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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 May 2014 (22.05.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/075734 A1

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04W 12/06* (2009.01) *G07C 9/00* (2006.01)

(21) International Application Number:
PCT/EP2012/072837

(22) International Filing Date:
16 November 2012 (16.11.2012)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **TELEFONAKTIEBOLAGET L M ERICSSON (publ)** [SE/SE]; S-164 83 Stockholm (SE).

(72) Inventors: **KÄRENEN, Ari**; Topparoikka 2E15, FI-02400 Kirkkonummi (FI). **ARKKO, Jari**; Välitie 1B, FI-02700 Kauniainen (FI).

(74) Agent: **ANDERSSON, Per**; Zacco Sweden AB, P.O. Box 142, SE-401 22 Göteborg (SE).

(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, 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, PA, 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, 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))*

(54) **Title**: VICINITY-BASED MULTI-FACTOR AUTHENTICATION

(57) **Abstract**: The invention relates to a wireless device, configured for ensuring authentication of a user, to a reference unit configured for ensuring authentication of a user of the wireless device and to a method for ensuring authentication of a user. The wireless device (1) comprises a checking unit (2) configured for scanning a distance to a reference unit (3) and for checking if the distance scanned lies within a predetermined range such that authentication of the user is ensured. In this way, a wireless device is provided which is simple and cost-effective to realize and increases security by making sure that the rightful owner is available without the need of asking for PIN codes, passwords or other measures, such as biometric recognition, i.e. voice recognition, fingerprint recognition, retina recognition and the like.

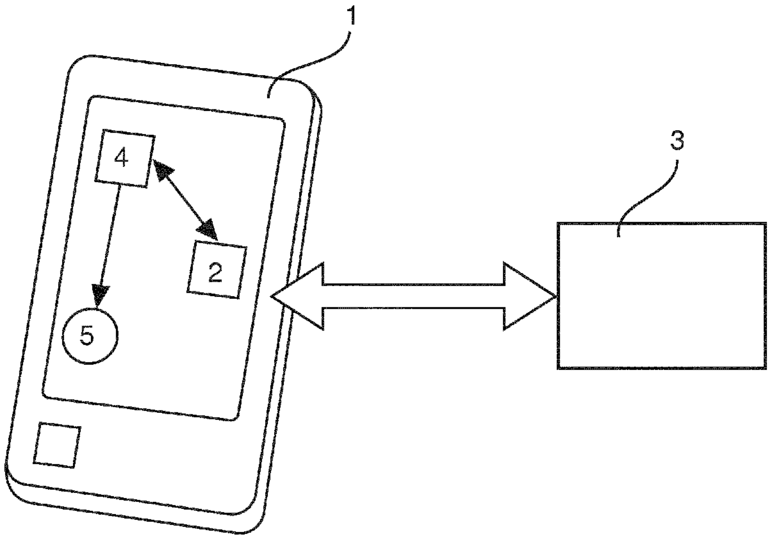

Fig. 1

Title

Vicinity-based multi-factor authentication

Technical Field

The invention relates to a wireless device, configured for ensuring authentication of a user.

Background

Wireless devices, such as Smartphones, are more and more replacing various other daily items individual persons carry along with them ranging from credit cards to home keys. Typically a home door is opened or an item is bought from a shop by swiping a mobile device, such as a phone, next to a receiver and optionally inserting a PIN code or a password on the phone. If the Smartphone is stolen or lost somewhere, anyone finding it could make payments or open doors on behalf of the rightful owner. Instead of having merely the possession of the Smartphone some form of extra security is required for authenticating the correct user. Usually a simple solution is to use a PIN code or a password on the device every time it is used but this is rather tedious since it requires user interaction and additionally remembering passwords or PIN codes, respectively. Further, a bystander may see the password or recognize the PIN code and if he or she steals the phone, he or she could have access to everything that is authenticated with the phone and the password.

Summary

It is the object of the invention to provide a possibility for authenticating a user with increased security which should be simple and cost-effective to realize while at the same time avoids using passwords, PIN codes or other measures, such as biometric recognition, for instance voice recognition, fingerprint recognition or retina recognition.

This object is achieved by the subject matter of the independent claims. Preferred embodiments are defined in the sub claims.

According to a first aspect of the invention, this object is achieved by a wireless device, configured for ensuring authentication of a user, comprising a checking unit configured for scanning a distance to a reference unit and for checking if the distance scanned lies within a predetermined range such that authentication of the user is ensured.

It is an idea of the invention to carry out a proximity measurement between two units, such as between a checking unit of the wireless device and a reference unit which is not part of the wireless device. The idea is based on the fact that two separate units are most likely not stolen or not lost at the same time. Thereafter, the measurement result is analyzed in order to check if authentication of the user should be approved. The wireless device preferably corresponds to a Smartphone or to a mobile device, such as a cell phone, or to any other equipment, such as a wristwatch or jewellery. The checking is preferably done by using radio techniques such as radio-frequency identification, RFID for short, in near field communication, NFC for short, applications, Bluetooth, ZigBee or similar technologies. The term “scanning a distance” means that a distance between the two units is measured, wherein the measurement can be performed in different ways. Preferably the measurement is done in certain predefined time intervals which repeat themselves in equidistant or non-equidistant steps or the measurement is performed constantly. It is also possible that the measurement is performed once during a predefined time period dependent on an action of a user.

According to a preferred embodiment of the invention, the checking unit is further configured for running a cryptographic challenge-response protocol which requests the reference unit to prove its identity using a shared secret cryptography and/or a public key cryptography while scanning the distance to the reference unit such that it is ensured that the wireless device and the reference unit are assigned to each other. The wireless device is thus reliable since the reference unit preferably signs a portion of data provided by the checking unit using a private key or a shared secret cryptography. The reference unit preferably proves by signing with its private key that it is the legitimate holder of the public key identity. Preferably, the cryptographic challenge-response protocol requests a public key identity of the reference unit and the public key identity of the reference unit matches the public key identity stored at the checking unit. With the matching it is preferably ensured that no attacker can pretend to be the reference unit since it is checked that the device with the right identification, ID for short, is present, for instance by additionally asking for a PIN code or for a password or by scanning an object which is in close proximity to identify predefined spatial features of the object.

According to a preferred embodiment of the invention, the predetermined range is selected by pairing the checking unit with the reference unit in such a way that the checking unit requests the position of the reference unit before calculating the distance between the reference unit and the checking unit. The term “position” refers to an “absolute position” but can also refer to a "relative position" dependent on the actual context or situation. Such a pairing can also be used in Bluetooth applications, also called Bluetooth pairing, and works in a first step with teaching, for instance, a phone that a headset is associated with it and, in a second step, the headset is taught that the phone is bonded to it.

According to a preferred embodiment of the invention, the predetermined range is adjusted by varying the radio power level at the checking unit and measuring the position of the reference unit such that the distance between the reference unit and the checking unit is extracted and compared with predetermined reference data. The predetermined reference data preferably comprises the predetermined range and is preset by previous measurements and/or preset to a range which is based on empiric values. An actual measurement may change the predetermined range such that it is adjusted to a different range fitting to the actual measurement result.

According to a preferred embodiment of the invention, the checking unit is further configured for detecting that at least one security unit is arranged within the predetermined range to the reference unit. Hence, there is no need for using passwords while at the same time security is increased so that the wireless device is able to check that a plurality of additional security devices, ASDs for short, are arranged in its vicinity to make sure that the wireless device is still with its rightful owner. By increasing the number of ASDs security can still be increased. The wireless device preferably uses short range radio and contacts the ASDs. Based on their capabilities the wireless device preferably checks that the plurality of ASDs is in close proximity to a reference unit or the wireless device performs a cryptographic challenge-response protocol to make sure that there is no attacker pretending as one of the ASDs. The ASDs are preferably integrated into other items that the user is carrying along anyway, such as into a wristwatch or into jewellery, or the ASD is a separate device, such as a key fob or a key chain. Preferably, the at least one security unit is configured for sending a command to an application unit which is configured for running a program ensuring authentication of the user, wherein the application unit is integrated into the wireless device. When the distance between the reference unit and the checking unit or the distance between the reference unit and the at least one security unit lies outside the predetermined range such that authentication of the user fails, the checking unit is preferably further configured for requesting a password and/or a PIN code from the user and/or for performing biometric recognition, such as voice recognition, fingerprint recognition and/or retina recognition. This way, these additional measures can further increase reliability and security. The voice recognition is preferably carried out by recording the voice of the user and comparing it with recorded data stored on the wireless device or in a database on a server.

According to a preferred embodiment of the invention, the at least one security unit is integrated into the wireless device. Therefore, the wireless device can be built very compact.

According to another preferred embodiment of the invention, the at least one security unit is integrated into a wristwatch, into jewellery, into clothing, into luggage, into a laptop, into a key fob or into a key chain. Hence, it is an idea of the invention that the security unit is positionable anywhere outside the wireless device and thus security further increases.

According to a second aspect of the invention, above mentioned object is achieved by a reference unit configured for ensuring authentication of a user of the wireless device according to the first aspect of the invention, wherein the reference unit is integrated into clothing, such as a hat, a shirt or underwear. Hence, the reference unit is not only allowed to be arranged at a fixed position but can also be carried along with the user.

According to a third aspect of the invention, above mentioned object is achieved by a method for ensuring authentication of a user comprising the steps of: a) scanning a distance to a reference unit and b) checking if the distance scanned in step a) lies within a predetermined range such that authentication of the user is ensured.

According to a preferred embodiment of the invention, the method further comprises the step of detecting that at least one security unit is arranged within the predetermined range to the reference unit. The method preferably further comprises the step of sending a command to an application unit which is configured for running a program ensuring authentication of the user.

Brief description of the drawings

Further objects and advantages of the present invention will become apparent from the following description of the preferred embodiments that are given by way of example with reference to the accompanying drawings. In the figures:

Fig. 1 shows a wireless device according to a first preferred embodiment of the invention;

Fig. 2 illustrates the steps of a method for ensuring authentication of a user according to a second preferred embodiment of the invention; and

Fig. 3 schematically illustrates the steps of the method according to the second preferred embodiment of the invention.

Detailed description

Fig. 1 shows a wireless device configured for ensuring authentication of a user according to a first preferred embodiment of the invention. The wireless device 1 comprises a checking unit 2 which scans a distance to a reference unit 3 which is not part of the wireless device 1. Furthermore, the checking unit 2 checks if the distance measured lies within a predetermined range such that authentication of the user is ensured. The predetermined range is set to an empirical value in this first preferred embodiment. The checking unit 2 measures a distance to the reference unit 3 which lies outside the wireless device 1 and compares the result with previous measurement results stored in a database in this first preferred embodiment. According to this first preferred embodiment of the invention the reference unit 3 corresponds to a passive RFID chip which does not need any battery and is arranged at a fixed position on a ground. According to other preferred embodiments of the invention, the reference unit 3 is integrated into underwear. Furthermore, the checking unit 2 detects one security unit 4 that is arranged within the predetermined range to the reference unit 3. This way it is guaranteed that the measurement results are verified which increases security. The security unit 4 sends a command to an application unit 5 which runs a program and is integrated into the wireless device 1. The application serves for opening a door in this first preferred embodiment of the invention.

Fig. 2 schematically shows a method for ensuring authentication of a user according to a second preferred embodiment of the invention. Initially, i.e. before a predetermined action, such as walking to a door and opening the door is performed, a Smartphone is paired with a headset and a key is exchanged. Afterwards, a proximity measurement between the checking unit 2 and the reference unit 3 as in the first preferred embodiment is performed and based on the result of this step the door is opened or it is refused to be opened. Basically, it is checked if the user is near the door. If yes, the distance to the reference object 3 is measured. If the reference object 3 is nearby, the door is opened and the method reaches its end. If the door is not nearby the method can also reach its end. Alternatively, if the distance to the reference object cannot be measured regardless for whatever reason, a PIN code is asked for and if the PIN code is verified, then the door is opened. Otherwise the method also reaches its end. Hence, security for Smartphone-based transactions and authorization is increased. Many wireless devices, such as Smartphones, already have various short range radios and it is thus simple to re-use them. Further, a dynamic security level is adjustable, i.e. if required after detecting a number of ASDs it is further asked for a pin code, for a password and/or voice recognition or similar measures are performed.

Fig. 3 schematically illustrates the steps of the method according to the second preferred embodiment of the invention. In a first step, the distance to a reference unit is scanned 6. Thereafter, in the checking step 7 it is controlled whether the distance scanned in the first step 6 lies within a predetermined range. In further steps, it is detected 8 that at least the one security unit is arranged within the predetermined range to the reference unit. Finally, a command is sent 9 to an application unit which is configured for running a program ensuring authentication of the user. In its simplest form, one application and one Bluetooth device is used.

While the invention has been illustrated and described in detail in the drawings and foregoing description, such illustration and description are to be considered illustrative or exemplarily and not restrictive; the invention is not limited to the disclosed embodiments.

Other variations to the disclosed embodiments can be understood and affected by those skilled in the art in practicing the claimed invention, from a study of the drawings, the disclosure, and the appended claims. In the claims, the word "comprising" does not exclude other elements or steps, and the indefinite article "a" or "an" does not exclude a plurality. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that the combination of these measures cannot be used to advantage. Any reference signs in the claims should not be construed as limiting the scope.

Claims:

1. A wireless device (1), configured for ensuring authentication of a user, comprising:

a checking unit (2) configured for scanning a distance to a reference unit (3) and for checking if the distance scanned lies within a predetermined range such that authentication of the user is ensured.

2. The wireless device according to claim 1, wherein the checking unit (2) is further configured for running a cryptographic challenge-response protocol which requests the reference unit (3) to prove its identity using a shared secret cryptography and/or a public key cryptography while scanning the distance to the reference unit (3) such that it is ensured that the wireless device (1) and the reference unit (3) are assigned to each other

3. The wireless device according to claim 2, wherein the cryptographic challenge-response protocol requests a public key identity of the reference unit (3) and the public key identity of the reference unit (3) matches the public key identity stored at the checking unit (2).

4. The wireless device according to claim 1, wherein the predetermined range is selected by pairing the checking unit (2) with the reference unit (3) in such a way that the checking unit (2) requests the position of the reference unit (3) before calculating the distance between the reference unit (3) and the checking unit (2).

5. The wireless device according to claim 1, wherein the predetermined range is adjusted by varying the radio power level at the checking unit (2) and measuring the position of the reference unit (3) such that the distance between the reference unit (3) and the checking unit (2) is extracted and compared with predetermined reference data.

6. The wireless device according to one of the preceding claims, wherein

the checking unit (2) is further configured for detecting that at least one security unit (4) is arranged within the predetermined range to the reference unit (3).

7. The wireless device according to claim 6, wherein the at least one security unit (4) is configured for sending a command to an application unit (5) which is configured for running a program ensuring authentication of the user, wherein the application unit (5) is integrated into the wireless device (1).

8. The wireless device according to one of claims 6 and 7, wherein when the distance between the reference unit (3) and the checking unit (2) or the distance between the reference unit (3) and the at least one security unit (4) lies outside the predetermined range such that authentication of the user fails, the checking unit (2) is further configured for requesting a password and/or a PIN code from the user and/or for performing biometric recognition, such as voice recognition, fingerprint recognition and/or retina recognition.

9. The wireless device according to one of claims 6 to 8, wherein the at least one security unit (4) is integrated into the wireless device (1).

10. The wireless device according to one of claims 6 to 8, wherein the at least one security unit (4) is integrated into a wristwatch, into jewellery, into clothing, into luggage, into a laptop, into a key fob or into a key chain.

11. A reference unit (3) configured for ensuring authentication of a user of a wireless device (1) according to one of claims 1 to 10, wherein the reference unit (3) is integrated into clothing, such as a hat, a shirt or underwear.

12. A method for ensuring authentication of a user, comprising the steps of:
a) scanning (6) a distance to a reference unit (3) and
b) checking (7) if the distance scanned in step a) lies within a predetermined range such that authentication of the user is ensured.

13. The method according to claim 12, further comprising the step of detecting (8) that at least one security unit (4) is arranged within the

predetermined range to the reference unit (3).

14. The method according to claim 13, further comprising the step of sending (9) a command to an application unit (5) which is configured for running a program ensuring authentication of the user.

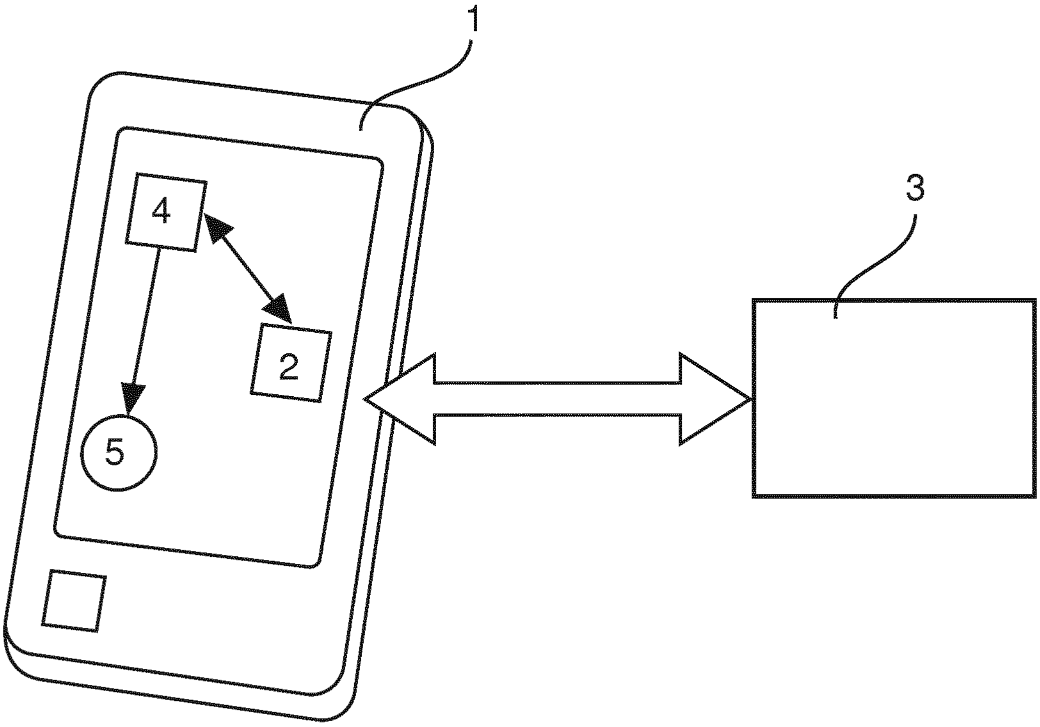

Fig. 1

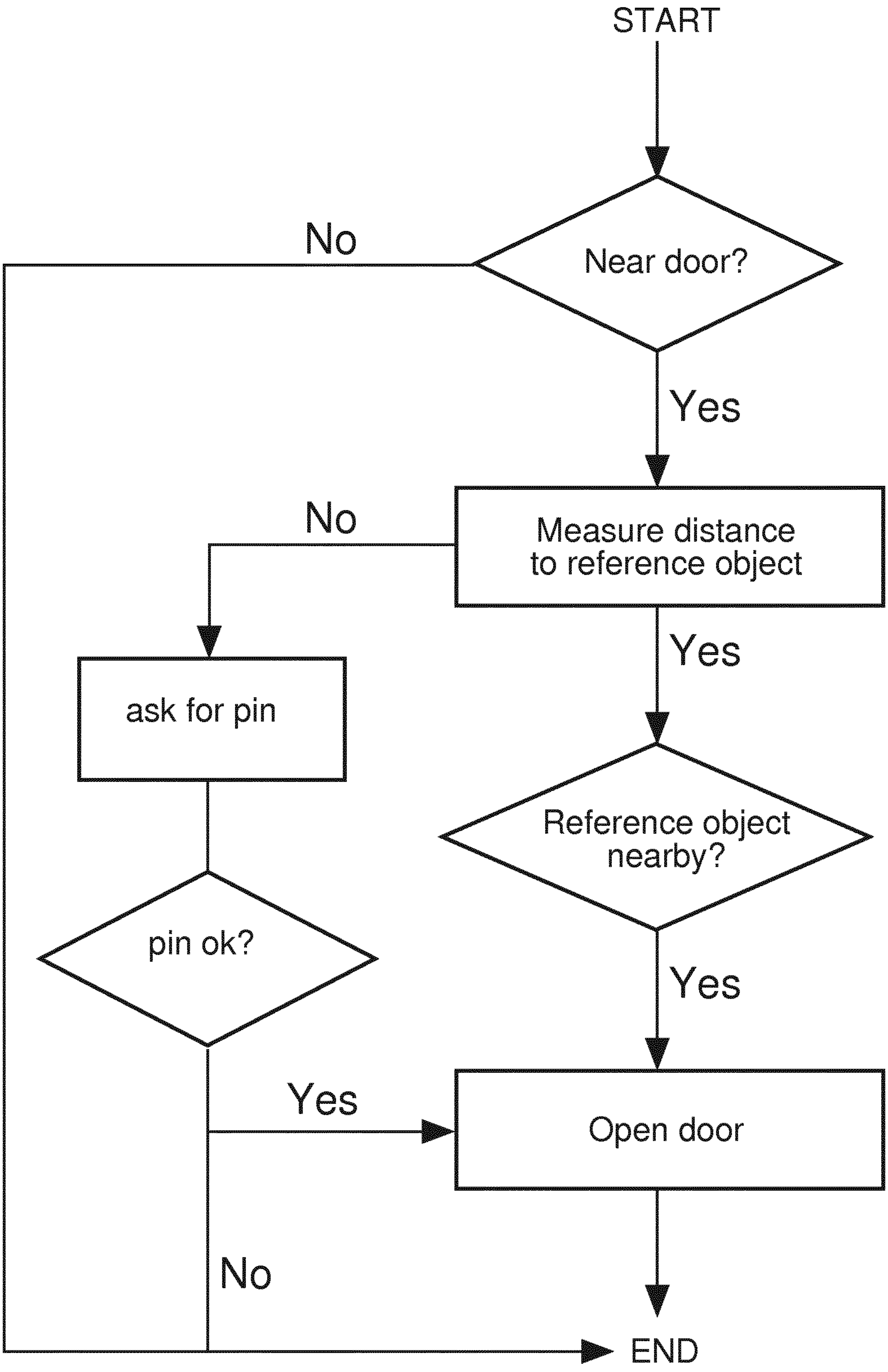
START
Near door?
No
Yes
Measure distance to reference object
No
Yes
ask for pin
Reference object nearby?
pin ok?
Yes
Yes
Open door
No
END

Fig. 2

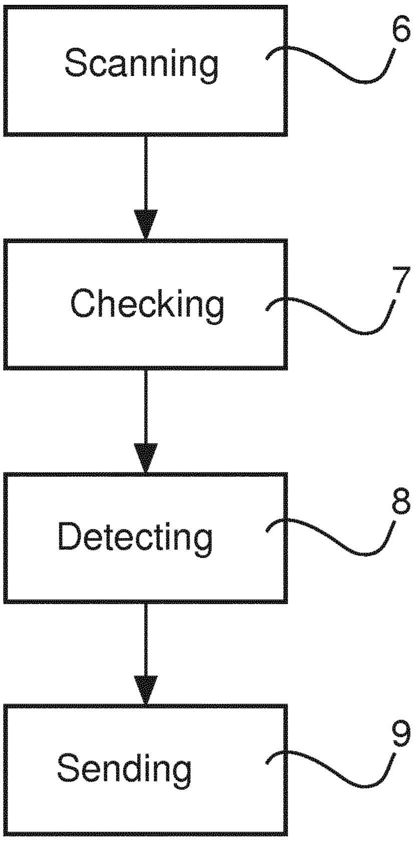

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/072837

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 G07C9/00 H04W12/06
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)
G07C H04L H04W G06F

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 2010/201482 A1 (ROBERTSON WILLIAM BENJAMIN [US] ET AL) 12 August 2010 (2010-08-12) abstract paragraph [0037] -----	1-14
X	DA-ZHI SUN ET AL: "A new design of wearable token system for mobile device security", IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, IEEE SERVICE CENTER, NEW YORK, NY, US, vol. 54, no. 4, 1 November 2008 (2008-11-01), pages 1784-1789, XP011239747, ISSN: 0098-3063, DOI: 10.1109/TCE.2008.4711235 abstract Sections I. III and IV ----- -/--	1-14

☒ 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 9 August 2013	Date of mailing of the international search report 20/08/2013
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 Bertolissi, Edy

1

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2012/072837

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JANSEN WAYNE A: "Authenticating Users on Handheld Devices", PROCEEDINGS OF THE CANADIAN INFORMATION TECHNOLOGY SECURITY SYMPOSIUM, MAY 2003, , 1 May 2003 (2003-05-01), pages 1-12, XP001556178, Retrieved from the Internet: URL:http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_devices/PP-AuthenticatingUsersOnPDAs.pdf Introduction Overview Proof by Possession -----	1-14
X	US 2008/055041 A1 (TAKENE KOUICHI [JP] ET AL) 6 March 2008 (2008-03-06) abstract paragraph [0031] - paragraph [0054] figures 1, 2 -----	1-14
X	US 2011/314539 A1 (HORTON MICHAEL [US]) 22 December 2011 (2011-12-22) abstract paragraph [0042] - paragraph [0049] -----	1-14
X	JANSEN W ET AL: "Proximity Beacons and Mobile Device Authentication: An Overview and Implementation", NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY,, 1 June 2005 (2005-06-01), XP008116239, page 5 - page 12 -----	1-14
A	HASAN AKRAM ET AL: "Laws of Identity in Ambient Environments: The HYDRA Approach", MOBILE UBIQUITOUS COMPUTING, SYSTEMS, SERVICES AND TECHNOLOGIES, 2008. UBICOMM '08. THE SECOND INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 29 September 2008 (2008-09-29), pages 367-373, XP031345722, ISBN: 978-0-7695-3367-4 abstract Sections 1 and 3 -----	1-14

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2012/072837

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010201482 A1	12-08-2010	AU 2010214013 A1	25-08-2011
		CA 2751893 A1	19-08-2010
		EP 2396984 A2	21-12-2011
		JP 2012517541 A	02-08-2012
		US 2010201482 A1	12-08-2010
		WO 2010093499 A2	19-08-2010
US 2008055041 A1	06-03-2008	CN 101135208 A	05-03-2008
		JP 4996175 B2	08-08-2012
		JP 2008057129 A	13-03-2008
		KR 20080020506 A	05-03-2008
		TW 200829781 A	16-07-2008
		US 2008055041 A1	06-03-2008
US 2011314539 A1	22-12-2011	NONE	