[Continued on next page]

(54) Title: METHOD FOR GETTING A USER VALIDATION OF A KEY
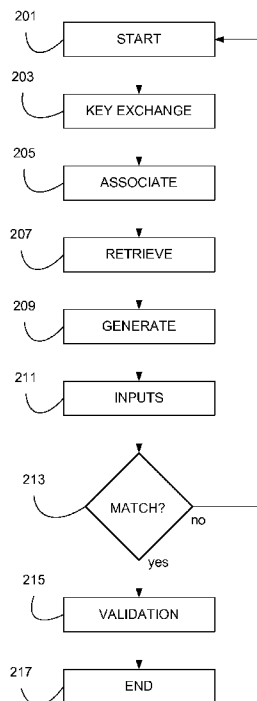
(57) Abstract: Present system relates to a method for getting a user validation of a key stored on a user equipment using a graphical user interface (GUI), the method being carried out by a processor of the user equipment controlling the GUI and comprising the acts of associating to one or more graphical sub-elements to be rendered in a first graphical element of the GUI a parameter set at an initial value function of the key, generating the first graphical element comprising the one or more graphical sub-elements, each one of the graphical sub-elements being displayed with a parameter set to an altered value different from its initial value, the parameter being editable through one or more user inputs on said graphical sub-element, receiving user inputs on the one or more graphical sub-elements to edit its parameter, so as to generate a second graphical elements on the GUI and wherein the validation of the key corresponds to the matching of the first and second graphical elements.

FIGURE 2

WO 2016/103046 A1

METHOD FOR GETTING A USER VALIDATION OF A KEY

FIELD OF THE PRESENT SYSTEM:

5   The present invention relates generally to communication devices, and more precisely to validation by a user of a key used during pairing process between user equipments.

BACKGROUND OF THE PRESENT SYSTEM:

10   User equipment like mobile device, tablets, or more generally electronic devices or computing devices comprising communication capabilities are nowadays quite common. With this proliferation of new technologies and the advancement of such user equipments, the user is presented with a choice of using multiple user equipments in a collaborative way. The user equipments may interact, establishing communications between themselves, in order to exchange

15   data such as contents for example. In order to facilitate communications between two user equipments, these user equipments may be paired (or bonded, linked). Pairing is a process used in digital communications that helps set up an initial linkage (or pairing) between user equipments to allow communications between them. The most common example is used in Bluetooth, where the pairing process is used to link two user equipments with Bluetooth capabilities. This pairing

20   process can be used for example to link a Bluetooth headset with a mobile phone. After completion of the pairing, the mobile phone may easily use the Bluetooth headset to render audio content. When a pairing process is launched between two user equipments, it is important to implement security rules to prevent the pairing to occur with a wrong user equipment or, even worse, without any consent from one of a user equipment owner. Another aspect of security rules

25   is to prevent man in the middle attack. Indeed, when a first and a second user equipments launch a pairing process, it may be easy, without sufficient security rules, for a third user equipment – the attacker -to act as a man in the middle. The attacker makes independent pairing with the two user equipments and relays messages between the two of them in order to make them believe that they are talking directly to each other over a private connection, when in fact the entire

30   conversation is controlled by the attacker, that is to say that all exchanges between the first and second user equipments are going through the third user equipment.

A traditional method of securing pairing process relies on a shared PIN code (Personal Identification Number). In a first method, illustrated in FIG. 1A, one of the two user equipments generates a key or PIN code and displays it on its screen. The user needs to enter the displayed key

35   on the other user equipment in order to validate the pairing between the two user equipments. Quite often, reading the key on the first user equipment screen and entering it on the other user

equipment is perceived as cumbersome by the users. In another method, to prevent the user from entering the key, the key is displayed on the screens of the two user equipments, the user is asked to confirm that the two keys are indeed equals on the two user equipments. But again, users find this verification step cumbersome and may just validate the key without giving much attention to the exact value of the keys displayed on each user equipment screen.

Thus, there is a need for a method for getting a user validation of a key that should be simple as to not being perceived cumbersome by the users, but that maintains an adequate level of security by not being bypassed by the users.

SUMMARY OF THE PRESENT SYSTEM:

It is an object of the present system to overcome disadvantages and/or make improvements in the prior art.

Present document discloses a method for getting a user validation of a key stored on a user equipment using a graphical user interface (GUI), the method being carried out by a processor of the user equipment controlling the GUI and comprising the acts of associating to one or more graphical sub-elements to be rendered in a first graphical element of the GUI a parameter set at an initial value function of the key, generating the first graphical element comprising the one or more graphical sub-elements, each one of the graphical sub-elements being displayed with a parameter set to an altered value different from its initial value, the parameter being editable through one or more user inputs on said graphical sub-element, receiving user inputs on the one or more graphical sub-elements to edit its parameter, so as to generate a second graphical element on the GUI and wherein the validation of the key corresponds to the matching of the first and second graphical elements.

Advantageously, this method replaces a cumbersome task of key validation by a user friendly graphical validation. It also improves the security as this system is more robust against man in the middle attack that could use simple digit permutation of a displayed key in order to deceive an inattentive user.

In one complementary embodiment of present disclosure, the parameter corresponds to one of at least a position, a color or a form of a graphical sub-element.

Advantageously, alteration of parameters such as position form or color of the sub-elements allows intuitive and simple implementation of the present method. It present also the advantage of being compatible with most of the user equipments used today as it is based on parameters widely used. So an application program implementing the method can be coded to be compatible with most of the user equipments.

In one complementary embodiment of present disclosure, the act of generating the first graphical element comprises the preliminary acts of retrieving a predetermined stored graphical element, retrieving a predetermined partitioning model, the partitioning model allowing the breakdown of a graphical element into one or more sub-elements, generating the first graphical

5   element comprising graphical sub-elements using the partitioning model on the retrieved graphical element and wherein the predetermined stored graphical element or the predetermined partitioning model is function of the key.

Advantageously, choosing a predetermined graphical element or a predetermined portioning model in function of the key improves the security of the system as it allows more diversity on the

10   graphical element rendered on the GUI. It prevents the user from considering the validation of the key as a routine, thus validating the key without really any attention, as graphical element rendered shall be different from one validation to another, in function of the key to be validated.

In one complementary embodiment of present disclosure, the method is carried out by a processor of a first user equipment, the key corresponding to a shared secret key obtained upon

15   performing a Diffie-Hellman key exchange with a second user equipment.

Advantageously, the method can be used to get the validation by the user of a key generated during a Diffie Hellman key exchange process conducted between two user equipments. This is improving the security of the Diffie Hellman key exchange process as it compensate for its weakness against man in the middle attack.

20   Another object of the disclosure concerns a system comprising a first user equipment using a first graphical user interface (GUI), a second user equipment using a second graphical user interface (GUI) wherein, upon performing a key exchange between the first and second user equipment, a processor of the first user equipment controlling the first GUI executes the method as described hereinbefore and a processor of the second user equipment controlling the second

25   GUI retrieves the predetermined stored graphical element to render it on the second GUI.

In one complementary embodiment of present disclosure, the key exchange is a Diffie-Hellman key exchange.

Another object of the disclosure concerns a user equipment using a graphical user interface (GUI), the user equipment comprising a processor controlling the GUI and adapted to associate to

30   one or more graphical sub-elements to be rendered in a first graphical element of the GUI a parameter set at an initial value function of the authentication code, generate the first graphical element of the GUI comprising the one or more graphical sub-elements, each one of the graphical sub-elements being displayed with a parameter set to an altered value different from its initial value, the parameter being editable through one or more user inputs on said graphical sub-

35   element, receive user inputs on the one or more graphical sub-elements to edit its parameter, so

4

as to generate a second graphical element on the GUI and validate the authentication code when the first and second graphical elements match.

Another object of the invention concerns a computer program or application software, in particular computer programs on or in a non-transitory computer readable medium, suitable for getting a user validation of a key as disclosed in present document. These programs can use any programming language, and be in the form of source code, binary code, or of code intermediate between source code and object code such as in a partially compiled form, or in any other desirable form for implementing the methods according to the invention.

The information medium may be any entity or device capable of storing the software. For example, the medium can comprise a persistent or transient storage means, such as a ROM, for example a CD/DVD ROM or a microelectronic circuit ROM, or else a magnetic recording means, for example a diskette (floppy disk) or a hard disk or else a transient memory such as EEPROM, FLASH, SRAM and RAM.

BRIEF DESCRIPTION OF THE DRAWINGS:

The invention is explained in further detail, and by way of example, with reference to the accompanying drawings wherein:

FIG. 1A shows an exemplary method of user validation as known by the man skilled in the art;

FIG. 1B shows an exemplary system comprising two user equipments according to one embodiment of present system;

FIG. 2 shows an exemplary flowchart of the method for getting a user validation of a key according to one embodiment of present system.

DETAILED DESCRIPTION OF THE PRESENT SYSTEM:

The following are descriptions of illustrative embodiments that when taken in conjunction with the following drawings will demonstrate the above noted features and advantages, as well as further ones. In the following description, for purposes of explanation rather than limitation, illustrative details are set forth such as architecture, interfaces, techniques, element attributes, etc. However, it will be apparent to those of ordinary skill in the art that other embodiments that depart from these details would still be understood to be within the scope of the appended claims. Moreover, for the purpose of clarity, detailed descriptions of well-known devices, circuits, tools, techniques and methods are omitted so as not to obscure the description of the present system. It should be expressly understood that the drawings are included for illustrative purposes and do not

represent the scope of the present system. In the accompanying drawings, similar reference numbers in different drawings may designate similar elements.

FIG. 1B is an exemplary system comprising a first user equipment 100 and a second user equipment 110 (in short, device) according to one embodiment of present system.

In this embodiment, the first user equipment 100 is typically a mobile phone, a tablet or any communication device. The user equipment 100 comprises for example a processor 101, a display device or screen 102, a network module 104 and possibly a database module 103. The database module 103 may store data or may be connected through a remote connection to others database hosted on servers not represented here. For simplicity sake, it shall be understood that the server 100 comprises a database, the database being either stored locally - the database module 103 -, or connected remotely through the network module 104.

The processor 101 of the user equipment 100 can control, either directly or via a graphical module not illustrated in FG. 1B, a graphical user interface (GUI) rendered on the screen 102. The GUI is adapted to render graphical elements, possibly comprising graphical sub-elements, that is to say graphical components that put together for the graphical element. Each graphical sub-element is characterized by various parameters, such as for example the position, the form or the color of the graphical sub-element. The user may interact with the GUI, either directly via user touch on the screen 102, the screen 102 being a touch screen or via pointing devices such as mouse, stylus or trackball connected or integrated to the user equipment 100. More generally, the user may interact with the GUI via any known method, such as for example registered gestures. The user can thus select and possibly edit a graphical sub-element. For example, the GUI can allow a user to select and move a graphical sub-element over the screen 102, or, via for example a user menu displayed on the GUI, modify the color of the graphical sub-element. In short, parameters of a graphical sub-element may be editable through one or more user inputs on said graphical sub-element.

The user equipment 100 comprises at least one network module 104. The network module 104 can integrate for example wireless technology such as *Bluetooth, ZigBee* or *Wi-Fi* (Wireless Fidelity). Such network module 104 allows in particular communication between the first device 100 and at least one user equipment 110. The user equipment 110 is similar to the user equipment 100, so description of user equipment 100 may be applied to user equipment 110.

Thus, the first user equipment 100 and the second user equipment 110 may be paired or bonded together. By pairing, it should be understood a process used in computer networking that helps set up an initial linkage between user equipment or computing devices to allow communications between them. In particular, the pairing process may comprise the establishment of a secured communication channel between the two user equipments 100 and 110.

The processor 101 of the user equipment 100 may execute a computer program implementing the method that shall be described hereafter. The method of present system may be executed by the processor 101 entirely or may be executed also partially by other modules of the user equipment 100.

5   The user equipment 100 may store locally any type of data, or connect to a server to retrieve data, as known to the man skilled in the art.

Thus, the user equipment 100 uses a graphical user interface (GUI) and comprises a processor 101 controlling the GUI. The processor 101 of the user equipment 100 (in short, the user equipment 100) is adapted for associating to one or more graphical sub-elements to be rendered

10   in a first graphical element of the GUI a parameter set at an initial value function of the authentication code, generating the first graphical element of the GUI comprising the one or more graphical sub-elements, each one of the graphical sub-elements being displayed with a parameter set to an altered value different from its initial value, the parameter being editable through one or more user inputs on said graphical sub-element, receiving user inputs on the one or more graphical

15   sub-elements to edit its parameter, so as to generate a second graphical element on the GUI and validating the authentication code when the first and second graphical elements match.

The flowchart of FIG. 2 illustrates an embodiment of the method for getting a user validation of a key in the specific context of a pairing process between a first and a second user equipment as

20   illustrated in FIG. 1B. The two user equipments may belong to a same user, or may belong to two different users.

In any case, the user, or the users, may decide in a step 201 to initiate a pairing process of the two user equipments. Such pairing process may typically be performed using a Bluetooth network module 104. The pairing process may be executed on each user equipment by using a

25   function integrated within the operating system of the user equipments or by using an application program, the application program being dedicated to the pairing process or comprising a pairing function to conduct the pairing process. In order to secure the future communications between the two user equipments a secure channel shall be established, such secure channels usually are based on a common secret key.

30   Protocols or methods such as Diffie-Hellman key exchange protocol as described in U.S. Patent 4,200,770 can be used. The Diffie-Hellman key exchange protocol or method allows two user equipments that have no prior knowledge of each other to jointly establish a shared secret key (in short, a key) over an insecure communication channel. This key is then be used to encrypt subsequent communications between the two user equipments using a symmetric key cipher.

35   A key exchange protocol such as the Diffie-Hellman method is executed between the two user equipments during a step 203.

Nevertheless, such protocol executed in step 203 presents a weakness to man in the middle attack, so a validation by the user(s) of the key obtained on the two user equipments is commonly implemented.

During a step 205, the first user equipment 100 associates to one or more graphical sub-elements to be rendered in a first graphical element of the GUI a parameter set at an initial value function of the key previously calculated in step 203. Thus, color or position of a graphical sub-element may be defined according to the value of the key or of a subpart of the key or of the resultant (in part or whole) of a function applied to the key.

In an optional step 207, the first user equipment 100 retrieves a predetermined stored graphical element, retrieves a predetermined partitioning model, the partitioning model allowing the breakdown of a graphical element into one or more sub-elements and generates a first graphical element comprising graphical sub-elements using the partitioning model on the retrieved graphical element wherein the predetermined stored graphical element or the predetermined partitioning model is function of the key. The predetermined stored graphical element and partitioning model can be stored within or accessed by the application program, the application program storing or being able to access to various predetermined graphical element and partitioning model.

If the step 207 is not executed, the first user equipment 100 may retrieve and use a predetermined graphical element as first graphical element.

In a step 209, the first user equipment 100 generates the first graphical element comprising the one or more graphical sub-elements, each one of the graphical sub-elements being displayed with a parameter set to an altered value different from its initial value, the parameter being editable through one or more user inputs on said graphical sub-element. In other words, the first user equipment 100 renders on its screen 102 the graphical element with the graphical sub-elements rendered in an altered way. For example, graphical sub-elements (or parts) of a graphical element (or image) may be altered by having a different color than the initial one. The position of said graphical sub-element (or parts) may be changed, displaying the graphical element (or image) as a jigsaw puzzle, composed by the graphical sub-elements, on the GUI rendered on the screen 102.

In parallel to the steps 205 to 209, after the step 203 of key exchange, the second user equipment 110 performs a similar method, except that the graphical element is rendered on its GUI on its screen without any alteration of the parameters of the graphical sub-elements. In other words, the graphical element is retrieved and rendered without any alteration on the second user equipment GUI.

Thus, the user(s) may see on the second user equipment 110 screen an un-altered version of the graphical element. This un-altered version of the graphical element may be visually compared

8

by the user(s) to the altered version of the graphical element displayed on the screen of the first user equipment 100.

In a step 211, the user equipment 100 receives user inputs on the one or more graphical sub-elements to edit its parameter, so as to generate a second graphical element on the GUI. The user, by looking at the graphical element rendered on the second user equipment 110 screen, can indeed, either via user inputs on the touch screen 102 if the screen 102 comprises a touch interface, or via a pointing device, edit the different graphical sub-elements rendered on the GUI of the first user equipment 100 in order to try to reconstitute the first graphical element.

In cases of man in the middle attack or unsolicited pairing request, the user will see a different graphical element displayed on the other user equipment or won't have access to the graphical element displayed on the other user equipment screen. So the user will not be able to reconstitute the graphical element.

In a step 213, the reconstituted graphical element (or second graphical element obtained after the user inputs in step 211) and the first graphical element are matched. If they do not match, then the validation of the key is considered failed and the pairing process may be aborted or repeated from step 203.

If the two graphical element match, in a step 215, then the key is considered validated, meaning that the user has validated that the two user equipments 100 and 110 share a same common secret key. Further secure communication channel may be established for example based on this common secure key. This process may be repeated every time the two user equipments need to communicate, or may be executed only one time during the first pairing process.

The application program may be stopped in a further step 217 once the communication between the two user equipment is terminated.

Finally, the above discussion is intended to be merely illustrative of the present system and should not be construed as limiting the appended claims to any particular embodiment or group of embodiments. Thus, while the present system has been described with reference to exemplary embodiments, such as embodiment described in the different figures, it should also be appreciated that numerous modifications and alternative embodiments may be devised by those having ordinary skill in the art without departing from the broader and intended spirit and scope of the present system as set forth in the claims that follow. Further, while exemplary illustrations were provided to facilitate an understanding of the present system, other system for implementing the method described here before may be provided in accordance with further embodiments of the present system.

The section headings included herein are intended to facilitate a review but are not intended to limit the scope of the present system. Accordingly, the specification and drawings are to be regarded in an illustrative manner and are not intended to limit the scope of the appended claims.

In interpreting the appended claims, it should be understood that:

a) the word "comprising" does not exclude the presence of other elements or acts than those listed in a given claim;

b) the word "a" or "an" preceding an element does not exclude the presence of a plurality of such elements;

c) any reference signs in the claims do not limit their scope;

d) several "means" may be represented by the same item or hardware or software implemented structure or function;

e) any of the disclosed elements may be comprised of hardware portions (e.g., including discrete and integrated electronic circuitry), software portions (e.g., computer programming), and any combination thereof;

f) hardware portions may be comprised of one or both of analog and digital portions;

g) any of the disclosed devices or portions thereof may be combined together or separated into further portions unless specifically stated otherwise;

h) no specific sequence of acts or steps is intended to be required unless specifically indicated;

i) the term "plurality of" an element includes two or more of the claimed element, and does not imply any particular range of number of elements; that is, a plurality of elements may be as few as two elements, and may include an immeasurable number of elements, and;

j) the term "greater than" (respectively "lower than") should be understood as "strictly greater than" (resp. "strictly lower than") or "greater than or equal to" (resp. "lower than or equal to"), both implementation being possible unless specifically indicated.

CLAIMS

1. A method for getting a user validation of a key stored on a user equipment using a graphical user interface (GUI), the method being carried out by a processor of the user equipment controlling the GUI and comprising the acts of:
- associating to one or more graphical sub-elements to be rendered in a first graphical element of the GUI a parameter set at an initial value function of the key,
- generating the first graphical element comprising the one or more graphical sub-elements, each one of the graphical sub-elements being displayed with a parameter set to an altered value different from its initial value, the parameter being editable through one or more user inputs on said graphical sub-element,
- receiving user inputs on the one or more graphical sub-elements to edit its parameter, so as to generate a second graphical element on the GUI,
wherein the validation of the key corresponds to the matching of the first and second graphical elements.

2. The method according to claim 1, the parameter corresponding to one of at least a position, a color or a form of a graphical sub-element.

3. The method according to one of the previous claim, the act of generating the first graphical element comprising preliminary acts of:
- retrieving a predetermined stored graphical element,
- retrieving a predetermined partitioning model, the partitioning model allowing the breakdown of a graphical element into one or more sub-elements,
- generating the first graphical element comprising graphical sub-elements using the partitioning model on the retrieved graphical element,
wherein the predetermined stored graphical element or the predetermined partitioning model is function of the key.

4. The method according to one of the previous claim, the method being carried out by a processor of a first user equipment, the key corresponding to a shared secret key obtained upon performing a Diffie-Hellman key exchange with a second user equipment.

5. A system comprising:
- a first user equipment using a first graphical user interface (GUI),

11

- a second user equipment using a second graphical user interface (GUI),

wherein, upon performing a key exchange between the first and second user equipment:

- a processor of the first user equipment controlling the first GUI executes the method according to one of the claims 1 to 4, and,

5

- a processor of the second user equipment controlling the second GUI retrieves the predetermined stored graphical element to render it on the second GUI.

6. A system according to previous claim, the key exchange being a Diffie Hellman key exchange.

10

7. A user equipment using a graphical user interface (GUI), the user equipment comprising a processor controlling the GUI and adapted for:

- associate to one or more graphical sub-elements to be rendered in a first graphical element of the GUI a parameter set at an initial value function of the authentication code,

15

- generate the first graphical element of the GUI comprising the one or more graphical sub-elements, each one of the graphical sub-elements being displayed with a parameter set to an altered value different from its initial value, the parameter being editable through one or more user inputs on said graphical sub-element,

- receive user inputs on the one or more graphical sub-elements to edit its parameter, so

20   as to generate a second graphical element on the GUI,

- validate the authentication code when the first and second graphical elements match.

8. An application program embodied on a non-transitory computer readable medium and arranged to execute the method of claims 1 to 4.
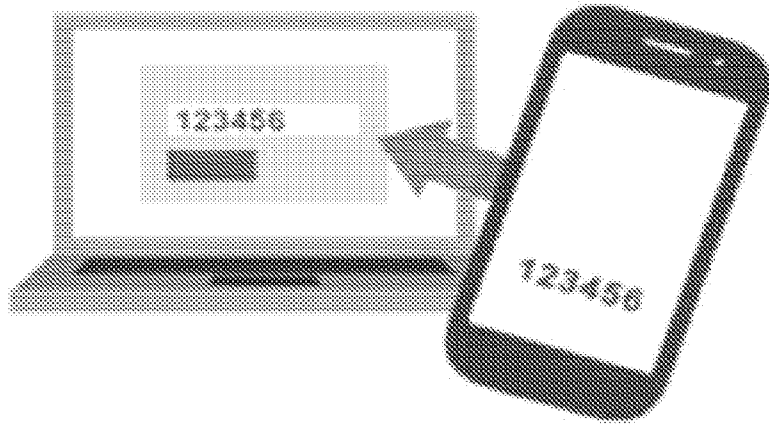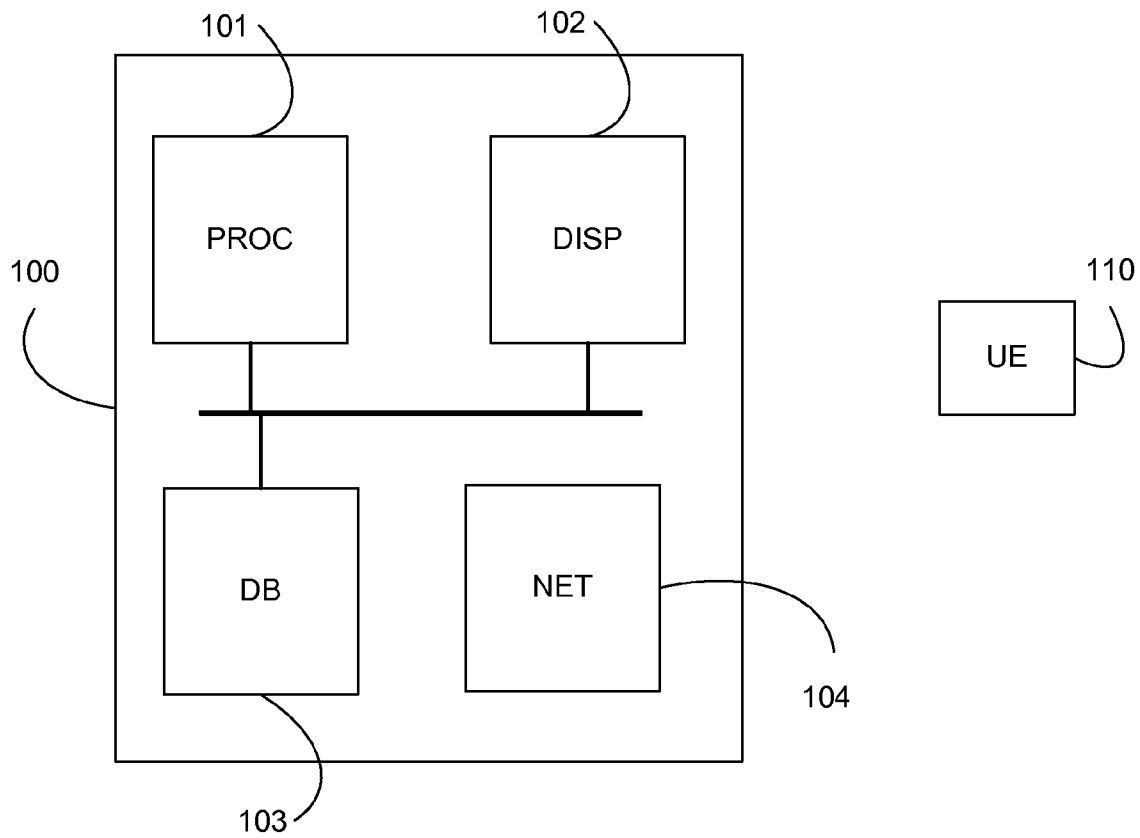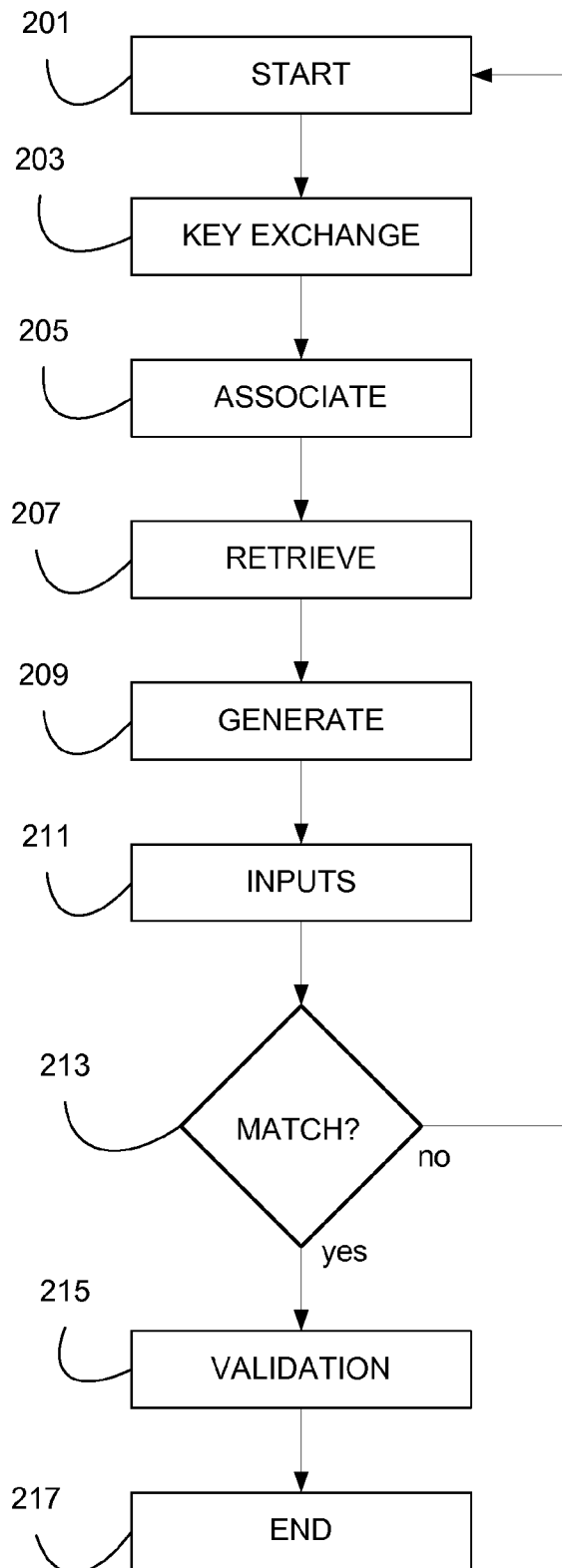
25

FIGURE 1A

FIGURE 1B

2/2

201 — START

203 — KEY EXCHANGE

205 — ASSOCIATE

207 — RETRIEVE

209 — GENERATE

211 — INPUTS

213 — MATCH?

no

yes

215 — VALIDATION

217 — END

FIGURE 2

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/36
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 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 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	US 2014/372754 A1 (AISSI SELIM [US] ET AL) 18 December 2014 (2014-12-18) abstract; figures 8-10 paragraph [0004] - paragraph [0006] paragraph [0020] - paragraph [0021] paragraph [0028] - paragraph [0029] paragraph [0047] paragraph [0070] - paragraph [0098] claims 1-20 -----	1-8

☐ 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	Date of mailing of the international search report
12 April 2016	20/04/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Powell, David

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT
Information on patent family members

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US 2014372754 A1	18-12-2014	AU	2014311784 A1	21-01-2016
		CN	105453483 A	30-03-2016
		EP	3008854 A2	20-04-2016
		US	2014372754 A1	18-12-2014
		WO	2015030903 A2	05-03-2015