



- (51) International Patent Classification:
G06F 21/31 (2013.01)
- (21) International Application Number:
PCT/IB2014/058406
- (22) International Filing Date:
20 January 2014 (20.01.2014)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant: **HERE GLOBAL B.V.** [NL/NL]; De Run 1115, NL-5503 LB Veldhoven (NL).
- (72) Inventors: **MAJANIEMI, Sami Kalervo**; Pesäkolonkatu 13, FI-33870 Tampere (FI). **CHERUKURI, Harshil**; Flat 304 Harbour Court, Sector 19 A Nerul Navi, Mumbai 400706 (IN). **D'MELLO, Sandesh**; B/408, Jeevan Vihar CHS opp Nahur Stn (E), Koparkar Marg, Mumbai 400042 (IN).
- (74) Agent: **RUUSKANEN, Juha-Pekka**; Page White & Farer, Bedford House, John Street, London Greater London WC1N 2BF (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, 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, LT, 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, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

- (54) Title: AUTHENTICATING A USER

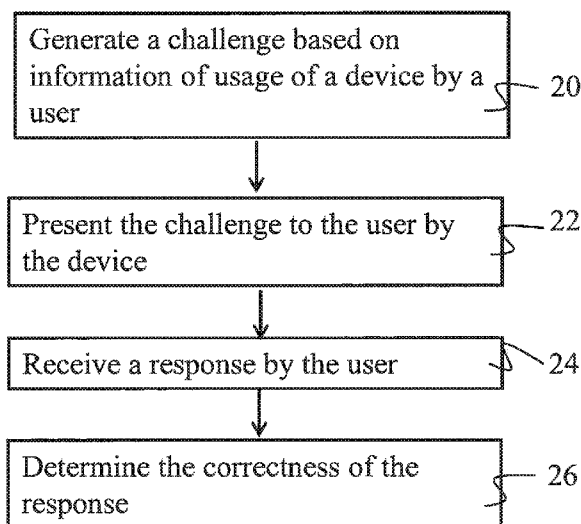


Fig. 2

(57) Abstract: A user is authenticated based on a challenge for authentication of the user that is generated based on information of usage of a device that is available for the device. The challenge is presented to the user by the device where after a response to the challenge is received. Acceptability of the response is determined based on said information of usage of the device.

Authenticating a user

This disclosure relates to security operations and more particularly to authentication of a user of a device.

Authentication of users is provided in various contexts to ensure that non-authorised users cannot access and use e.g. a device and/or a service. Commonly used authentication methods are based on character strings typically referred to as passcodes or passwords. An example of the passcodes is the Personal Identification Number (PIN) that is used e.g. to unlock a communication device and/or a subscriber identity module (SIM) thereof. Such characters strings comprising text and/or numbers may be vulnerable to dictionary attacks. A password can also be easy to guess if the password is selected such that it is easy to remember. On the other hand, a password that is harder to crack (e.g. is sufficient in length and a combination of numbers, characters, special characters and upper/lower case characters) may be fairly difficult to remember. Such a string of code may also be difficult to key in, especially into a small user device such as handheld or otherwise mobile device. Users might wish thus to be able to have possibility of quicker and/or easier authentication which nevertheless provides a reasonable level of security.

In accordance with an aspect there is provided a method for authentication of a user, comprising generating a challenge for authentication of the user based on information of usage of a device available for the device, presenting the challenge to the user by the device, receiving a response to the challenge, and determining acceptability of the response based on said information of usage of the device.

In accordance with another aspect there is provided an apparatus for a device comprising at least one processor, and at least one memory including computer program code, wherein the at least one memory and the computer program code are configured, with the at least one processor, cause the apparatus at least to generate a challenge for authentication of a user of the device based on information of usage of the device available for the device,

present the challenge to the user, receive a response to the challenge, and determine acceptability of the response based on said information of usage of the device.

5 In accordance with a more detailed aspect the challenge is generated by determining a plurality of items based on said information of usage of the device, a response is received comprising at least one item selected by the user from the plurality of items, and the at least one selected item is compared with said information of usage of the device.

10 The challenge may comprise at least one first item that has been used by the user and at least one second item that has not been used by the user.

Generating of the challenge may comprise selecting from a memory of the device at least one recently and/or frequently used item for the challenge.

A fresh challenge may be generated for each authentication instance.

15 Failed authentication may be determined in response to determining that the response does not correspond in a predefined manner to information of recent usage of the device.

At least one another authentication method can be used. A user may be authenticated based on the other authentication method periodically and/or in response to a predefined event.

20 Processing of the received response may comprise use of a predefined mathematical function. According to a possibility the function determines a trend of correctness of the responses.

25 Authentication based on the challenge is enabled only within a predefined period after authentication of user based on another authentication method and/or when the device is in a predefined location.

The number of correctly selected items required for a valid authentication may be varied.

30 The usage information may be based on information of at least one of contacts of the user, communication log of the user, applications used by the user, content data used by and/or stored in the device, location of the device, ringtones, and battery of the device.

A device comprising the described apparatus and arranged to implement the embodiments can also be provided. The device may comprise a

communication device, for example a mobile user device. The mobile user devices can be a mobile communication device such as a mobile phone, a smart phone, a personal data assistant, a notebook, a tablet computer or a laptop computer, or a wearable device such as a smart watch, smart
5 eyeglasses or clothing, decorative items or jewellery, for example rings, bracelets, necklaces and pendants with communication and data processing capabilities. A system comprising at least one of such device can also be provided.

A computer program comprising program code adapted to perform the
10 herein described methods may also be provided. In accordance with further embodiments apparatus and/or computer program product that can be embodied on a computer readable medium for providing at least one of the above methods is provided.

It should be appreciated that any feature of any aspect may be combined
15 with any other feature of any other aspect.

Embodiments will now be described in further detail, by way of example only, with reference to the following examples and accompanying drawings, in which:

20 Figure 1 shows an example of a user device,
Figures 2 and 3 are flowchart in accordance with certain embodiments,
Figures 4 to 7 show examples of possible displays presented to a user,
and

Figure 8 is a flowchart in accordance with an embodiment.
25

In the following certain illustrative examples for authentication of a user of a device will be described. In accordance with one possible use scenario, Figure 1 shows a schematic, partially sectioned view of a communication device. More particularly, a handheld or otherwise mobile communication
30 device 10 is shown. An appropriate mobile communication device can be provided by any device capable of sending and receiving radio signals. Non-limiting examples include a mobile station (MS) such as a mobile

phone or what is known as a 'smart phone', a portable computer such as a laptop or a tablet computer provided with a wireless interface card or other wireless interface facility, personal data assistant (PDA) provided with wireless communication capabilities, or any combinations of these or the like. Further examples include wearable wireless devices such as those integrated with watches or smart watches, eyewear, helmets, hats, clothing, ear pieces with wireless connectivity, jewelry and so on, universal serial bus (USB) sticks with wireless capabilities, modem data cards or any combinations of these or the like.

10 A mobile communication device can be provided with wireless communication capabilities and appropriate electronic control apparatus for enabling operation thereof in accordance with the herein described principles. Thus the mobile device of Figure 1 is shown being provided with at least one data processing entity 13, for example a central processing unit and/or a core processor, at least one memory 15 and other possible components such as additional processors 14 and memories 16 for use in software and hardware aided execution of tasks it is designed to perform. The data processing, storage and other relevant control apparatus can be provided on an appropriate circuit board 17 and/or in chipsets. Data processing and memory functions provided by the control apparatus of the mobile device are configured to cause control and signalling operations in accordance with certain embodiments of the present invention as described later in this description.

25 The user may control the operation of the mobile device by means of a suitable user interface such as touch sensitive display screen or pad 12 and/or a key pad, voice commands, combinations of these or the like. A control button 11, for example an on/off switch and/or a multitask switch is shown to illustrate this. A speaker and a microphone are also typically provided. Furthermore, a mobile communication device may comprise appropriate connectors (either 30 wired or wireless) to other devices and/or for connecting external accessories, for example hands-free equipment, thereto.

The mobile device may communicate wirelessly with other devices via appropriate apparatus for receiving and transmitting signals. In Figure 1 the transceiver apparatus is designated schematically by block 18. The transceiver may be provided for example by means of a radio part and associated antenna arrangement. The antenna arrangement may be arranged internally or externally to the mobile device.

A user can use a user device in for various purposes, for example for work and private uses. The user can have the possibility of securing the device by an authentication method, for example a passcode or the like. In case of sensitive information being stored in the device, or being available through it, an additional level of security beyond a normal passcode based entry may be desired. Also, users might wish to have a quicker and/or simpler way of accessing their devices that through a passcode. For example, a lock screen feature of a device can be used to lock the device after the device has been idle for a certain period of time. In some cases this period can be a relatively short and the user needs to input the passcode constantly, possibly tens of times a day. Users might find it more convenient if they could quickly and in a simple manner authenticate themselves to the device to unlock it. This could be particularly desired when the device is in constant use, or at least the user has it constantly with him/her, while the system is kept reasonably secure through a stronger authentication such as a passcode when it is switched or and/or e.g. in the morning. Stronger authentication may nevertheless be required for example when the device has not been used for a while or in response to an event indicative of possibility of attempt to access the device by an unauthorized person.

A quick authentication of a user to a device and/or a service can be based on information of such personal usage of the device that is known to the true authorised user of the device. For example, information about the past usage of the device can be used for unlocking the device and/or for accessing and using a service or application. The usage information can be based e.g. on call and other connection and usage history available in a memory holding the connection log of the device. For example, made and/or received calls and/or Short Message Service (SMS) messages, emails, web sites visited, games

played etc. can be used as the basis of generating an authentication challenge. Usage information can also be based on information such as contact information, stored images, names of stored / played music pieces and/or artists, audio clips and so forth information available got the device. That is, pretty much any information that the user knows and that is available in the device or to the device can be used. More examples of possible basis for the challenge are described below.

An authentication challenge can be generated based on the personal usage information. Figure 2 illustrates a flowchart for an authentication method wherein a challenge for authentication of a user is generated at 20 based on information of usage of a device available for the device. The challenge is then presented to the user by the device at 22, and a response to the challenge is received at 24. The acceptability of the response is determined at 26 based on said information of usage of the device. If the response is incorrect, or deviates from a correct response more than an allowed amount, the authentication fails.

In accordance with a possibility the generated challenge comprises also false entries. That is, if a challenge is based on multiple items, the items to be presented to the user can be defined such that only one or less than all of them are correct answers whereas there are also correct looking but incorrect i.e. bogus answers. For example, user of device can be shown on display a list of songs/artists where after the user has to select one or ones that are stored in the device. A possibility is to prompt the user to select ones he has listened recently, for example during the last day or week. The list can have a certain number of songs/artists taken from the memory of the device and a certain number of bogus songs/artists that are randomly added to the list.

The information used for the challenges can be selected such that a malicious user should not be able to easily guess the correct answer while the proper user can easily recognise the correct answer. The false items can be completely bogus options taken from an appropriate source (an internal database, a server, etc.) or these can be non-matching real entries. In the latter case recentness of the data can be used as criteria.

Figure 3 illustrates an example of such method for authentication. A challenge for authentication of a user is generated at 30 by dynamically

determining a plurality of items based on information of usage of a device, at least one of the items is correct answer whereas the rest are bogus. The challenge is presented at 32 to the user by the device. The user then input his/hers response to the challenge, and the response comprising at least one item selected by the user from the plurality of items is received at 34. The at least one selected item is compared at 36 with said information of usage of the device. Based on the comparison the validity of the authentication can then be decided.

A challenge can be defined by one of the processors 13 and 14 of device 10 of Figure 1 based on information of the usage of the device available e.g. from one of the memories 15, 16 of the device 10.

A possibility for generation of the challenge is to use contact names stored in a memory of a communication device as the basis of items selected for an authentication challenge. A candidate list of names can be determined including such contacts which are deemed as ones the user is most likely to call, and which are thus easiest to remember. A candidate list of "correct" contacts used by the user can be defined by the user. According to a possibility the most frequently used contact is or contacts are selected. Bogus names can be fetched and/or generated by the communication phone or created by the true owner.

It is possible to have a policy according to which certain contact names that are easy to guess (e.g. home, mum, dad etc.) are automatically excluded by the processor of the device from the candidate list.

Information about the most recent phone calls, text messages and so on is something a user is likely to remember. Therefore a possible option can be to provide a challenge based on call and/or other communication log within a predefined period, for example in the last twenty four hours.

Information of usage of content such as music played by the device can also be used as a basis for the challenges. Choices for the items for the authentication challenge can be taken e.g. from the "most played" list of a music player. Names of songs in such list can be refreshed by the device whenever the device recognizes that a certain song is or songs are being listened to more than some other songs. In an authentication challenge tracks from the recently

played play list as well as some bogus tracks, for example from the internet or from the playlist but not in the most played list can be presented. The user will then have to select the track he/she listens to a lot. Instead of the existing "recently/most played" list from a music player the users can be given the option
5 to create such a list.

Similarly to music information about videos, electronic books and other content downloaded and/or viewed and/or stored in the device and viewing habits can also be captured from a video playing application and/or mobile TV application or similar application of the device.

10 Information of frequently used application (apps) can also be used as the basis of a dynamically personalised authentication challenge. A policy can be set that commonly used apps like the most popular social media and email applications are automatically excluded.

Personalised ringtones may also be used as authentication basis as a
15 user is likely to know his/hers ringtone. The authentication can also be based on ringtones that are associated with specific contacts. For example, a user may be asked to identify a special ringtone set for a specific contact.

Location based authentication is also possible. For example, unlocking of a device can require identifying a location the user visited within a predefined
20 period, or at a certain time, or a location the user frequently visits. This information can be provided by a location application of the device.

Information regarding battery may also be used. For example, information regarding the battery charge level when the device was locked may also be used. Users tend to keep eye on the battery status and therefore have
25 this at the back of their minds. The battery status may be presented as a range. The time when the user last charged the battery may also be used for the challenge.

A new challenge can be generated for each authentication attempt. The challenge can be generated dynamically based on the latest usage information
30 available for the device. A one-time password can thus be provided and there is no need to store those one-time passwords anywhere as the true user should know the correct answer based on his/hers recollection of recent usage of the device.

The selection of items can be done from one source, for example from a register of recent calls, or from a multiple of sources, for example registers of calls, SMSs, emails, songs, games, contacts and so forth. Successive challenges can be based on different information categories. The selection of options for the challenge can also be arranged such that if there has been an event in the device recently relating to a particular category of information this category is used, thus making it easier for the user to remember.

According to a possibility a controller of the device generates and maintains the candidate list based on information of real usage of the device. In accordance with a possibility the user defines an initial list that is then maintained based on information of real usage. This can include inclusion of new items and deletion existing items from the list. Also, the items on the list can be ranked, and the ranking can vary based on real usage, e.g. how many times a contact has been selected during the last week.

A challenge can be presented to the user and response received in various manners, certain examples being shown in Figures 4 to 7.

Figure 4 shows an example of a list of challenges displayed on a screen 12. In this example a list of contact name items is displayed. Only one of the name items on the list is correct whereas the others are bogus entries. In case of a touchscreen device the user can tap the correct name on the touch sensitive screen. The user may also input the correct answer by entering the associated number via a keypad (either a physical keypad or virtual keypad on a touchscreen) or give the correct number or name via a voice recognition interface. For example, input "4" would mean selection of the 4th option "Charlie" on the list 40. Input of the associated number can be used particularly in a non-touch screen device but is also a possible way to input the answer via a touch screen.

The challenge does not have to be in a form of a list, and there are many other ways to present a challenge can be used. Figure 5 shows an example where the challenge is presented as icons wherefrom the user has to select the correct one or ones. In Figure 5 icon 52 depicts the correct answer where the remaining icons 54 are bogus answers.

Tapping the correct icon or another item is not the only possible way to interact with a device. For example, Figure 6 shows an example where dragging of items 60 on the screen 12 can be used. For example, a user needs to drag at least one correct item of those into a correct response "box" 62. According to a possibility a number of items are to be dragged into corresponding response boxes 62, 64. For example, there can be contact items and the user would have to arrange those to "friends", "relatives" and "colleagues" boxes.

A user-specific secret part can be added to the final answer. For example, a short one or two character suffix or prefix can be added to the answer. A user can just add the secret part to the answer. For example, if the challenge is in form of a list, and if the second option would be right and the secret number would be "3" then the user would actually need to select the fifth option from the list.

A possibility to increase security is to use mathematical functions as a part of the response input and authentication approval process. A user can define a mathematical function (e.g. multiplication, division, addition, subtraction and so on) and a secret number. The final answer would then be the value associated with the correct answer taken together with the secret number by using the mathematical function. So in an example illustrated by Figure 7 prompt 70 is shown on a display 12 asking for an additional character. if the correct item is the 4th item on the list 30, the pre-defined mathematical function is multiplication and the secret number the user needs to input at display item 70 is 3, then the actual correct answer is $4 \times 3 = 12$. Other ways to create an additional secret part can also be used.

The number items presented for selection to the user can be kept relatively low in order to keep the authentication relatively simple and quick. For example, only five alternatives where there is one correct option can be shown. In this case the possibility of guessing the right answer is 20%. The trade-off between security and quickness of use can be determined by the user. The list can made longer and there can be an arbitrary number of right choices to mix things up. Alternatively, there can be many rounds of authentication, so the attacker would have to guess right a multiple of times in succession. For example, a two round authentication would mean probability $0.2 \times 0.2 = 0.04$.

Thus adding a second question would already bring the probability to guess correctly down to 4% in this example.

In accordance with a possibility the look and feel (personalization) of the device can be used as a "challenge". In this case the user needs to know e.g.
5 which image is used as a background in a certain view and/or what applications (apps) are available in a certain menu.

It can be defined through settings of the device how many items on the candidate list are to be displayed in an authentication challenge. It can also be defined how long the challenge list will be. For example, the size of the
10 challenge can be set to four items. One, two, three or even all names in a candidate list can be displayed and the remaining item slots will be filled with bogus names. The communication device can search for the bogus names e.g. from the internet or another source or take names from the contact list associated with the device that do not form a part of the authentication
15 candidate list.

The number of correct choices can be varied between the challenges. That is, sometimes only one out of e.g. five options would be correct and some other times maybe three out of the five options would be needed.

The security can be improved by various other measures. For example,
20 getting the answer wrong even one time can take the user to a "normal" passcode based authentication screen or trigger another more robust authentication method. This is illustrated by the flowchart of Figure 8 where unsuccessful quick authentication at 86 will result return to a more robust authentication at 80. A valid quick authentication process will authenticate the
25 user at 88.

In accordance with a possibility the "quick" authentication may be used only at 84 when a previous "normal" authentication has been done at 80 within a predetermined time period. A rule can for example be that the "quick" authentication may be determined at 82 to have been enabled only when the
30 device has not moved more than a certain distance within a certain period of time or from a certain location (e.g. home, office etc.). In these scenarios it is likely that that the real owner is still in the possession of the device. A forced periodic "normal" authentication may also be provided.

The user interface of a device configured for the quick authentication can be provided with the possibility to revert back to the "normal" authentication (passcode or otherwise) in case the user for some reason does not know, remember or for some other reason cannot input the correct answer.

5 A user or a policy can define the information that shall be used in the challenges. A challenge profile can be stored in the device. A certain number of correct choices and/or the size of the challenge and/or the number of correct items can be selected according to the profile.

10 A device may be offline at the time of generation of a challenge, and therefore may not be able to use an external source for generation of the false items. If external entries are nevertheless desired, the false entry database in the device can be updated with new entries when a connection is available. For example, when the profile of the user is changed a new set of corresponding false entries is downloaded. The update may also be attempted periodically, or
15 in response to another event, e.g. triggered by a predefined number of authentications.

The arrangement can be such that no duplicates are presented in a single authentication event. That is, "John Smith" shall not be present twice if for example recent calls are used as the basis.

20 Recently used data is currently considered a good basis to provide the authentication. The number of times something has been used by the user is also considered an advantageous way of defining the authentication basis. This can be limited to a certain time period that can be longer than what is used for the recent action arrangement.

25 It can be that the true owner may not be confident to be able to pinpoint to names, songs etc. with 100% accuracy. A tolerance threshold may be used to address this. For example, a user may be allowed to unlock the device when he gets 70 % of the name and/or song selections right. In accordance with a possibility a valid authentication is determined once or twice with a lower
30 percentage (e.g. the 70%), but the overall (average) percentage should be above a certain threshold or the authentication event will fail. Thus valid authentication cannot be obtained if there is constantly a low percentage.

Constant low percentage may also trigger need to provide an authentication by means of another method as discussed above.

According to an example appropriate apparatus or means are provided for controlling a device, for example a handheld, wearable or otherwise mobile device, to provide the various embodiments. For example, means can be provided for authentication of a user, comprising means for generating a challenge for authentication of the user based on information of usage of a device available for the device, means for presenting the challenge to the user by the device, means for receiving a response to the challenge, and means for determining acceptability of the response based on said information of usage of the device.

The means can be configured to generate the challenge by determining a plurality of items based on said information of usage of the device, receive a response comprising at least one item selected by the user from the plurality of items, and compare the at least one selected item with said information of usage of the device.

It is noted that whilst embodiments have been described using a mobile user device as an example, similar principles can be applied to any other user devices where authentication of the user may be needed. Therefore, although certain embodiments were described above by way of example with reference to certain exemplifying mobile devices and technologies and uses thereof, the principles can be applied to any other suitable forms of devices, applications and services than those illustrated and described herein.

The required data processing apparatus, functions and circuitry at the relevant devices may be provided by means of one or more data processors and other hardware and software. The described functions may be provided by separate processors or by an integrated processor. The data processing apparatus may be of any type suitable to the local technical environment, and may include one or more of general purpose computers, special purpose computers, microprocessors, digital signal processors (DSPs), application specific integrated circuits (ASIC), gate level circuits and processors based on dual-core or multi-core processor architecture, as non-limiting examples. The data processing may be distributed across several data processing modules. A

data processor may be provided by means of, for example, at least one chip. Appropriate memory capacity can also be provided in the relevant devices. The memory or memories may be of any type suitable to the local technical environment and may be implemented using any suitable data storage
5 technology, such as semiconductor based memory devices, magnetic memory devices and systems, optical memory devices and systems, fixed memory and removable memory, including appropriate types of random access memory (RAM) and read-only memory (ROM).

In general, the various embodiments may be implemented in hardware or
10 special purpose circuits, software, logic or any combination thereof. Some aspects of the invention may be implemented in hardware, while other aspects may be implemented in firmware or software which may be executed by a controller, microprocessor or other computing device, although the invention is not limited thereto. While various aspects of the invention may be illustrated
15 and described as block diagrams, flow charts, or using some other pictorial representation, it is well understood that these blocks, apparatus, systems, techniques or methods described herein may be implemented in, as non-limiting examples, hardware, software, firmware, special purpose circuits or logic, for example for controlling communications, user interface, and data processing,
20 general purpose hardware or controller or other computing devices, or some combination thereof. The software may be stored on such physical media as memory chips, or memory blocks implemented within the processor, magnetic media such as hard disk or floppy disks, and optical media such as for example DVD and the data variants thereof, CD, and a cloud storage arrangement.

25 As used in this specification, the term circuitry refers to all of the following: (a) hardware-only circuit implementations (such as implementations in only analog and/or digital circuitry) and (b) to combinations of circuits and software (and/or firmware), such as (as applicable): (i) to a combination of processor(s) or (ii) to portions of processor(s)/software (including digital signal
30 processor(s)), software, and memory(ies) that work together to cause an apparatus, such as a mobile phone or server, to perform various functions) and (c) to circuits, such as a microprocessor(s) or a portion of a microprocessor(s), that requires software or firmware for operation, even if the software or firmware

is not physically present. This definition of circuitry applies to all uses of this term in this specification, including in any claims. As a further example, as used in this specification, the term circuitry also covers an implementation of merely a processor (or multiple processors) or portion of a processor and its (or their) accompanying software and/or firmware. The term circuitry also covers, for example and if applicable to the particular claim element, a baseband integrated circuit or applications processor integrated circuit for a mobile device.

The foregoing description has provided by way of exemplary and non-limiting examples a full and informative description of the exemplary embodiment of this invention. However, various modifications and adaptations may become apparent to those skilled in the relevant arts in view of the foregoing description, when read in conjunction with the accompanying drawings and the appended claims. However, all such and similar modifications of the teachings of this invention will still fall within the spirit and scope of this invention as defined in the appended claims. Indeed there is a further embodiment comprising a combination of one or more of any of the other embodiments previously discussed.

Claims

1. A method for authentication of a user, comprising
5 generating a challenge for authentication of the user based on information of usage of a device available for the device,
presenting the challenge to the user by the device,
receiving a response to the challenge, and
determining acceptability of the response based on said information of
10 usage of the device.
2. A method according to claim 1, comprising
generating the challenge by determining a plurality of items based on said
information of usage of the device,
15 receiving a response comprising at least one item selected by the user from the plurality of items, and
comparing the at least one selected item with said information of usage of the device.
- 20 3. A method according to claim 2 wherein the generating of the challenge comprises selecting at least one first item that has been used by the user and at least one second item that has not been used by the user.
4. A method according to any preceding claim wherein the generating of the
25 challenge comprises selecting from a memory of the device at least one recently and/or frequently used item for the challenge.
5. A method according to any preceding claim comprising generating a fresh challenge for each authentication instance.
- 30 6. A method according to any preceding claim comprising determining failed authentication in response to determining that the response does not correspond in a predefined manner to information of recent usage of the device.

7. A method according to any preceding claim comprising using at least one another authentication method.
- 5 8. A method according to any preceding claim wherein processing of the received response comprises use of a predefined mathematical function.
9. A method according to any preceding claim comprising authenticating the user based on another authentication method periodically and/or in response to
10 a predefined event.
10. A method according to any preceding claim wherein authentication based on the challenge is enabled only within a predefined period after authentication of user based on another authentication method and/or when the device is in a
15 predefined location.
11. A method according to any preceding claim comprising varying the number of correctly selected items required for a valid authentication.
- 20 12. A method according to any preceding claim wherein the usage information is based on information of at least one of contacts of the user, communication log of the user, applications used by the user, content data used by and/or stored in the device, location of the device, ringtones, and battery of the device.
- 25 13. An apparatus for a device comprising at least one processor, and at least one memory including computer program code, wherein the at least one memory and the computer program code are configured, with the at least one processor, cause the apparatus at least to generate a challenge for authentication of a user of the device based on information of usage of the
30 device available for the device, present the challenge to the user, receive a response to the challenge, and determine acceptability of the response based on said information of usage of the device.

14. An apparatus according to claim 13, configured to
generate the challenge by determining a plurality of items based on said
information of usage of the device,
receive a response comprising at least one item selected by the user from
5 the plurality of items, and
compare the at least one selected item with said information of usage of
the device.
15. An apparatus according to claim 13 or 14, configured to generate the
10 challenge by selecting at least one first item that has been used by the user and
at least one second item that has not been used by the user.
16. An apparatus according to any of claims 13 to 15, configured to select
from the memory at least one recently and/or frequently used item for the
15 challenge.
17. An apparatus according to any of claims 13 to 16, configured to generate
a fresh challenge for each authentication instance.
- 20 18. An apparatus according to any of claims 13 to 17, configured to use at
least one another authentication method.
19. An apparatus according to any of claims 13 to 18, configured to use a
predefined mathematical function in determining the acceptability of the
25 response.
20. An apparatus according to any of claims 13 to 19, configured to enable
authentication based on the challenge only within a predefined period after
authentication of user based on another authentication method and/or when the
30 device is in a predefined location.
21. A device comprising an apparatus according to any of claims 13 to 20.

22. A device according to claim 21, comprising a mobile user device.

23. A computer program comprising code means adapted to cause performing
of the steps of any of claims 1 to 12 when the program is run on data
5 processing apparatus.

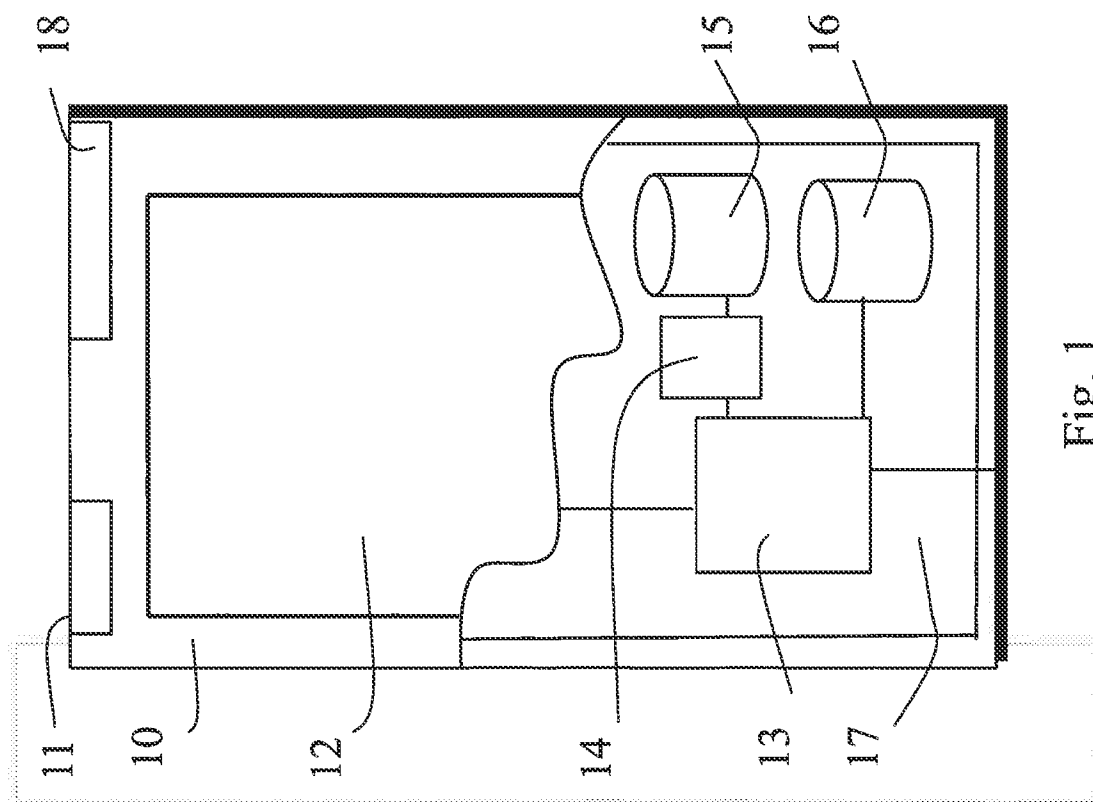


Fig. 1

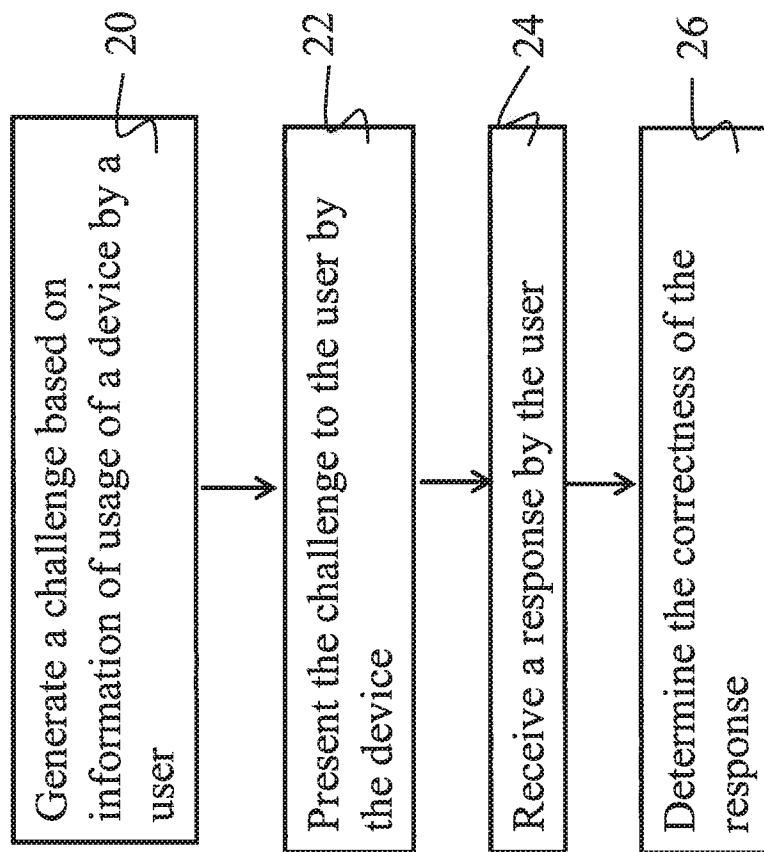


Fig. 2

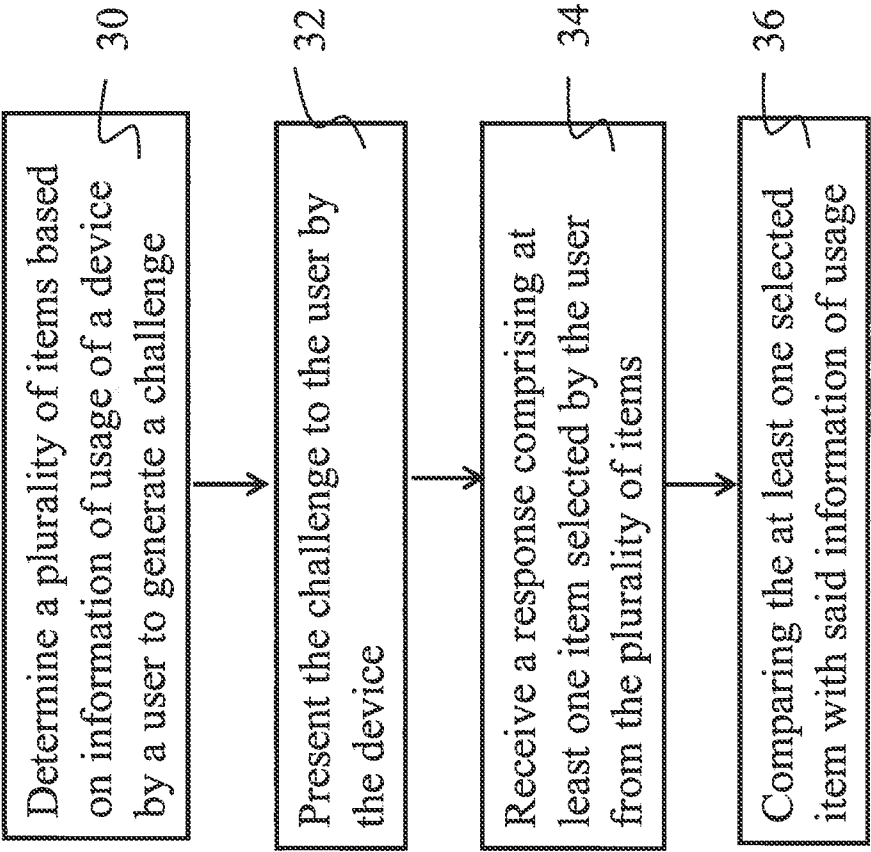
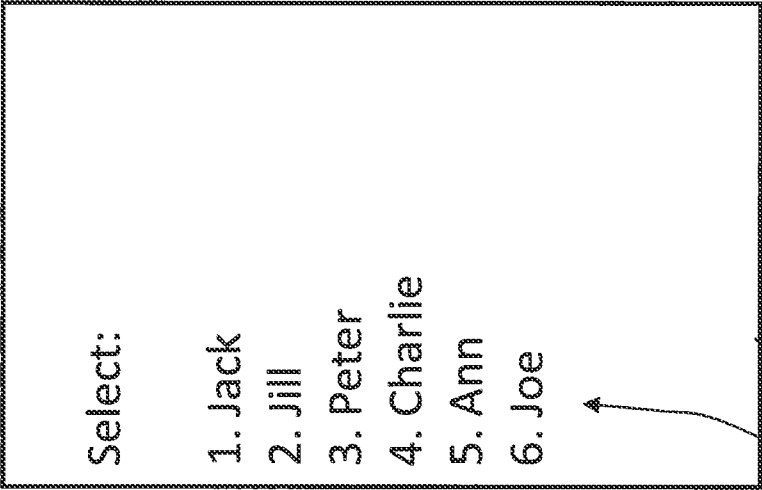


Fig. 3



40 12 Fig. 4

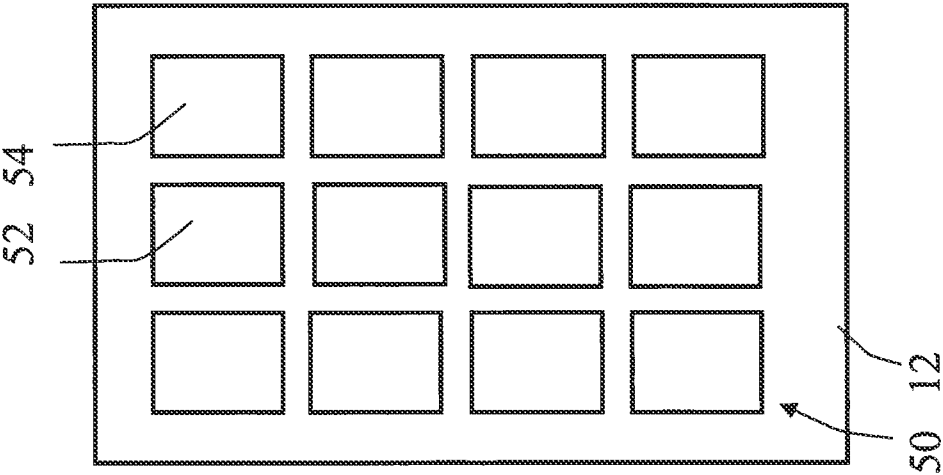


Fig. 5

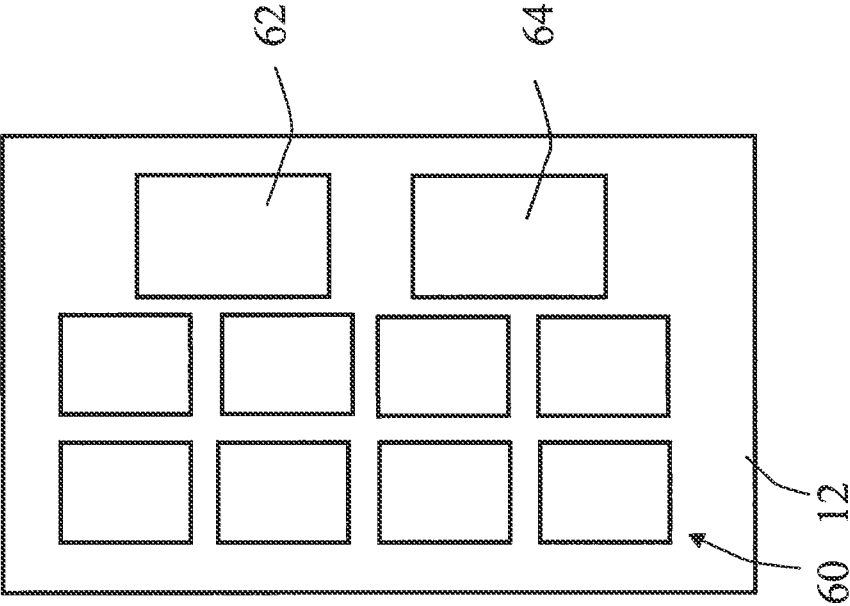


Fig. 6

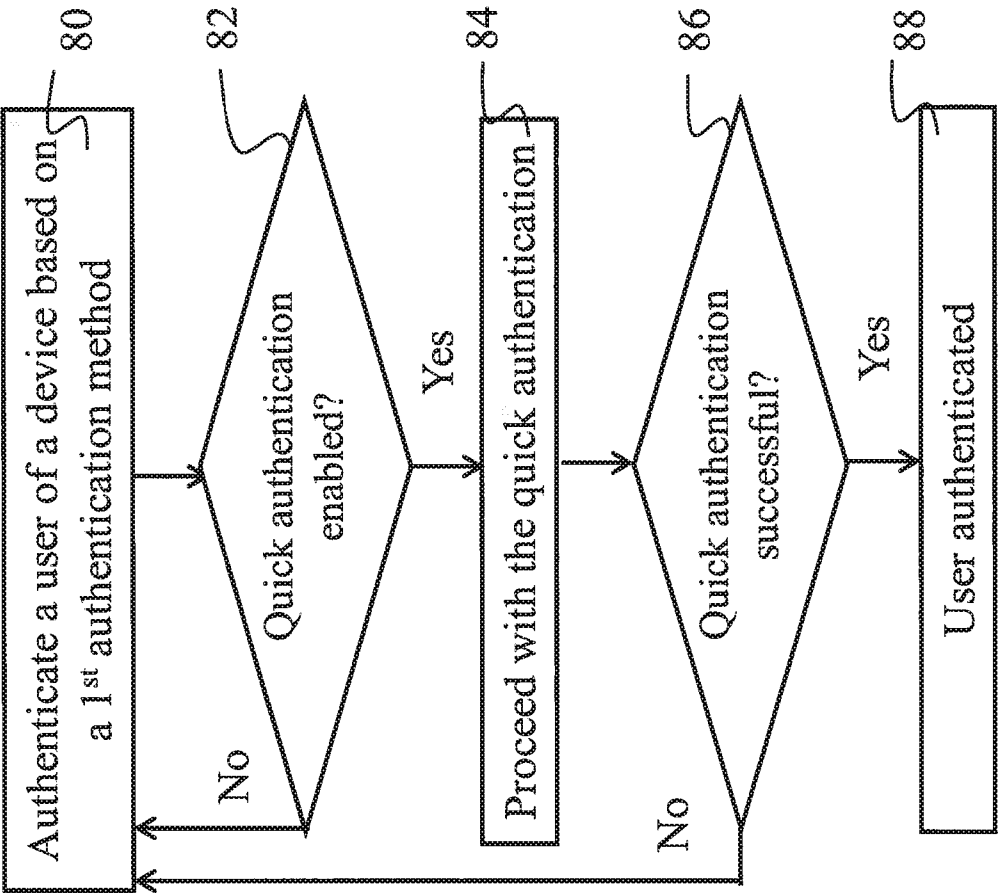


Fig. 8

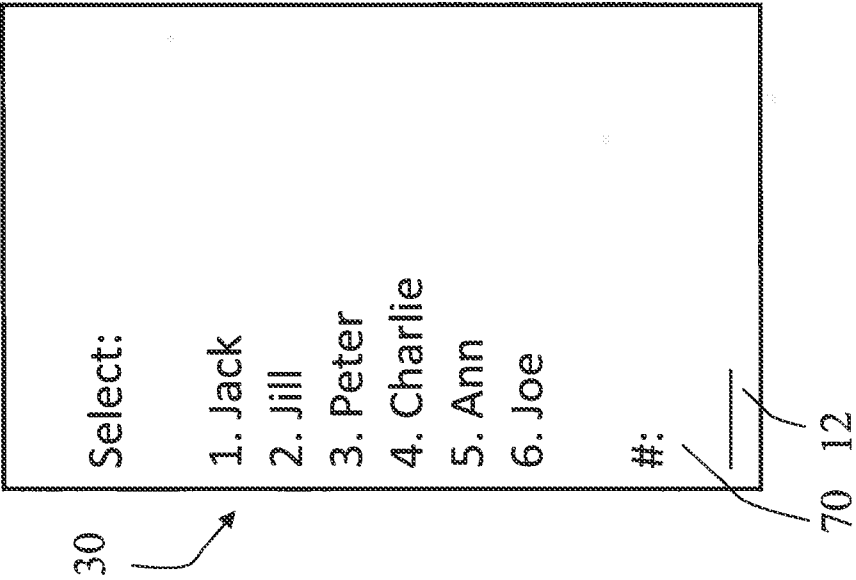


Fig. 7

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2014/058406

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/31

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)

G06F H04M 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 practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 431 904 A1 (RESEARCH IN MOTION LTD [CA]; CERTICOM CORP [CA]) 21 March 2012 (2012-03-21) the whole document	1-23
A	----- William Cheswick: "Johnny Can Obfuscate; Beyond Mother's Maiden Name", HOTSEC'06 Proceedings of the 1st USENIX Workshop on Hot Topics in Security, 31 July 2006 (2006-07-31), pages 31-36, XP055113800, Berkeley, CA, USA Retrieved from the Internet: URL:https://www.usenix.org/legacy/event/hotsec06/tech/full_papers/cheswick/cheswick.pdf [retrieved on 2014-04-11] the whole document -----	1-23



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 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

11 April 2014

Date of mailing of the international search report

25/04/2014

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

Meis, Marc

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2014/058406

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2431904	A1	21-03-2012	CA 2807818 A1 29-03-2012
			EP 2431904 A1 21-03-2012
			US 2012072975 A1 22-03-2012
			WO 2012040325 A1 29-03-2012
