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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 January 2012 (05.01.2012)

PCT

(10) International Publication Number
WO 2012/001614 A1

(51) **International Patent Classification:**
H04L 9/00 (2006.0 1) ***E06B 7/30*** (2006.0 1)
H04L 9/32 (2006.0 1) ***G07C 9/00*** (2006.0 1)

(21) **International Application Number:**
PCT/IB20 11/052820

(22) **International Filing Date:**
27 June 201 1 (27.06.201 1)

(25) **Filing Language:** Italian

(26) **Publication Language:** English

(30) **Priority Data:**
GE2010A000072 1 July 2010 (01 .07.2010) IT

(72) **Inventor; and**
(71) **Applicant : GHIO, Marco** [IT/IT]; via G.B. Monti 27/41, 1-1615 1 Genova (GE) (IT).

(74) **Agent: LUNATI & MAZZONI S.R.L.;** Via Carlo Pisacane 36, 1-20129 Milano (IT).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available):* AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

WO 2012/001614 A1

(54) Title: AUTHENTICATION DEVICE OF A SUBJECT MAKING A HOUSE CALL

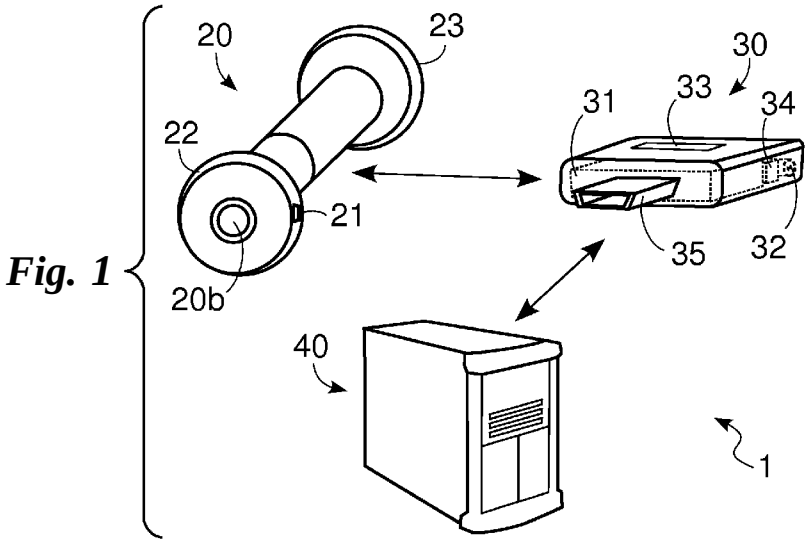


Fig. 1

(57) Abstract: It is provided an authentication device (1) of a subject making a house call comprising a fixed terminal (20) adapted to be fastened in the vicinity of an entrance (10) of the house; a mobile terminal (30) including identification data of the coming subject and adapted to be carried by the coming subject in the vicinity of the entrance (10); the fixed terminal (20) being adapted to be brought into connection with the mobile terminal (30), so as to receive the activation energy from the mobile terminal (30) and therefore identify it.

AUTHENTICATION DEVICE OF A SUBJECT MAKING A HOUSE CALL

The present invention relates to an authentication device for a subject paying a house call or visit, of the type pointed out in the preamble of the first claim.

In particular, the invention relates to a device that, in case of a visit to an office or a dwelling, is able to carry out preventive verification and control of the visitor's identity and therefore enables the resident to grant the visitor access to the office/house in full security.

It is known that house calls are necessary for carrying out services of public interest such as for instance notification of deeds, delivery of registered letters, meter reading for the different user bases, interventions for extraordinary maintenance. In addition, house calls are often made by suitable staff that, for commercial purposes, perform a "door-to-door" activity for selling goods or offering services and promoting activities.

For the above reasons, the resident is often obliged to open the door to unknown visitors whose identity he/she is therefore unable to ascertain, unless he/she bases himself/herself on that which is declared or shown by the visitor. This lack of knowledge concerning a visitor is frequently utilised as an expedient by delinquents that, giving wrong personal particulars, succeed in illegally getting into the resident's houses.

Very often the victims of these tricks are "weak" persons such as persons living alone, old people, disabled people or all those categories having low self-defence and reaction capacity, easily prone to persuasion on the basis if a simple declaration by the visitor. In particular, for easily verifying the visitor's identity, they are often brought to instinctively open the door on ringing of the bell thus determining elimination of the only efficient protection for their

defence.

In order to solve this problem many front doors have been provided with a peephole, i.e. a through hole adapted to enable the resident to see the visitor and therefore carry out a first evaluation of same.

This solution however is weakly reliable because it can be easily overcome by the delinquent who may wear a uniform or show previously prepared visiting cards or a badge.

In order to solve this problem, the institutions have made available specific freephone numbers against fraud that are directly coordinated by the police and enable control of the identity by a telephone call to these numbers.

Unfortunately, this operation is often neglected by the resident who, due to inattention, lack of information, laziness, confidence, opens the door and enables access to the house without any certification.

Therefore, taking into account the importance of a correct identification of the visitor, many apparatus have been developed that utilising videocameras, microphones or other similar means allow opening of the door by the resident only after the visitor has been recognised.

A first example is described in patent US20030861 86A1 in which a videocamera is used for catching the visitor and a display enabling the resident to obtain a convenient and quick image of the visitor.

Another device is described in patent WO2007012831A1 .

In this document, arrangement of a particular fixed terminal is provided which is placed at the front door and is equipped with a database containing the visitors' data and with an identification system made up of keyboard and microphone.

According to the provided authentication process, the visitor types in his/her identification code on the keyboard, speaks on the microphone and the device opens the door and allows access only if the visitor's voice is substantially coincident with that stored in the database in correspondence with the previously inputted code.

In other authentication apparatus, in addition to use of the aforesaid fixed terminal, adoption of a mobile terminal is provided, for example a mobile phone, in possession of the visitor.

A first example of these authentication apparatus is described in patent US2007085662A1 disclosing a fixed terminal, i.e. the terminal placed at the door, comprising a videocamera, a database and a screen.

According to the authentication procedure described in this patent, when the visitor comes close to the front door, he/she must send, through the mobile terminal, a code to the fixed terminal that retrieves in the database, a first image corresponding to the code it has received, records a second image of the visitor through the videocamera and then shows the two images to the resident who decides on opening the door or not.

Further examples of these authentication apparatus are disclosed in patent US2005060555A1 and in document "Personal Servers as Digital Keys" by Allan Beaufour.

In this case, when the visitor comes to the front door, the fixed terminal sends an encrypted signal to the mobile terminal that, based thereon, creates a second signal which, in turn, is sent to the fixed signal that will verify whether it is correct and will grant access to the visitor.

The above described known art has some important drawbacks.

A first important fault resides in the complexity of known authentication apparatus. In particular, this fault can be found in the fixed terminals placed at the front door which, being provided with a complex identification system, are both very complicated in manufacture and very expensive.

Another problem is represented by the fact that fixed devices, due to their complexity, are of difficult assembly at the front door.

In particular, due to the above described identification means, the fixed terminal is particularly bulky and therefore of difficult installation. This problem is further increased by the presence of powering means consisting of a battery and/or electric cables electrically feeding the fixed terminal by connecting it to the mains.

A further problem consists in the high installation cost of known authentication apparatus because, due to the bulkiness of same and the required connections for operation, they are not suitable for the front door presently in use and therefore replacement of these doors is required.

Another important problem resulting from the complexity of the authentication device is represented by the poor reliability of same and the reduced lifetime.

Under this situation, the technical task underlying the present invention is to conceive an authentication device of a subject paying a house call capable of substantially obviating the mentioned drawbacks.

Within the scope of this technical task, it is an important aim of the invention to provide an authentication device of simple manufacture and reduced costs.

Another important aim of the invention consists in obtaining an authentication device of easy installation.

A further aim of the invention is to make available an authentication device

that is adapted for the presently used front doors, i.e. without being obliged to replace them.

Also an important result of the invention is the achievement of an authentication device characterised by high reliability that practically does not require servicing.

The technical task mentioned and the aims specified are achieved by an authentication device of a subject paying a house call as claimed in the appended Claim 1.

Preferred embodiments are highlighted in the sub-claims.

The features and advantages of the invention are hereinafter clarified by the detailed description of a preferred embodiment of the invention, with reference to the accompanying drawings, in which:

Fig. 1 as a whole shows an authentication device of a subject paying a house call in accordance with the invention;

Fig. 2 shows a component of the authentication device disposed at an entrance; and

Fig. 3 highlights, through a block diagram, an authentication process utilising the authentication device.

With reference to the drawings, the authentication device of a subject making a house call in accordance with the invention is generally identified by reference numeral **1.**

It is adapted to be used for verifying the identity of a subject making a house call in a building, flat or office. Device 1 can therefore be positioned at an entrance **10** such as a door or gate or other similar element and is adapted to prevent access to the house without the resident's consent.

The authentication device 1 fundamentally comprises a fixed terminal **20** adapted to be connected in the vicinity of an entrance 10 and a mobile terminal **30** adapted to be carried by the coming subject and to be brought into connection with the fixed terminal 20.

The mobile terminal 30, shown in Fig. 1, consists of an electronic device comprising a storage component **31** adapted to store information such as alphanumeric codes for example, a battery **32,** preferably of the rechargeable type, or other powering systems adapted to enable energy supply to at least said storage component 31. The mobile terminal 30 therefore may selectively consist of a mobile phone, a USB (Universal Serial Bus) key suitably provided with a battery 32 or other similar device. Preferably, the mobile terminal 30 is a USB key comprising a battery 32.

The mobile terminal 30 can be further provided with a recognition apparatus **33** adapted to enable use of the mobile terminal 30 exclusively by authorised subjects and a time meter **34** adapted to measure elapsing of time and to enable the mobile terminal 30 to know, date and time, instant by instant, i.e. the elapsed time from creation of the first signal.

The time meter 34 can consist of a clock/watch or other similar device adapted to enable the mobile terminal 30 to know date and time, at each instant. Alternatively, it may consist of a decreasing counter, a timer for example that, as better clarified in the following, enables the residual lifetime of the data stored in the mobile terminal 30 to be quantified.

The recognition apparatus 33 can consist, if it is a mobile phone, of a keypad adapted to enable introduction of a PIN (Personal Identification Number) or, if it is a USB key, of a fingerprint reader or other similar apparatus adapted to

identify the subject using the mobile terminal 30.

In order to enable the coming subject to mutually connect the two terminals 20 and 30, as hereinafter clearly described, the mobile terminal 30 and fixed terminal 20 comprise first connecting means **35** and **21** respectively, that is adapted to carry out connection.

Said first means 35 and 21 is suitable to make a connection capable of allowing at least passage of current between the two terminals 20 and 30 so as to enable the mobile terminal 30 to supply the fixed terminal 20 with the activation energy, i.e. the energy adapted to enable the fixed terminal 20 to be activated and carry out the authentication process described below.

In addition, the first connecting means 35 and 21 creates a data passage connection between the mobile terminal 30 and fixed terminal 20 so as to enable the mobile terminal 30 to provide the fixed terminal 20 with data necessary for authentication of the coming subject.

The first connecting means 35 and 21 therefore may consist of USB (Universal Serial Bus) connectors or other similar means adapted to allow both passage of current and passage of data between terminals 20 and 30.

In particular, in some cases, to facilitate connection between the two terminals 20 and 30, device 1 can have a further connecting means such as a cable having two USB connectors at the ends so as to be connected to the first means 35 and 21, and therefore being operatively interposed between terminals 20 and 30.

The fixed terminal 20 is fastened in the vicinity of entrance 10, for example to a wall portion close to said entrance, and preferably terminal 20 is secured to the entrance itself. More preferably, the fixed terminal 20 is housed in the

through hole **10a** present in the entrance 10 that is usually employed as a peephole.

In order to enable the fixed terminal 20 to be housed in the through hole 10a, the fixed terminal 20, as shown in Fig. 1, comprises an outer block **22,** facing the outside of the house and an inner block **23** facing the inside of the house, which blocks have a portion of smaller section adapted to be inserted in the through hole 20a, and a portion of bigger section adapted to abut against the entrance 10.

In addition, the fixed terminal 20 has tightening means **24** adapted to mutually fasten blocks 22 and 23 at the through hole 10a bringing them into abutment with the entrance 10 on opposite sides relative to said entrance. In particular, the tightening means 24 consists of screws, threaded couplings, friction fits or other similar elements adapted to mutually fasten blocks 22 and 23 varying their distance and therefore the length of the fixed terminal 20 so as to make the sizes of the fixed terminal 20 suit the thickness of said entrance 10.

Preferably, the tightening means 24 is positioned in such a manner that said means is operable for assembling or disassembling the two blocks 22 and 23 exclusively from the inside of their housing seat. Therefore said means 24, if screws for example, have their head at the inner block 23, as shown in Fig. 2.

The outer block is adapted to be connected to the mobile terminal 30 and therefore has said connecting means 21 such arranged that it can be brought into connection for data and power passage with the mobile terminal 30.

The inner block 23 is adapted to perform the authentication process and therefore it comprises a card **23a** adapted to process the information of the mobile terminal 30 so as to perform authentication of the coming subject, and

signalling members **23b** adapted to signal the presence of the coming subject and the occurred authentication to the resident.

The signalling members 23b is adapted to carry out signalling of the presence of an authenticated coming subject through emission of a suitable acoustic and/or visual signal. Therefore they can comprise a loud-speaker adapted to reproduce a message or a sound and/or LEDs or other similar means adapted to emit a light signal.

To enable the card 23a to have the necessary power and data for carrying out authentication of the coming subject, the card 23a and therefore the inner block 23 are brought into connection for data and power passage with the outer block 22 and therefore the mobile terminal 30.

To this aim the fixed terminal 20 comprises second connecting means **25** adapted to carry out such a connection between the two blocks 22 and 23.

Preferably, the second connecting means 25 consists of sliding/revolving contacts or other similar means adapted to carry out an electric connection between two components, i.e. blocks 22 and 23, irrespective of their mutual position.

In particular, the second connecting means 25 consists of sliding contacts and, more particularly linear sliding contacts adapted to connect the two blocks 22 and 23, irrespective of the sizes of the fixed terminal 20. The second connecting means 25 therefore consists of plates that, when the two blocks 22 and 23 are joined, comes mutually into contact and consequently carry out connection between the two blocks 22 and 23.

The second connecting means 25 is preferably made of gold or other material that does not oxidise when in contact with air.

Finally, in order to enable the resident to see the coming subject before opening the door, blocks 22 and 23 are provided with inner recesses that, when tightening is carried out, comes into mutual alignment so as to define an inner hole **20a** substantially coaxial with the through hole 10a, through which the resident can visually identify the coming subject.

In particular, the fixed terminal 20 can comprise at least one lens **20b** disposed in register with the inner hole 20a and adapted to improve the quality and width of the field of vision through said through hole. Preferably, lens 20b consists of a wide-angle lens capable of widening the field of vision of the resident and is fastened to the outer block 22.

The authentication device 1 is finally associable with a central server **40** comprising a database including the identification codes of all houses/offices, provided with a fixed terminal 20, the identification codes of the subjects/companies provided with a fixed terminal 20, and the history of all visits paid. In the database of the central server 40 also the identification codes of the coming subjects are present, i.e. the codes enabling the mobile terminal 30 to identify the coming subject through the recognition apparatus 33.

It is adapted to generate the first authentication signal and therefore supply the mobile terminal 30 with the necessary data for authentication. Therefore the central server 40 can consist of a computer or other similar device adapted to be connected to the mobile terminal 30 through the connecting means 35, for example.

Alternatively, if terminal 30 is a mobile phone, this connection can be a Bluetooth connection or other wireless connection typical of a mobile phone.

The invention comprises a new authentication process **100** for identifying a subject making a house call.

In this process, provision is made for a hashing calculation in combination with a shared secret consisting of the calculation algorithm and of elements that are fully known by the central server 40, while they are only partly known by the fixed terminal 20. In detail, as hereinafter better described, the fixed terminal 20, receiving the missing data in a plain form through the mobile terminal 30, is able to calculate an authentication signal of its own in an autonomous manner. If this signal is fully coincident with the signal stored by the central server 40 on the mobile terminal 30, the fixed terminal certifies the identity of the coming subject asking for entry.

Alternatively, process 100 is based on an asymmetric scheme cryptography, i.e. a cryptography in which the key used for encrypting the information differs from the key used for decrypting the information.

It should be pointed out that in both the aforesaid cases the mobile terminal 30 only carries out a function of making server 40 and fixed terminal 20 communicate with each other but it does not implement any information decrypting procedure.

The authentication process 100, diagrammatically shown in Fig. 3, contemplates an association step **110** in which the coming subject is associated with a first authentication signal; a connection step **120** in which the two terminals are mutually connected; an authentication step **130** in which the identity of the coming subject is ascertained; and a signalling step **140** in which the presence of the coming subject is signalled.

In the association step 110 the coming subject before coming to the house,

connects the mobile terminal 30 to the central apparatus 40 to which, in order to obtain the first authentication signal, communicates the house he/she wishes to visit, the date and time of the visit and, more specifically, the date and time band in which the visit is foreseen.

The central apparatus 40 retrieves the identification codes corresponding to the residence that is wished to be visited and to the mobile terminal 30 connected thereto and processes the first authentication signal. In particular, this first authentication signal substantially consists of an alphanumeric code suitably processed by apparatus 40 as a function of the theoretical visit date and time, identification code of the residence, identification code of the coming subject.

After the first authentication signal has been obtained, the central apparatus 40 combines some information in plain form to this first signal, which information as better described hereinafter will help in providing part of the information to the fixed terminal 20 in such a manner as to enable it to calculate the second authentication signal in an autonomous manner.

The central server 40 stores on the storage component 31, the first authentication signal, theoretical date and time of the visit, comprising the validity time of the first signal, that together with the identification code of the mobile terminal 30 already present on the storage element 31, constitute the data required for authentication.

In addition, during the association step 110, the coming subject can ask for several first authentication signals in order to program a series of visits to different residents and therefore different fixed terminals 20, to be made at different dates and times.

In particular, in this case the central apparatus 40 creates different first authentication signals using, for each first signal, the identifier associated with the given fixed terminal 20 of the residence to which access is wished using that particular first identification code.

At this point the association step 110 is terminated and the connection step 120 begins.

Once the coming subject has reached the entrance 10 he/she, through the recognition apparatus 33, activates the mobile terminal 30 that is therefore ready to be brought into connection with the fixed terminal 20 through the first connecting means 21 and 35.

This connection enables current and data passage between the mobile terminal 30 and fixed terminal 20. In particular, due to this connection, the fixed terminal 20 receives the energy necessary for its activation and the energy necessary for performing authentication of the coming subject from battery 32. The fixed terminal 20, through the previously made connection, receives the energy necessary to its activation, retrieves the data for authentication from the mobile terminal 30 and starts processing these data.

In particular, the fixed terminal 20 identifies among all data saved on the storage component 31, the data corresponding to the unique first signal that can be coded through the unique identifier belonging to the same fixed terminal.

After retrieval of the first authentication signal, of the identification code of the fixed terminal 20 as well as of the theoretical date and time of the visit, it calculates the second authentication signal in an autonomous manner, based both on the aforesaid data, and on data the terminal itself possesses.

In particular, it processes a second authentication signal, based on its identification code suitably stored on the fixed terminal 20 when installed, on the identification code of the mobile terminal 30 and on the theoretical date and time of the visit.

At this point, the fixed terminal 20 compares the first authentication signal obtained by the central server 40, with the second authentication signal obtained by the fixed terminal 20. At this point, if the two signals differ, the authentication gives a negative result and therefore the coming subject is not allowed to enter the residence. On the contrary, if the two signals are coincident, the authentication gives a positive result and therefore the coming subject is allowed to enter the residence.

In particular, the result of the comparison between the two signals is preferably stored on both terminals 20 and 30 and, in addition, the first authentication signal and the different data connected thereto are preferably deleted.

Should the comparison result be positive, the authentication process 100 contemplates the signalling step 140.

In this step 140, the fixed terminal 20, by utilising the signalling members 23b, announces the presence of the coming subject to the resident who, through the second through hole 20a, can carry out a further visual control on the coming subject or, alternatively, directly grant access to the subject through the entrance 10.

Once all visits have been completed, the authentication process 100 terminates with a closing step **150** in which the coming subject connects the mobile terminal 30 to the central server 40 and updates the history of the visits he/she has made storing the outcomes of said visits on server 40.

In addition, the authentication process 100 may comprise one or more verification steps that can take place at any moment after the association step 110 and before the closing step 150.

In detail, in the verification step one of terminals 20 or 30, preferably the mobile terminal 30, analyses the validity of the first authentication signal comparing theoretical date and time of the visit, corresponding to the first signals stored thereon, with the examination time, i.e. the time that when the verification step is carried out, has elapsed from creation and storage of the first signal, which time is measured through the time meter 34. In particular, in this step the mobile terminal 30 obtains the examination time from the time meter 34, i.e. the elapsed time from storage of the first signal on the mobile terminal 30, and compares said examination time with the validity time included in the theoretical date and time of the visit, i.e. the theoretical duration associated with the first signal from server 40. If the validity time of a first signal is lower than the examination time, the mobile terminal 30 deletes the first authentication signal and the data connected thereto.

The invention enables important advantages to be achieved.

A first advantage is represented by the high security degree ensured by the authentication device 1 and the authentication process 100. This security resides in the high complexity and therefore decrypting difficulty of the different authentication signals making it almost impossible to tamper with device 1 or process 100.

This impossibility of the data being tampered with is ensured by use of very complicated cryptographic algorithms making it very difficult to identify the residence corresponding to a first authentication signal and therefore to use

said first signal in a fraudulent manner.

The high security of device 1 is also ensured by the fact that card 23a, i.e. the component carrying out analysis of the signals, is housed in the inner block 23 and therefore can be hardly tampered with.

A further advantage is ensured by the fact that the first authentication signals, due to accomplishment of the verification procedure, have a time limit and therefore can be exclusively used during a given time gap.

In conclusion, due to the limited time duration of the first authentication signals and the difficulty in associating a given residence to one of said first signals, use of device 1 is impossible for an unauthorised person. This impossibility is further ensured by the recognition apparatus 33 according to which use of the fixed terminal 30 is made possible to the authorised coming subject alone.

Another advantage is represented by the fact that, unlike presently known authentication devices, device 1 can be easily incorporated into the doors presently in use without modifications being required. This advantage is given by the possibility of arranging the fixed terminal inside a housing normally present in a door or an entrance, i.e. the through hole 10a.

In addition, since powering of the fixed terminal 20 is given by the mobile terminal 30 alone, the presence of batteries, cables or other similar elements is avoided, which elements would increase the sizes of the fixed terminal 20 and make installation of same much more complicated.

A further advantage resides in that device 1 and process 100 do not grant access to the residence but merely prove the truth and reliability of the coming subject while the choice of opening or not is left to the resident.

Another important advantage is represented by the presence of a history of all

visits enabling identification, at any moment, of the person who has made the visit to a given residence at a given time.

Another achieved goal is represented by the low cost of terminals 20 and 30. In fact, the calculation complexity has been advantageously gathered on the central server 40 and therefore the fixed terminal 20 and mobile terminal 30 only need cheap and simple electronic components.

Also to be noted is the absence of operations by the resident who, in fact, must merely wait for a visual/acoustic signal emitted by the signalling members 23b.

An important goal is finally represented by the full absence of maintenance for the fixed terminal 20 because the routine maintenance for loading the authentication signals and recharging the powering battery is concentrated in the user base of the mobile terminal 30.

CLAIMS

1. An authentication device (1) of a subject making a house call comprising a fixed terminal (20) adapted to be fastened in the vicinity of an entrance (10) of said house; a mobile terminal (30) adapted to be carried by said subject making a house call in the vicinity of said entrance (10), said fixed terminal (20) being adapted to be brought into connection with said mobile terminal (30) identifying said mobile terminal (30), **characterised in that** said connection between said mobile terminal (20) and fixed terminal (30) is adapted to enable said mobile terminal (30) to supply said fixed terminal (20) with activation energy.

2. An authentication device (1) as claimed in claim 1, wherein said connection between said mobile terminal (20) and fixed terminal (30) is adapted to enable passage of data between said fixed terminal (30) and mobile terminal (20).

3. An authentication device (1) as claimed in one or more of the preceding claims, wherein said fixed terminal (30) and mobile terminal (20) comprise first connecting means (35, 21) adapted to carry out said connection, and wherein said first connecting means (35, 21) consists of USB connectors.

4. An authentication device (1) as claimed in one or more of the preceding claims, wherein said mobile terminal (30) comprises a time meter (34) adapted to enable said mobile terminal (30) to measure the elapsed time.

5. An authentication device (1) as claimed in one or more of the preceding claims, wherein said mobile terminal (30) comprises a battery (32) adapted to store energy and to enable said mobile terminal (30) to power said fixed terminal (20).

6. An authentication device (1) as claimed in one or more of the preceding claims, wherein said entrance (10) comprises a through hole (10a) adapted to enable a resident to see said coming subject without moving said entrance (10); and wherein said fixed terminal (20) is adapted to be housed in said through hole (10a).

7. An authentication device (1) as claimed in the preceding claim, wherein said fixed terminal (20) comprises an outer block (22) and an inner block (23) adapted to be tightened together at said through hole (10a) so as to abut against said entrance (10) on opposite sides relative to said entrance (10).

8. An authentication device (1) as claimed in the preceding claim, wherein said fixed terminal (20) comprises second connecting means (25) adapted to bring said outer block (22) into connection for data and current passage with said inner block (23).

9. An authentication device (1) as claimed in one or more of the preceding claims, wherein said fixed terminal (20) comprises signalling members (23b) adapted to signal the presence of said coming subject to said resident.

10. An authentication process (100) of a subject making a house call, comprising a fixed terminal (20) fastened in the vicinity of an entrance (10) and a mobile terminal (30) adapted to be carried by said subject making a house call in the vicinity of said entrance (10), said authentication process comprising a connection step (120) in which said mobile terminal (30) is connected to said fixed terminal (20), **characterised in that** when said mobile terminal (30) is connected to said fixed terminal (20), said mobile terminal (30) supplies said fixed terminal (20) with energy causing activation of said fixed terminal (20).

11. An authentication process (100) as claimed in the preceding claim, wherein in said identification step (130) said mobile terminal (20), based on at least said authentication data, creates a second authentication signal, and wherein it compares said second authentication signal with said first authentication signal.

12. An authentication process (100) as claimed in the preceding claim, comprising an association step (110) in which said mobile terminal (30) is connected to a central apparatus (40) and wherein said central apparatus (40) creates a first authentication signal and supplies said mobile terminal with said authentication data including said first authentication signal; and a signalling step (140) in which, if said second authentication signal is coincident with said first authentication signal, said fixed terminal gives notice of the presence of said subject to the resident.

13. An authentication process (100) as claimed in one or more of claims 10-12, wherein associated with said first signal is a validity time; said authentication process (100) comprising at least one verification step in which said mobile terminal (30) compares said validity time with the examination time and wherein if the examination time is higher than said validity time, said first opening signal is deleted from said mobile terminal (30).

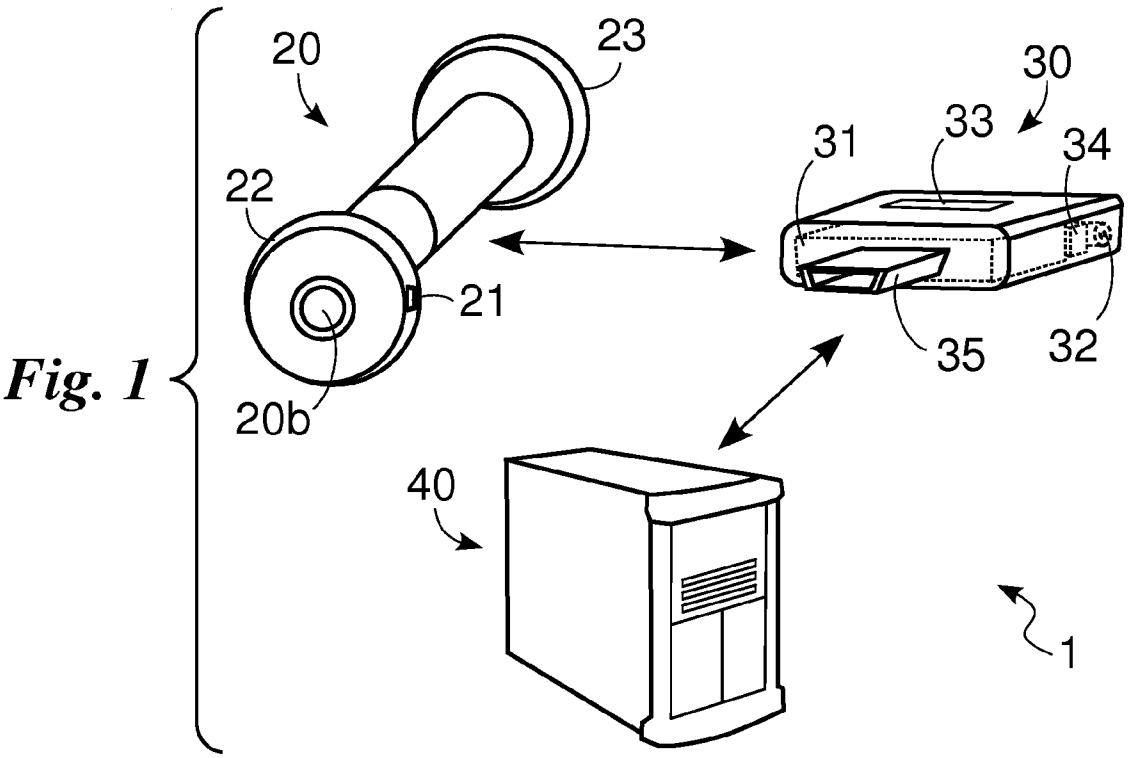

20
23
30
33
31
34
22
21
35
32
20b
40
1

Fig. 1

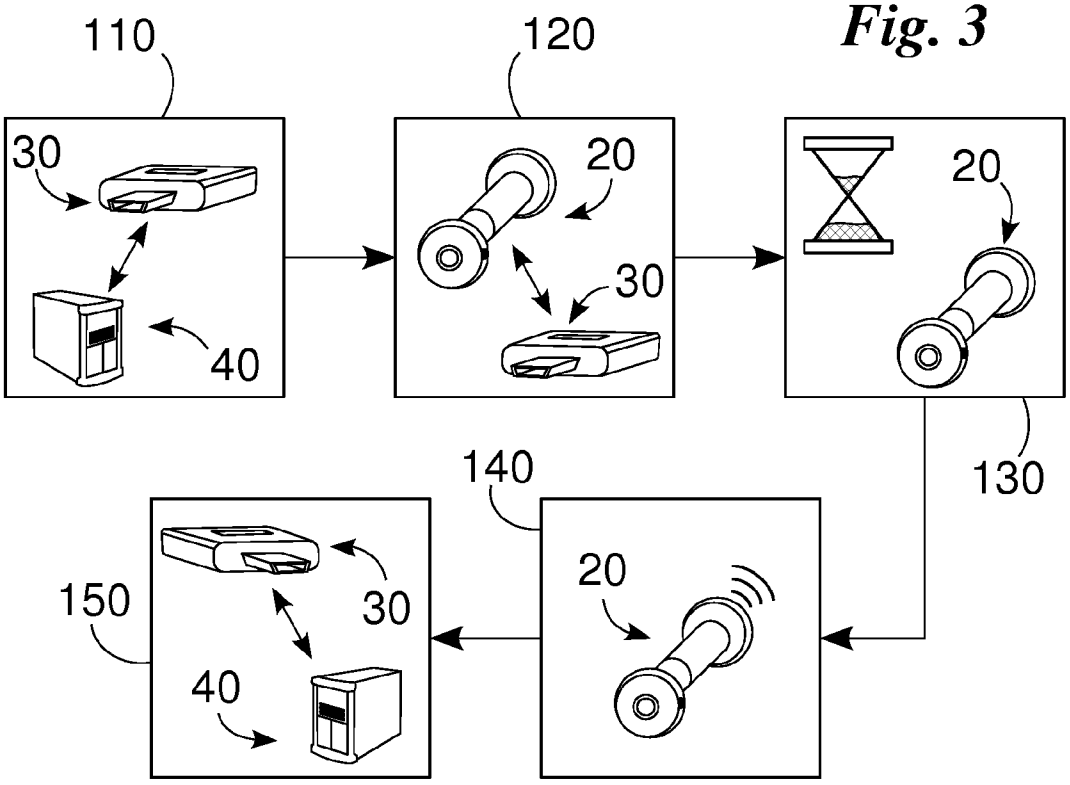
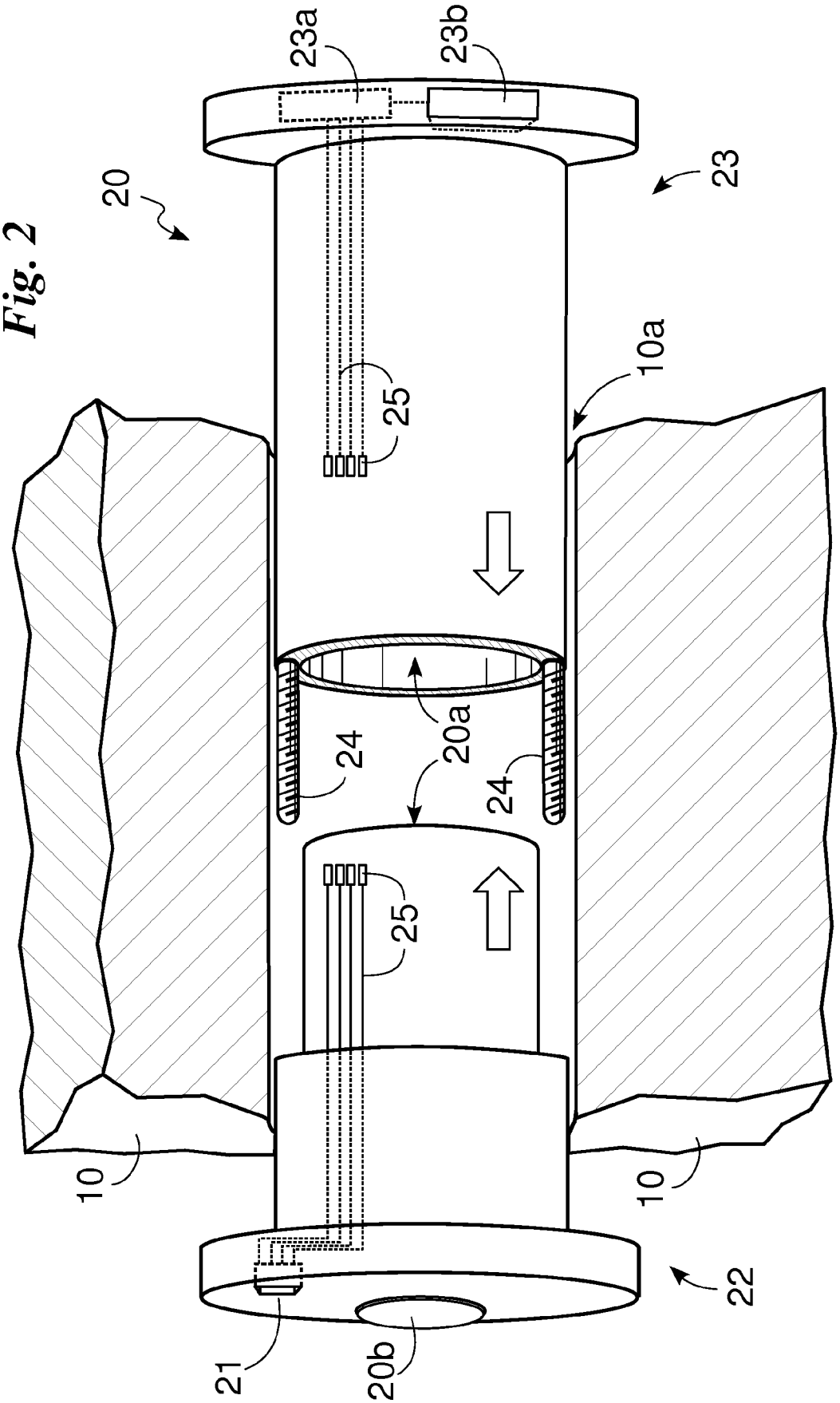

110
120
30
20
20
30
40
130
140
20
150
30
40

Fig. 3

Fig. 2



INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2011/052820

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/00 H04L9/32 E06B7/30 G07C9/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L E06B G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	BEAUFOUR A ET AL: "Personal servers as digital keys", PERVASIVE COMPUTING AND COMMUNICATIONS, 2004. PROCEEDINGS OF THE SECON D I EEE ANNUAL CONFERENCE ON MAR. 14-17, 2004, PISCATAWAY, NJ, I EEE, US, 14 March 2004 (2004-03-14), pages 319-328, XP010689694, D0I: D0I: 10. 1109/PERCOM. 2004. 1276869 ISBN: 978-0-7695-2090-2 abstract secti on 1, "Introducti on" secti on 2, "Di gi tal Key System" secti on 4, "Secure Access Control " f i gure 1 ----- -/- ·	1-13

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

"E" earlier document but published on or after the international filing date

"L" documentwhich 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 docu¬ments, 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
21 October 2011	28/10/2011

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	Di Fel i ce, M

1

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

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6 663 420 B1 (XIAO HUI [CN]) 16 December 2003 (2003-12-16) the whole document	1-13
A	US 2007/085662 A1 (MATSUMOTO FUMIAKI [JP] ET AL) 19 April 2007 (2007-04-19) abstract paragraphs [0008] - [0016] paragraphs [0031] - [0039] figure 1	1-13
A	US 2005/060555 A1 (RAGHUNATH MANDAYAM THONDANUR [US] ET AL RAGHUNATH MANDAYAM THONDANUR [] 17 March 2005 (2005-03-17) abstract paragraphs [0003] - [0017]	1-13
A	US 2006/014564 A1 (KUNG SHA0-TSU [TW]) 19 January 2006 (2006-01-19) abstract paragraphs [0008] - [0012]	1-13
A	US 2010/159953 A1 (AUBERT DENIS [FR] ET AL) 24 June 2010 (2010-06-24) abstract paragraphs [0020] - [0022]	1-13

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2011/052820

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6663420 B1	16-12-2003	NONE	
US 2007085662 A1	19-04-2007	JP 4727378 B2	20-07-2011
		JP 2007110490 A	26-04-2007
US 2005060555 A1	17-03-2005	US 2008235516 A1	25-09-2008
US 2006014564 A1	19-01-2006	NONE	
US 2010159953 A1	24-06-2010	NONE	