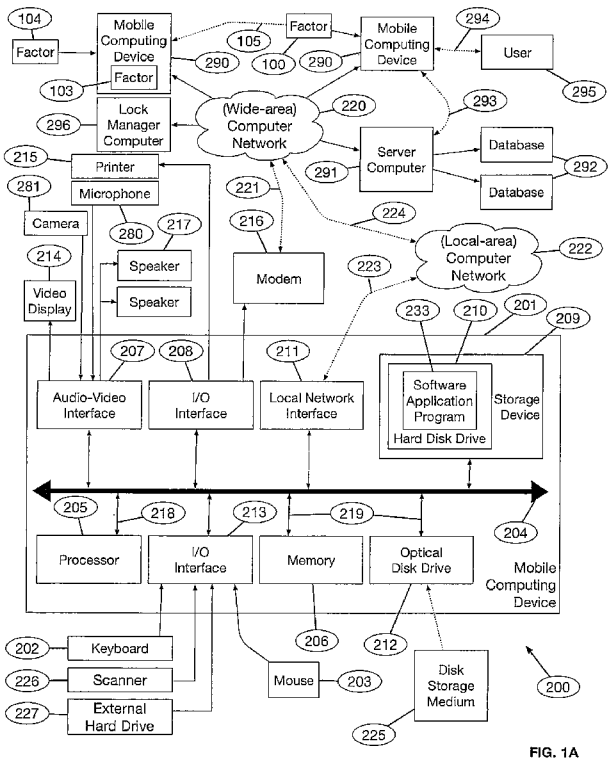

FIG. 1A

(57) Abstract: A method of unlocking a computer readable medium or an electronic process using a computer readable medium comprising: receiving a request to use a locked computer readable medium or a locked electronic process using a computer readable medium from a user computing device; matching one or more stored or acquired factors with at least one other stored or acquired factors to verify the user computing device; unlocking the computer readable medium or electronic process using a computer readable medium if a match results; and using the unlocked computer readable medium or unlocked electronic process using the computer readable medium to complete a transaction.

WO 2016/101009 A1

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))*

TITLE

UNLOCKING OF A COMPUTER READABLE MEDIUM OR OF AN ELECTRONIC PROCESS USING A COMPUTER READABLE MEDIUM

FIELD OF THE INVENTION

[001] The present invention relates to unlocking a computer readable medium or an electronic process using a computer readable medium. More particularly, the invention relates to unlocking the computer readable medium or electronic process using one or more stored or acquired factors to confirm the computer readable medium or process is to be unlocked for a client device.

BACKGROUND TO THE INVENTION

[002] The increase in total number of networked devices and in the type of devices that are being networked means that more and more processes are being carried out electronically and more electronic tokens are being used. Furthermore, this level of networking provides greater opportunities for dissemination of information including promotional or other offers relating to goods and services.

[003] With this increased capacity comes increased risk that a networked device will be accessed by someone other than those intended to have access.

[004] Accordingly, improved methods for unlocking an electronic process or electronic token are desirable.

SUMMARY OF THE INVENTION

[005] The present invention is broadly directed to unlocking a computer readable medium or an electronic process using the computer readable medium.

[006] In a broad form, the invention relates to unlocking a computer readable medium or an electronic process using a computer readable medium using one or more stored or acquired factors to confirm the computer readable medium or process is to be unlocked.

[007] A preferred advantage of the present invention is that access can be controlled intelligently and fluidly.

[008] In a first aspect, the present invention provides a method of unlocking a computer readable medium or an electronic process using a computer readable medium comprising:

using one or more stored or acquired factors to unlock the computer readable medium or electronic process using the computer readable medium for a user computing

device.

[009] In another embodiment of the first aspect, the method further comprises:

receiving one or more factors from the user computing device.

[0010] In yet another embodiment of the first aspect, the method further comprises:

receiving a request to unlock the computer readable medium or electronic process using the computer readable medium.

[0011] When the one or more factors are received from the user computing device, it may be matched with one or more stored factors.

[0012] In a second aspect the present invention provides a method of unlocking a computer readable medium or an electronic process using a computer readable medium comprising:

receiving a request to use a locked computer readable medium or a locked electronic process using a computer readable medium from a user computing device;

matching one or more stored or acquired factors with at least one other stored or acquired factors to verify the user computing device;

unlocking the computer readable medium or electronic process using a computer readable medium if a match results; and

using the unlocked computer readable medium or unlocked electronic process using the computer readable medium to complete a transaction.

[0013] The one or more stored or acquired factors may be entered on or captured by the user computing device or receiver computing device or may be obtained from the user computing device or receiver computing device by a software application running on the user computing device or receiver computing device.

[0014] The one or more stored or acquired factors may comprise a location, a time, or a number.

[0015] When the one or more stored or acquired factors comprises an acquired factor it may be matched with a stored factor comprised in a database.

[0016] The one or more stored or acquired factors comprise one or more user computing device acquired factors and one or more receiver computing device acquired factors. The one or more user computing device acquired factors and one or more receiver computing

device acquired factors may comprise complementary user computing device and receiver computing device factors. Complementary user computing device and received computing device factors may comprise identical or similar values such as, identical or similar location or time.

[0017] In another embodiment of any above aspect, the unlocking may be temporally or numerically limited. That is, the unlocking may only occur for a selected time period or for only a limited number of events.

[0018] In yet another embodiment of any above aspect, the one or more computer readable medium may comprise a barcode such as, a QR code, the barcode may be captured using a camera comprised on the user computing device.

[0019] The barcode may be captured from advertising displayed for example in print or television media.

[0020] According to any above aspect, any request, token, confirmation, confirmation code or unique token identification may be encrypted. The encryption may comprise Public IUKeys or Public OUKeys. Any received encoded request, token or confirmation may be decrypted using Private IUKeys or Private OUKeys.

[0021] The sending and receiving may be performed through an application stored on the mobile computing device or through a mobile communications system such as, SMS (short messaging service), Bluetooth or NFC (Near Field Communication).

[0022] The method of any above aspect may further include a step of sending a confirmation message. The confirmation message may be sent by SMS, Bluetooth or NFC.

[0023] In one embodiment of the first or second aspect, the computer readable medium or an electronic process using a computer readable medium may be for authorising a service. The service may for example comprise: a governmental service; a professional service; a trade service; a healthcare service; or a childcare and/or education service.

[0024] The one or more stored or acquired factors may comprise a device unique ID (DU-ID). The (DU-ID) may comprise one or more of a manufacturer serial number (MSN); an international mobile subscriber identity (IMSI) and a integrated circuit card identifier (ICCID). The (DU-ID) may be encrypted with the Public IUKey.

[0025] A software application comprised on the user computing device may comprise a user account and a Issuer Unique Public/Private Keys. The user account may comprise one

or more acquired user computing device factors and a Owner Unique ID and a computer readable medium storage. The computer readable medium storage may comprise one or more computer readable medium comprising respective one or more Alias-URL and computer readable medium UID. The computer readable medium Image may point to a shortened URL that has an ID. The shortened URL may itself point to a (True-QR-UID) or a (False-QR-UID) depending on the computer readable medium locking status.

[0026] The matching may comprise matching with one or more stored or acquired factors comprised on one or more databases. The one or more databases may comprise an Info-Action section; an Info-Action Request section; and a computer readable medium section. The Info-Action section may comprise an Info-Action-URL; A computer readable medium-UID; an Owner Unique ID (OU-ID); a Issuer Unique ID (IU-ID); and a Device Unique ID (DU-ID). The Info-Action Request section may comprise computer readable medium-UID and one or more user computing device Factors. The QR Image section may comprises an Alias-URL and a (QR-UID).

[0027] The database may also comprise a computer readable medium Domain comprising Issuer Unique Public/Private Keys.

[0028] A server computer may decrypt a received Owner (DU-ID) using Private IUKey.

[0029] The user computing device may be registered by sending Owner Name and Owner Mobile Number, (DU-ID) encrypted with Public IUKey. Upon registration, the user computing device may receive a Registration Confirmation Code.

[0030] The server computer may generate one or more Unique Public/Private Keys for the user computing device Owner Public OUKeys / Private OUKeys. The Unique Public/Private Keys for the user computing device Owner Public OUKeys / Private OUKeys may be stores in a database.

[0031] The user computing device may receive a Registration-Confirmation-Code by SMS which is sent to the server computer to activate the account. The server computer may validate and activate the account in response to the received Registration-Confirmation-Codes and respond by sending a secured URL to download the Public and Private OUKeys to the user computing device. The user computing device may then download the Public and Private OUKeys and send an Activate-Account command to the server computer. When the server computer receives the Activate-Account command the Public and Private

OUKeys may be deleted. The Registration-Confirmation-Code may be received by SMS.

[0032] An issuer of the locked computer readable medium may maintain a consumer account on the server computer. The server computer may send notification to a consumer computing device comprising account credentials. The consumer computing device may generate a Device Unique ID Consumer (DU-ID) using a software application and stores it encrypted using Public IUKey. The encrypted (DU-ID) stored on consumer computing device may be sent to the sever computer. In response to receiving the encrypted (DU-ID) stored on consumer computing device, the server computer may send a Registration-Confirmation-Code to the consumer computing device. The server computer may decrypt the Consumer (DU-ID) using Private IUKey and check if it is not associated with Consumer-Mobile-Number then create a temporary device entry in the database and store in it the decrypted database. The platform may send a Registration-Confirmation-Code to a Consumer-Mobile-Number which is directed to the consumer computing device. The consumer computing device may enter the Registration-Confirmation-Code in the software application and send an Account-Activation-Request to the server computer. In response to the received Account-Activation-Request the sever computer may validate the activation request and sending a secured URL to download the Public and Private OUKeys to the consumer computing device. The consumer computer device may download the Public and Private OUKey and then activate the consumer user account.

[0033] An owner computing device may encrypt an Info-Action and Owner (DU-ID) using Public IUKey and send a QR-Generation-Request to the server. The server computer may decrypt Info-Action and Owner (DU-ID) and generate (QR-UID), associate Info-Action and Owner (DU-ID) with (QR-UID) and store them in the database. The server computer may associate the Info-Action-URL with the Info-Action, and associate the Alias-URL with (QR-UID) and decodes the Alias-URL which comprises the (QR-UID) as a QR-Image, and store the QR-Image in the database. The server computer may send the QR-Image-URL and (QR-UID) encrypted using Public OUKey to the owner computing device. The owner computing device may receive and decrypt the QR-Image-URL and (QR-UID) using Private OUKey and fetch the QR-Image from the server computer. The fetched QR-image may be displayed on a screen of the owner computer device.

[0034] The owner computing device may encrypt the (QR-UID) and Owner (DU-ID) using Public IUKey and send a QR-Lock-Request to the server computer. The server

computer may receive the QR-Lock-Request, decrypt the (QR-UID) and Owner (DU-ID) and fetch from the database the Owner (DU-ID) associated with (QR-UID), if matched with the received Owner (DU-ID), the Alias-URL is updated to point to False-(QR-UID). The server computer responds to owner computing device by sending QR-Lock-Confirmation. The owner computing device receives QR-Lock-Confirmation from the server computer and displays the QR-Lock-Icon.

[0035] The owner computing device may encrypt the (QR-UID) and the Owner (DU-ID) using Public IUKey and send a QR-Unlock-Request to the server computer. The server computer may decrypt the (QR-UID) and Owner (DU-ID), fetch from the database the Owner (DU-ID) associated with (QR-UID) and if matched with the received Owner (DU-ID), the Alias-URL may be updated to point to (True-QR-UID). The server computer may respond to owner computing device by sending QR-Unlock-Confirmation.

[0036] The consumer computer device may scan the QR-Image using the computer software and the consumer computing device may display Info-Action if the Alias-URL points to the (True-QR-UID).

[0037] The consumer computing device may select action from the Info-Action and the software application may encrypt the (QR-UID) and Consumer (DU-ID) using Public IUKey and submit an Info-Action-Request to the server computer. The server computer may decrypt the (QR-UID) and Consumer (DU-ID), and if Consumer computing device is authorised to perform the Info-Action, the Info-Action is performed.

[0038] In a third aspect the present invention provides a method for transferring an electronic cash token comprising:

receiving a cash-to request comprising the electronic cash token or a unique token identification associated with the electronic cash token, one or more user computing device factors, a Device Unique Identifier (DU-ID) associated with a current owner of the electronic cash token and a recipient mobile telephone number;

validating cash token ownership by matching the electronic cash token or the unique token identification with an electronic database;

sending a cash-to token and a cash-to confirmation code to the mobile computing device associated with the current owner;

receiving a cash-to confirmation comprising the cash-to confirmation code and the

cash-to token;

matching the received cash-to confirmation code with the received cash-to token;

matching the one or more user computing device factors with one or more receiver device factors; and

transferring the electronic cash token by updating the electronic database to associate the electronic cash token with an account linked to the recipient mobile telephone number.

[0039] In one embodiment of the third aspect, one or more of the recipient mobile number, one or more user computing device factors and one or more receiver device factors may be received at a different time to the cash-to request.

[0040] In another embodiment of the third aspect, the method may further comprise recoding a computer readable medium associated with the electronic cash token. The computer readable medium may be associated with the current owner and/or the recipient.

[0041] In a fourth aspect the invention provides a method of authorising cash dispensing comprising:

receiving a cash-out request comprising a cash token or a unique token identification associated with the electronic cash token and one or more receiver device factors from a cash dispenser;

sending a cash-out confirmation code to an owner of the cash token and storing the cash-out confirmation code in an electronic database;

receiving from the cash dispenser a cash-out confirmation comprising the cash-out confirmation code;

receiving from the owner of the cash token one or more user computing device factors;

matching the received cash-out confirmation code with the stored cash-out confirmation code;

matching the one or more user computing device factors with one or more stored or acquired receiver device factors; and

sending a cash-out authorisation to the cash dispenser authorising the dispensing of cash.

[0042] The method of the fourth aspect may further comprise a step of the cash dispenser obtaining the cash token or the unique token identification from the cash token owner. The obtaining may comprise scanning for example, an electronic barcode such as QR-Image displayed on the owner's personal computing device.

[0043] The method of the fourth aspect may further comprise sending an electronic cash-out token to the dispenser.

[0044] In one embodiment of the fourth aspect, the receiving from the cash dispenser a cash-out confirmation further comprises receiving a cash-out token.

[0045]

[0046] In one embodiment of either the third or fourth aspect, the method for transferring an electronic cash token or authorising a cash dispensing may be for payment or part payment for goods or a service. The service may comprise: a governmental service; a professional service; a trade service; a healthcare service; or a childcare and/or education service.

[0047] According to any above aspect, the service, or where applicable government service, may be for vehicle licensing and/or renewal.

[0048] Where the terms "comprise", comprises", "comprising", "include", "includes", "included" or "including" are used in this specification, they are to be interpreted as specifying the presence of the stated features, integers, steps or components referred to, but not to preclude the presence or addition of one or more other feature, integer, step, component or group thereof.

[0049] Further, any prior art reference or statement provided in the specification is not to be taken as an admission that such art constitutes, or is to be understood as constituting, part of the common general knowledge.

BRIEF DESCRIPTION OF THE FIGURES

[0050] In order that the present invention may be readily understood and put into practical effect, reference will now be made to the accompanying illustrations, wherein like reference numerals refer to like features and wherein:

[0051] Figure 1A and 1B: shows a graphical representation of one embodiment of a personal mobile computing device suitable for use with the invention.

[0052] Figure 2A and Figure 2B: shows the structure of a personal mobile computing

device and a server computer according to one embodiment of the invention.

[0053] Figure 3A, 3B and 3C: shows various embodiments of a system according to the invention.

[0054] Figure 4: shows a flowchart illustrating the method according to one embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0055] The present invention relates to unlocking a computer readable medium or an electronic process using the computer readable medium. In one particular aspect, the invention relates to unlocking a computer readable medium or an electronic process using a computer readable medium using one or more stored or acquired factors to confirm the computer readable medium or process is to be unlocked.

[0056] The present invention is partly predicated on the present inventor's diligent study which has resulted in discovery that application of a factor such as, location or time, can be used to validate a user.

[0057] Just one of the significant advantages of the present invention is that access can be controlled intelligently and fluidly. That is, a lock manager can readily inspect any factor to confirm or override any unlocking and can amend any limitations placed on the unlocking. For example, unlocking may be for a limited time period and/or for a limited location range.

[0058] One embodiment of a personal mobile computing device 200 suitable for use in the present invention is shown in Figs. 1A and 1B. In the embodiment shown personal mobile computing device 200 comprises a computer module 201 comprising input devices such as a keyboard 202, a mouse pointer device 203, a scanner 226, a camera 281, an external hard drive 227, a touchscreen video display 214 and a microphone 280; and output devices including a printer 215, the touchscreen video display device 214 and loudspeakers 217. In some embodiments video display 214 may comprise a touchscreen.

[0059] A Modulator-Demodulator (Modem) transceiver device 216 may be used by the computer module 201 for communicating to and from a communications network 220 via a connection 221. The network 220 may be a wide-area network (WAN), such as the Internet, a cellular telecommunications network, or a private WAN. Through the network 220, computer module 201 may be connected to; and may have system interaction 293

with; other similar personal mobile computing devices 290 or server computers 291 and may have user interaction 294 with user 295. Where the connection 221 is a telephone line, the modem 216 may be a traditional "dial-up" modem. Alternatively, where the connection 221 is a high capacity (e.g.: cable) connection, the modem 216 may be a broadband modem. A wireless modem may also be used for wireless connection to network 220.

[0060] The computer module 201 typically includes at least one processor 205, and a memory 206 for example formed from semiconductor random access memory (RAM) and semiconductor read only memory (ROM). The module 201 also includes a number of input/output (I/O) interfaces including: an audio-video interface 207 that couples to the touchscreen video display 214, loudspeakers 217 and microphone 280; an I/O interface 213 for the keyboard 202, mouse 203, scanner 226 and external hard drive 227; and an interface 208 for the external modem 216 and printer 215. In some implementations, modem 216 may be incorporated within the computer module 201, for example within the interface 208. The computer module 201 also has a local network interface 211 which, via a connection 223, permits coupling of the personal mobile computing device 200 to a local computer network 222, known as a Local Area Network (LAN).

[0061] As also illustrated, the local network 222 may also couple to the wide network 220 via a connection 224, which would typically include a so-called "firewall" device or device of similar functionality. The interface 211 may be formed by an Ethernet circuit card, a Bluetooth wireless arrangement or an IEEE 802.11 wireless arrangement, a Near Field Communication, NFC, arrangement or other suitable interface.

[0062] The I/O interfaces 208 and 213 may afford either or both of serial and parallel connectivity, the former typically being implemented according to the Universal Serial Bus (USB) standards and having corresponding USB connectors (not illustrated).

[0063] Storage devices 209 are provided and typically include a hard disk drive (HDD) 210. Other storage devices such as, an external HD 227, a disk drive (not shown) and a magnetic tape drive (not shown) may also be used. An optical disk drive 212 is typically provided to act as a non-volatile source of data. Portable memory devices, such as optical disks (e.g.: CD-ROM, DVD, Blu-Ray Disc), USB-RAM, external hard drives and floppy disks for example, may be used as appropriate sources of data to the personal mobile computing device 200. Another source of data to personal mobile computing device 200 is provided by the at least one server computer 291 through network 220.

[0064] The components 205 to 213 of the computer module 201 typically communicate via an interconnected bus 204 in a manner which results in a conventional mode of operation of personal mobile computing device 200. In the embodiment shown in Figs. 1A and 1B, processor 205 is coupled to system bus 204 through connections 218. Similarly, memory 206 and optical disk drive 212 are coupled to the system bus 204 by connections 219. Examples of a personal mobile computing device 200 on which the described arrangements can be practiced include smart phones; tablet computers, gaming consoles, media players, TVs, wearable devices such as watches and glasses or a like device comprising a computer module like computer module 201. It is to be understood that when personal mobile computing device 200 comprises a smart phone or a tablet computer some illustrated input and output devices may not be included such as, mouse pointer device 201; keyboard 202; scanner 226; and printer 215.

[0065] Fig. 1B is a detailed schematic block diagram of processor 205 and a memory 234. The memory 234 represents a logical aggregation of all the memory modules, including the storage device 209 and semiconductor memory 206, which can be accessed by the computer module 201 in Fig. 1A.

[0066] The methods of the invention may be implemented using personal mobile computing device 200 wherein the methods may be implemented as one or more software application programs 233 executable within computer module 201. In particular, the steps of the methods of the invention may be effected by instructions 231 in the software carried out within the computer module 201

[0067] The software instructions 231 may be formed as one or more code modules, each for performing one or more particular tasks. The software 233 may also be divided into two separate parts, in which a first part and the corresponding code modules performs the method of the invention and a second part and the corresponding code modules manage a graphical user interface between the first part and the user.

[0068] The software 233 may be stored in a computer readable medium, including in a storage device of a type described herein. The software is loaded into the personal mobile computing device 200 from the computer readable medium or through network 221 or 223, and then executed by personal mobile computing device 200. In one example the software 233 is stored on storage medium 225 that is read by optical disk drive 212. Software 233 is typically stored in the HDD 210 or the memory 206.

[0069] A computer readable medium having such software 233 or computer program recorded on it is a computer program product. The use of the computer program product in the personal mobile computing device 200 preferably effects a device or apparatus for implementing the methods of the invention.

[0070] In some instances, the software application programs 233 may be supplied to the user encoded on one or more disk storage medium 225 such as a CD-ROM, DVD or Blu-Ray disc, and read via the corresponding drive 212, or alternatively may be read by the user from the networks 220 or 222. Still further, the software can also be loaded into the personal mobile computing device 200 from other computer readable media. Computer readable storage media refers to any non-transitory tangible storage medium that provides recorded instructions and/or data to the computer module 201 or personal mobile computing device 200 for execution and/or processing. Examples of such storage media include floppy disks, magnetic tape, CD-ROM, DVD, Blu-ray Disc, a hard disk drive, a ROM or integrated circuit, USB memory, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the computer module 201. Examples of transitory or non-tangible computer readable transmission media that may also participate in the provision of software application programs 233, instructions 231 and/or data to the computer module 201 include radio or infra-red transmission channels as well as a network connection 221, 223, 334, to another computer or networked device 290, 291 and the Internet or an Intranet including email transmissions and information recorded on Websites and the like.

[0071] The second part of the application programs 233 and the corresponding code modules mentioned above may be executed to implement one or more graphical user interfaces (GUIs) to be rendered or otherwise represented upon display 214. Through manipulation of, typically, touchscreen 214 a user of personal mobile computing device 200 and the methods of the invention may manipulate the interface in a functionally adaptable manner to provide controlling commands and/or input to the applications associated with the GUI(s). Other forms of functionally adaptable user interfaces may also be implemented, such as an audio interface utilizing speech prompts output via loudspeakers 217 and user voice commands input via microphone 280. The manipulations including screen touches, speech prompts, device movement gestures and/or user voice commands may be transmitted via network 220 or 222.

[0072] When the computer module 201 is initially powered up, a power-on self-test (POST) program 250 may execute. The POST program 250 is typically stored in a ROM 249 of the semiconductor memory 206. A hardware device such as the ROM 249 is sometimes referred to as firmware. The POST program 250 examines hardware within the computer module 201 to ensure proper functioning, and typically checks processor 205, memory 234 (209, 206), and a basic input-output systems software (BIOS) module 251, also typically stored in ROM 249, for correct operation. Once the POST program 250 has run successfully, BIOS 251 activates hard disk drive 210. Activation of hard disk drive 210 causes a bootstrap loader program 252 that is resident on hard disk drive 210 to execute via processor 205. This loads an operating system 253 into RAM memory 206 upon which operating system 253 commences operation. Operating system 253 is a system level application, executable by processor 205, to fulfill various high level functions, including processor management, memory management, device management, storage management, software application interface, and generic user interface.

[0073] Operating system 253 manages memory 234 (209, 206) in order to ensure that each process or application running on computer module 201 has sufficient memory in which to execute without colliding with memory allocated to another process. Furthermore, the different types of memory available in the personal mobile computing device 200 must be used properly so that each process can run effectively. Accordingly, the aggregated memory 234 is not intended to illustrate how particular segments of memory are allocated, but rather to provide a general view of the memory accessible by computer module 201 and how such is used.

[0074] Processor 205 includes a number of functional modules including a control unit 239, an arithmetic logic unit (ALU) 240, and a local or internal memory 248, sometimes called a cache memory. The cache memory 248 typically includes a number of storage registers 244, 245, 246 in a register section storing data 247. One or more internal busses 241 functionally interconnect these functional modules. The processor 205 typically also has one or more interfaces 242 for communicating with external devices via the system bus 204, using a connection 218. The memory 234 is connected to the bus 204 by connection 219.

[0075] Application program 233 includes a sequence of instructions 231 that may include conditional branch and loop instructions. Program 233 may also include data 232 which is

used in execution of the program 233. The instructions 231 and the data 232 are stored in memory locations 228, 229, 230 and 235, 236, 237, respectively. Depending upon the relative size of the instructions 231 and the memory locations 228-230, a particular instruction may be stored in a single memory location as depicted by the instruction shown in the memory location 230. Alternately, an instruction may be segmented into a number of parts each of which is stored in a separate memory location, as depicted by the instruction segments shown in the memory locations 228 and 229.

[0076] In general, processor 205 is given a set of instructions 243 which are executed therein. The processor 205 then waits for a subsequent input, to which processor 205 reacts by executing another set of instructions. Each input may be provided from one or more of a number of sources, including data generated by one or more of the input devices 202, 203, or 214 when comprising a touchscreen, data received from an external source across one of the networks 220, 222, data retrieved from one of the storage devices 206, 209 or data retrieved from a storage medium 225 inserted into the corresponding reader 212. The execution of a set of the instructions may in some cases result in output of data. Execution may also involve storing data or variables to the memory 234.

[0077] The disclosed arrangements use input variables 254 that are stored in the memory 234 in corresponding memory locations 255, 256, 257, 258. The described arrangements produce output variables 261 that are stored in the memory 234 in corresponding memory locations 262, 263, 264, 265. Intermediate variables 268 may be stored in memory locations 259, 260, 266 and 267.

[0078] The register section 244, 245, 246, the arithmetic logic unit (ALU) 240, and the control unit 239 of the processor 205 work together to perform sequences of micro-operations needed to perform "fetch, decode, and execute" cycles for every instruction in the instruction set making up the program 233. Each fetch, decode, and execute cycle comprises:

(a) a fetch operation, which fetches or reads an instruction 231 from memory location 228, 229, 230;

(b) a decode operation in which control unit 239 determines which instruction has been fetched; and

(c) an execute operation in which the control unit 239 and/or the ALU 240 execute

the instruction.

[0079] Thereafter, a further fetch, decode, and execute cycle for the next instruction may be executed. Similarly, a store cycle may be performed by which the control unit 239 stores or writes a value to a memory location 232.

[0080] Each step or sub-process in the methods of the invention may be associated with one or more segments of the program 233, and may be performed by register section 244-246, the ALU 240, and the control unit 239 in the processor 205 working together to perform the fetch, decode, and execute cycles for every instruction in the instruction set for the noted segments of program 233.

[0081] One or more other personal mobile computer device 290 may be connected to the communications network 220 as seen in Fig. 1A. Each such personal mobile computer device 290 may have a similar configuration to personal mobile computer device 200 comprising a computer module 201 and corresponding peripherals.

[0082] One or more other server computer 291 may be connected to the communications network 220. These server computers 291 respond to requests from personal mobile computing device 200, 290 or other server computers to provide information. Each server computer 291 may comprise or be associated with one or more database 292.

[0083] The methods of the invention may alternatively be implemented in dedicated hardware such as one or more integrated circuits performing the functions or sub functions of the described methods. Such dedicated hardware may include graphic processors, digital signal processors, or one or more microprocessors and associated memories.

[0084] Figs. 2A and 2B show the structure of personal mobile computing device 290 and server computer 291, respectively, according to one embodiment of the invention.

[0085] Turning first to Fig. 2A, personal mobile computing device 290 comprises a software application 233 and a device unique identifier (DU-ID) 269 that may be used by software application 233 and the methods of the invention. The (DU-ID) 269 identifies personal mobile computing device 200 and may comprise a manufacturer serial number (MSN) and/or an international mobile subscriber identity (IMSI). In another embodiment, when remote computing device 200 is a smartphone or tablet comprising a subscriber identification module (SIM), the unique identification number may comprise the international mobile subscriber identity (IMSI) or the integrated circuit card identifier

(ICCID).

[0086] Software application 233 comprises user account 110 and Issuer Unique ID (IU-ID) 112. The user account 110 comprises one or more acquired user computing device factors 104 and a Owner Unique ID (OU-ID) 106 and a QR Box 108. QR Box 108 comprises one or more QR image 130 comprising respective one or more Alias-URL 131 and (QR-UID) 132. The (QR-Image) may point to a shortened URL that has an ID. The shortened URL may itself point to a (True-QR-UID) 133 or a (False-QR-UID) 134 depending on the QR locking status.

[0087] Turning now to Fig. 2B, one or more databases 292 are shown to comprise an Info-Action section 120; an Info-Action Request section 122; and a QR Image 130 Section. The Info-Action section 120 comprises an Info-Action-URL 121; A (QR-UID) 132; a Owner Unique ID (OU-ID) 106; a Issuer Unique ID (IU-ID) 112; and a Device Unique ID (DU-ID) 269. The Info-Action Request section 122 comprises (QR-UID) 132 and one or more User computing device Factors 100. The QR Image 130 section comprises an Alias-URL 131 and a (QR-UID) 132.

[0088] Fig. 3A shows a graphical representation of one embodiment of system 10 of the invention. A user 295 operates a camera 281 comprised on their mobile computing device 290 to photograph a QR image 130 comprised on a gift voucher 131. In other embodiments, QR image 130 may be displayed in a television or printed advertisement. The user 295 wishes to exchange the electronic copy of the (QR-UID) 132 captured on device 290 for a discount on a purchase at store 300.

[0089] Both store computer 291 and user mobile computing device 290 are connected to computer network 220 and thereby may have one or more system interactions 293 (not shown in FIG. 3A) with the lock manager computer 296. Upon receiving a copy of the QR image 130 from one or both of device 290 and store computer 291 and a request for unlocking, lock manager computer 296 may unlock the electronic copy of the QR image 130 captured. The unlocking may only be performed if the one or more factors are validated. For example, the lock manager computer 296 may only allow the QR image 130 to be unlocked and the discount to be obtained within a defined geographical location or for limited time offer. This may be determined by comparing the stored factor 100s with the transmitted factor 100a of device 290 or the transmitted factor 100b of server 291 or the transmitted factors 100a, 100b of both device 290 and server 291, respectively. For

example, the transmitted factor 100a, 100b, 100s may comprises the time or location; which may be obtained using GPS (Global Positioning System); of device 290 or 291 or both.

[0090] Fig. 3B shows a graphical representation of another embodiment of system 10 of the invention. Fig. 3B shows an example of the exchange of an electronic cash token 140. The electronic cash token 140 may be as explained in the Australian provisional patent application filed by IN4MA PTY LTD on 31 October 2014 assigned Patent Number 2014904388 or PCT patent application PCT/AU2015/000618. For further information on the electronic cash tokens and methods using the tokens see that application.

[0091] As shown with reference to Fig. 3B, a user wishes to exchange unreadable public electronic cash token 140, comprising a QR image 130 stored on mobile computing device 290 for the associated cash amount and displays the QR image 130 associated with token 140 to cash dispenser 400 along with a request that the token 140 be unlocked. The cash dispenser 400 obtains a copy of the token 140 by photographing or scanning and transmits the associated (QR-UID) 132 to lock manager computer 296. Like the situation described with respect to Fig. 3A, lock manager computer 296 may unlock the token 140 only if one or more factors 100 (100a, 100b, 100s) are validated.

[0092] As is the case with the embodiment shown in Fig. 3A, as shown in Fig. 3B, in addition to one or more user computing device factors 100a, the one or more factors 100 may comprise one or more receiver device factors 100b. The one or more receiver device factors 100b may be stored on or provided by the mobile computing device 290 operated by the receiver of the cash token 140.

[0093] Fig. 3C shows an example in which services are authorised for payment according to another embodiment of a system 10 according to the invention. In this example, childcare services are authorised for payment using QR image 130 and one or more factors 100.

[0094] A parent 295 operating mobile computing device 290 uses a QR image 130 to pay or partly pay for childcare services. The QR image 130 may have been provided to the parent 295 by a public service department, government agency or other provider of such benefits. The provider of the childcare services uses camera 281 to obtain a copy of the QR image 130 from parent 295 of they QR image they received and sends the copy to lock

manager computer 296. The received copy of QR image 130 along with one or more of user computing device factor 100a; receiver device factors 100b and stored factor 100s may be reviewed by the lock manager computer 296 for a match before the payment or part-payment is authorised or actioned.

[0095] The one or more factors 100 (100a, 100b, 100s) may comprise a location, a time, or a number.

[0096] The one or more factors 100 (100a, 100b, 100s) may be a stored or acquired factor.

[0097] When the one or more factors 100a are received from the user computing device 290, it may be matched with one or more stored factors 100s and or one or more receiver device factors 100b. The one or more stored factors 100s may comprise a geographical location, a Device Unique ID (DU-ID) 269 identifying a personal mobile computing device.

[0098] The one or more factors 100 may be entered on or captured by the user computing device 290 or receiver device 290, 291 or may be obtained from the user computing device 200, 290 or recipient by a process running on the user computing device 290, 291 or receiver device 290, 291.

[0099] When the one or more factors comprise an acquired factor 100a, 100b it may be matched with a stored factor 100s comprised in a database.

[00100] In one embodiment, the one or more factors 100 comprise one or more user computing device acquired factors 100a and one or more receiver device acquired factors 100b. The one or more user computing device acquired factors 100a and one or more receiver device acquired factors 100b may comprise complementary user computing device and receiver device factors 105 (not shown). Complementary user computing device and exchange device factors 105 may comprise identical or similar values such as, identical or similar location.

[00101] The unlocking may be temporally or numerically limited. That is, the unlocking may only occur for a selected time period or for only a limited number of events. In this way, an administrator may ensure only a set number of offers are redeemed or that the offer remains open for only a limited period of time or for within only a limited geographical area.

[00102] As will be apparent from the above description, the one or more computer

readable medium that may be unlocked using the invention may comprise a barcode such as, a QR image 130, the barcode may be captured using a camera 281 comprised on the user computing device 290. The barcode may be captured from advertising displayed 131 for example in print or television media.

Registration Use Cases

[00103] *Issuer Registration Use Case:* The Issuer registers their domain on the platform comprised, for example, on server computer 291 and database 292. The platform, method and systems of the invention may be referred to as the IN4Scan Platform, IN4Scan Method and IN4Scan System. The platform then creates the Domain and generates Unique Public/Private Keys for the Issuer (Public IUKey / Private IUKey), which is stored in database 292. The Developer then embeds (Public IUKey) in (Owner App) 233 and compiles a distribution copy of the owner smart application 233. The Developer then also embeds (Public IUKey) in (Private App) 233 and compiles a distribution copy of the consumer smart application 233.

[00104] *Device & Owner Registration Use Case:* The Owner 295 Installs the application 233 on their device, e.g. device 200, 290, and initiates the application 233 for the first time. The Owner App 233 generates Device Unique ID Owner (DU-ID) 269, stores it locally on the device 200, 290, e.g. in storage device 209, encrypts it using (Public IUKey) and sends it to the platform for device registration. The platform decrypts the Owner (DU-ID) 269 using (Private IUKey) and checks if it is not associated with a mobile number then creates a temporary device entry in database 292 and stores in it the Owner (DU-ID) 269. The Owner 295 submits a new user registration form with (Owner Name) and (Owner Mobile Number) specified, encrypts the Owner (DU-ID) 269 using (Public IUKey) and includes it in their submission to server computer 291, then waits for (Registration-Confirmation-Code).

[00105] The Platform decrypts the Owner (DU-ID) 269 using (Private IUKey) and checks if it exists in the temporary device list database 292 then completes device registration and associates Owner (DU-ID) 269 with (Owner Mobile Number). The Platform generates a Unique Public/Private Keys for the Owner (Public OUKey / Private OUKey), stores the (Public OUKey) in database 292, keeps the (Private OUKey) in Database 292 which comprises a Trust-base and sends (Registration-Confirmation-Code) to (Owner Mobile Number), for example mobile computer Device 200, 290. The Trust-

base is a highly restricted access database that temporarily stores the Owner's generated Private keys (OU-ID) till they are downloaded by their associated devices 200, 290 and then deleted from the Trust-base.

[00106] The Owner 295 receives (Registration-Confirmation-Code) by SMS, enters it in the application 233 and sends to the platform (Account-Activation-Request). The Platform 291 validates (Account-Activation-Request) and responds by sending a secured URL to download the (Private OUKey) to the device 200, 290. The Owner App 233 downloads the (Private OUKey) and stores it in the device 200, 290 and then sends (Activate-Account) command to the platform 291. The Platform 291, on activation of account, deletes the (Private OUKey) from the Trust-base 292.

[00107] *Device & Consumer Registration Use Case:* The Issuer maintains consumer accounts and activation on the platform. The platform sends notification to the consumer 295 with account credentials 108. The Consumer 295 installs application 233 on their device 290, and initiates the application 233 for the first time. The Private App 233 generates a Device Unique ID Consumer (DU-ID) 269, stores it locally on the device 290, encrypts it using (Public IUKey) and sends it to the platform and waits for (Registration-Confirmation-Code). The platform decrypts the Consumer (DU-ID) 269 using (Private IUKey) and checks if it is not associated with (Consumer-Mobile-Number) then creates a temporary device entry in the database 292 and stores in it the decrypted database. The platform sends (Registration-Confirmation-Code) to (Consumer-Mobile-Number) which is directed to device 290. The consumer 295 receives a (Registration-Confirmation-Code) by, for example, SMS, enters it in the application 233 and sends an (Account-Activation-Request). The platform validates the activation request and responds by sending a secured URL to download the (Private IUKey) to the device 290. The Private App 233 downloads the (Private IUKey) and stores it in the device 290 and then activates the user account.

Operation Use Cases

[00108] *QR Code Generation Use Case:* The Owner 295 provides (Info-Action) 120 to be decoded as (QR-Image) 130 and presses (Generate-QR-Button). The Owner App 233 encrypts the (Info-Action) 120 and Owner (DU-ID) 269 using (Public IUKey) and submits the (QR-Generation-Request) to the platform and waits for the platform response. The platform receives (QR-Generation-Request), decrypts (Info-Action) 120 and Owner (DU-ID) 269, generates (QR-UID) 132, associates (Info-Action) 120 and Owner (DU-ID) 269

with (QR-UID) 132 and stores them in database 292. The platform associates (Info-Action-URL) 121 with the (Info-Action) 120, associates (Alias-URL) 131 with (QR-UID) 132, decodes (Alias-URL) 131 which includes (QR-UID) 132 as (QR-Image) 130, and stores it in the platform. The platform responds to owner 295 request by sending the (QR-Image-URL) and (QR-UID) 132 both encrypted using (Public OUKey). The Owner App 233 receives and decrypts (QR-Image-URL) 131 and (QR-UID) 132 using (Private OUKey) and fetches the (QR-Image) 130 from platform and displays it on screen 214 of device 290.

[00109] *QR Code Locking Use Case:* The Owner 295 views (QR-Image) 130, presses on (Lock-Button). The Owner App 233 encrypts the (QR-UID) 132 and Owner (DU-ID) 269 using (Public IUKey) and submits the (QR-Lock-Request) to the platform and waits for the platform response. The platform receives (QR-Lock-Request), decrypts (QR-UID) 132 and Owner (DU-ID) 269, fetches from the database 292 the Owner (DU-ID) 269 associated with (QR-UID) 132; if matched with the received Owner (DU-ID) 269 the (Alias-URL) 131 is updated to point to (False-QR-UID) 134. The platform responds to (Owner-App) 233 by sending (QR-Lock-Confirmation). The Owner App 233 receives (QR-Lock-Confirmation) from the platform 291 and displays the (QR-Lock- Icon) on the screen 214.

[00110] *QR Code Unlocking Use Case:* The owner 295 views (QR-Image) 130 on device 200 or 290, presses on (Unlock-Button). The Owner App 233 encrypts the (QR-UID) 132 and Owner (DU-ID) 269 using (Public IUKey) and submits the (QR-Unlock-Request) to the platform and waits for the platform response. The platform receives (QR-Unlock-Request), decrypts (QR-UID) 132 and Owner (DU-ID) 269, fetches from the database 292 the Owner (DU-ID) 269 associated with (QR-UID) 132; if matched with the received Owner (DU-ID) 269 updates the (Alias-URL) 131 to point to (True-QR-UID) 133. The platform responds to (Owner-App) 233 by sending (QR-Unlock-Confirmation). The owner App 233 receives (QR-Unlock-Confirmation) from the platform and displays the (QR- Unlock-Icon) on the screen 214.

[00111] *Public QR Code Scanning Use Case:* The consumer 295 scans (QR-Image) 130 using QR-scan (Public-App) 233. The public app 233 displays (Info-Action) 120 if (Alias-URL) 131 is pointing to (True-QR-UID) 133, otherwise if (Alias-URL) 131 is pointing to (False-QR-UID) 134 it will display (System-Lock-Message).

[00112] *Private QR Code Scanning Use Case:* The consumer 295 scans (QR-Image)

130 using QR-scan (Private-App) 233. The Private App 233 displays (Info-Action) 120 if (Alias-URL) 131 is pointing to (True-QR-UID) 133, otherwise if (Alias-URL) 131 is pointing to (False-QR-UID) 134 it will display (System-Lock-Message). The consumer 295 selects action from the (Info-Action) 120 and presses (Submit-Button). The Private App 233 encrypts the (QR-UID) 132 and Consumer (DU-ID) 269 using (Public IUKey) and submits the (Info-Action-Request) 122 to the platform and waits for the platform response. The platform receives (Info-Action-Request) 122, decrypts (QR-UID) 132 and Consumer (DU-ID) 269, if Consumer 295 is authorised to perform the (Info-Action) 120, the (Info-Action) 120 is performed. The platform responds to (Private-App) 233 by sending (Action-Result-Message). The Private App 233 receives (Action-Result-Message) from the platform and displays it on the screen 214.

[00113] The general flow of data according to one embodiment of the platform, methods and systems of the invention is shown in Fig. 4. A user computing device, such as mobile computing device 290, comprises a (DU-ID) 269 and is loaded with a (IU-ID) as described herein. The Owner 295 has their own (OU-ID) 106 Key comprised on, for example, device 290. The Info-Action 120 comprises a URL 121 and generates a (QR UID) 132. The (QR-UID) 132 comprises a generateAliasURL. As described above, if the Alias-URL 131 is pointing to a (True-QR-UID) 133, the (Info-Action) 121 is displayed, otherwise a Lock Message is displayed.

[00114] As noted above, the invention defined herein is applicable to unlocking electronic cash tokens. As such, in one embodiment the invention provides a method for transferring an electronic cash token 140. The method may be a secure method involving selective and secure unlocking of the token 100.

[00115] The Owner 295 of personal mobile computer device 290 selects 294 a (Cash-Token) 140 displayed on touchscreen 214 and presses 294 (Cash-To-Button) also displayed on touchscreen 214.

[00116] The personal mobile computer device 290 encrypts *(Cash-Token-ID)*, one or more user computing device factors 100 and the sender *Owner (DU-ID)* 269 using *(Public IUKey)* and includes them to request 293 a (Cash-To-Token-ID) from the server computer 291.

[00117] The server computer 291 encrypts (Cash-Token-ID) 102, the one or more

user computing device factors 100 and the sender *(Owner UDID)* 269 using *(Private UIKey)*, generates *(Cash-To-Token-ID)*, associates it with *(Cash-Token-ID)* 102 and the sender *Owner (DU-ID)* 269, stores it in Database 292, encrypts *(Cash-To-Token-ID)* using *(Public OUKey)* and sends 293 it as a response to the Owner software application program 233 on personal mobile computer device 290.

[00118] The personal mobile computer device 290 decrypts the *(Cash-To-Token-ID) using (Private OUKey)* and displays the (Cash-To-Form) on touchscreen 214.

[00119] The Owner 295 then specifies 293 the (Receiver-Mobile-Number) and presses 293 the (Send-Button). The personal mobile computer device 290 encrypts the *(Cash-Token-ID)* 140, *(Cash-To-Token-ID)* and the sender *Owner (DU-ID)* 269 using *(Public IUKey)* and submits 294 the (Cash-to-Request) to the server computer 291, and waits for the (Cash-To-Confirmation-Code).

[00120] The server computer 291 decrypts the *(Cash-Token-ID)* 140, *(Cash-To-Token-ID)* and the sender *Owner (DU-ID)* 269, validates the ownership and the intention to send a specific (Cash-Token) 140, fetches the receiver *Owner (DU-ID)* 269 associated with the (Receiver-Mobile-Number), associates it with the *(Cash-To-Token-ID)*, saves to the Database 292, then sends 294 a (Cash-To-Confirmation-Code) to (Sender-Mobile-Number) by SMS.

[00121] The owner 295 of personal mobile computer device 290 receives and enters 294 (Cash-To-Confirmation-Code) and presses 294 on the (Submit- Button) on touchscreen 214.

[00122] The personal mobile computer device 290 encrypts the (Cash-To-Token-ID) using *(Public UIKey)*, includes it in the (Cash-To- Confirmation-Form) and submits 293 them all to the server computer 291.

[00123] The server computer 291 matches (Cash-To-Token-ID) with (Cash-To-Confirmation-Code), authorises (Cash- To-Transaction) and completes it by associating the (Cash-Token-ID) 102 with the receiver Owner (DU-ID) 269, encrypts (Cash-Token-ID) 102 using (Public IUKey), encodes it as (QR-Image) 130 and store it in the Database 292.

[00124] The server computer 291 may also match the one or more user computing device factors 100 with one or more receiver device factors 100. The one or more receiver device factors 100 may be stored in one or more database 292 or may be sent to server

computer 291 by receiver device 290.

[00125] The server computer 291 then encrypts the (QR-URL) using receiver *(Public OUKey)* and sends 293 it to the receiver device 290.

[00126] The owner 295 of the receiver device 290 receives 294 notification from the server computer 291, refreshes 294 the (Cash-Box) QR-Box 108 to view (Cash-Token) List, clicks 294 on a (Cash-Token) 100 on the associated touchscreen 214 to view it.

[00127] The receiver device 290 decrypts the (QR-URL) using *(Private OUKey),* fetches the (QR-Image) 130 from the server computer 291 and displays it on the associated touch screen 214.

[00128] In another embodiment the invention also provides a method of authorising cash dispensing.

[00129] The owner 295 of personal mobile computing device 290 displays 294 the (QR Image) 130 of the (Cash-Token) 100 on touchscreen 214 and presents it to a Cashier 295.

[00130] The Cashier 295 scans 294 the (QR Image) 130 of the (Cash-Token-ID) 102 using a cashier personal mobile computer device 290, reads the (Cash-Token-Amount) 104 to the Owner, presses 294 the (Confirm-Button) and waits for (Cash-Out-Confirmation-Code).

[00131] The cashier personal mobile computing device 290 encrypts the *(Cash-Token-ID)* 102, one or more receiver device factors 100 and *(Cashier UDID)* 269 using *(Public IUKey)* and includes them to request 293 (Cash-Out-Token-ID) from the server 291.

[00132] The cash dispenser is referred to as the receiver device in this embodiment as it is receiving the token 140.

[00133] The server 291 decrypts the (Cash-Token-ID) 102 and the *Cashier (DU-ID)* 269 using *(Private IUKey)*, generates *(Cash-Out-Token-ID),* associates it with *(Cash-Token-ID)* 102 and *Cashier (DU-ID)* 269, stores in Database 292, encrypts *(Cash-To-Token-ID)* using *(Public IUKey)* and sends 293 it as a response to the Cashier software application program 233 and sends 293 (Cash-Out-Confirmation- Code) to (Owner-Mobile-Number) by SMS.

[00134] Cashier personal mobile computing device 290 decrypts the *(Cash-Out-*

Token-ID) using (Private IUKey) and displays the (Cash- Out-Form) on screen 214 and the cashier 295 asks the owner 295 for (Cash-Out-Confirmation-Code).

[00135] The owner 295 of personal mobile computing device 290 receives and reads 294 (Cash-Out-Confirmation-Code) to the Cashier 295.

[00136] The Cashier 295 enters 294 (Cash-Out-Confirmation-Code) and presses 294 (Submit-button).

[00137] The Cashier software application program 233 encrypts *(Cash-Out-Token-ID)* and *Cashier (DU-ID)* 269 using *(Public IUKey)* and includes them with the (Cash-Out-Confirmation-Code) and request 293 (Cash-Out- Authorisation-ID) from the server 291.

[00138] The server 291 also receives from device 290 one or more user computing device factors 100. The server 291 matches (Cash-Out-Token-ID) with (Cash-Out-Confirmation-Code), generates (Cash- Out-Authorisation-ID), associates it with (Cash-Token-ID) 102 and *Cashier(DU-ID)* 269 and stores it in the Database 292.

[00139] The server 291 encrypts (Cash-Out-Token-ID), (Cash-Out-Authorisation-ID) and *Cashier (DU-ID)* 269 using *(Public IUKey)* and sends 293 it as a response to cashier personal mobile computer device 290.

[00140] The Cashier personal mobile computer device 290 decrypts *(Cash-Out-Authorisation-ID)* and *Cashier (DU-ID)* 269 using *(Private IUKey)*, checks if received *Cashier (DU-ID)* 269 is matching with locally stored *Cashier (DU-ID)* 269 then displays the (Cash-Dispensing-Form) which includes (Cash-Out-Authorisation-ID).

[00141] The user computing device factors 100 are also matched with one or more stored or acquired recipient device factors 100. In one embodiment, this matching is done by the lock manager computer 296.

[00142] The Cashier 295 reviews 294 the (Cash-Dispensing-Form), presses 294 (Redeem-Cash-Token-Button) and waits for (Cash-Token-Redemption-Confirmation). The Cashier personal mobile computer device 290 encrypts (Cash-Out-Token-ID), *(Cash-Out-Authorisation-ID)* and *Cashier (DU-ID)* 269 using *(Public IUKey)* and sends 293 (Cash-Token-Redemption-Advise) to the server 291.

[00143] The server 291 decrypts (Cash-Out-Token-ID), *(Cash-Out-Authorisation-ID)* and *Cashier (DU-ID)* 269 using *(Private IUKey)*, if all matching then redeems the (Cash-Token) 100 and updates the Database 292 and sends 293 (Redemption-Completion-

Advise) as a response to the cashier personal mobile computer device 290.

[00144] The Cashier 295 dispenses Cash to the Owner 295 and closes 294 transaction.

[00145] The sending and receiving steps described herein may be performed through an application 233 stored on the mobile computing device 290 or through a mobile communications system such as SMS (short messaging service) or NFC (near field communication).

[00146] The methods of the invention may further include a step of sending a confirmation message. The confirmation message may be sent by SMS or NFC.

[00147] Throughout the specification the aim has been to describe the preferred embodiments of the invention without limiting the invention to any one embodiment or specific collection of features. It will therefore be appreciated by those of skill in the art that, in light of the instant disclosure, various modifications and changes can be made in the particular embodiments exemplified without departing from the scope of the present invention.

CLAIMS

1. A method of unlocking a computer readable medium or an electronic process using a computer readable medium comprising:

receiving a request to use a locked computer readable medium or a locked electronic process using a computer readable medium from a user computing device;

matching one or more stored or acquired factors with at least one other stored or acquired factors to verify the user computing device;

unlocking the computer readable medium or electronic process using a computer readable medium if a match results; and

using the unlocked computer readable medium or unlocked electronic process using the computer readable medium to complete a transaction.

2. The method of Claim 1 or Claim 2 wherein the one or more stored or acquired factors are entered on or captured by the user computing device or receiver computing device or obtained from the user computing device or recipient by a process running on the user computing device or receiver computing device.

3. The method of any one of the previous Claims wherein the one or more stored or acquired factors comprise a location, a time, or a number.

4. The method of any one of the previous Claims wherein when the one or more stored or acquired factors comprise an acquired factor it is matched with a stored factor comprised in a database.

5. The method of any one of the previous Claims wherein the one or more stored or acquired factors comprises one or more user computing device acquired factors and one or more receiver computing device acquired factors.

6. The method of Claim 5 wherein the one or more user computing device acquired factors and one or more receiver computing device acquired factors comprise complementary user computing device and receiver computing device factors.

7. The method of Claim 6 wherein the complementary user computing device and exchange device factors comprise identical or similar values such as, identical or similar location or time.

8. The method of any one or the previous Claims wherein the unlocking is temporally or numerically limited.

9. The method of any one of the previous Claims wherein the one or more computer readable medium may comprise a barcode such as, a QR code, the barcode may be captured using a camera comprised on the user computing device.

10. The method of Claim 9 wherein the barcode is captured from advertising displayed for example in print or television media.

11. The method of any one of the previous Claims wherein any request, token, confirmation, confirmation code or unique token identification may be encrypted.

12. The method of Claim 11 wherein the encryption may comprise Public IUKey or Public OUKey.

13. The method of any one of the previous Claims wherein the sending and receiving is performed through an application stored on the mobile computing device or through a mobile communications system such as, SMS (short messaging service), Bluetooth or NFC (Near Field Communication).

14. The method of any one of the previous claims wherein the method is for authorising a service.

15. The method of claim 14 wherein the service comprises: a governmental service; a professional service; a trade service; a healthcare service; or a childcare and/or education service.

16. The method of any one of the previous Claims wherein the one or more stored or acquired factors comprises a device unique identifier (DU-ID).

17. A method for transferring an electronic cash token comprising:

receiving a cash-to request comprising the electronic cash token or a unique token identification associated with the electronic cash token, one or more user computing device factors, a Device Unique Identifier (DU-ID) associated with a current owner of the electronic cash token and a recipient mobile telephone number;

validating cash token ownership by matching the electronic cash token or the unique token identification with an electronic database;

sending a cash-to token and a cash-to confirmation code to the mobile computing

device associated with the current owner;

receiving a cash-to confirmation comprising the cash-to confirmation code and the cash-to token;

matching the received cash-to confirmation code with the received cash-to token;

matching the one or more user computing device factors with one or more receiver device factors; and

transferring the electronic cash token by updating the electronic database to associate the electronic cash token with an account linked to the recipient mobile telephone number.

18. The method of Claim 17 wherein the one or more of the recipient mobile number, one or more user computing device factors and one or more receiver device factors are received at a different time to the cash-to request.

19. The method of Claim 17 or Claim 18 wherein the method further comprises recoding a computer readable medium associated with the electronic cash token.

20. A method of authorising cash dispensing comprising:

receiving a cash-out request comprising a cash token or a unique token identification associated with the electronic cash token and one or more receiver device factors from a cash dispenser;

sending a cash-out confirmation code to an owner of the cash token and storing the cash-out confirmation code in an electronic database;

receiving from the cash dispenser a cash-out confirmation comprising the cash-out confirmation code;

receiving from the owner of the cash token one or more user computing device factors;

matching the received cash-out confirmation code with the stored cash-out confirmation code;

matching the user computing device factors with one or more stored or acquired receiver device factors; and

sending a cash-out authorisation to the cash dispenser authorising the dispensing of cash.

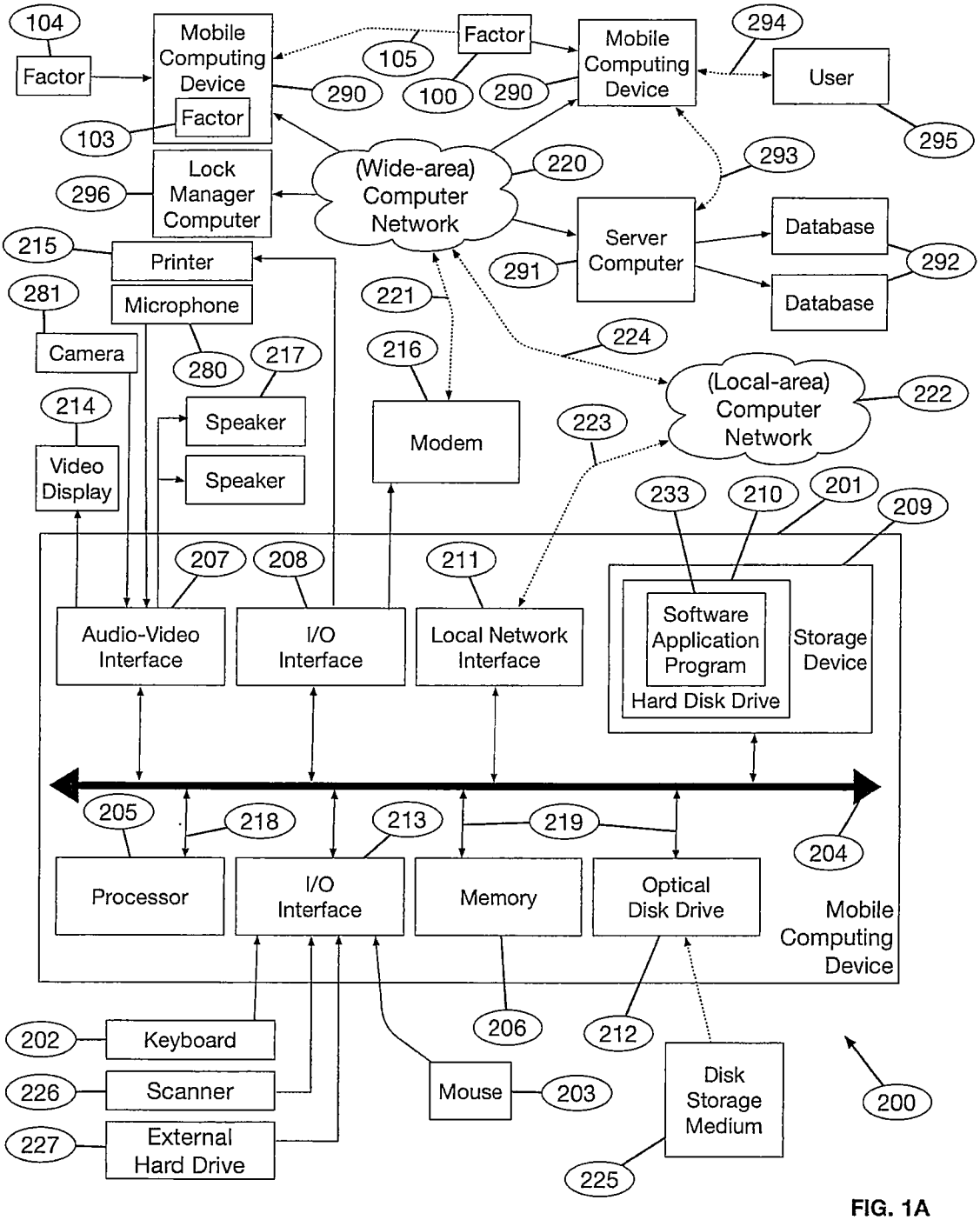
104
Factor
Mobile Computing Device
Factor
103
105
Factor
290
100
290
Mobile Computing Device
294
User
295
293
Lock Manager Computer
296
(Wide-area) Computer Network
220
Server Computer
Database
Database
292
291
215
Printer
281
Microphone
221
224
Camera
280
217
216
(Local-area) Computer Network
222
214
Speaker
Modem
223
Video Display
Speaker
233
210
201
209
207
208
211
Audio-Video Interface
I/O Interface
Local Network Interface
Software Application Program
Hard Disk Drive
Storage Device
205
218
213
219
204
Processor
I/O Interface
Memory
Optical Disk Drive
Mobile Computing Device
202
Keyboard
206
212
226
Scanner
Mouse
203
Disk Storage Medium
200
227
External Hard Drive
225

FIG. 1A

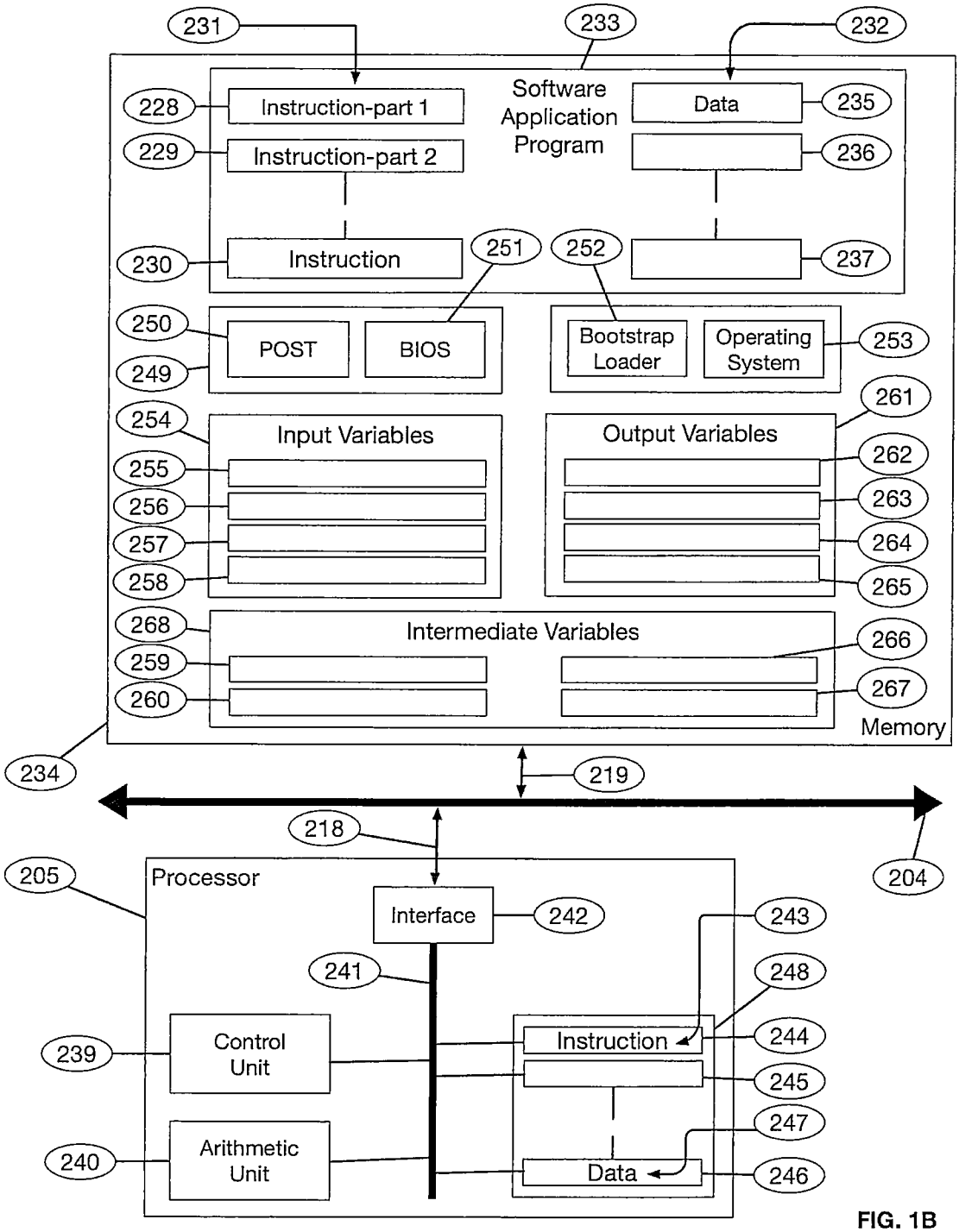
231
233
232
228
Instruction-part 1
Software Application Program
Data
235
229
Instruction-part 2
236
230
Instruction
251
252
237
250
POST
BIOS
Bootstrap Loader
Operating System
253
249
254
Input Variables
Output Variables
261
255
262
256
263
257
264
258
265
268
Intermediate Variables
266
259
267
260
Memory
234
219
218
204
205
Processor
Interface
242
243
241
248
239
Control Unit
Instruction
244
245
247
240
Arithmetic Unit
Data
246

FIG. 1B

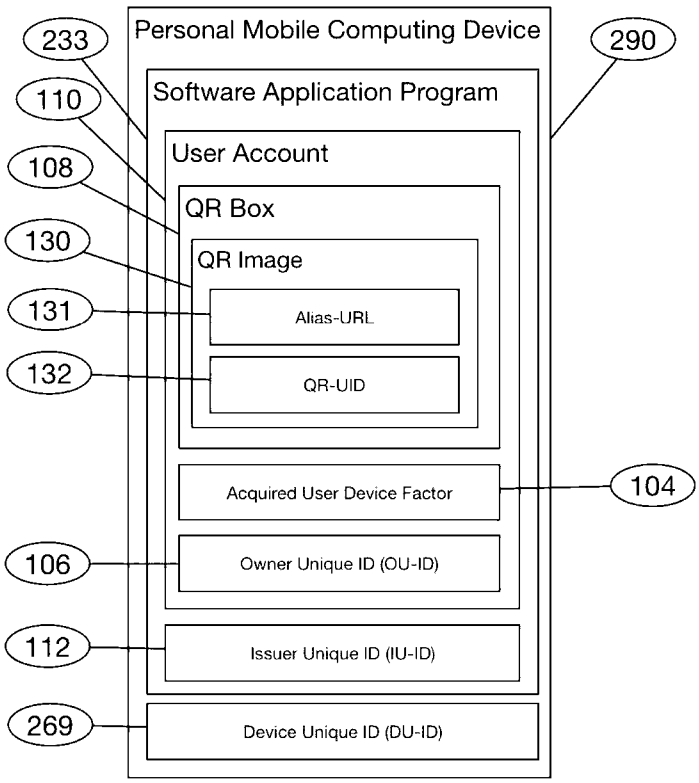

FIG. 2A

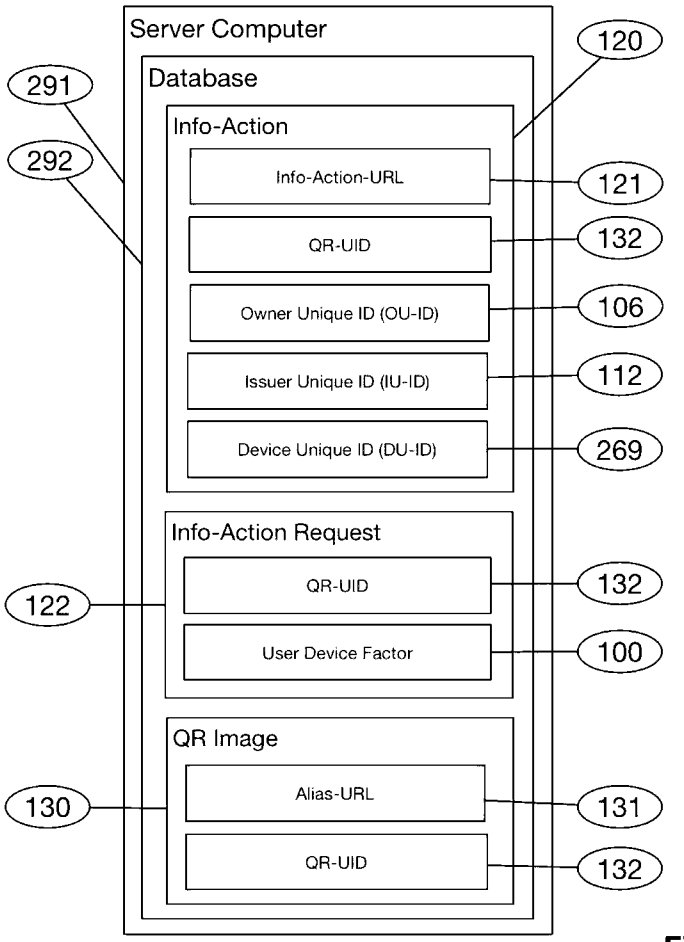

FIG. 2B

Figure 2

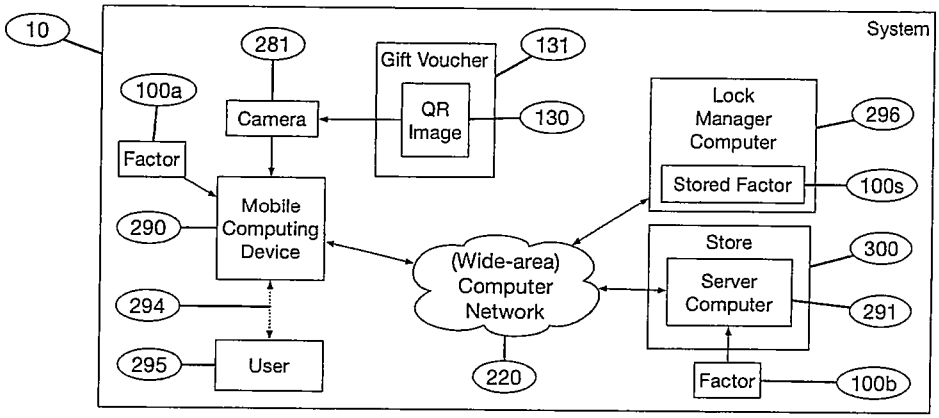

FIG. 3A

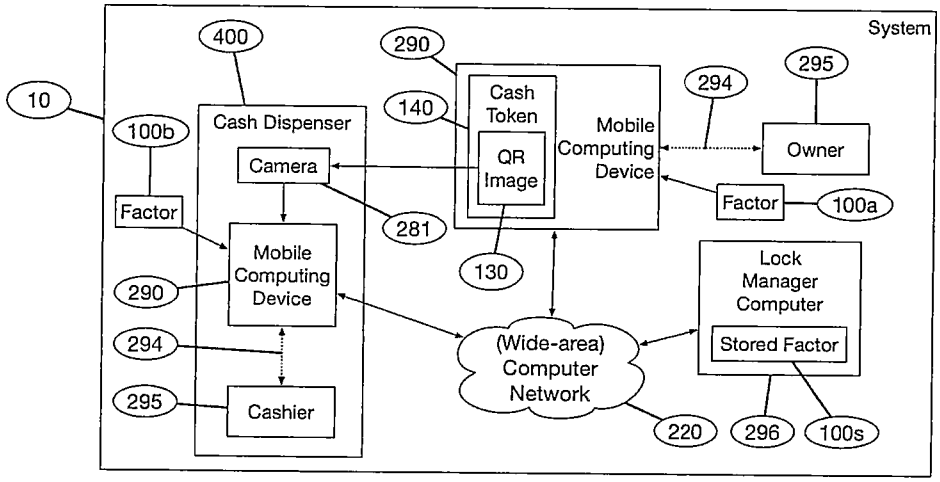

FIG. 3B

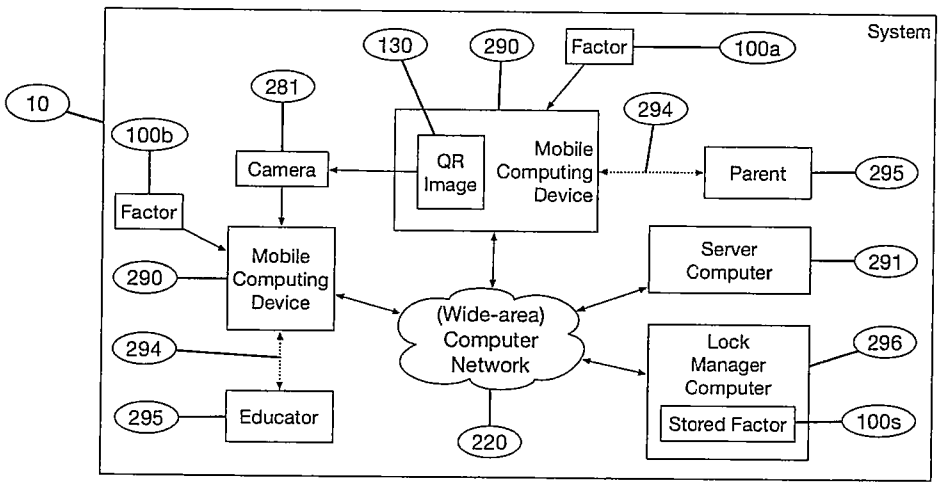

FIG. 3C

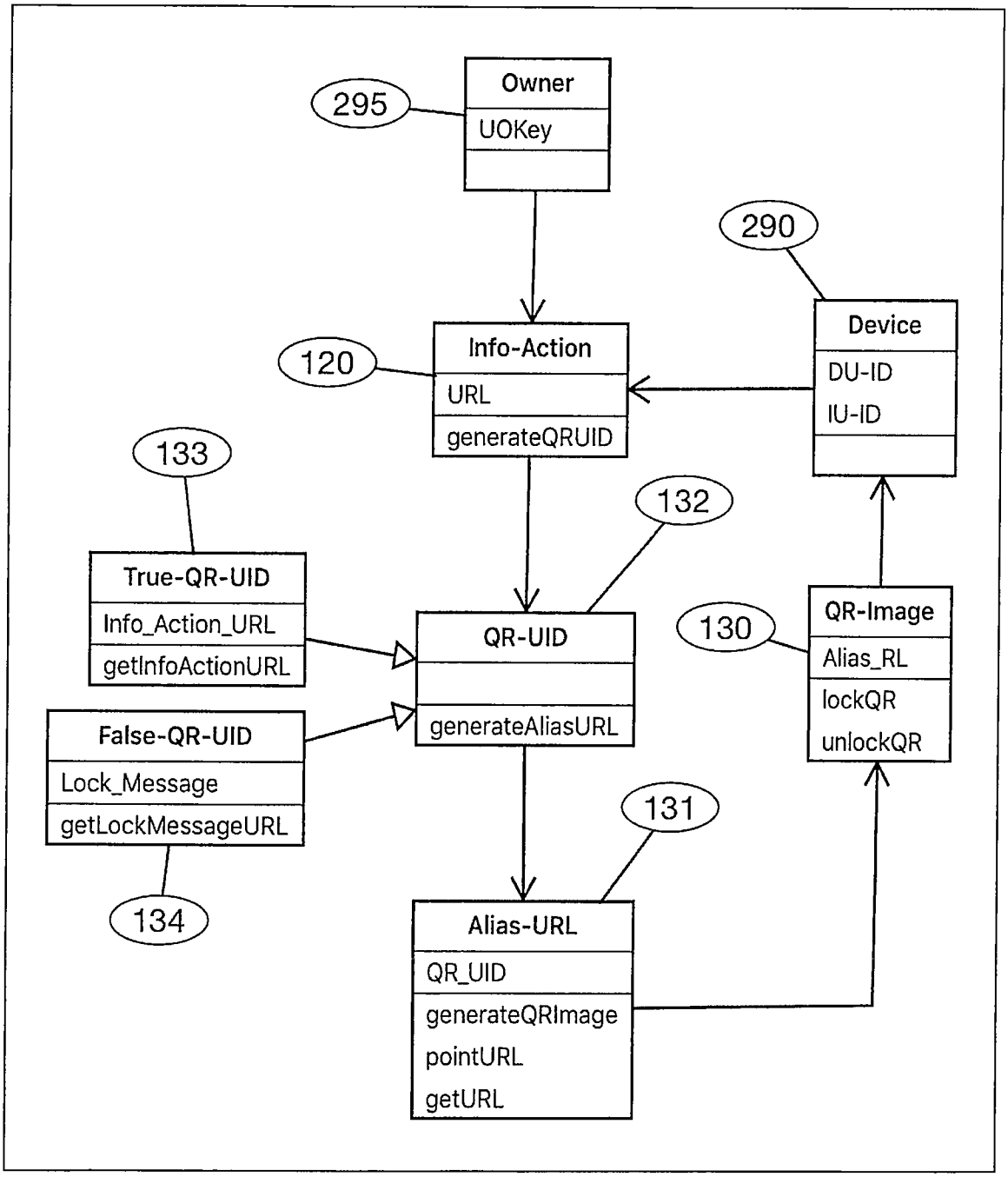
Owner
UOKey
295
290
Device
DU-ID
IU-ID
Info-Action
URL
generateQRUID
120
133
132
True-QR-UID
Info_Action_URL
getInfoActionURL
QR-UID
generateAliasURL
130
QR-Image
Alias_RL
lockQR
unlockQR
False-QR-UID
Lock_Message
getLockMessageURL
131
134
Alias-URL
QR_UID
generateQRImage
pointURL
getURL

FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2015/000759

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/10 (2013.01) G06F 21/30 (2013.01) G06Q 20/04 (2012.01) G06Q 20/36 (2012.01)

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)

EPOQUE INTERNAL (WPIAP): IPC (G06F21/IC), search terms (transact+, lock+, de_activat+, match+, authen+, author+, verif+, time, date?, location+, position+) & like terms; EPOQUE INTERNAL (WPIAP): search terms (e_currenc+, electronic, money, e_cash+, unique, identi+, user?, owner?, device?, mobile+, serial, number+, token?, match+, compar+, factor?, authent+, recei+, time+, position+, confirm+, valid+, authoris+, un_lock+ , send+, transfer+, receiv+, recipient?, tell+, machin+, dispens+) & like terms; GOOGLE PATENTS: transaction, time, location, match, identifier, authorized, POS, equipment, id, enable, activate, unlock, disabled, deactivate, lock; GOOGLE PATENTS: multi, factor, authentication, location, time, gps, transaction, matching, electronic, money; GOOGLE PATENTS: mobile, phone, transaction, verification, enable, disable, computer, pos, reader, factors, time, location; GOOGLE: transfer, identifier, qr, code, dispense, atm; ESPACENET: Inventor & Applicant name search; AUSPAT: Inventor & Applicant name search; IP Australia's internal databases (NOSE, INTESS): Inventor & Applicant name search.

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
28 January 2016	28 January 2016
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 Thong AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. +61 262832128

INTERNATIONAL SEARCH REPORT C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		International application No. **PCT/AU2015/000759**
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/0187492 A1 (GRAVES et al.) 16 August 2007 Paragraphs 4, 28, 31, 46, 50, 51, 53, 56, 69, 72 and figure 1 in particular.	1-16
X	US 2002/0108062 A1 (NAKAJIMA et al.) 08 August 2002 Paragraphs 173, 205 to 206, 209, 211 to 215, 222, 264, figure 20 and figures 24 to 25 in particular.	1-16
A	WO 2014/158817 A1 (FEXCO MERCHANT SERVICES) 02 October 2014	
A	US 2011/0202466 A1 (CARTER) 18 August 2011	
A	WO 2012/027585 A2 (AMERICAN CASH EXCHANGE, INC.) 01 March 2012	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2015/000759

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.:
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:

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:

See Supplemental Box for Details

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 III**

This International Application does not comply with the requirements of unity of invention because it does not relate to one invention or to a group of inventions so linked as to form a single general inventive concept. This Authority has found that there are three different inventions based on the following features that separate the claims into distinct groups:

- Claims 1 to 16 are directed to an arrangement for unlocking a computer readable medium or an electronic process using a computer readable medium which features the reception of a request to use a locked computer readable medium or a locked electronic process using a computer readable medium from a user computing device, the matching of one or more stored or acquired factors with at least one other stored or acquired factors to verify the user computing device, the unlocking of the computer readable medium or electronic process using a computer readable medium if a match results and the utilisation of the unlocked computer readable medium or unlocked electronic process using the computer readable medium to complete a transaction. The feature of an arrangement for unlocking a computer readable medium or an electronic process using a computer readable medium is specific to this group of claims.

- Claims 17 to 19 are directed to an arrangement for transferring an electronic cash token which features receiving a cash–to request comprising the electronic cash token or a unique token identification associated with the electronic cash token, one or more user computing device factors, a Device Unique Identifier (DU–ID) associated with a current owner of the electronic cash token and a recipient mobile telephone number, validating cash token ownership by matching the electronic cash token or the unique token identification with an electronic database, sending a cash–to token and a cash–to confirmation code to the mobile computing device associated with the current owner, receiving a cash–to confirmation comprising the cash–to confirmation code and the cash–to token, matching the received cash–to confirmation code with the received cash–to token, matching the one or more user computing device factors with one or more receiver device factors and transferring the electronic cash token by updating the electronic database to associate the electronic cash token with an account linked to the recipient mobile telephone number. The feature of an arrangement for transferring an electronic cash token is specific to this group of claims.

- Claim 20 is directed to an arrangement for authorising cash dispensing which features receiving a cash–out request comprising a cash token or a unique token identification associated with the electronic cash token and one or more receiver device factors from a cash dispenser, sending a cash–out confirmation code to an owner of the cash token and storing the cash–out confirmation code in an electronic database, receiving from the cash dispenser a cash–out confirmation comprising the cash–out confirmation code, receiving from the owner of the cash token one or more user computing device factors, matching the received cash–out confirmation code with the stored cash–out confirmation code, matching the user computing device factors with one or more stored or acquired receiver device factors and sending a cash–out authorisation to the cash dispenser authorising the dispensing of cash. The feature of an arrangement for authorising cash dispensing is specific to this claim.

PCT Rule 13.2, first sentence, states that unity of invention is only fulfilled when there is a technical relationship among the claimed inventions involving one or more of the same or corresponding special technical features. PCT Rule 13.2, second sentence, defines a special technical feature as a feature which makes a contribution over the prior art.

When there is no special technical feature common to all the claimed inventions there is no unity of invention.

In the above groups of claims, the identified features may have the potential to make a contribution over the prior art but are not common to all the claimed inventions and therefore cannot provide the required technical relationship. Therefore there is no special technical feature common to all the claimed inventions and the requirements for unity of invention are consequently not satisfied a priori.

This Authority believes that a search and examination for the additional inventions will not involve more than negligible additional search and examination effort over that for the first invention and so no additional search fee is required in order to search and examine the additional inventions.

INTERNATIONAL SEARCH REPORT Information on patent family members	International application No. **PCT/AU2015/000759**

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 2007/0187492 A1	16 August 2007	US 2007187492 A1	16 Aug 2007
		US 7578439 B2	25 Aug 2009
		AU 2002336770 A1	07 Apr 2003
		AU 2006246462 A1	21 Jun 2007
		AU 2006246462 B2	07 May 2009
		AU 2008200269 A1	21 Aug 2008
		AU 2008200269 B2	01 Jul 2010
		BR PI0414135 A	31 Oct 2006
		CA 2457087 A1	03 Apr 2003
		CA 2480353 A1	05 Mar 2005
		CA 2487194 A1	14 May 2005
		CA 2487196 A1	13 May 2005
		CA 2487197 A1	14 May 2005
		CA 2537445 A1	17 Mar 2005
		CA 2569403 A1	01 Jun 2007
		CA 2618235 A1	07 Aug 2008
		CA 2681997 A1	02 Oct 2008
		CN 1975776 A	06 Jun 2007
		CN 1998019 A	11 Jul 2007
		CN 101256653 A	03 Sep 2008
		CN 101641703 A	03 Feb 2010
		EP 1442404 A2	04 Aug 2004
		EP 1442404 B1	01 Jan 2014
		EP 1522972 A2	13 Apr 2005
		EP 1531416 A1	18 May 2005
		EP 1534043 A2	25 May 2005
		EP 1534043 B1	05 Jan 2011
		EP 1690151 A2	16 Aug 2006
		EP 1806705 A1	11 Jul 2007
		EP 1956542 A2	13 Aug 2008
		EP 2135191 A1	23 Dec 2009
		GB 2408373 A	25 May 2005
		GB 2408373 B	26 Mar 2008
		IL 174065 A	31 Aug 2011
		JP 2007509381 A	12 Apr 2007
		JP 5021306 B2	05 Sep 2012

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/AU2015/000759**

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**
		JP 2010182320 A	19 Aug 2010
		JP 5265602 B2	14 Aug 2013
		JP 2010522927 A	08 Jul 2010
		JP 5307115 B2	02 Oct 2013
		JP 2005505033 A	17 Feb 2005
		JP 2007179539 A	12 Jul 2007
		JP 2008204448 A	04 Sep 2008
		KR 20070057668 A	07 Jun 2007
		KR 20080074039 A	12 Aug 2008
		MX PA04002541 A	31 May 2004
		MX PA04008647 A	12 Jan 2006
		MX PA04011153 A	26 Oct 2005
		MX PA04011154 A	26 Oct 2005
		MX PA04011155 A	26 Oct 2005
		MX PA06002448 A	20 Jun 2006
		MX PA06013922 A	16 Oct 2008
		MX 2008001521 A	24 Feb 2009
		MX 2009010274 A	13 Oct 2009
		US 6575361 B1	10 Jun 2003
		US 2004195316 A1	07 Oct 2004
		US 6918537 B2	19 Jul 2005
		US 2005060248 A1	17 Mar 2005
		US 7028891 B2	18 Apr 2006
		US 2003205616 A1	06 Nov 2003
		US 7083084 B2	01 Aug 2006
		US 2004118914 A1	24 Jun 2004
		US 7093761 B2	22 Aug 2006
		US 2004129777 A1	08 Jul 2004
		US 7168615 B2	30 Jan 2007
		US 2007118478 A1	24 May 2007
		US 7292998 B2	06 Nov 2007
		US 2006255135 A1	16 Nov 2006
		US 7293704 B2	13 Nov 2007
		US 2004153402 A1	05 Aug 2004
		US 7311249 B2	25 Dec 2007
		US 2004133511 A1	08 Jul 2004

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/AU2015/000759**

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 7328190 B2	05 Feb 2008
		US 2003172031 A1	11 Sep 2003
		US 7333955 B2	19 Feb 2008
		US 2007118477 A1	24 May 2007
		US 7437328 B2	14 Oct 2008
		US 2006161490 A1	20 Jul 2006
		US 7630926 B2	08 Dec 2009
		US 2005107068 A1	19 May 2005
		US 7991386 B2	02 Aug 2011
		US 2010049617 A1	25 Feb 2010
		US 8244612 B2	14 Aug 2012
		US 2010235249 A1	16 Sep 2010
		US 8655309 B2	18 Feb 2014
		US 2005051619 A1	10 Mar 2005
		US 8706630 B2	22 Apr 2014
		US 8751401 B1	10 Jun 2014
		US 2014166748 A1	19 Jun 2014
		US 2007094129 A1	26 Apr 2007
		US 2008020734 A1	24 Jan 2008
		US 2008052108 A1	28 Feb 2008
		US 2010124912 A1	20 May 2010
		US 2011068168 A1	24 Mar 2011
		US 2011071913 A1	24 Mar 2011
		US 2014054375 A1	27 Feb 2014
		WO 03027805 A2	03 Apr 2003
		WO 2005024591 A2	17 Mar 2005
		WO 2008118175 A1	02 Oct 2008

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/AU2015/000759**

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 2002/0108062 A1	08 August 2002	US 2002108062 A1	08 Aug 2002
		CN 1381008 A	20 Nov 2002
		EP 1286285 A1	26 Feb 2003
		TW 589855 B	01 Jun 2004
		WO 0188790 A1	22 Nov 2001
WO 2014/158817 A1	02 October 2014	WO 2014158817 A1	02 Oct 2014
		US 2014263618 A1	18 Sep 2014
US 2011/0202466 A1	18 August 2011	US 2011202466 A1	18 Aug 2011
		AU 2009305365 A1	22 Apr 2010
		EP 2350941 A1	03 Aug 2011
		EP 2491523 A1	29 Aug 2012
		LU 91488 A1	19 Apr 2010
		LU 91679 A1	20 Apr 2011
		RU 2011119760 A	27 Nov 2012
		US 2012208557 A1	16 Aug 2012
		WO 2010043722 A1	22 Apr 2010
		WO 2011048106 A1	28 Apr 2011
WO 2012/027585 A2	01 March 2012	WO 2012027585 A2	01 Mar 2012
		CA 2845801 A1	01 Mar 2012
		CN 103180868 A	26 Jun 2013
		EP 2609549 A2	03 Jul 2013
		MX 2013002228 A	28 Oct 2013
		RU 2013112668 A	27 Sep 2014
		US 2013151418 A1	13 Jun 2013

End of Annex

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