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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 September 2012 (13.09.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/120253 A1

(51) International Patent Classification: *H04L 29/06* (2006.01)

(21) International Application Number: PCT/GB2012/000206

(22) International Filing Date: 1 March 2012 (01.03.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1103737.1 4 March 2011 (04.03.2011) GB

(71) Applicant *(for all designated States except US)*: **INTERCEDE LIMITED** [GB/GB]; Lutterworth Hall, St. Mary's Road, Lutterworth, Leicestershire, LE17 4PS (GB).

(72) **Inventor; and**

(75) **Inventor/Applicant** *(for US only)*: **EDWARDS, Christopher Paul** [GB/GB]; 5 Ancaster Gardens, Wollaton, Nottingham, Nottinghamshire, NG8 1FR (GB).

(74) **Agents**: **WALLIS, Helen** et al.; Olswang LLP, 90 High Holborn, WC1V 6XX (GB).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR TRANSFERRING DATA

(57) Abstract: A method and apparatus for transferring data to a mobile device is described. In an embodiment, authentication information associated with a user is received and used to authenticate the user. A one-time-use password is determined and an identity of a mobile device and/or a mobile device operator is verified. Encrypted data is transmitted to the mobile device, where the encryption is based, at least in part, on the one-time-use password. On receipt of the password at the mobile device, the data may be decrypted for use by the mobile device.

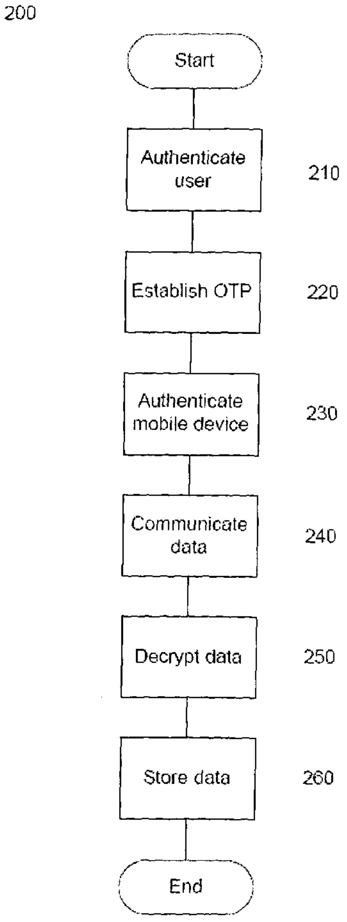

Fig. 2

HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

Method and Apparatus for Transferring Data

Background

[0001] It is often desired to transfer data to mobile devices, such as telephones, personal digital assistants etc. However, securely transferring data to such devices can be problematic.

[0002] The embodiments described below are not limited to implementations which solve any or all of the disadvantages of known methods and systems for transferring data.

Summary

[0003] The following presents a simplified summary of the disclosure in order to provide a basic understanding to the reader. This summary is not an extensive overview of the disclosure and it does not identify key/critical elements or delineate the scope of the specification. Its sole purpose is to present a selection of concepts disclosed herein in a simplified form as a prelude to the more detailed description that is presented later.

[0004] A method and apparatus for transferring data to a mobile device is described. In an embodiment, authentication information associated with a user is received and used to authenticate the user. A one-time-use password is determined and an identity of a mobile device and/or a mobile device operator is verified. Encrypted data is transmitted to the mobile device, where the encryption is based, at least in part, on the one-time-use password. On receipt of the password at the mobile device, the data may be decrypted for use by the mobile device.

[0005] Many of the attendant features will be more readily appreciated as the same becomes better understood by reference to the following detailed description considered in connection with the accompanying drawings.

Brief Description of the Drawings

[0006] The present description will be better understood from the following detailed description read in light of the accompanying drawings, wherein:

Figure 1 shows a schematic diagram of an example system 100 for transferring data;

Figure 2 shows an example method of transferring data;

Figure 3 shows example communication flows;

Figure 4 shows an example data packet;

Figure 5 shows a further example method of transferring data; and

Figure 6 shows an exemplary computing-based device.

Detailed Description

[0007] The detailed description provided below in connection with the appended drawings is intended as a description of the present examples and is not intended to represent the only forms in which the present example may be constructed or utilized. The description sets forth the functions of the example and the sequence of steps for constructing and operating the example. However, the same or equivalent functions and sequences may be accomplished by different examples.

[0008] Figure 1 illustrates a system 100 for transferring data. The system 100 comprises a user 110, a client computer 120, a mobile device 130, one or more communication networks 140 and a server computer 150.

[0009] The user 110 may be a possessor of the mobile device 130 i.e. a person to whom the mobile device belongs or is assigned. However, the various embodiments described herein are not limited in this respect. The user 110 may be, for example, an administrator of the mobile device 130, such as a person responsible within an organisation for ensuring that the mobile device 130 has any necessary data stored thereon for use by one or more other persons. In some embodiments, information associated with the user is stored in a user profile 151 accessible to the server 150, as will be explained.

[0010] In some embodiments, the user 110 is in possession or is associated with a smart card or token 115. The smart card 115 is used in some embodiments to enable authentication of the user 110 to the server 150.

[0011] The client computer 120 is a computer via which the user 110 authenticates with the server 150. In some embodiments, however, the client computer 120 and server 150 are the same machine. That is, the user 110 may directly access the server 150, without the client computer 120, to transfer data to the mobile device 130. As noted above, the authentication may involve presentation of the smart card 115 to the client computer 120, in some embodiments, such as by being received in a communication port or reader of the client computer 120. However, in other embodiments the client computer 120 may receive one or more items of authentication information from the user 110, such as via data entry to a keyboard of the client computer 120. The authentication may alternatively or additionally involve the client computer 120 receiving information indicating one or more biometric characteristics of the user, such as fingerprint, iris recognition, etc.

[0012] Although the client computer 120 is shown in Figure 1 as a desktop computer, it will be understood that this is by way of example only and is not a limitation. The client computer 120 may be any type of device which allows an identity of the user to be verified by the server 150. In some embodiments, the client computer 120 has a separate communication path to the server 150 than the mobile device 130 i.e. the client computer 120 and the mobile device 130 communicate data with the server 150 via paths which are at least partly separate. The client computer 120 may be, for example, a computer kiosk which the user 110 accesses to request data be transferred to the mobile device 130. In embodiments wherein the user 110 utilises the smart card 115, the client computer 120 includes an interface arranged to facilitate communication between the smart card 115 and the client computer 120. The interface may be contact-based, for example it may comprise physical contacts for engaging with terminals of the smart card 115, or the interface may be contactless, such as utilising induction based communication techniques.

[0013] The mobile device 130 may be any type of mobile device. In particular, although not exclusively, the mobile device 130 may be any of a mobile telephone, a smart phone, personal digital assistant, tablet computer, or the like. In some embodiments, the mobile device 130 includes a software module or component 131. The software module 131 may be a Java applet which is stored on the mobile device 130 prior to executing a method according to an embodiment described herein. For example, the software module 131 may be downloaded to the mobile device 130 from the server 150 or from another source, such as an application store or other repository of applications.

[0014] In Figure 1, the communication network 140 is shown as being a single entity, such as the Internet. However, it is envisaged that in some embodiments, the communications network will comprise a plurality of communication networks. For example, it is envisaged that the client computer 120 will communicate data with the server computer via one or more computer networks, such as over an IP protocol, whilst the mobile device 130 will communicate data with the server 150, at least partly, over a mobile communication network, such as GPRS, GSM, 3G standards such as UMTS, 4G standards such as LTE-Advanced, mobile WiMAX (IEEE 802.16e-2005) or the like.

[0015] The server computer 150 may be any type of computer system capable of implementing a method of transferring data as described herein. Although the server 150 is shown in Figure 1 as a single computer, this is merely for illustration and the server computer 150 may comprise a plurality of computer systems and/or a computer system having multiple processors etc. The server 150 is communicatively coupled to the client computer 120 and mobile device 130 to authenticate the user 110 via the client computer 120 and the mobile device 130, and then send data to the mobile device 130 for storage in a location which is accessible to the mobile device 130, as will be explained. In some embodiments, the server 150 has access to one or more stores 151, 152. In some embodiments, the store may store user information 151 associated with one or more users of the system 100. In some embodiments the user information 151 comprises one or more user records including a user record associated with the user 110 of the system. The user records 151 may store identification information of each user, such as name and contact details. The user information 151 may also include, in some embodiments, mobile device 130 identification information (MDID). The MDID may be any information which uniquely identifies the mobile device 130, such as a telephone number or IP address of the mobile device 130. The store may also hold data 152 which is to be securely communicated to the mobile device.

[0016] In various embodiments utilising the smart card 115, the smart card 115 is a device for authenticating the user 110. The smart card 115 or integrated circuit card may be a device issued to the user 110 which comprises a memory portion and a logic portion (not shown for clarity). The memory portion may comprise one or more items of data which enable the server 150 to verify the identity of the user 110, such as encryption keys and/or certificates. The logic may be logic for enabling a device, such as the client computer 120, to decrypt received data using the encryption key(s) stored in the memory portion.

[0017] A method of transferring data will now be described with reference to Figures 2 and 3 in particular.

[0018] Figure 2 illustrates an example method 200 of transferring data. As shown in Figure 2, a step 210 comprises authenticating the user 110. As discussed above, the user 110 may be authenticated to the server 150 in a variety of ways. In one embodiment, the user 110 is authenticated by multi-factor authentication using the smart card 115. The multi-factor authentication may be two-factor authentication involving use of the smart card and authentication information such as a password or PIN. Alternatively, bioinformatics may be used as a factor of the authentication process.

[0019] Figure 3 illustrates authentication information, such as the PIN and smart card, being provided 310 from the user 110 to the client 120. The PIN may be used to authenticate to the smart card to generate authentication information which is then sent from 311 the client computer 120 to the server 150. However, it will be realised that step 210 may also involve communication of data from the server 150 to the client computer 120 and from the client computer 120 to the user 110. For example, in some embodiments, the server 150 may provide a logon screen, such as a secure web page, which requests a user to enter a logon ID and password i.e. such embodiments may not require the smart card 115. In response, the user enters their user ID and password into the client computer 120 which communicates this data to the server 150, thus step 210 may involve bi-directional communication which is not specifically illustrated in Figure 2. Following receipt of the authentication information 311 by the server 150, the server communicates an authentication response 312 to the client computer. The authentication response indicates whether the authentication information has been verified by the server 150. In response, the client computer 120 may output 313 an authentication response 313 to the user 110, such as indicating on a display of the client computer 120 that the authentication has been successful.

[0020] Step 220 comprises establishing a one-time password (OTP) between the user 110 and server 150. In some embodiments, the OTP may be established by the client computer 120 outputting a request for the OTP to the user 110 and receiving 320 the OTP from the user 110, which is then transmitted 321 to the server 150 from the client computer 120. In some embodiments, although not necessarily, the server 150 may verify that the OTP is unique i.e. has not been used previously by the user 110.

[0021] In other embodiments indicated with dashed lines in Figure 3, the server 150 may generate the OTP which is then communicated 325 to the client computer 120 and output 326, for example on a display, to the user 110. The OTP may be communicated to the client computer 120 in a variety of way, such as part of a web page forming the authentication process which is displayed to the user. In still further embodiments, the OTP may be generated by the server 150 and communicated to the user via other means, such as by email, by post in printed form or to their mobile device 130 such as in a text, SMS message or using another notification service. Therefore it will be realised that steps 210 and 220 shown in Figure 2 may take place in any order.

[0022] In step 230 the mobile device is authenticated. In some embodiments, the operator of the mobile device may alternatively or additionally be authenticated. The mobile device is authenticated to confirm the identity of the mobile device 130. As part of step 150, the server 150 generates a reference for the data transfer. In some embodiments, the reference is unique or substantially unique i.e. will not be reused for a considerable period of time. The reference is then communicated 330 to the mobile device 130, as shown in Figure 3. The reference may be communicated to the mobile device in a variety of ways. In some embodiments, the reference is communicated to the mobile device in a text or SMS message to the telephone number of the mobile device which is retrieved from the user profile associated with the user 110 authenticated in step 210. In other embodiments, the reference may be communicated 330 to the mobile device 130 in an email, using an alternative notification service, or via another communication protocol. The reference may be communicated to the mobile device 130 as a data packet 400, as shown in Figure 4. The data packet 400 includes a header portion 410 and a data portion 420 comprising the reference generated by the server 150. The header portion 410 may be used to automatically activate an authentication module or software component on the mobile device 130, as explained below. The user of the mobile device 130 may be asked to enter a value, such as a password known to the server, which is also sent to the server 150 to verify the identity of the user of the mobile device 130.

[0023] In response to receiving the reference 420 at the mobile device 130, the authentication module or software component 131, such as a Java applet, (herein all referred to as remote agent 131) may be executed. The remote agent 131 may be executed on the mobile device 130 in response to a user input at the mobile device 130 i.e. the user may manually activate the remote agent 131, such as by activating a menu option or graphical icon on a user interface of the mobile device 130, or the remote agent 131 may be automatically activated in response to the mobile device 130 detecting the received header 410 of a predetermined format.

[0024] Once activated, the remote agent 131 on the mobile device 130 establishes communication with the server 150. The remote agent 131 may establish communication with a counterpart piece of authentication software executing on the server 150. The remote agent 131 5 may communicate with the server 150 over http or https, for example. The remote agent 131 is arranged to communicate 331, in some form, the reference 420 to the server 150. The reference 420 may be communicated to the server 150 in the form that it was received by the mobile device 130, with or without the header 410. In one embodiment, the remote agent 131 on the mobile device 130 is arranged to compute a hash value of the reference 420. The hash value is then communicated to the server 150, thereby enabling the server 150 to verify that the reference 420 was received by a device having an appropriate hash function. Furthermore, in some embodiments, the reference 420 may be combined with information derived from the mobile device 130 or remote agent 131 to further improve security. In one embodiment, the hash value is computed based on the received reference 420 and identification information of the remote agent 131, such as an ID or serial number thereof, thereby enabling the server 150 to verify the ID of the remote agent 131 and the reference 420.

[0025] In step 240, the server 150 communicates 340 encrypted data to the mobile device 130. The data is encrypted, at least in part, based on the OTP established in step 220.

[0026] In some embodiments, the data may also be encrypted based on other information, such as a username of the user 110 etc. In response to receiving the encrypted data, the remote agent 131 executing on the mobile device 130 requests that the user 110 enters 350 the OTP into the mobile device 130. For example, the remote agent 131 may cause a message to be displayed on a display of the mobile device 130 requesting that the user 110 enters 350 the OTP via a keypad of the mobile device 130. The user may also be requested to enter any further information required to decrypt the received data. The received OTP is then used to decrypt the received data in step 250. In some embodiments, the OTP may be entered 350 into the mobile device 130 prior to the encrypted data being received. In these embodiments, the mobile device 130 may communicate the OTP, or a value derived there from, to the server 150 in order to initiate the communication 340 of the encrypted data to the mobile device 130.

[0027] Once decrypted, the data is stored in a storage location or memory accessible to the mobile device 130. The data may be stored within a volatile or non-volatile memory accessible to the mobile device 130. The memory may be located within the mobile device 130, such as a built-in memory, or the memory may be a removable or external memory device, such as a memory card or external storage device. In some embodiments, the memory is located on a Subscriber Identity Module (SIM) card of the mobile device 130, or on another removable memory device, such as a micro-SD or a cryptographically protected memory card. In further embodiments, the data may be stored in another device which is, or may be periodically, communicably connected to the mobile device 130. Such devices may be those having a data storage portion, such as cameras, navigation devices etc. Such devices may communicate with the mobile device 130 at least periodically over a wired or wireless connection, such as Bluetooth or Wi-Fi, although these are merely exemplary. In some embodiments, the data may be stored in encrypted form and only decrypted using the OTP when required.

[0028] As a result of the method 200, data is securely transferred from the server 150 to the mobile device 130 and is stored in a location accessible to the mobile device 130 for later use by the mobile device 130.

[0029] Further embodiments will now be described with reference to Figure 5.

[0030] In order to improve security in computer systems, especially distributed computer systems where a client computer or device communicates with a remotely located server computer, users are often provided with a smart card or integrated chip card (ICC). A smart card typically comprises a memory storage component and logic. Frequently the memory storage component is used to hold one or more keys and/or certificates. The one or more keys may be public or private keys and the certificates may enable an identity of a person to be verified, as is known in the art. The smart card may be used in authenticating a holder to the computer system by inserting the smart card into a card reader communicatively coupled to the computer system. Once inserted into the card reader, the smart card may, for example, provide a decryption service for the computer system using the stored key and logic on the smart card. The stored keys may be used to decrypt received data, such as encrypted data received at the client computer from the server computer. The received data may be communication data, such as emails or other forms of communication data.

[0031] Often, users wish to utilise a smart card with a computing device, such as to access encrypted data with the device. For example, users may wish to read encrypted emails on the device. However, it is sometimes difficult or inconvenient for the device to access the smart card to utilise keys and/or certificates stored thereon to encrypt/decrypt data or to digitally sign data. One prior solution to this is the use of an external smart card reader. The external smart card reader connects to the device to provide an interface to the smart card. The smart card reader may connect to the device via a wired interface, such as via a USB connection, or via a wireless interface, such as Bluetooth. Some of the embodiments described herein reduce the problems associated with using security data, such as keys and/or certificates, with mobile computing devices, such as portable computers, tablet computers, mobile phones, personal digital assistants, smart phones etc.

[0032] An embodiment will now be described with reference to Figure 5 for transferring security data, such as keys and/or certificates, to a mobile device. The embodiment described with reference to Figure 5 may be used to transfer a copy of security data, such as one or more keys and/or certificates, stored on a smart card to a storage location accessible by the mobile device, thereby enabling the mobile device to perform security operations, such as encrypting/decrypting data, without requiring the mobile device to communicate with the smart card.

[0033] This embodiment is similar in operation to that previously described with reference to Figures 1-4 so, unless otherwise stated, the details provided above with respect to those Figures apply to the embodiment of Figure 5. Figure 5 shows a method 500 which may be implemented in a system 100 comprising a user 110, a client computer 120, a mobile device 130, one or more communication networks 140 and a server computer 150, as previously discussed with reference to Figure 1.

[0034] In step 510, the user 110 provides authentication information to the client computer 5 120. The authentication information may be, as previously described, a PIN and the smart card 115 being provided 310 from the user 110 to the client computer 120. The PIN may be utilised with the smart card 115 to generate authentication information which is sent from 511 the client computer 120 to the server 150. However in other embodiments, the user may enter a user ID and password into the client computer 120 which communicates 511 this data to the server 150 i.e. the authentication of the user 110 to the server may not involve the smart card 115. The user 110 may also provide the authentication information directly to the server computer, for example by inserting the smart card into a reader associated with the server 150, or by inputting information directly into the server 150, for example using a keyboard of the server computer.

[0035] Once having determined the authentication of the user, the server 150 communicates an authentication response 512 to the user via, in some embodiments, the client computer 120. The authentication response indicates whether the authentication information has been authenticated by the server 150. In response, the client computer 120 may output an authentication response 513 to the user 110, such as indicating on a display of the client computer 120 that the authentication has been successful.

[0036] A one-time password (OTP) is established between the user 110 and server 150. As discussed above, in some embodiments, the OTP may be established by the client computer 120 outputting a request for the OTP to the user 110 and receiving 520 the OTP from the user 110, which is then transmitted 521 to the server 150 from the client computer 120. However, in other embodiments indicated with dashed lines in Figure 5, the server 150 may generate the OTP which is then communicated 525 to the client computer 120 and output 526, for example on a display, to the user 110. In still further embodiments, the OTP may be generated by the server 150 and communicated to the user via other means, such as by email, by post in printed form or to their mobile device

130 such as in a text or SMS message or using another notification service. In these embodiments, the OTP is not necessarily communicated via the client computer 120.

[0037] The mobile device 130 is authenticated to confirm the identity of the mobile device 130. The server 150 generates a reference which, in some embodiments, is unique or substantially unique i.e. will not be reused for a considerable period of time. The reference is communicated 530 to the mobile device 130. The reference may be communicated to the mobile device 130 in a text or SMS message to the telephone number of the mobile device 130 which is retrieved from the user profile associated with the user 110. In other embodiments, the reference may be communicated 530 to the mobile device 130 in an email, or via another communication method or protocol (e.g. using an alternative notification service).

[0038] The reference may be communicated to the mobile device 130 as a data packet 400, as shown in and previously discussed with reference to Figure 4. The data packet 400 may include the header portion 410 and the data portion 420 comprising the reference.

[0039] In response to receiving the reference 420 at the mobile device 130, the remote agent 131 may be executed on the mobile device 130. The remote agent 131 may be manually or automatically activated on the mobile device 130. Once activated, the remote agent 131 establishes communication with the server 150 and is arranged to communicate 331, in some form, the reference 420 back to the server 150. The reference 420 may be communicated to the server 150 in the form that it was received or in a modified form, such as a hash value of the reference 420. In some embodiments, the reference 420 may be combined with information derived from the mobile device 130 or remote agent 131 to further improve security, as discussed above.

[0040] The server 150 communicates 540 encrypted security data, such as one or more keys and/or certificates, to the mobile device 130. The security data is encrypted, at least in part, based on the OTP. In some embodiments, the data may also be encrypted based on other information, such as a username of the user 110 etc. In response to receiving the encrypted data, the remote agent 131 executing on the mobile device 130 requests that the user 110 enters 550 the OTP into the mobile device 130. For example, the remote agent 131 may cause a message to be displayed on a display of the mobile device 130 requesting that the user 110 enters 550 the OTP via a keypad of the mobile device 130. The user may also be requested to enter any further information required to decrypt the received data. The received OTP is then used to decrypt the received security data.

[0041] Once decrypted, the security data is stored in a storage location or memory accessible to the mobile device 130, such as within a volatile or non-volatile memory accessible to the mobile device 130. The memory may be located within the mobile device 130, such as a built-in memory, or the memory may be a removable or external memory device, such as a memory card or external storage device. In some embodiments, the memory is located on a Subscriber Identity Module (SIM) card of the mobile device 130, or on another removable memory device, such as a micro-SD or a cryptographically protected memory card.

[0042] The security data may then be used by the mobile device 130 to perform security operations. For example, in cases where the security data comprises one or more keys (public or private keys) they may be used to encrypt and/or decrypt data. The data may be data received by and/or sent by the mobile device 130, such as communication data i.e. emails. The security data may also be used to digitally sign data in the cases that the security data comprises one or more digital certificates.

[0043] Figure 6 illustrates various components of an exemplary computing-based device 600 which may be implemented as any form of a computing and/or electronic device, and in which embodiments of the methods of transferring data described herein may be implemented. For example, any of the client computer 120, mobile device 130 and server computer 150 may be provided by computing-based devices in accordance with, or similar or related to, the exemplary device 600.

[0044] Computing-based device 600 comprises one or more processors 601 which may be microprocessors, controllers or any other suitable type of processors for processing computer executable instructions to control the operation of the device in order to implement aspects or all of one or more of the various embodiments described herein. In some examples, for example where a system on a chip architecture is used, the processors 601 may include one or more fixed function blocks (also referred to as accelerators) which implement a part of the method of transferring data in hardware (rather than software or firmware). Platform software comprising an operating system 602 or any other suitable platform software may be provided at the computing-based device to enable application software 603 to be executed on the device. The application software 603 may comprise software module 131, as described above, where the computing-based device 600 is a mobile device. Where the computing-based device 600 is a server, the application software 603 may comprise an authentication module arranged to authenticate the user and/or a verification module arranged to verify the identity of a mobile device and/or mobile operator.

[0045] The computer executable instructions may be provided using any computer-readable media that is accessible by computing based device 600. Computer-readable media may include, for example, computer storage media such as memory 604 and communications media. Computer storage media, such as memory 604, includes volatile and non-volatile, removable and non-removable media implemented in any method or technology for storage of information such as computer readable instructions, data structures, program modules or other data. Computer storage media includes, but is not limited to, RAM, ROM, EPROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other non-transmission medium that can be used to store information for access by a computing device. In contrast, communication media may embody computer readable instructions, data structures, program modules, or other data in a modulated data signal, such as a carrier wave, or other transport mechanism. As defined herein, computer storage media does not include communication media. Therefore, a computer storage medium should not be interpreted to be a propagating signal per se. Although the computer storage media (memory 604) is shown within the computing-based device 600 it will be appreciated that the storage may be distributed or located remotely and accessed via a network or other communication link (e.g. using communication interface 605). Memory 604 may also provide one or more data stores 610 (e.g. data stores 151 as described above, where computing-based device 600 is a server).

[0046] The communication interface 605 may be arranged to enable communication between the computing-based device 600 and other computing-based devices. For example, where the device 600 is a server, the communication interface 605 may be used to communicate with a mobile device via the network and where the device 600 is a mobile device, the communication interface 605 may be used to communicate with a server via the network.

[0047] The computing-based device 600 also comprises an input/output controller 606 arranged to output display information to a display device 607 which may be separate from or integral to the computing-based device 600. The display information may provide a graphical user interface. The input/output controller 606 is also arranged to receive and process input from one or more devices, such as a user input device 608 (e.g. a mouse, keyboard, camera, microphone or other sensor). In some examples the user input device 608 may detect voice input, user gestures or other user actions and may provide a natural user interface. This user input may be used to input the OTP or other information or data for use in the embodiments of transferring data. In an embodiment the display device 607 may also act as the user input device 608 if it is a touch sensitive display device. The input/output controller 606 may also output data to devices other than the display device, e.g. a locally connected printing device (not shown in FIG. 6).

[0048] The input/output control 606 may also be arranged to receive and output data from/to other devices, either internal or external to the computing-based device 600, for example smart-card reader 609.

[0049] Further aspects are set out in the following paragraphs:

[0050] An example comprises a method of transferring data to a mobile device, the method comprising: receiving authentication information associated with a user and authenticating the user based on the authentication information; determining a one-time use password; verifying an identity of a mobile device and/or a mobile device operator; transmitting encrypted data to the mobile device, the encryption based, at least in part, on the password; and receiving, at the mobile device, the password and decrypting the data for use by the mobile device.

[0051] The authentication information may be determined, at least in part, based on an encryption key. The encryption key may be stored in a smart card. The authentication information may be received from a client computer. The authentication information may be determined based, at least in part, on information received from a user.

[0052] The password may be received from a user or the password may be generated and output to the user. The password may be output on a display device (e.g. a display device of a client computer), as a printed document, or in an electronic message. The method may further comprise receiving the password at a server computer.

[0053] The identity of the mobile device may be verified by sending a message to the mobile device. This message may comprise a reference value (which may be generated by a server) and the method may further comprise receiving a response message from the mobile device based at least partly on the response value. In an example, the response message contains the reference value or a value determined according to the reference value. The message may be sent to the mobile device based on mobile device identification information associated with a user profile. In an example, the message is a short message service (SMS) message or an email.

[0054] The method may further comprise storing the data in a storage location accessible to the mobile device and in some examples, the data may be security data and in such an example, the security data may comprise one or more keys and/or certificates. These one or more keys may be used to decrypt or encrypt communication data received by the mobile device.

[0055] Another example comprises a server for sending data to a mobile device, wherein the server is arranged to: receive authentication data associated with a user and to authenticate the user based on the authentication data; determine a one-time-use password; verify an identity of a mobile device and/or mobile device operator; transmit encrypted data to the mobile device, the data being encrypted based, at least in part, on the password.

[0056] The authentication information may be at least partly received from a user. The authentication information may be received from a client computer. The authentication information may be determined, at least in part, based on an encryption key.

[0057] The one time use password may be determined by the server and output to a user. The server may be arranged to output the password on a display device or to communicate the password to another device for outputting the password to the user.

[0058] The server may be arranged to verify the identity of the mobile device by sending a message to the mobile device. The server may be arranged to generate a reference value and to include the reference value in the message. The server may be arranged to receive a response message from the mobile device and to compare a value derived from the response message against the generated reference value.

[0059] The server may be arranged to determine identification information of the mobile device and to send the message to the mobile device based on the identification information. The identification information may be determined from a user profile associated with the user.

[0060] The server may be arranged to encrypt the data based, at least in part, on the password. The data may be security data and in such an example, the server may be arranged to obtain the security data based on a user profile associated with the user. The security data may comprise one or more keys and/or certificates.

[0061] A further example comprises a computer system, the system comprising a server as described above and a mobile device. The mobile device may, for example, be one of a mobile telephone, a smart phone, a tablet computer or a portable computer.

[0062] The system and methods described above may, in some embodiments, be used to securely transfer data, such as security data, to mobile devices.

[0063] Computer software may be arranged to perform any of the methods described above when executed on a computer and this computer software may be stored on a computer readable medium.

[0064] The term 'computer' or 'computing-based device' is used herein to refer to any device with processing capability such that it can execute instructions. Those skilled in the art will realize that such processing capabilities are incorporated into many different devices and therefore the terms 'computer' and 'computing-based device' each include PCs, servers, mobile telephones (including smart phones), tablet computers, set-top boxes, media players, games consoles, personal digital assistants and many other devices.

[0065] It will be appreciated that embodiments described herein can be realised in the form of hardware, software or a combination of hardware and software. Any such software may be stored in the form of tangible (or non-transitory) volatile or non-volatile storage such as, for example, a storage device like a ROM, whether erasable or rewritable or not, or in the form of memory such as, for example, RAM, memory chips, device or integrated circuits or on an optically or magnetically readable medium such as, for example, a CD, DVD, magnetic disk or magnetic tape. These examples of tangible (or non-transitory) storage media do not include propagated signals. Propagated signals may be present in tangible storage media, but propagated signals per se are not examples of tangible storage media. It will be appreciated that the storage devices and storage media are embodiments of machine-readable storage that are suitable for storing a program or programs that, when executed, implement embodiments described herein. Accordingly, embodiments provide a program comprising code for implementing a system or method as described herein when the code is run on a computer and tangible machine readable storage storing such a program. The software can be suitable for execution on a parallel processor or a serial processor such that the method steps may be carried out in any suitable order, or simultaneously.

[0066] This acknowledges that software can be a valuable, separately tradable commodity. It is intended to encompass software, which runs on or controls “dumb” or standard hardware, to carry out the desired functions. It is also intended to encompass software which “describes” or defines the configuration of hardware, such as HDL (hardware description language) software, as is used for designing silicon chips, or for configuring universal programmable chips, to carry out desired functions.

[0067] Those skilled in the art will realize that storage devices utilized to store program instructions can be distributed across a network. For example, a remote computer may store an example of the process described as software. A local or terminal computer may access the remote computer and download a part or all of the software to run the program. Alternatively, the local computer may download pieces of the software as needed, or execute some software instructions at the local terminal and some at the remote computer (or computer network). Those skilled in the art will also realize that by utilizing conventional techniques known to those skilled in the art that all, or a portion of the software instructions may be carried out by a dedicated circuit, such as a DSP, programmable logic array, or the like.

[0068] All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive. The steps of the methods described herein may be carried out in any suitable order, or simultaneously where appropriate. Additionally, individual blocks may be deleted from any of the methods without departing from the spirit and scope of the subject matter described herein. Aspects of any of the examples described above may be combined with aspects of any of the other examples described to form further examples without losing the effect sought.

[0069] Each feature disclosed in this specification (including any accompanying claims, abstract and drawings), may be replaced by alternative features serving the same, equivalent or similar purpose, or altered or extended unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a generic series of equivalent or similar features.

[0070] Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims.

[0071] It will be understood that the benefits and advantages described above may relate to one embodiment or may relate to several embodiments. The embodiments are not limited to those that solve any or all of the stated problems or those that have any or all of the stated benefits and advantages. It will further be understood that reference to 'an' item refers to one or more of those items.

[0072] The term 'comprising' is used herein to mean including the method blocks or elements identified, but that such blocks or elements do not comprise an exclusive list and a method or apparatus may contain additional blocks or elements.

[0073] It will be understood that the above description is given by way of example only and that various modifications may be made by those skilled in the art. The above specification, examples and data provide a complete description of the structure and use of exemplary embodiments. Although various embodiments have been described above with a certain degree of particularity, or with reference to one or more individual embodiments, those skilled in the art could make numerous alterations to the disclosed embodiments without departing from the spirit or scope of this specification.

CLAIMS

1. A method of transferring data to a mobile device, comprising:

receiving authentication information associated with a user and authenticating the user based on the authentication information;

determining a one-time use password;

verifying an identity of a mobile device and/or a mobile device operator; and

transmitting encrypted data from a server computer to the mobile device, the encryption based, at least in part, on the password.

2. The method of claim 1, further comprising: receiving, at the mobile device, the password and decrypting the data for use by the mobile device.

3. The method of claim 1 or 2, wherein the authentication information is determined, at least in part, based on an encryption key.

4. The method of claim 3, wherein the encryption key is stored in a smart card.

5. The method of any preceding claim, wherein the authentication information is received from a client computer.

6. The method of any preceding claim, wherein the authentication information is determined based, at least in part, on information received from a user.

7. The method of any preceding claim, wherein the password is received from a user.

8. The method of any preceding claim, wherein the password is generated and output to the user.

9. The method of claim 8, wherein the password is output on a display device, as a printed document, or in an electronic message.

10. The method of claim 9, wherein the display device is a display device of a client computer.

11. The method of any of claims 7 to 10, comprising receiving the password at a server computer.

12. The method of any preceding claim, wherein the identity of the mobile device is verified by sending a message to the mobile device.

13. The method of claim 12, wherein the message comprises a reference value and the method comprises receiving a response message from the mobile device based at least partly on the response value.

14. The method of claim 13, wherein the response message contains the reference value or a value determined according to the reference value.

15. The method of any of claims 12 to 14, wherein the message is sent to the mobile device based on mobile device identification information associated with a user profile.

16. The method of any of claims 12 to 15, wherein the message is a short message service (SMS) message or an email.

17. The method of claim 13 or any claim dependent thereon, wherein the reference is generated by a server.

18. The method of any preceding claim, comprising storing the data in a storage location accessible to the mobile device.

19. The method of any preceding claim, wherein the data is security data.

20. The method of claim 19, wherein the security data comprises one or more keys and/or certificates.

21. The method of claim 20, comprising decrypting or encrypting communication data received by the mobile device using the one or more keys.

22. A server for sending data to a mobile device, wherein the server is arranged to:

receive authentication data associated with a user and to authenticate the user based on the authentication data;

determine a one-time-use password;

verify an identity of a mobile device and/or mobile device operator;

transmit encrypted data to the mobile device, the data being encrypted based,

at least in part, on the password.

23. The server of claim 22, wherein the authentication information is at least partly received from a user.

24. The server of claim 23, wherein the authentication information is received from a client computer.

25. The server of claim 22, 23 or 24, wherein the authentication information is determined, at least in part, based on an encryption key.

26. The server of any of claims 22 to 25, wherein the one time use password is determined by the server and output to a user.

27. The server of claim 26, wherein the server is arranged to output the password on a display device or to communicate the password to another device for outputting the password to the user.

28. The server of any of claims 22 to 27, wherein the server is arranged to verify the identity of the mobile device by sending a message to the mobile device.

29. The server of claim 28, wherein the server is arranged to generate a reference value and to include the reference value in the message.

30. The server of claim 29, wherein the server is arranged to receive a response message from the mobile device and to compare a value derived from the response message against the generated reference value.

31. The server of claim 28, 29 or 30, wherein the server is arranged to determine identification information of the mobile device and to send the message to the mobile device based on the identification information.

32. The server of claim 31, wherein the identification information is determined from a user profile associated with the user.

33. The server of any of claims 22 to 32, wherein the server is arranged to encrypt the data based, at least in part, on the password.

34. The server of any of claims 22 to 33, wherein the data is security data.

35. The server of claim 34, wherein the server is arranged to obtain the security data based on a user profile associated with the user.

36. The server of claim 34 or 35, wherein the security data comprises one or more keys and/or certificates.

37. A computer system, comprising the server of any of claims 22 to 36 and a mobile device.

38. The computer system of claim 37, wherein the mobile device is one or a mobile telephone, a smart phone, a tablet computer or a portable computer.

39. Computer software arranged to perform the method of any of claims 1 to 21 when executed on a computer.

40. The computer software of claim 39 stored on a computer readable medium.

41. A method substantially as described hereinbefore with reference to the accompanying drawings.

42. A server computer substantially as described hereinbefore with reference to the accompanying drawings.

43. A computer system substantially as described hereinbefore with reference to the accompanying drawings.

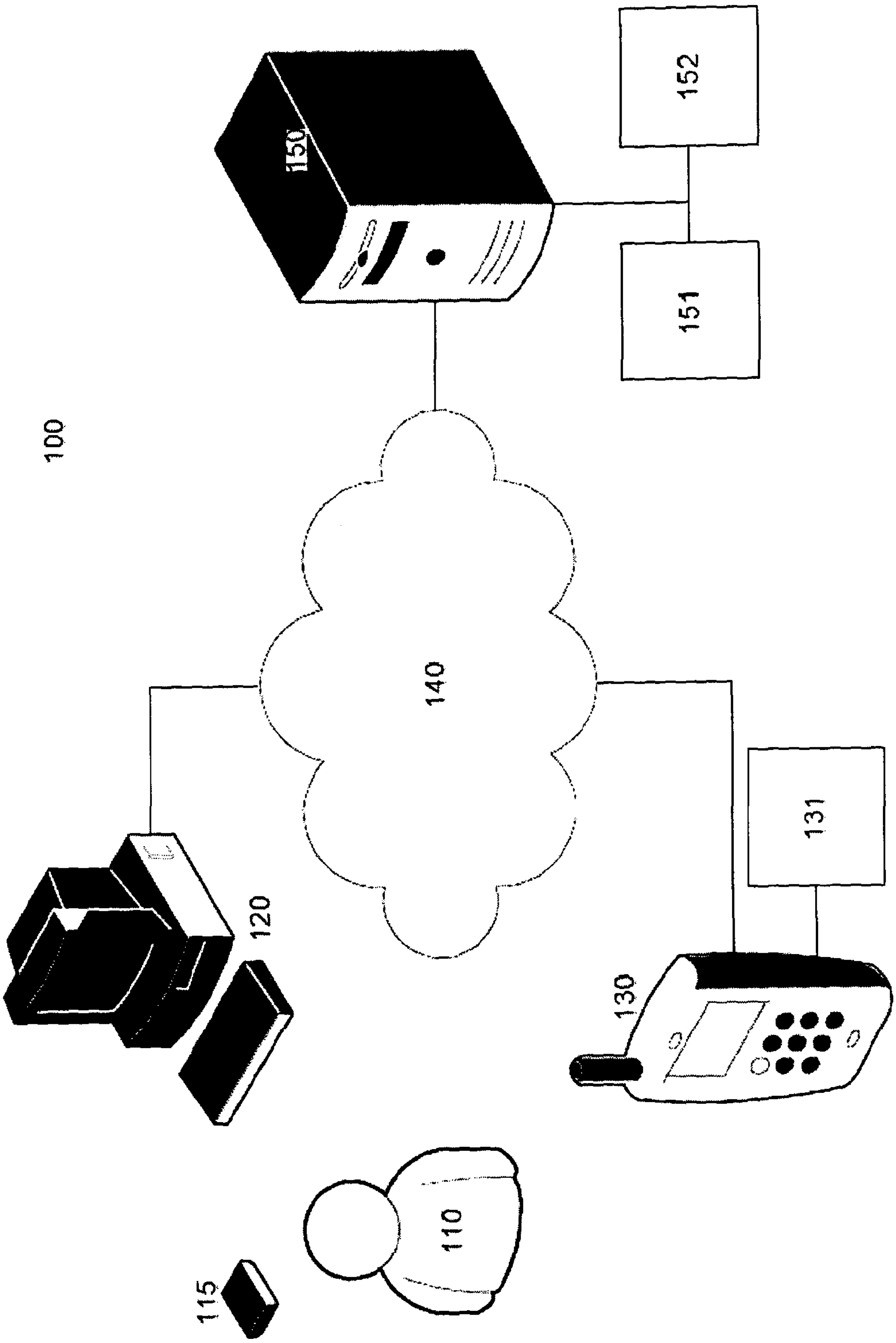

Fig. 1

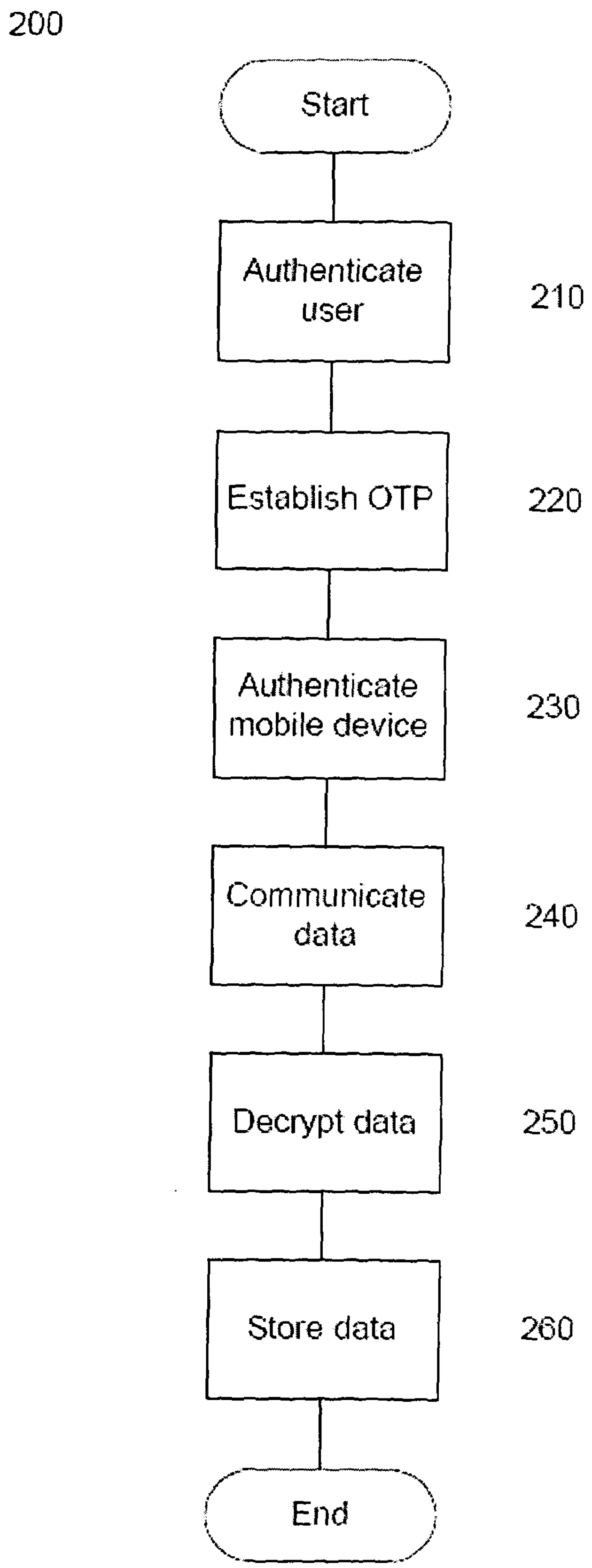
200
Start
Authenticate user
210
Establish OTP
220
Authenticate mobile device
230
Communicate data
240
Decrypt data
250
Store data
260
End

Fig. 2

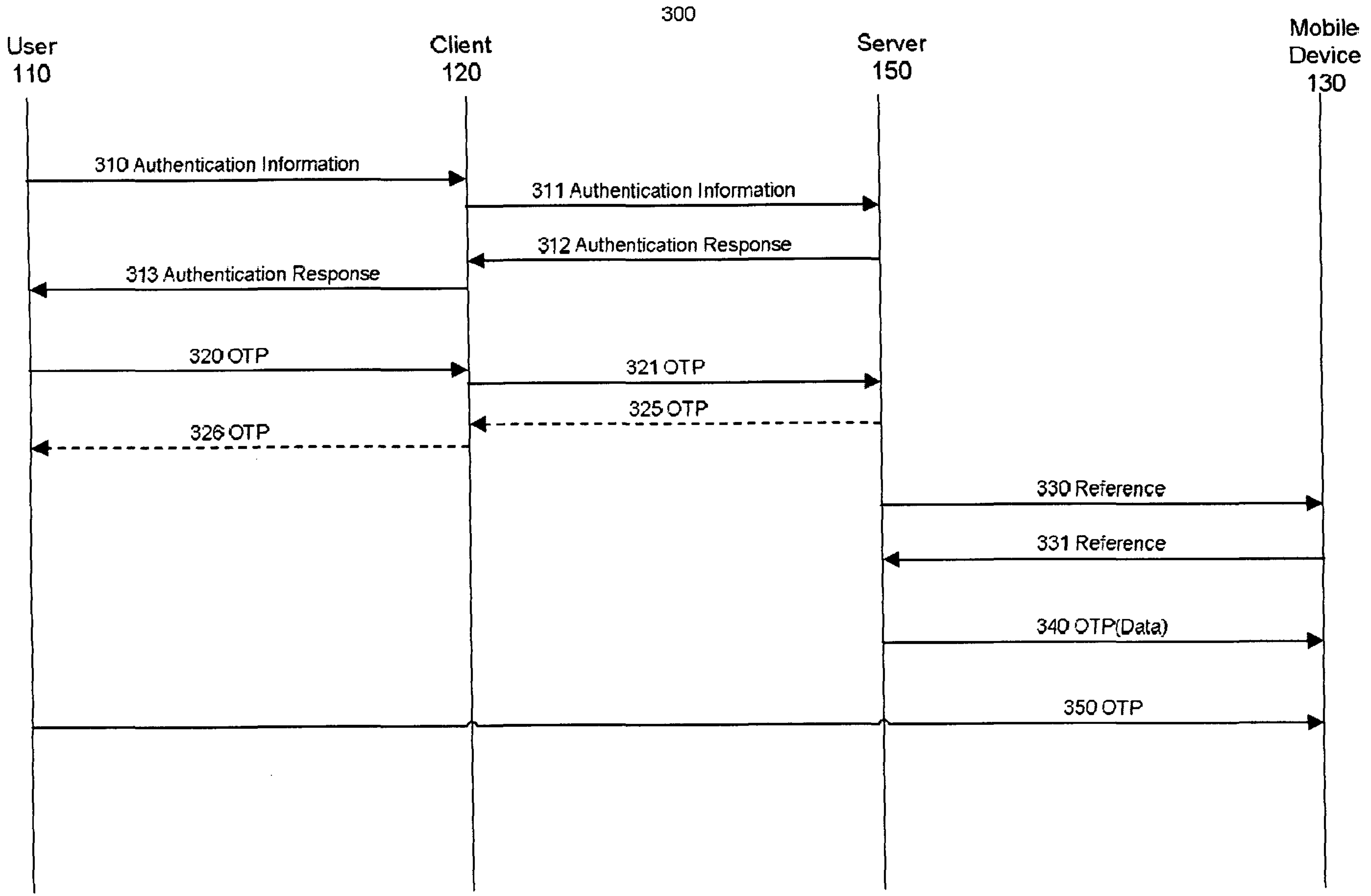
300
User
110
Client
120
Server
150
Mobile
Device
130
310 Authentication Information
311 Authentication Information
312 Authentication Response
313 Authentication Response
320 OTP
321 OTP
325 OTP
326 OTP
330 Reference
331 Reference
340 OTP(Data)
350 OTP

Fig. 3

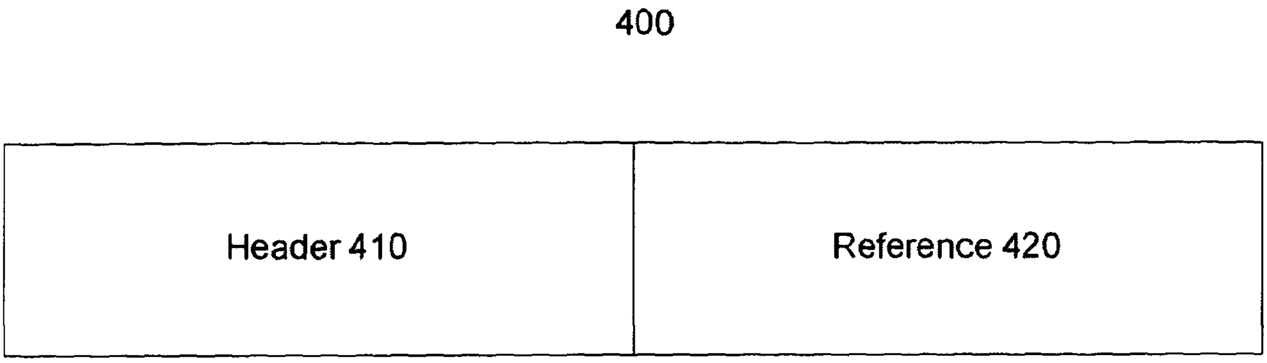

Fig. 4

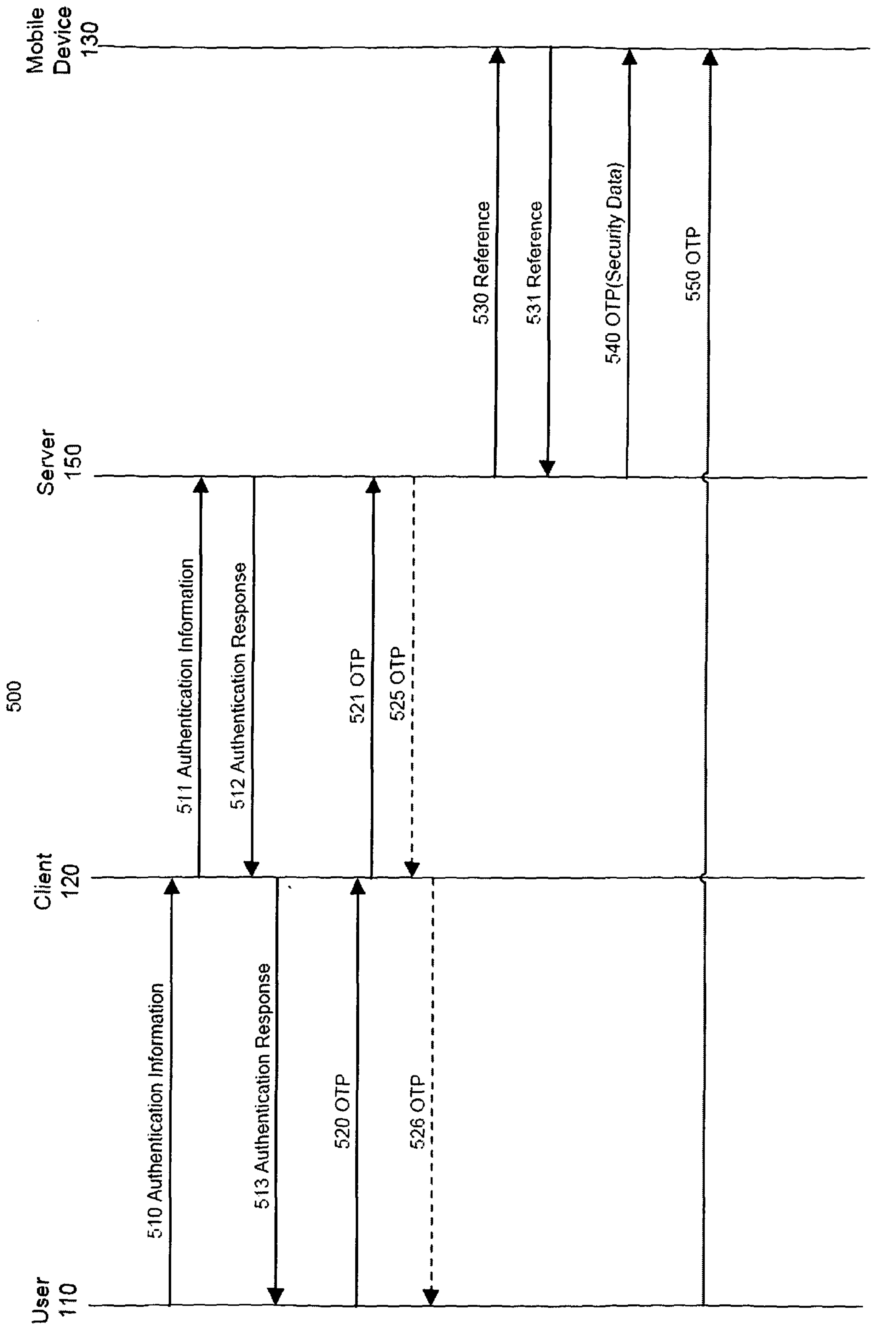
500
User 110
Client 120
Server 150
Mobile Device 130
510 Authentication Information
511 Authentication Information
512 Authentication Response
513 Authentication Response
520 OTP
521 OTP
525 OTP
526 OTP
530 Reference
531 Reference
540 OTP(Security Data)
550 OTP

Fig. 5

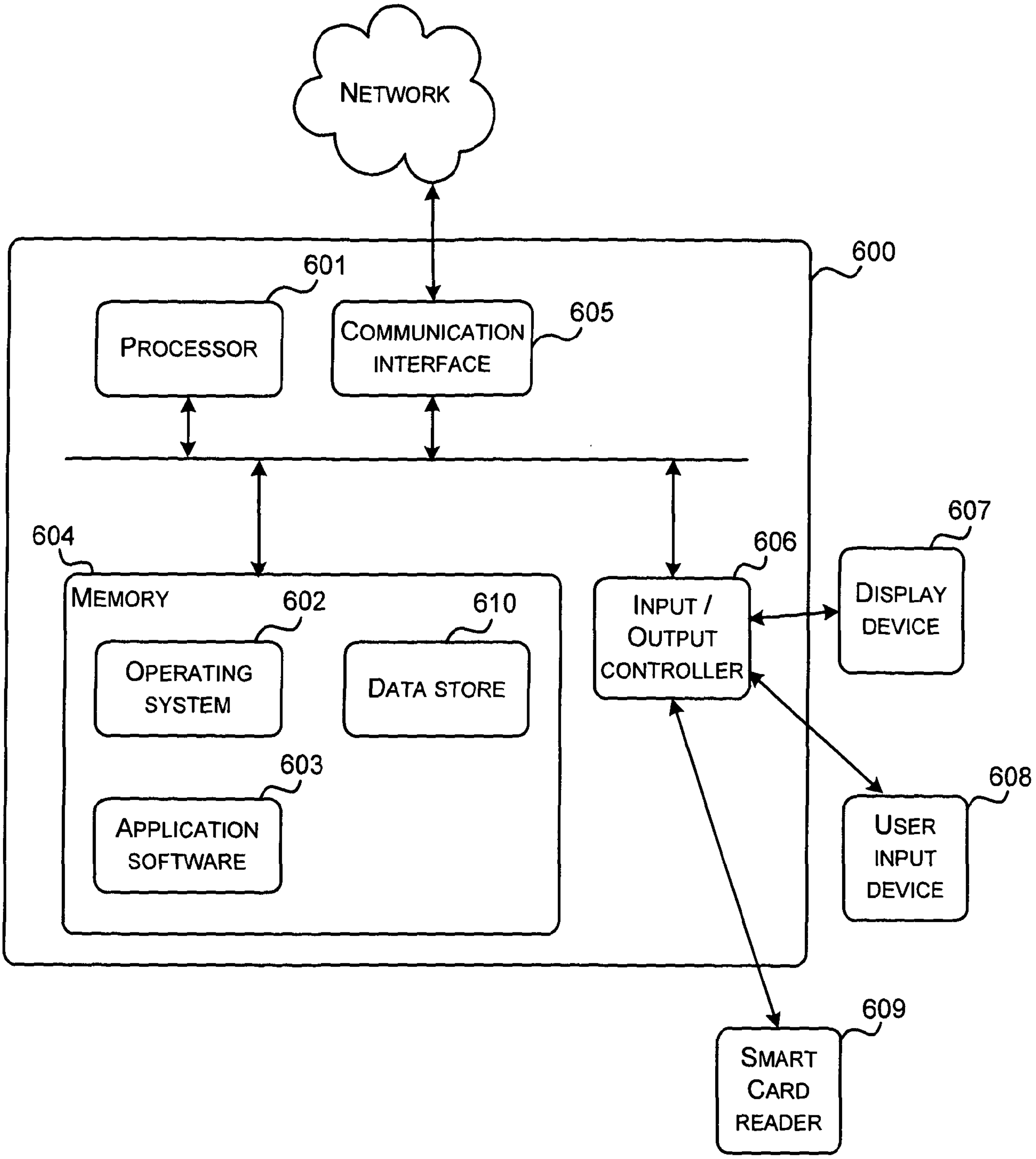
NETWORK
600
601
PROCESSOR
COMMUNICATION INTERFACE
605
604
MEMORY
602
OPERATING SYSTEM
610
DATA STORE
603
APPLICATION SOFTWARE
606
INPUT / OUTPUT CONTROLLER
607
DISPLAY DEVICE
608
USER INPUT DEVICE
609
SMART CARD READER

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2012/000206

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06
ADD.

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)
H04L H04W

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 practical, search terms used)

EPO-Internal, WPI Data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/235339 A1 (MENNES FREDERIK [BE] ET AL) 17 September 2009 (2009-09-17) abstract; figures 1a,2,3,6,7,8,10 paragraphs [0084], [0091], [0094] paragraphs [0120] - [0129] paragraphs [0167] - [0183] paragraphs [0207] - [0210] -----	1-43
X	US 2008/034216 A1 (LAW ERIC CHUN WAH [US]) 7 February 2008 (2008-02-07) abstract; figures 1-3 paragraphs [0030], [0032], [0033] paragraphs [0043] - [0051] paragraphs [0059] - [0071] ----- -/--	1-43

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

"E" earlier document 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 20 April 2012	Date of mailing of the international search report 27/04/2012
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Schossmaier, Klaus

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2012/000206

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/158033 A1 (JEONG YOUNSEO [KR] ET AL) 18 June 2009 (2009-06-18) abstract; figures 2-6 paragraphs [0048] - [0051] paragraphs [0070], [0077], [0082] paragraphs [0085] - [0089] -----	1-43

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/GB2012/000206

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009235339 A1	17-09-2009	CN 101999132 A EP 2252961 A1 US 2009235339 A1 WO 2009145964 A1	30-03-2011 24-11-2010 17-09-2009 03-12-2009
US 2008034216 A1	07-02-2008	EP 2052485 A2 TW 200818838 A US 2008034216 A1 WO 2008019194 A2	29-04-2009 16-04-2008 07-02-2008 14-02-2008
US 2009158033 A1	18-06-2009	KR 20090061915 A US 2009158033 A1	17-06-2009 18-06-2009