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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 March 2006 (16.03.2006)

PCT

(10) International Publication Number
WO 2006/027725 A1

(51) International Patent Classification[7]: H04L 12/28, 12/56

(21) International Application Number: PCT/IB2005/052854

(22) International Filing Date: 31 August 2005 (31.08.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
04104326.6 8 September 2004 (08.09.2004) EP

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **VAUCLAIR, Marc** [BE/BE]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **SERRET, Xavier** [ES/BE]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **ETIENNE, Lionel, G.** [BE/BE]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL). **TEUWEN, Philippe** [BE/BE]; c/o Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Agents: **ELEVELD, Koop, J.** et al.; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

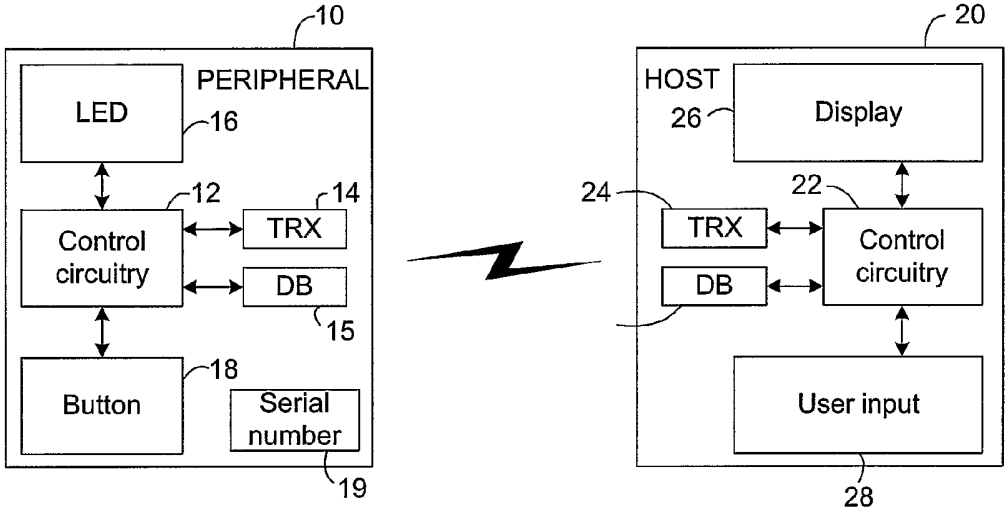
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK,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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE PAIRING FOR WIRED OR WIRELESS COMMUNICATIONS DEVICES



(57) Abstract: Pairing is achieved between a host communications device and a peripheral communications device, in order to establish an ad hoc wireless or wired network. A device identification, relating uniquely to the peripheral device, is displayed on the host device. In order to accept the pairing, the user confirms that th.- device identification displayed on the host device matches that printed on the peripheral diwice, and then completes the pairing procedure by pressing a key on the peripheral device, or, if Near Field Communication (NFC) techniques are implemented in the devices, by placing the peripheral device in contact with, or sufficiently close to, the host device. Thus, secure pairing is achieved, without requiring a complex user interface on the peripheral device.

WO 2006/027725 A1

Secure pairing for wired or wireless communications devices

The invention relates to wired and wireless communications devices and in particular relates to a method and apparatus for allowing secure pairing of wired or wireless communications devices.

Ad hoc wireless networks are becoming common, in which suitably equipped wireless devices can communicate with each other wirelessly, avoiding the need to connect the two devices by means of a cable.

In order for the two separate wireless devices to communicate securely with each other, and avoid the possibility that data transmitted from one of the devices can be detected and/or tampered with by a device owned by a third party, it is necessary to 'pair' the devices. This pairing process involves the communication and establishment of 'trust-foundation' information between the devices involved. This 'trust-foundation' information has the role of ensuring that devices can only communicate with communication peers that the user designates as trusted (for example because the user owns or controls the peer device).

There are several wireless communication standards, such as Bluetooth and IEEE 802.11b/g, and each contains a mechanism for device pairing. These mechanisms involve either the user typing a series of symbols (for example decimal digits for Bluetooth, hexadecimal or ASCII characters for IEEE 802.11b's Wireless Equivalent Privacy (WEP) protocol) or the use of a secondary communication channel that is already secure or considered secure because of its physical properties (for example Ethernet wires for IEEE 802.11 access points or Near Field Communication (NFC)).

However, existing pairing mechanisms can be difficult to use, and may increase significantly the requirements placed on the devices, which mean that it is difficult to implement them successfully in commercial products. This means that many deployments are insecure. For example, IEEE 802.11 networks may be implemented without encryption, with the result that communications between two devices can potentially be overheard, and/or tampered with, by third parties. In other cases, a wireless device may be provided with

a USB connector for the sole purpose of performing the pairing operations, which increases the cost of the device unnecessarily.

Many of these disadvantages with pairing mechanisms are also present in wired networks in which the host device is connected directly or indirectly to the peripheral device by cabling or other physical connectors.

Therefore, there is a need for a method and apparatus for allowing simple, secure pairing of communications devices that does not require the input of symbols nor a secondary secure communication channel.

According to a first aspect of the invention, there is provided a method of pairing a trusted device and a second device, the method comprising receiving a request to pair the second device with a first device; mutually authenticating the first device and the second device and obtaining from said first device a device identification relating to said first device; putting the first device into a trusted mode in which it will not engage in a pairing procedure with any device other than the second device; obtaining a device identification from the trusted device; comparing the device identification from the trusted device with the device identification obtained in the authenticating step; if the device identification relating to the first device matches the device identification obtained from the trusted device, determining that the first device is the trusted device and sending a pairing acceptance to the trusted device; and pairing the trusted device and the second device in response to the receipt of a second pairing acceptance from a user entered into the trusted device.

According to a second aspect of the present invention, there is provided a peripheral communications device, comprising means for authenticating the peripheral device to a host device, and transmitting a peripheral device identification to said host device; means for authenticating the said host device to the peripheral device, and receiving said host device identification; means for putting the peripheral device into a trusted mode in which it will not engage in a pairing procedure with any device other than said host device; means for receiving a pairing acceptance input from a user and for confirming pairing with said host device in response to the pairing acceptance input.

According to a third aspect of the present invention, there is provided a host communications device, comprising means for receiving a request to pair said host device with a peripheral device; means for authenticating the peripheral device and obtaining from said peripheral device a device identification relating to said peripheral device; means for

authenticating to the peripheral device and transmitting a host device identification to said peripheral device; means for displaying the device identification relating to said peripheral device; and means for pairing the host and peripheral communications devices in response to the receipt of a pairing confirmation from the peripheral device and a host pairing acceptance from the user entered into the host device.

According to a fourth aspect of the invention, there is provided a host communications device, comprising means for receiving a request to pair said host device with a peripheral device; means for authenticating the peripheral device and obtaining from said peripheral device a device identification relating to said peripheral device; means for authenticating to the peripheral device and transmitting a host device identification to said peripheral device; means for obtaining a device identification relating to a trusted device; and means for comparing the device identification relating to the peripheral device and the device identification relating to the trusted device; means for pairing the host and peripheral devices in the event that the device identification relating to the peripheral device and the device identification relating to the trusted device match, and in response to the receipt of a pairing confirmation from the peripheral device.

The invention therefore allows device pairing to be performed simply by the user, without requiring significant increases in the manufacturing costs of devices, in particular those devices that are built for applications that would not otherwise require a feature-rich user interface (e.g. a wireless USB "memory key"). As a result, the invention provides a method and apparatus, which allow pairing of relatively inexpensive devices in a straightforward manner. The level of security that is in fact implemented in wireless and wired networks is therefore likely to be increased.

Fig. 1 is a block schematic diagram of an ad hoc wireless communications network, including wireless communications devices in accordance with an aspect of the present invention.

Fig. 2 illustrates a method performed in the network of Fig. 1, according to a second aspect of the present invention.

Fig. 3 is a flow chart, further illustrating the method of Fig. 2.

Fig. 4 is a state diagram, illustrating the operation of one of the devices in the network of Fig. 1.

Fig. 5 is a further state diagram, illustrating the operation of the other of the devices in the network of Fig. 1.

Fig. 6 illustrates a method performed in the network of Fig. 1 according to an alternative embodiment of the invention.

Fig. 7 is a flow chart, further illustrating the method of Fig. 6.

Although the invention will be described herein as being implemented in wireless networks, it will be appreciated that the invention can also be applied to wired networks in which the host device is connected directly or indirectly to the peripheral device by cabling or other physical connectors.

Figure 1 is a block schematic diagram, showing two electronic devices 10, 20, which have a wireless connection, such that they form an ad hoc wireless network.

In this illustrated embodiment of the invention, the first electronic device 10 is regarded as a peripheral device, while the second electronic device 20 is regarded as a host device. For example, the first electronic device 10 may be a portable memory device, a mobile telephone handsfree kit or a wireless network access point (such as a Wi-Fi Access Point), while the second electronic device 20 may be a camera, mobile telephone or personal computer, and the ad hoc wireless network is formed to allow data to be transferred from the first device 10 to the second device 20. In this case, the ad hoc wireless network is formed by allowing the first device 10 and the second device 20 to communicate according to the Wireless USB (Universal Serial Bus) (WUSB) protocol. However, the first and second devices could communicate according to any wireless or wired protocol, for example such as the IEEE 802.15 and the IEEE 802.11 standard series, Bluetooth, Zigbee, Ethernet or IP.

It will be appreciated that the first and second electronic devices are each potentially complex, and so, for ease of understanding, they will be described here only so far as is necessary for an understanding of the present invention, that is, for an understanding of the method by which the devices are paired to allow secure communications between them.

The peripheral first electronic device 10 has control circuitry 12, in the form of a suitably programmed processor. The control circuitry 12 has other features required for the performance of the primary function of the device 10, but only those features relating to the establishment of device pairing will be described here. The control circuitry 12 is connected to transceiver (TRX) circuitry 14, which handles radio frequency communications with other electronic devices able to use the same wireless protocol.

The control circuitry 12 is also connected to a database (DB) 15, which stores information about devices with which the device 10 has been paired.

Since the first electronic device is relatively simple to operate, it is not provided with a complex user interface. Instead, it is provided with an LED 16, which operates under the control of the control circuitry 12, and a single button 18, which can be pressed by the user to send a signal to the control circuitry 12.

A serial number 19, which uniquely identifies the first electronic device 10, is written on the outside of the device in a user-readable form.

The host second electronic device 20 has control circuitry 22, in the form of a suitably programmed processor. The control circuitry 22 has other features required for the performance of the primary function of the device 20, but only those features relating to the establishment of device pairing will be described here. The control circuitry 22 is connected to transceiver (TRX) circuitry 24, which handles radio frequency communications with other electronic devices able to use the same wireless protocol.

The control circuitry 22 is also connected to a database (DB) 25, which stores information about devices with which the device 20 has been paired.

Since the second electronic device is much more complex than the first, it is provided with a more complex user interface. In this illustrated example, it is provided with a display 26, which operates under the control of the control circuitry 22, and can for example display detailed messages, or menu options, to the user. The second electronic device is also provided with user input 28, which may for example include a keypad, and one or more scroll buttons, allowing the user to select from available menu options, to send a signal to the control circuitry 22.

In the embodiments of the invention illustrated in Figures 2 to 7, the user would like to pair the "trusted" host device 20 with a "trusted" peripheral device 10. The host and peripheral devices are considered to be "trusted" if, for example, the user owns the host or peripheral device, and these are the devices that the user wishes to pair together. A third party device that is in range of the host device 20 is therefore not considered to be a "trusted" device.

Briefly, the methods illustrated in Figures 2 to 7 provide a means for pairing a first communications device 10 (a peripheral device) and a second communications device 20 (a host device). Firstly, a mutual authentication is performed between the second device and a first device. At this stage, it is possible that the first device with which the second device is communicating is not the first device owned by the user (i.e. it is not the "trusted" device).

Therefore, the methods according to the various embodiments of the invention provide a means by which the user can verify that the first device with which the second device is communicating is indeed the "trusted" device and vice versa. In addition, these methods are robust to various types of attack.

The process of pairing the first and second electronic devices 10, 20 according to a first embodiment of the invention will now be described with reference to Figure 2, which shows the signals sent between the devices, Figure 3, which shows the procedure performed in the host device 20, Figure 4, which shows the state of the peripheral device 10, and Figure 5, which shows the state of the host device 20.

As shown in Figure 2, the pairing process may start when the first and second electronic devices 10, 20 have each been powered on (steps S1 and S2 respectively in Figure 2). Each of the devices then enters its respective Idle state 102, 202.

When the user wishes to establish an ad hoc wireless network between the first and second electronic devices 10, 20, for example in order to be able to transfer data between the two devices, he operates the host device 20 as required in order to control this process. For example, to initiate the process, the user may select a pairing option from a menu, using the user input 28.

In step P1 of the process in Figure 3, the host device 20 then seeks a nearby peripheral device. Specifically, it does this by sending a beacon signal (S3 in Figure 2) containing its identification.

The peripheral device 10 detects the beacon signal, and enters a Beacon Detect sub-state 104 of its Link Initialization state 106. The peripheral device 10 then replies with an announcement (S4 in Figure 2) containing its identification, and enters its Announced sub-state 108.

The host device 20 receives the peripheral device identification in step P2 of the process in Figure 3, and then passes to step P3, in which a mutual authentication procedure is performed.

In this illustrated embodiment of the invention, the mutual authentication procedure is a generally conventional cryptographic authentication procedure, based on the use of "public key" cryptography. The first and second devices 10, 20 enter their respective Authenticating states 110, 204. The host device 20 sends an unpredictable challenge (S5 in Figure 2) to the peripheral device 10. Then the peripheral device 10 processes the challenge by leveraging the knowledge of a private key to generate a response (S6 in Figure 2), that also includes its own public key information. Finally, the host device verifies the correctness

of the response with the conveyed public key uniquely associated to the private key of the peripheral device.

The challenge-response (S5 and S6 in Figure 2) message interchange is then repeated, with the roles of the host and peripheral devices inverted, to achieve a mutual authentication. It is well known in the art how to piggyback challenges and responses issued by the two devices, in order to minimize the number of messages interchanged, for example according to the STS (Station to Station) protocol, the SSL (Secure Socket Layer) protocol or SSH (Secure Shell) protocol.

It will be appreciated by a person skilled in the art that various different protocols or algorithms can be used to mutually authenticate the devices. Examples of protocols that can be used include EAP-TTLS, EAP-PEAP, STS, Diffie-Hellman or EC/DH. Examples of algorithms that can be used include RSA, DSA or ECDSA.

As is known, device identifications can be associated to public keys by three main techniques. One possibility is to use certificates issued by a trusted authority that binds these two values together (e.g. X509). Another possibility is to perform a cryptographic digest (e.g. SHA-1) of the public key to directly obtain the device identification. A third possibility is to perform a cryptographic digest (e.g. SHA-1) of a document (e.g. X509 certificate) containing the public key.

In this case, the peripheral device 10 associates its printed serial number 19 to its public key when authenticating with the host device 20.

It is also known in the art that the transmitted device identifications can be the result of a random process, for example they can be generated using a random (or pseudo random) number, such that the random process will only generate the same device identification twice with negligible probability.

As a by-product of the authentication procedure, the host device 20 and peripheral device 10 generate a common secret key, that is used to secure all subsequent message interchanges between them.

Once the authentication procedure has been performed, the first and second devices 10, 20 check in their respective paired device databases 15, 25 whether they are in fact already paired with the respective other device. If so, the first and second devices 10, 20 enter their respective Paired states 112, 206, and they are then able to perform secure wireless (or wired) communications (states 114, 208), until such time as one or both of them is powered off.

If, on the other hand, the first and second devices determine that they are not already paired with the respective other device (S7 in Figure 2), the first and second devices 10, 20 enter their respective Ready to Pair states 116, 210.

In step P4 of the process shown in Figure 3, the host device 20 requests the initiation of a pairing procedure with the peripheral device 10. Specifically, it sends a pairing request signal (S8 in Figure 2) to the peripheral device, and the first and second devices 10, 20 enter their respective Pairing states 118, 212. The peripheral device 10 then returns a pairing started signal (S9 in Figure 2) to the host device 20, and the first and second devices 10, 20 enter their respective Pairing Started states 120, 214.

In this illustrated embodiment of the invention, the LED 16 on the peripheral device 10 then starts to blink, to indicate to the user that pairing is in process (S10 and S11 in Figure 2). Other simple signaling mechanisms are also possible. At this stage (step P5 in the procedure of Figure 3), the peripheral device 10 enters a state referred to herein as a "Trusted Critical Section". In the Trusted Critical Section, the first trusted device is guaranteed to communicate only with a specific second device for the purpose of pairing.

In step P6 of the process shown in Figure 3, the host device 20 presents to the user the identification of the peripheral device 10. Specifically, it displays on the display 26 (S12 in Figure 2) the identification of the peripheral device. In this illustrated embodiment of the invention, the identification uniquely identifies the peripheral device 10. However, in other embodiments of the invention, the identification could simply identify the peripheral device such that it becomes highly improbable that any other nearby peripheral device could share that identification. For example, the identification can be the result of a hash function performed on the public key of the peripheral device 10.

In this illustrated embodiment of the invention, all that is then required is for the user to compare the device identification 19 physically written on the first device 10 and the device identification displayed on the display 26 of the second device 20, in order to confirm (step P7 in Figure 3) that the two identifications match. If so, the user accepts the presented device identification (step P8 in Figure 3), for example by pressing an "OK" key on the user input 28 on the host device 20 (S13 in Figure 2).

If, for example at this stage, the peripheral device 10 receives a second pairing request signal (S14 in Figure 2) from a third party's host device, it returns a pairing wait signal (S15 in Figure 2), and the pairing with the third party's device does not continue.

Otherwise, the host 20 then sends a pairing confirm signal (S16 in Figure 2) to the peripheral device 10, and presents on its display 26 a message to the user indicating that

he can accept the pairing (S17 in Figure 2) by pressing the button 18 on the first device 10. No further typing of passwords or complicated sequences of symbols will be then necessary. The first and second devices 10, 20 then enter their respective Pairing Confirmed states 122, 216.

The peripheral device 10 then sends a pairing acknowledge signal (S18 in Figure 2) to the host 20, which enters its Pairing Acknowledged state 218, while the peripheral device 10 exits the Trusted Critical Section (step P9 in the procedure of Figure 3), and the LED 16 stops blinking.

In step P10 of the process shown in Figure 3, the pairing procedure is completed, and the first and second devices 10, 20 then enter their respective Paired states 112, 206, and the host device 20 confirms on its display 26 that it is paired with the peripheral device 10 (S19 in Figure 2). Finally, each of the devices 10, 20 stores the identifier of the other device in its respective paired devices database 15, 25.

As shown in Figure 2, a timer starts when the first device 10 enters its Pairing Started state 120. If pairing is not completed within a set time period (30 seconds in this case), the first device 10 returns to its Ready to Pair 116, and notifies the second device 20 with a PairingWait message. Upon reception of this message, the second device 20 notifies the user of the condition by means of a message on its display 26, and returns to its Ready to Pair state 210 once the time specified in the PairingWait message (for example 30 seconds) has elapsed.

The security of this pairing protocol thus arises because the user trusts the first device (e.g. because he owns it), and the user trusts the second device (e.g. because he owns it). The result is that the second device does not lie to the user, the first device does not lie to the user, and, in particular, the first device does not lie to the second device.

In an alternative embodiment of the invention, the first electronic device 10 and second electronic device 20 include additional circuitry, separate to the transceiver circuitry 14 and 24 respectively, for allowing communication between the devices over a short-range radio link. This short-range radio link uses a different protocol to the protocol used for the main transmissions between the devices. One such protocol that could be used by this circuitry is that proposed in the Near Field Communication (NFC) Interface and Protocol (NFCIP-1) by ECMA that transmits at 13.56 MHz. In a further alternative embodiment, the second electronic device 20 includes additional circuitry, separate to the transceiver circuitry 24, for allowing communication with an NFC token (for example an RFID tag) in the first electronic device 10.

Figures 6 and 7 illustrate a method performed in accordance with the alternative embodiment of the invention. Steps S1 to S11 in Figure 6 and steps P1 to P5 in Figure 7 are as described above in relation to Figures 2 and 3.

After step S11 in Figure 6 and step P5 in Figure 7, the first device 10 is in the "Trusted Critical Section" state, in which it is guaranteed to engage in a pairing procedure with only one second device at a time.

In step P6A of the process shown in Figure 7, the host device 20 presents the user with an instruction to initiate communications between the devices using the alternative protocol. Specifically, if the protocol is an NFC protocol, the device 20 displays on the display 26 (S20 in Figure 3) an instruction to touch the host device 20 to the trusted peripheral device 10 (i.e. the peripheral device possessed by the user). Alternatively, the host device 20 can be brought sufficiently close to the trusted peripheral device 10 to initiate communications using the NFC protocol.

Once the user has touched the devices or moved the devices sufficiently close together (S21 in Figure 6 and P7A in Figure 7), the NFC interface is activated, and the identification of the peripheral device 10 (which was also provided to the second device in step P2 if the first device 10 is indeed the trusted peripheral device) is transmitted to the second device 20 (step S22). This transmission takes place without any interaction by the user, other than touching or moving the two devices together. In the further alternative embodiment, the NFC interface is activated, the signal activates the NFC token which communicates the peripheral device identification to the second device 20.

In this embodiment of the invention, the identification uniquely identifies the peripheral device 10. However, in other embodiments of the invention, the identification could simply identify the peripheral device such that it becomes highly improbable that any other nearby peripheral device could share that identification. For example, the identification can be the result of a hash function performed on the public key of the peripheral device 10.

In this illustrated embodiment of the invention, the second device 20 compares the device identification received in step S22 and P7A with the device identification received from the first device in step P2, in order to confirm (step P7B in Figure 7) that the two identifications match.

If, for example at this stage, the peripheral device 10 receives a second pairing request signal (S14 in Figure 6) from a third party's host device, it returns a pairing wait signal (S15 in Figure 6), and the pairing with the third party's device does not continue.

Otherwise, if the second device 20 determines that the identifications do match, then the second device 20 accepts the first device 10 (step P7B in Figure 7), and transmits a pairing confirm signal (S16 in Figure 6) to the peripheral device 10, and presents on its display 26 a message to the user indicating that he can accept the pairing (S17 in Figure 6) by pressing the button 18 on the first device 10 (step P8 in Figure 7). No typing of passwords or complicated sequences of symbols is necessary. The first and second devices 10, 20 then enter their respective Pairing Confirmed states 122, 216.

The peripheral device 10 then sends a pairing acknowledge signal (S18 in Figure 6) to the host 20, which enters its Pairing Acknowledged state 218, while the peripheral device 10 exits the Trusted Critical Section (step P9 in the procedure of Figure 7), and the LED 16 stops blinking.

In step P10 of the process shown in Figure 7, the pairing procedure is completed, and the first and second devices 10, 20 then enter their respective Paired states 112, 206, and the host device 20 confirms on its display 26 that it is paired with the peripheral device 10 (S19 in Figure 6). Finally, each of the devices 10, 20 stores the identifier of the other device in its respective paired devices database 15, 25.

As with the first embodiment of the invention, a timer starts when the first device 10 enters its Pairing Started state 120. If pairing is not completed within a set time period (30 seconds in this case), the first device 10 returns to its Ready to Pair 116, and notifies the second device 20 with a PairingWait message. Upon reception of this message, the second device 20 notifies the user of the condition by means of a message on its display 26, and returns to its Ready to Pair state 210 once the time specified in the PairingWait message (for example 30 seconds) has elapsed.

In order to illustrate the security of the pairing procedure, the reaction of the system to various attempts to attack the procedure will be considered.

In a first possible attack, a third party has a peripheral device of the same type as the user's peripheral device 10. If the third party's peripheral device responds to the beacon signal (S3 in Figure 2) with its own announcement, and then successfully authenticates with the host device 20, the result would be that, in the first embodiment of the invention at step P6 in the procedure of Figure 3, it would be the device identification of the third party's peripheral device that would be presented on the display 26 of the host device 20. The user would then be able to reject the proposed pairing, for example by pressing a "NO" key on the user input 28 of the second device 20.

Thus, although it authenticates the third party's device, the user's host device 20 will not lie to the user and so it will present a device identification that does not match the device identification printed on the user's peripheral device 10 (the "trusted" device). Therefore, the user has all the information required to discover the attack and refuse the pairing.

In the alternative embodiment of the invention where the devices use NFC or another short-range radio link, the result of carrying out step P6A in Figure 7 will be that the identification of the user's peripheral device 10 will be sent to the host device 20. This identification will then be compared with the identification received from the third party's peripheral device in the announce step (S4 in Figure 6). The host device 20 will determine that the identifications do not match, and will refuse the pairing.

In a second possible attack, a third party has a host device, which may or may not be of the same type as the user's host device 20. At a time when the peripheral device 10 is in its Ready to Pair state 210, but before the pairing request (S8 in Figure 2 or Figure 6) is sent from the user's host device 20, the third party's host device initiates the pairing procedure with the peripheral device. In response, the LED 16 of the peripheral device 10 starts blinking, as described above. However, the user's host device 20 can determine that a third party's device is now pairing with the peripheral device, and can indicate this on its display 26, in order to warn the user. Meanwhile, it enters its Pairing Wait state 220. Since the user does not know about this third party's device, he does not press the button 18 on the peripheral device, but instead waits for the LED 16 to stop blinking. When the LED 16 stops blinking, the third party's device is put into "quarantine" by the peripheral device for some time, and the pairing procedure with the user's host device 20 can resume.

Thus, when the user's peripheral device 10 enters the Trusted Critical Section, it will inform the user's host device 20 that it is not available for pairing at that moment by replying with a pairing wait signal, in response to the pairing request signal S8. This is guaranteed because of the trust flow described above. This will allow the user's host device 20 to list the peripheral device 10 on its display 26, while warning the user that the peripheral device 10 is now pairing with a third party's device. Therefore, again, the user has all the information required to discover the condition and refuse the pairing with the third party's device.

In a third possible attack, a third party has a host device, which may or may not be of the same type as the user's host device 20. At a time when the peripheral device 10 is in its Pairing state 212, the third party seeks the user's peripheral device and instructs his

own host device to start the pairing process. As described above, the peripheral device 10 receives a second pairing request signal (S14 in Figures 2 and 6) from the third party's host device, and returns a pairing wait signal (S15 in Figures 2 and 6) in order to refuse the third party's pairing request, and the pairing with the third party's device does not continue.

Thus, these attacks can be rejected, regardless of the exact implementation of the third party's devices.

In order to ensure that the user knows the procedure to follow, in order to prevent a successful attack on the pairing procedure, suitable instructions are provided to the user on the display 26 of the second device 20, such that the user is instructed to manipulate the trusted peripheral device 10 only in response to instructions from the second device 20.

In a further embodiment of the invention, the functionality of the host device described above can be split between two paired devices, a delegator device and a delegatee device, such that the delegator device and delegatee device together act as a single host for purposes of pairing the delegator device to a peripheral device.

In this embodiment, the delegator device delegates the responsibility for conducting the pairing procedure between itself and the peripheral device to the delegatee device with which the delegator device is already paired. This delegation may be implemented using the RADIUS protocol.

There is thus provided a pairing procedure, which allows secure pairing of two devices, even when one of the devices has the simplest possible user interface, for example with only a single LED as a display, and a single button for user inputs.

CLAIMS:

1. A method of pairing a trusted device and a second device, the method comprising:

receiving a request to pair the second device with a first device;

mutually authenticating the first device and the second device and obtaining from said first device a device identification relating to said first device;

putting the first device into a trusted mode in which it will not engage in a pairing procedure with any device other than the second device;

obtaining a device identification from the trusted device;

comparing the device identification from the trusted device with the device identification obtained in the authenticating step;

if the device identification relating to the first device matches the device identification obtained from the trusted device, determining that the first device is the trusted device and sending a pairing acceptance to the trusted device; and

pairing the trusted device and the second device in response to the receipt of a second pairing acceptance from a user entered into the trusted device.

2. A method as claimed in claim 1, wherein the step of obtaining a device identification from the trusted device comprises a user reading a device identification printed on the trusted device; and wherein the step of comparing comprises a user visually comparing the device identification relating to the first device that is displayed on said second device and said device identification printed on the trusted device.

3. A method as claimed in claim 1, wherein the step of obtaining a device identification from the trusted device comprises:

activating a short range radio link between the trusted device and the second device; and

transmitting the device identification of the trusted device to the second device.

4. A method as claimed in claim 3, wherein the step of activating the short range radio link comprises physically touching the second device to the trusted device.

5. A method as claimed in claim , wherein the step of activating the short range radio link comprises moving the second device close to the trusted device.

6. A method as claimed in claim 3, 4 or 5, wherein the short range radio link uses a Near Field Communication protocol.

7. A method as claimed in claim 3, 4 or 5, wherein the device identification of the trusted device is stored in a RFID tag.

8. A method as claimed in any preceding claim, wherein the first and second devices:

establish a common secret key after or during the mutual authentication;

use the shared common secret key to ensure the authenticity and sequencing of subsequent messages between the first and second devices.

9. A method as claimed in any preceding claim, wherein the second pairing acceptance comprises a single keypress on the trusted device.

10. A method as claimed in any preceding claim, further comprising, after putting the first device into the trusted mode, notifying the second device that the first device will pair exclusively with the second device while first device is in the trusted mode.

11. A method as claimed in any preceding claim, the method comprising:

in response to receiving said request to pair the first and second devices, transmitting a beacon signal from said second device, wherein said beacon signal indicates the identification of said second device; and

in response to receiving said beacon signal from said second device, transmitting a response signal from said first device.

12. A method as claimed in claim 11, wherein the identification of said second device in said beacon signal is unique.

13. A method as claimed in claim 11, comprising generating said identification of said second device by means of a random process.

14. A method as claimed in claim 13, wherein said random process will only generate the same identification of said second device twice with negligible probability.

15. A method as claimed in claim 12, 13 or 14, wherein said unique identification of said second device can be directly computed from the said second device authentication.

16. A method as claimed in any preceding claim, the method comprising after authenticating said first device, indicating on said first device that said first device is in a pairing procedure.

17. A method as claimed in claim 16, comprising indicating on said first device that said first device is in a pairing procedure, by means of a light on said first device.

18. A method as claimed in any preceding claim, wherein said device identification uniquely identifies said first device.

19. A method as claimed in claim 18, comprising generating said identification of said first device by means of a random process.

20. A method as claimed in claim 19, wherein said random process will only generate the same identification of said first device twice with negligible probability.

21. A method as claimed in claim 18, 19 or 20, wherein said device identification can be directly computed from the said first device authentication.

22. A method as claimed in any preceding claim, further comprising establishing a secure ad hoc wireless communications network between said first and second devices.

23. A method as claimed in claim 22, comprising establishing a wireless USB connection between said first and second devices.

24. A peripheral communications device, comprising:

means for authenticating the peripheral device to a host device, and transmitting a peripheral device identification to said host device;

means for authenticating the said host device to the peripheral device, and receiving said host device identification;

means for putting the peripheral device into a trusted mode in which it will not engage in a pairing procedure with any device other than said host device;

means for receiving a pairing acceptance input from a user and for confirming pairing with said host device in response to the pairing acceptance input.

25. A peripheral device as claimed in claim 24, wherein the device further comprises a second means for transmitting the peripheral device identification to the host device, the second means using a short range radio link.

26. A peripheral device as claimed in claim 25, wherein the short range radio link uses a Near Field Communication protocol.

27. A peripheral device as claimed in claim 25, wherein the second means comprises a RFID tag.

28. A peripheral device as claimed in any of claims 24 to 27, wherein said peripheral device further comprises:

means for establishing a common secret key with said host device after or during the authentication with the said host device;

means for producing messages with the said secret key whose authenticity, integrity and sequencing can be verified by the said host device;

means for verifying the authenticity, integrity and sequencing of the messages produced by the host device with the said secret key;

29. A peripheral device as claimed in any one of claims 24 to 28, wherein said peripheral device identification uniquely identifies said peripheral device.

30. A peripheral device as claimed in any of claims 24 to 28, wherein said peripheral device identification is a result of a random process.

31. A peripheral device as claimed in claim 30, wherein said random process will only generate the same peripheral device identification twice with negligible probability.

32. A peripheral device as claimed in one of claims 24 to 31, the device comprising means for receiving a beacon signal from said host device, and transmitting a response signal.

33. A peripheral device as claimed in one of claims 24 to 32, the device comprising means for indicating that said first device is in a pairing procedure, after completing said authentication.

34. A peripheral device as claimed in claim 33, wherein said means for indicating comprises a light on said peripheral device.

35. A peripheral device as claimed in one of claims 24 to 34, adapted for establishing a wireless USB connection with said host device.

36. A peripheral device as claimed in one of claims 24 to 34, adapted for establishing an Internet Protocol connection with said host device.

37. A peripheral device as claimed in one of claims 24 to 36, wherein the pairing acceptance input from a user comprises a single keypress.

38. A host communications device, comprising:

means for receiving a request to pair said host device with a peripheral device;

means for authenticating the peripheral device and obtaining from said peripheral device a device identification relating to said peripheral device;

means for authenticating to the peripheral device and transmitting a host device identification to said peripheral device;

means for displaying the device identification relating to said peripheral device; and

means for pairing the host and peripheral communications devices in response to the receipt of a pairing confirmation from the peripheral device and a host pairing acceptance from the user entered into the host device.

39. A host communications device, comprising:

means for receiving a request to pair said host device with a peripheral device;

means for authenticating the peripheral device and obtaining from said peripheral device a device identification relating to said peripheral device;

means for authenticating to the peripheral device and transmitting a host device identification to said peripheral device;

means for obtaining a device identification relating to a trusted device; and

means for comparing the device identification relating to the peripheral device and the device identification relating to the trusted device;

means for pairing the host and peripheral devices in the event that the device identification relating to the peripheral device and the device identification relating to the trusted device match, and in response to the receipt of a pairing confirmation from the peripheral device.

40. A host device as claimed in claim 38 or 39, wherein the means for obtaining comprises a means for establishing a short range radio link with the peripheral device.

41. A host device as claimed in claim 40, wherein the short range radio link uses a Near Field Communication protocol.

42. A host device as claimed in claim 38, 39, 40 or 41, wherein said host device further comprises:

means for establishing a common secret key with said peripheral device after or during the authentication with the said peripheral device;

means for producing messages with the said secret key whose authenticity, integrity and sequencing can be verified by the said peripheral device;

means for verifying the authenticity, integrity and sequencing of the messages produces by the peripheral device with the said secret key.

43. A host device as claimed in any one of claims 38 to 42, wherein in response to receiving said request to pair the host and peripheral devices, said host device is adapted to transmit a beacon signal, wherein said beacon signal indicates the identification of said host device.

44. A host device as claimed in any one of claims 38 to 43, wherein said device identification uniquely identifies said peripheral device.

45. A host device as claimed in one of claims 38 to 43, wherein said peripheral device identification is a result of a random process.

46. A host device as claimed in claim 45, wherein said random process will only generate the same peripheral device identification twice with negligible probability.

47. A host device as claimed in one of claims 38 to 46, wherein said host device identification uniquely identifies said host device.

48. A host device as claimed in one of claims 38 to 46, adapted for establishing a secure wireless USB connection with said peripheral device.

49. A host device as claimed in one of claims 38 to 47, adapted for establishing an Internet Protocol connection with said peripheral device.

50. A host device as claimed in one of claims 38 to 49, wherein the host device comprises a delegator device and a delegatee device, wherein the delegator device is adapted to forward a request to pair said host device with a peripheral device to the delegatee device, and wherein the delegatee device is adapted to perform at least a part of the pairing procedure on behalf of the delegator device.

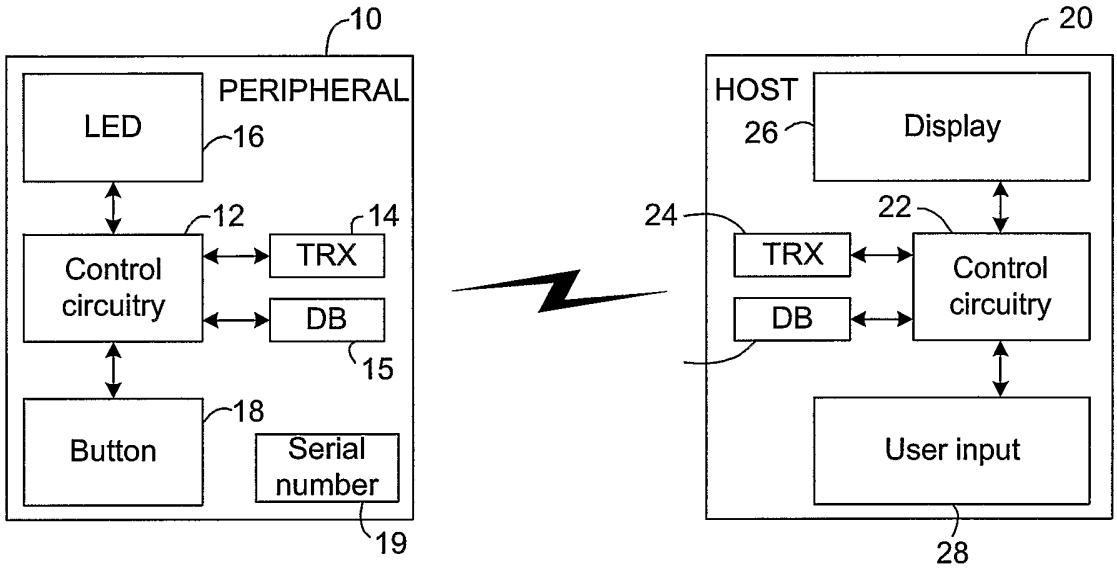

10
PERIPHERAL
LED
16
12
14
Control circuitry
TRX
DB
15
18
Button
Serial number
19
20
HOST
26
Display
24
22
TRX
Control circuitry
DB
User input
28

FIG. 1

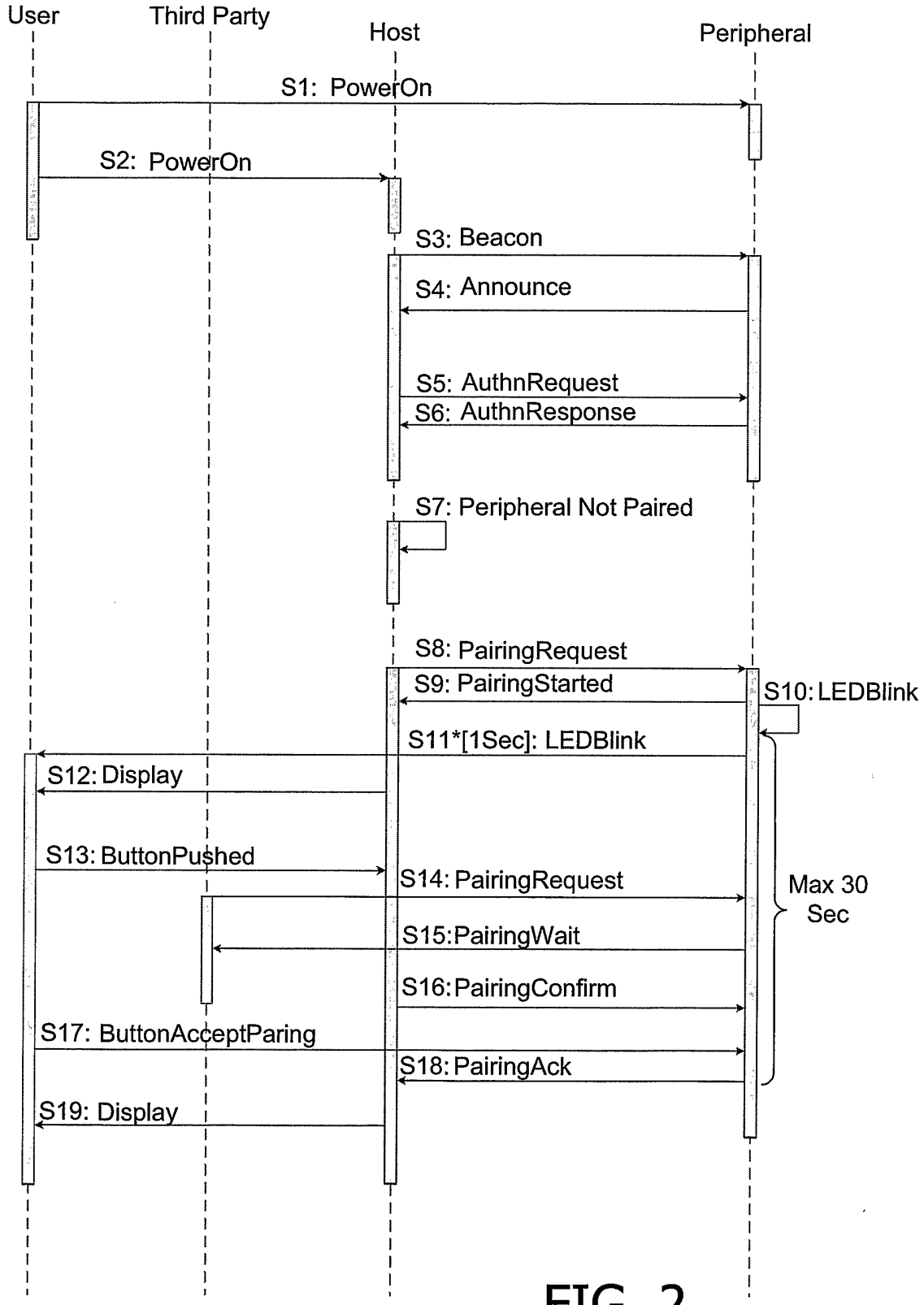

User
Third Party
Host
Peripheral
S1: PowerOn
S2: PowerOn
S3: Beacon
S4: Announce
S5: AuthnRequest
S6: AuthnResponse
S7: Peripheral Not Paired
S8: PairingRequest
S9: PairingStarted
S10: LEDBlink
S11*[1Sec]: LEDBlink
S12: Display
S13: ButtonPushed
S14: PairingRequest
S15:PairingWait
S16:PairingConfirm
S17: ButtonAcceptParing
S18: PairingAck
S19: Display
Max 30 Sec

FIG. 2

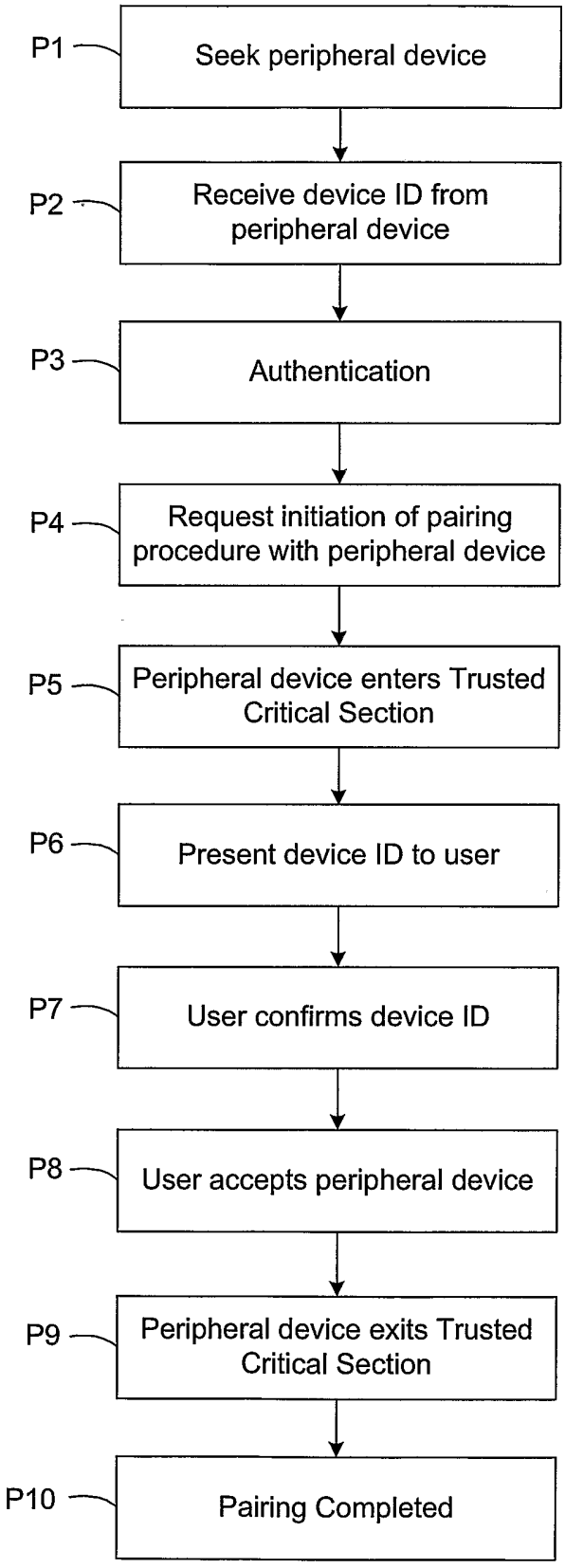

P1
Seek peripheral device
P2
Receive device ID from peripheral device
P3
Authentication
P4
Request initiation of pairing procedure with peripheral device
P5
Peripheral device enters Trusted Critical Section
P6
Present device ID to user
P7
User confirms device ID
P8
User accepts peripheral device
P9
Peripheral device exits Trusted Critical Section
P10
Pairing Completed

FIG. 3

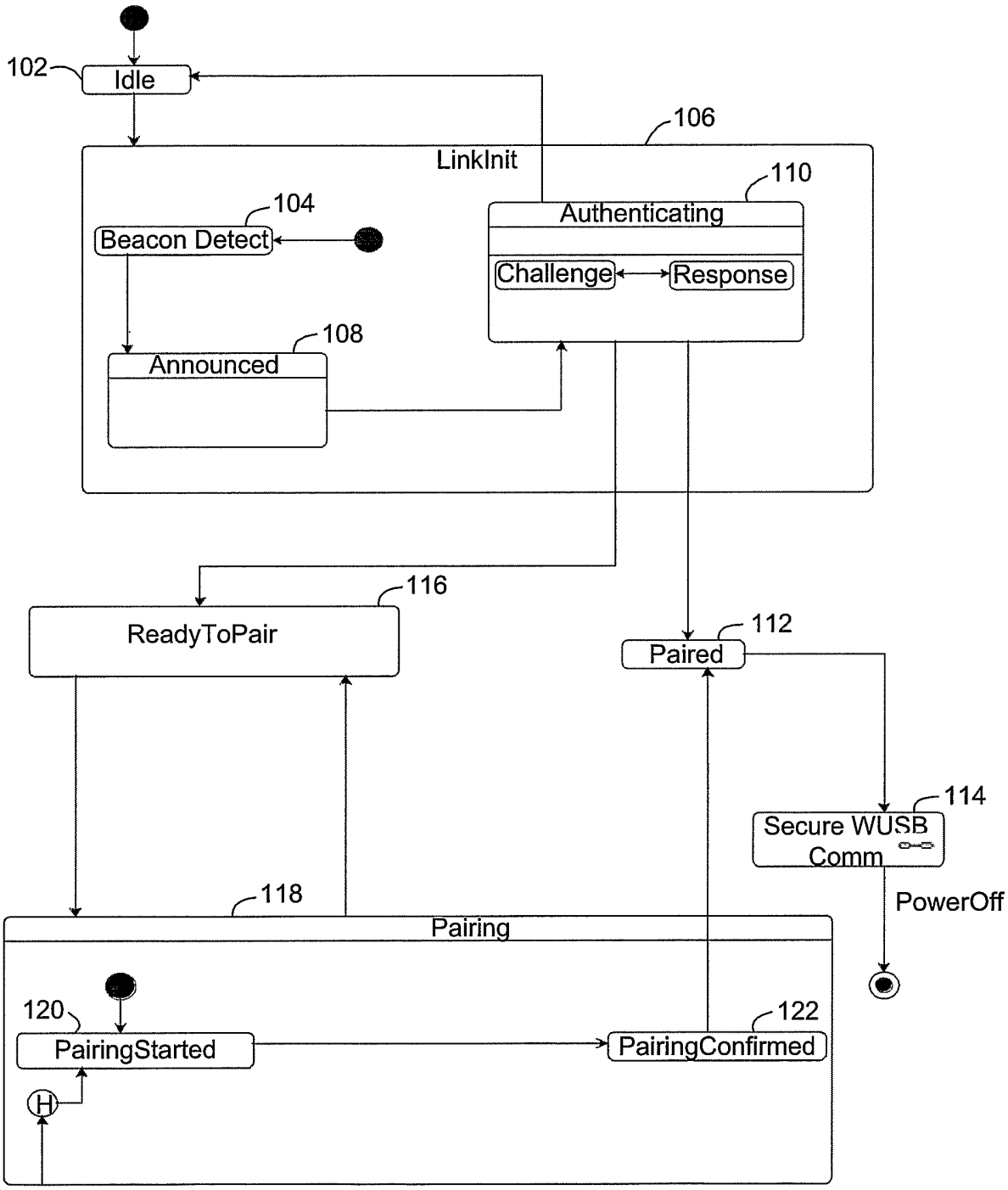

102
Idle
106
LinkInit
110
Authenticating
104
Beacon Detect
Challenge
Response
108
Announced
116
ReadyToPair
112
Paired
114
Secure WUSB Comm
PowerOff
118
Pairing
120
PairingStarted
122
PairingConfirmed
H

FIG. 4

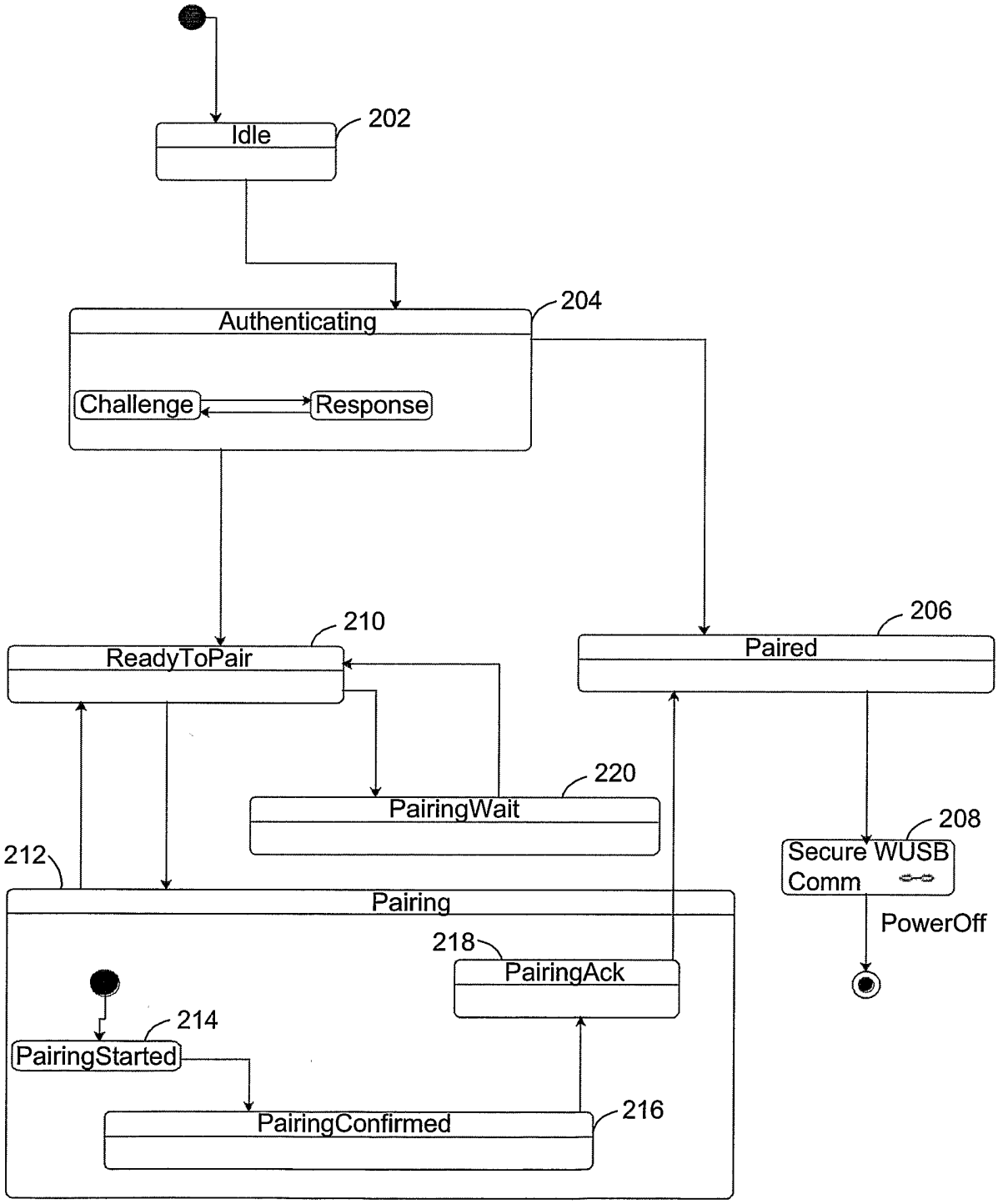

Idle
202
Authenticating
204
Challenge
Response
ReadyToPair
210
Paired
206
PairingWait
220
208
Secure WUSB
Comm
PowerOff
212
Pairing
218
PairingAck
214
PairingStarted
PairingConfirmed
216

FIG. 5

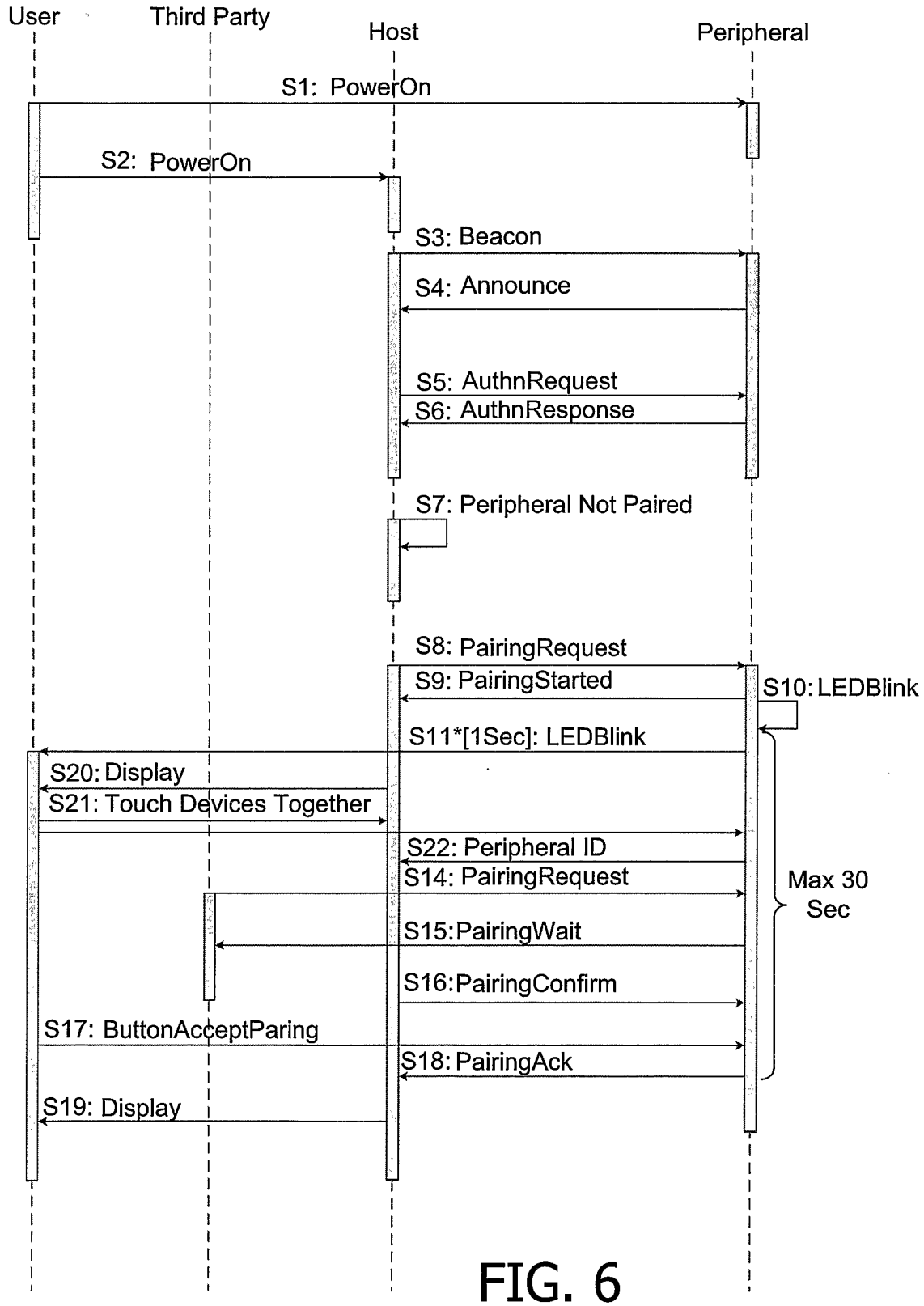

User
Third Party
Host
Peripheral
S1: PowerOn
S2: PowerOn
S3: Beacon
S4: Announce
S5: AuthnRequest
S6: AuthnResponse
S7: Peripheral Not Paired
S8: PairingRequest
S9: PairingStarted
S10: LEDBlink
S11*[1Sec]: LEDBlink
S20: Display
S21: Touch Devices Together
S22: Peripheral ID
S14: PairingRequest
S15:PairingWait
S16:PairingConfirm
S17: ButtonAcceptParing
S18: PairingAck
S19: Display
Max 30 Sec

FIG. 6

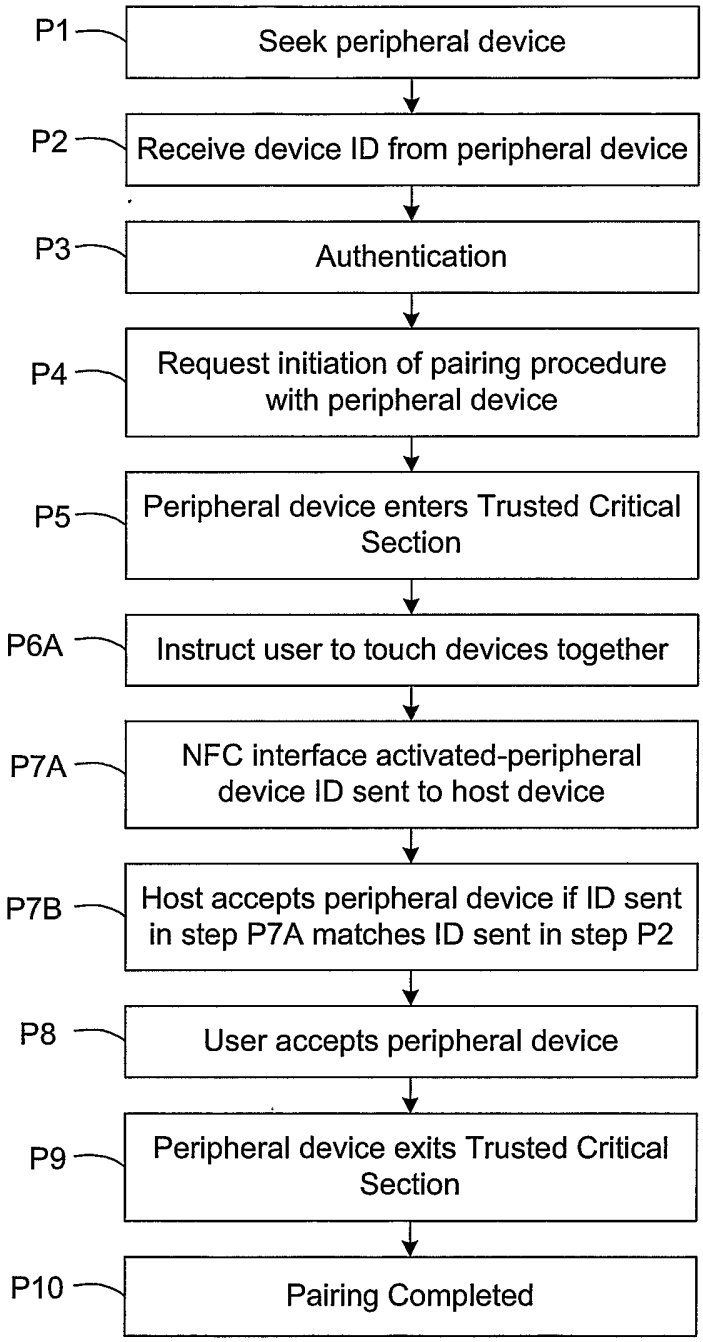

P1
Seek peripheral device
P2
Receive device ID from peripheral device
P3
Authentication
P4
Request initiation of pairing procedure with peripheral device
P5
Peripheral device enters Trusted Critical Section
P6A
Instruct user to touch devices together
P7A
NFC interface activated-peripheral device ID sent to host device
P7B
Host accepts peripheral device if ID sent in step P7A matches ID sent in step P2
P8
User accepts peripheral device
P9
Peripheral device exits Trusted Critical Section
P10
Pairing Completed

FIG. 7

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2005/052854

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/28 H04L12/56

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)
IPC 7 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 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.
A X	US 2003/065952 A1 (OTSUKA NAOKI) 3 April 2003 (2003-04-03) paragraphs '0011!, '0012!, '0057!, '0059!; figures 2-5	1-37, 39-50 38
A	WO 2004/025921 A (TELEFONAKTIEBOLAGET L M ERICSSON ; GEHRMANN, CHRISTIAN) 25 March 2004 (2004-03-25) claims 1-22	1-50
A	US 2003/095521 A1 (HALLER AMIT ET AL) 22 May 2003 (2003-05-22) paragraphs '0057!, '0061!, '0062!, '0068!, '0072!, '0085!, '0093!	1-50
A	EP 0 600 695 A (XEROX CORPORATION; XEROX CORP) 8 June 1994 (1994-06-08) claims 1-10	1-50

-/--

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

[X] Patent family members are listed in 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" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 November 2005	16/11/2005

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, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bischof, J-L

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB2005/052854

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2004/064339 A (KONINKLIJKE PHILIPS ELECTRONICS N.V; HARNISCH, MARKUS; POSCH, STEFAN;) 29 July 2004 (2004-07-29) claims 1-29	1-50
A	WO 2004/036467 A (VODAFONE GROUP PLC; JEAL, DAVID; DEBNEY, CHARLES, WILLIAM) 29 April 2004 (2004-04-29) page 1, line 1 - page 2, line 5	1-50

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB2005/052854

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003065952 A1	03-04-2003	JP 2003110551 A	11-04-2003
WO 2004025921 A	25-03-2004	AU 2003266320 A1	30-04-2004
US 2003095521 A1	22-05-2003	AU 2002352709 A1	10-06-2003
		EP 1456985 A1	15-09-2004
		JP 2005510946 T	21-04-2005
		WO 03047135 A1	05-06-2003
		US 2005232187 A1	20-10-2005
EP 0600695 A	08-06-1994	DE 69330861 D1	08-11-2001
		DE 69330861 T2	28-03-2002
		JP 2528259 B2	28-08-1996
		JP 6233348 A	19-08-1994
		US 5437057 A	25-07-1995
WO 2004064339 A	29-07-2004	AU 2003288646 A1	10-08-2004
WO 2004036467 A	29-04-2004	AU 2003271923 A1	04-05-2004
		AU 2003271926 A1	04-05-2004
		AU 2003282212 A1	04-05-2004
		EP 1552444 A1	13-07-2005
		EP 1552661 A1	13-07-2005
		EP 1552484 A1	13-07-2005
		WO 2004036866 A1	29-04-2004
		WO 2004036513 A1	29-04-2004