



(51) International Patent Classification:

H04W 12/08 (2009.01) *H04W 12/06* (2009.01)
H04L 29/06 (2006.01) *H04W 84/18* (2009.01)
H04W 12/04 (2009.01)

(21) International Application Number:

PCT/EP2015/081231

(22) International Filing Date:

24 December 2015 (24.12.2015)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

14307210.6 30 December 2014 (30.12.2014) EP

(71) Applicant: **GEMALTO SA** [FR/FR]; 6, rue de la Verrerie, 92190 Meudon (FR).

(72) Inventors: **GULLBERG, Peter**; Gemalto SA, Intellectual Property Department, 6, rue de la Verrerie, 92190 Meudon (FR). **JOSEFSSON, Johan**; C/O Gemalto SA, Intellectual Property Department, 6, rue de la Verrerie, 92190 Meudon

(FR). **SIMONSSON, Johan**; C/O Gemalto SA, Intellectual Property Department, 6, rue de la Verrerie, 92190 Meudon (FR).

(74) Agent: **CASSAGNE, Philippe**; C/O Gemalto SA, Intellectual Property Department, 6, rue de la Verrerie, 92190 Meudon (FR).

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU,

[Continued on next page]

(54) Title: A METHOD FOR ACCESSING A SHARED WIRELESS DEVICE USING A CLIENT WIRELESS COMMUNICATIONS DEVICE, AND DEVICES FOR THE SAME

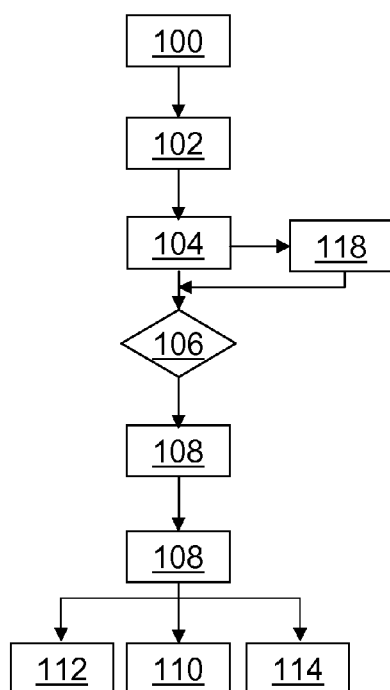


Fig. 3

(57) Abstract: A method for accessing a shared wireless device (4) using a client wireless communications device (2), said method comprising steps of : requesting a connection from an application running on said client device; exchanging cryptographic keys (102) between the client and shared devices, in response to said request, in order to authenticate the client device with the shared device; allowing said client device (104), once authenticated, to access said shared device by recording an identifier (ID) of said client device into a database; creating a communication link (108) between the client and shared devices, only if the identifier is present into the database; in which said application is able to access said database, in order to modify the contents of said database.



TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

**A METHOD FOR ACCESSING A SHARED WIRELESS DEVICE USING A
CLIENT WIRELESS COMMUNICATIONS DEVICE, AND DEVICES FOR
THE SAME**

5 The present invention relates to a method for accessing a shared peripheral wireless communication device using a client wireless communications device. The invention also relates to a communication system comprising a shared wireless device and a client wireless communications device, and to an information storage medium which contains instructions for executing said method.

10

 Mobile communication devices are known, such as Smartphone, which allow users of said devices to use and exchange data with a shared peripheral wireless device, such as a printer or a chip card reader, through a wireless data connection. One such example of such a wireless connection is the Bluetooth protocol.

15

 The current version of the Bluetooth standard (version 4.1) describes a known method to access a shared device using a client device. The devices are first “paired”, typically at the request of a user, in order to confirm the identity of both devices. Identification data of the client device is then recorded into a white list of the shared
20 device. Once a client device is recorded into said white list, it can then be allowed to establish a data link (“bonding”) with the shared device. Once said bonding is effective, the client device may use the shared device. This bonding is permitted only with client devices which are recorded in the white list. If bonding with a client device is terminated, it can be resumed later with this same client device without having to pair
25 anew the devices, as long as the client device is recorded in the white list.

 A drawback of this known method is that it lacks usability and reliability, especially when multiple clients attempt to access the same shared device, or in case of failure of the bonding between client and shared devices. This results in degraded
30 usability for the user of said devices.

It is therefore an object of the present invention to provide a method for accessing a shared wireless device using a client wireless communications device, each having a wireless communication interface, said method comprising steps of:

- requesting a connection from a client application running on said client device;
- 5 - exchanging cryptographic keys between a client wireless communications device and a shared peripheral device, in response to said request, in order to authenticate the client device with the shared device;
- allowing said client device, once authenticated, to access the shared device, this step comprising the recording of an entry containing an identifier of said client device into a database of devices allowed by the shared device, said database
10 being stored by said shared device;
- creating a secure communication link, over said communication interface, between the client device and the shared device, said link being created only if the entry containing the identifier of said client device is present into the white
15 list;

and in which said client application is able to access said database, through said secure communication link, in order to modify the contents of said database.

In another mode of realisation, the database contains a plurality of entries
20 corresponding to different devices that had been previously allowed to access said shared device, and the step of allowing said client device further comprises the automatic deletion of an entry of the database, selected according a predefined criterion, the entry containing the identifier of said client device being recorded in place of said deleted entry.

25

In another mode of realisation, the entry automatically deleted according to the predefined criterion is the one corresponding to the least frequently used entry of the database.

30 In another mode of realisation, the method further comprises a step of selectively removing from said database, using said client application of the allowed client device,

an entry corresponding to the identifier of another device that has been previously allowed to access said shared device.

In another mode of realisation, the method further comprises a step of
5 associating a name tag to the recorded identifier in said database using said user client application of the allowed client device.

In another mode of realisation, the wireless communication interface is a
Bluetooth communication interface.
10

In another mode of realisation, said shared wireless device is a chip card reader.

In another mode of realisation, said client wireless device is a mobile computing device such as a computer or a Smartphone or a tablet.
15

The invention also relates to an information storage medium, which comprises instructions for implementing the method for accessing a shared wireless device using a client wireless communications device according to the invention when said instructions are executed by an electronic data processor.
20

The invention also relates to a communication system comprising:

- a shared wireless device, having a wireless communication interface;
- a client wireless communications device, having a wireless communication interface and able to run a client application;

25 said client device and shared device being able to exchange cryptographic keys with each other, in response to a request from the client application, in order to authenticate the client device with the shared device;

30 the shared device being further able to:

- allow said client device, once authenticated, to access the shared device by recording an entry containing an identifier of said client device into a database of

devices allowed by the shared device, said database being stored by said shared device;

- create a secure communication link, over said communication interface, between the client device and the shared device, said link being created only if the entry containing the identifier of said client device is present into the database;
- 5 in which that said client application is able to access said database, through said communication link, in order to modify the contents of said database.

By giving said application on the allowed client device an access to the database, or white list, of the shared device, the user of said client device may read and/or modify the contents of said white list, and thus directly resolve a problem resulting from white list management on the shared device's side.

10

For example, in case of a failed bonding between said devices, the user may directly resolve the situation himself, simply by appropriately altering the white list. Thus, usability of said devices is greatly enhanced.

15

In another situation, if several other client devices are already connected to the shared device, the user may remove them from the white list to terminate those connections if they are deemed undesirable, e.g. for privacy or security reasons.

20

The advantage of the present invention will become apparent from the following description, given solely as a non limiting example and with reference to the accompanying drawings, in which:

- Figure 1 is a diagrammatic simplified representation of a communications system containing a shared wireless communications device and a client wireless communications device;
 - Figure 2 is a simplified block diagram of a client application and an operating system of the client wireless communications device of Fig. 1;
 - Figure 3 is a flowchart of a method for accessing the shared wireless device of Fig. 1 using the client wireless communications device of Fig. 1.
- 25
- 30

In this description, the features and functions that are well known to those skilled in the art are not described in detail.

Figure 1 is a schematic representation of an exemplary communications system 1 including a client wireless communication device 2 and a shared wireless peripheral communication device 4. In this setup, devices 2 and 4 are able to exchange data with each other wirelessly, so that device 2 can gain access to and use a shared resource 6 of said device 4, thanks to a secure (e.g. encrypted) communication link such as a wireless data connection 8.

10 To this end, device 2 advantageously comprises:

- a wireless communication interface 10,
- a user interface 12,
- an electronic data processing unit 14,
- an information storage medium 16, and
- 15 - an electrical power source 18.

In this example, device 2 is a mobile communication device such as a Smartphone.

20 Interface 10 is able to receive and transmit data wirelessly with another wireless device. In this embodiment, wireless interface 10 is a Bluetooth compliant communication interface.

In this description, "Bluetooth" refers to the Bluetooth® wireless short-range radio communication standard developed by the Bluetooth Special Interest Group. As is known, Bluetooth allows short-range exchange of data between computing devices using UHF (ultra high frequency) radio waves, typically in the ISM (instrument, scientific and medical) frequency band.

30 For example, interface 10 comprises a Bluetooth driver module and a Bluetooth-compliant radio antenna piloted by said driver module. This driver module is programmed to execute steps of establishing and managing a data connection with

another Bluetooth-compliant wireless device, as will be described in greater detail in what follows. In this embodiment, said interface 10 includes a unique identifier ID, which distinguishes device 2 from all other client devices. Identifier ID may for example be a string of alphanumerical characters encoded in digital form. For example,
5 identifier ID is hard-coded into said driver module.

Here, interface 12 includes a data input device and an optical display (not shown in detail). Interface 12 allows a user to control and provide instructions to device 2, for example through a graphical user interface. Said data input device may include a
10 keyboard or a touch-screen interface.

Unit 14 automatically processes data to and from interfaces 10, 12 and medium 16. For example, unit 14 contains a programmable microprocessor. Unit 14, interface 10, 12 and medium 16 are connected to each other through an internal data bus (not
15 drawn) and exchange data through this bus.

Storage medium 16 stores instructions for implementing a method for connecting to device 4, such as the method of Fig. 3, when said instructions are executed by unit 14. For example, medium 16 comprises a computer-readable non-
20 volatile memory such as Flash or EEPROM.

Electrical source 18 powers device 2. For example, source 18 is an electrical rechargeable battery.

25 Figure 2 is a simplified block diagram illustrating further the functioning of device 2. Device 2 is configured to run an operating system OS and an application APP.

As is known, the operating system OS is software programmed to manage hardware resources of device 2 when it is running. For example, the operating system
30 OS is stored in medium 16 as instructions able to be executed by an electronic data processor. Said operating system OS is run by system 2 by executing said instructions

on unit 14 with for example the aid of other hardware resources of device 2 such as a random access memory (not shown).

Here, application APP is a software application. Said application APP is able to
5 switch between a running state, in which it is executed by operating system OS, and an offline state, where it is not executed by operating system OS and resides in medium 16.

When it is running, said application APP is able to perform predetermined functions and especially to request access to hardware features of device 2, such as
10 interfaces 10 and 12, through the operating system OS. Said application APP is thus able to receive input from a user of device 2 on interface 12.

For example, said application APP is programmed to request and manage the establishment of communication link 8 with device 4, at the request of a user of device
15 2.

This device 4 may be shared, that is to say that its shared resource 6 can be used remotely by different wireless client devices, either simultaneously or one at a time.

20 Device 4 advantageously comprises:

- a wireless communication interface 20,
- an electronic data processing unit 22, for example identical to unit 14,
- an information storage medium 24, for example identical to medium 16,
- an electrical power source 26, for example identical to source 18, and
- 25 - shared resource 6.

In this example, device 4 is a peripheral security device that includes a chip card reader. In that case, the resource 6 is the card reader. Said resource 6 can be accessed remotely by client 2 so that an application running on client 2 can, in this case, use said
30 card reader, for example to provide a digital signature in a secure online transaction.

In this example, the application APP is used by a user of device 2 to perform a secure online transaction on a communication network, such as internet. The user of device 2 uses said card reader to read a chip card, in order to provide a digital signature required to complete said secure online transaction on device 2.

5

Interface 20 is for example identical to and has the same role as interface 10, except that it further comprises a security module 28 and a database 30 of devices authenticated by device 4.

10 Module 28 is programmed to grant access to the shared resource 6 only to client devices which have appropriate security credentials. To do so, module 28 maintains in database 30 a list of entries which identify client devices that have been authenticated and are thus allowed to access resource 6. Thus, database 30 is a list of all the client devices that are allowed to establish and maintain secure connections with the device 4.

15 If a client device is not listed in database 30, then it may not establish nor maintain a secure connection with device 4. Database 30 is also known as a “white list”. In what follows, the names “database 30” and “white list 30” will mean to designate the same object.

20 For example, white list 30 is a data structure, recorded in a memory element of module 28 and able to contain a plurality of entries, each corresponding to a client device. Each entry contains an identifier of the corresponding client device, analogous to identifier ID.

25 Unit 22 and power source 26 perform the same functions as, respectively, unit 14 and source 18 with respect to device 4 and will therefore not be described in further detail. Storage medium 24 stores instructions for implementing a method for connecting to device 4, such as the method of Fig. 3, when said instructions are executed by unit 22. Unit 22, interface 20, medium 24 and resource 6 are connected to each other through
30 an internal data bus (not drawn) and exchange data through this bus.

An exemplary method for accessing resource 6 of device 4 using device 2 is described according to the flowchart of Figure 3 and with the aid of Figures 1 and 2.

During a step 100, the device 2 initiates a data connection to device 4, in order to
5 access the resource 6. Here, data connection 8 is a Bluetooth connection link.

This step 100 is for example executed in response to a connection request inputted by a user of application APP running on device 2, using interface 12. Here, said request is generated by application APP and sent to the driver module of interface
10 10.

Typically, a Bluetooth connection is established in two sequential stages. Firstly, both devices 2 and 4 must authenticate each other before a secure data connection can be established. This first stage is usually known as “pairing”.

15

Then, once devices 2 and 4 are authenticated (i.e. paired), then secure communication link 8 is created. This second stage is usually known as “bonding”. Once communication link 8 is established (i.e. both devices are bonded), devices 2 and 4 can exchange data over communication link 8, until that link 8 is terminated.
20 Communication link 8 may be restored at a later time, for example at the request of a user of device 2, as long as devices 2 and 4 are still paired.

During this first stage, devices 2 and 4 may communicate each other wirelessly thanks to interfaces 10 and 20. At this stage, device 2 cannot yet access resource 6.

25

This stage of pairing comprises, to this end, a step 102 in which devices 2 and 4 exchange cryptographic keys through their respective interfaces 10 and 20, so that device 4 can authenticate device 2 and grant it access to shared resource 6.

30 The precise details of the implementation of said key exchange and authentication method can for example be found in the Bluetooth standard version 4.0 or version 4.1, available from the Bluetooth Special Interest Group.

Once the exchange of cryptographic keys between devices 2 and 4 is completed, and once that said device 2 is said to be authenticated by device 4, then the stage of pairing further comprises a step 104 in which device 4 grants the permission to device 2 to access shared resource 6.

5

Here, this is performed by having the module 28 to write an entry associated to device 2 into white list 30. This entry for example contains the identifier ID of device 2 and said cryptographic key associated to this device, for example encoded in binary form. Device 2 is then said to be 'paired' with device 4.

10

If, alternatively, device 2 has not been deemed authenticated by device 4 at the end of step 102, then step 104 is not performed and the entry containing identifier ID is not recorded into white list 30. Therefore, device 2 is then not paired with device 4.

15

Once this pairing stage is completed, then, during the stage of 'bonding', the secure data communication link 8 is created. This creation occurs only if device 2 has been previously paired with device 4. If both devices are not paired, then pairing will have to be performed before bonding can be allowed to occur. If connection 8 is terminated (for example because the user of device 2 request so), then it can be resumed later, as long as device 2 is still paired with device 4. The bonding stage will be executed, without having to execute again the pairing stage.

20

Thus, the bonding stage comprises a step 106, in which device 4 checks whether device 2 has been previously authenticated. Here, module 28 checks whether an entry containing identifier ID is stored in white list 30. If the identifier ID is not stored in white list 30, then the communication 8 is not established.

25

If said identifier ID is present, then the connection 8 is allowed to occur. Thus, during a step 108, the connection 8 is created and devices 2 and 4 are said to be bonded.

30

The device 2 can then access resource 6 through the connection 8.

The application APP is able to access white list 30, once device 2 has been authenticated during step 104.

For example, white list 30 is mirrored in device 2, for example in application
5 APP, so that a user of device 2 can read and/or modify its contents. Such modifications are then forwarded to device 4 in order to update white list 30.

For example, during a step 110, the contents of white list 30 are modified, by
application APP, over communication link 8, for example by a user of device 2.
10

This feature is especially advantageous in the event of a malfunction during the bonding stage. For example, the connection 8 could not be established properly even though the devices 2 and 6 were properly paired with each other (and thus an entry associated to device 2 is present in white list 30). Usually, the failed connection cannot
15 be restored from device 2. In order to resolve the situation, the failed connection must be reset by removing the entry from white list 30, manually, using an operating system of device 4. Then, pairing must take place anew before establishing connection 8. This causes unnecessary inconvenience to the user of device 2. Worse, this user may not even have access to the operating system of device 4 and thus may not reset the failed
20 connection.

Here, on the contrary, the connection is managed at the application level. The user of device 2 can modify the white list 30 through the application APP running on device 2. The user of device 2 is thus given the ability to modify white list 30 to reset
25 the failed connection by removing directly the incriminated entry. A connectivity-related issue may thus be resolved easily, directly from device 2, without having to access the operating system of device 4. The usability of device 2 is thus greatly enhanced.

30 The overall security of the system is preserved, since this feature is accessible only from an authenticated client device.

Another advantage is that, by allowing white list 30 to be managed remotely from application APP, it is not necessary for device 4 to feature a user interface, such as a display or a keyboard, for this specific purpose. This simplifies the conception and reduces the cost of device 4.

5

A further advantage is that the user may see in real time whether other client devices are currently bonded with 4 and likely to use resource 6. This feature can be of great interest in applications where the use of resource 6 may prompt security and/or privacy concerns.

10

This feature of accessing white list 30 from device 2 is also advantageous to resolve situations arising from the fact that multiple other client devices can also have access to resource device 4.

15

Here, multiple client devices have been previously paired with and bonded to device 4. In that case, white list 30 also contains a plurality of entries each corresponding to another client device that has been previously paired with device 4. The expression “another client device” designates here a third-party client device that is not device 2.

20

In a further embodiment, during a step 112, a name tag is associated, in white list 30, with the recorded entry corresponding to device 2. This name tag is for example a string of ASCII characters chosen by a user of device 2. Here, the user inputs said name tag through the interface 8 of device 2. Said name tag is then conveyed to device 4 through communication 8 link and is then stored into the corresponding entry of white list 30.

When white list 30 is displayed on interface 12, device 2 appears under the chosen name tag. Reading and browsing white list 30 over interface 12 is thus made easier for the user. This is especially useful in situations where many identifiers of various devices are listed in white list 30, as they are usually not displayed in a human-

30

readable form, and users would otherwise have some difficulty to recognize which client device is associated with a given identifier.

Alternatively, during a step 114, an entry corresponding to another client device
5 is selectively removed from white list 30, using interface 12 of device 2.

For example, a user of device 2 selects, through interface 12, an entry of white list 30 corresponding to a currently bonded client device whose connection link with device 4 must be terminated, and sends a command to terminate it to device 4 through
10 interface 10. This command is then received by device 4 and forwarded to module 28 which deletes the corresponding entry from white list 30. Once said entry is removed from white list 30, module 28 terminates the secure connection between device 4 and that client device.

15 This way, said user may know if other devices are connected and decide to revoke the permission to access resource 6, for example because of security and/or privacy concerns.

In another mode of realisation, the entries corresponding to all other currently
20 bonded client devices are automatically removed from white list 30 at the moment the connection link 8 is established between devices 2 and 6. This means that active connection links between device 4 and other client devices are terminated when connection 8 is established with device 2. This feature is useful for applications which require that device 4 may maintain an active connection link with only one client device
25 at a time.

In another mode of realisation, during the step 104, the operation of writing the entry of device 2 into the white list 30 is preceded by a test to check whether the white list 30 contains enough free memory space to receive said entry. If there is enough
30 space, then said entry is written into the white list 30. However, if there is not enough space, for example because the white list 30 is filled with entries associated to other client devices, then, during a step 118, one of said entries is automatically deleted from

the white list 30, according to a predetermined criterion, and the entry of device 2 is written in its place in white list 30.

In an embodiment of this operation, said predetermined criterion is chosen as follows: the entry to be removed is the one that is the least frequently used. The least frequently used entry is said to be the one which corresponds to the client device which, among all client devices corresponding to the entries of white list 30, has not bonded with device 4 for the longest time.

For example, each entry in the white list 30 further comprises a timestamp indicating the last time at which the corresponding device has been successfully bonded to device 4. Thus, during step 118, the timestamps are automatically read and said entries are sorted from the most recently used to the oldest used, the latter being then automatically deleted.

One advantage of this embodiment is that the entries corresponding to the client devices that are the most frequently used with device 4 are not deleted during this operation 118, thus dispensing their respective users from having to set up again a pairing routine the next time they want to connect their device to device 4. A user of a device that connects to device 4 only very infrequently would then be less impacted than one that connects more often.

Many other modes of realisation are possible.

Device 2 may be different. For example, it can be a computer, or a tablet, or a personal assistant.

Device 4 may also be different. For example, it can be a pair of headphones or a loudspeaker unit, or a printer, or a data storage system, or a home or vehicular entertainment system.

The precise implementation of the pairing or the bonding stages may be different.

Database 30 may be different. It may be stored in a memory of device 4 distinct
5 from module 28 or interface 20.

Step 112 and 114 may be omitted. In fact, only one of steps 110, 112 and 114 may be executed, as well, alternatively, as any combination thereof.

10 The name tag may be chosen differently, or may be encoded differently (e.g. as an image or a pictogram). It may be pre-recorded in device 2, thus dispensing users from having to input it every time they bond to device 4.

During step 114, entries corresponding to client devices that are paired but not
15 currently bonded can also be removed.

Step 118 may be different. A different criterion can be used to choose which identifier is to be deleted. For example, the oldest identifier is deleted, irrespective of its usage frequency. Said criterion can be chosen by a user of device 2.
20

Alternatively, the identifier of a client device, such as identifier ID, may be different. For example, it is not stored or hardcoded into interface 10. Instead, it is defined at the application level. For example, it is coded in application APP. Thus, if several other applications besides application APP are installed on device 2, they may
25 each have their own identifier. If any of said applications requests the opening of connection link 8 with the device 4, then the method for establishing said connection will be the same as if it was another client device. Thus, said identifier ID does not allow distinguishing device 2 from all other client devices. It serves only to distinguish application APP from other devices.

30

CLAIMS

1. A method for accessing a shared wireless device (4) using a client wireless communications device (2), each having a wireless communication interface (10, 20), said method comprising steps of :
- requesting a connection from an client application (APP) running on said client device (2);
 - exchanging cryptographic keys (102) between a client wireless communications device and a shared peripheral device, in response to said request, in order to authenticate the client device with the shared device;
 - allowing said client device (104), once authenticated, to access the shared device, this step comprising the recording of an entry containing an identifier (ID) of said client device into a database (30) of devices allowed by the shared device, said database being stored by said shared device (4);
 - creating (108) a secure communication link (8), over said communication interface, between the client device and the shared device, said link being created only if the entry containing the identifier of said client device is present into the white list;
- characterized in that said client application is able to access said database (30), through said secure communication link (8), in order to modify the contents of said database.
2. The method of claim 1, in which :
- the database contains a plurality of entries corresponding to different devices that had been previously allowed to access said shared device, and
 - the step of allowing said client device further comprises the automatic deletion (118) of an entry of the database, selected according a predefined criterion, the entry containing the identifier of said client device being recorded in place of said deleted entry.

3. The method of claim 2, in which the entry automatically deleted (118) according to the predefined criterion is the one corresponding to the least frequently used entry of the database.
- 5 4. The method of claim 1, further comprising a step of selectively removing (114) from said database, using said client application of the allowed client device, an entry corresponding to the identifier of another device that has been previously allowed to access said shared device.
- 10 5. The method of claim 1, further comprising a step of associating a name tag (112) to the recorded identifier in said database (30) using said user client application of the allowed client device.
6. The method of claim 1, in which the wireless communication interface (10, 20) is a
15 Bluetooth communication interface.
7. The method of claim 1, in which said shared wireless device (4) is a chip card reader.
- 20 8. The method of claim 1, in which said client wireless device (2) is a mobile computing device such as a computer or a smartphone or a tablet.
9. An information storage medium (16, 24), which comprises instructions for implementing the method for accessing a shared wireless device using a client
25 wireless communications device of claim 1 when said instructions are executed by an electronic data processor.
10. A communication system comprising:
 - a shared wireless device (4), having a wireless communication interface;
 - 30 - a client wireless communications device (2), having a wireless communication interface and able to run a client application (APP);

said client device and shared device being able to exchange cryptographic keys with each other, in response to a request from the client application, in order to authenticate the client device with the shared device;

the shared device being further able to:

- 5 - allow said client device, once authenticated, to access the shared device by recording an entry containing an identifier (ID) of said client device (2) into a database (30) of devices allowed by the shared device, said database being stored by said shared device (4);
- 10 - create a secure communication link (8), over said communication interface, between the client device and the shared device, said link being created only if the entry containing the identifier of said client device is present into the database;

characterized in that said client application is able to access said database, through said communication link (8), in order to modify the contents of said database.

1/1

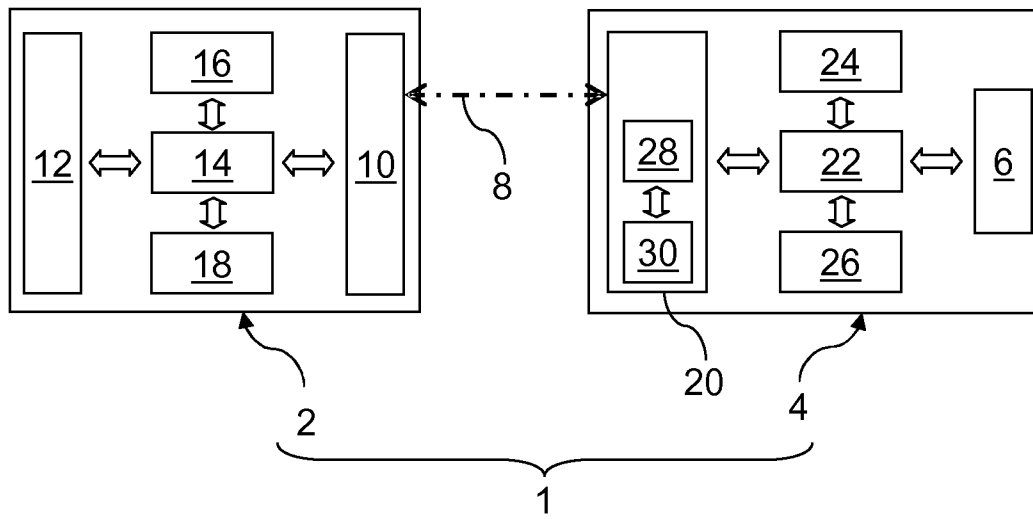


Fig. 1

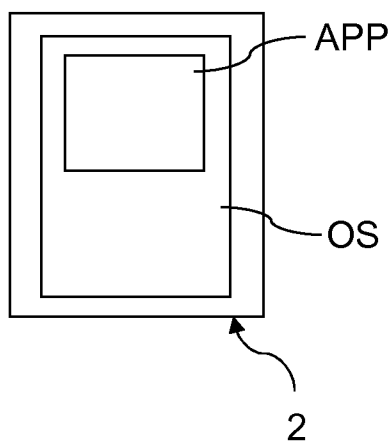


Fig. 2

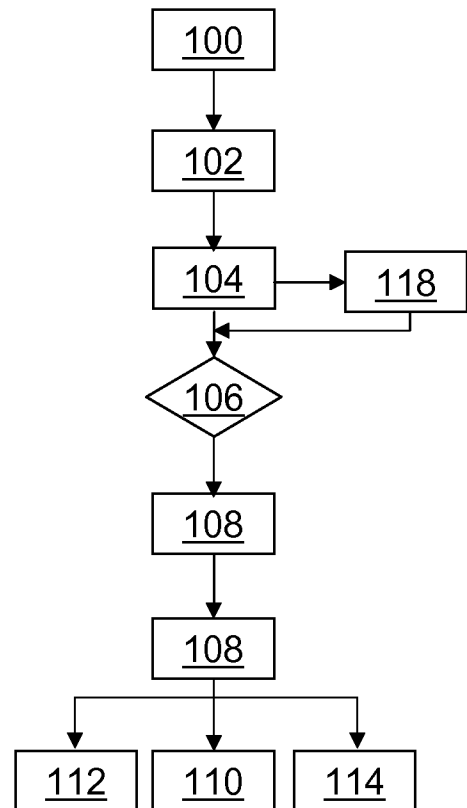


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/081231

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04W12/08

ADD. H04L29/06 H04W12/04 H04W12/06 H04W84/18

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)

H04W H04L

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 2012/135683 A1 (LEE REO [CA] ET AL) 31 May 2012 (2012-05-31) abstract; figures 1,2 paragraphs [0043], [0046], [0047] paragraph [0050] - paragraph [0053] paragraph [0069]	1-10
A	----- "Supertooth Bluetooth Handsfree Light User Manual", 6 March 2007 (2007-03-06), XP055191788, Retrieved from the Internet: URL: http://www.myblueant.com/downloads/manuals/STL_manual.pdf [retrieved on 2015-05-28] page 6 ----- -/-	1-10



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

10 March 2016

Date of mailing of the international search report

18/03/2016

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

Barla Harter, I

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/081231

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 443 714 A1 (DEUTSCHE TELEKOM AG [DE]) 4 August 2004 (2004-08-04) abstract paragraphs [0002], [0007], [0009], [0010], [0014] -----	1-10
A	"NETGEAR Support Answer Configuring Access Control on Nighthawk Wi-Fi Router", 14 April 2014 (2014-04-14), XP055191784, Retrieved from the Internet: URL: http://kb.netgear.com/app/answers/detail/a_id/24830/~configuring-access-control-on-nighthawk-wi-fi-router [retrieved on 2015-05-28] page 1 - page 4 -----	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2015/081231

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012135683	A1	31-05-2012	NONE

EP 1443714	A1	04-08-2004	AT 368341 T 15-08-2007
		DE 10304040 A1	05-08-2004
		EP 1443714 A1	04-08-2004
