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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 July 2002 (18.07.2002)

PCT

(10) International Publication Number
WO 02/056536 A1

(51) International Patent Classification[7]: H04L 9/06

(21) International Application Number: PCT/NL01/00008

(22) International Filing Date: 9 January 2001 (09.01.2001)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON** [SE/SE]; Telefonvagen 30, S-126 25 Stockholm (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **WEINANS, Erwin** [NL/NL]; Vechtvoorde 96, NL-7772 VC Hardenberg (NL).

(74) Agent: **VAN DER AREND, A., G., A.**; Exter Polak & Charlouis B.V., P.O. Box 3241, NL-2280 GE Rijswijk (NL).

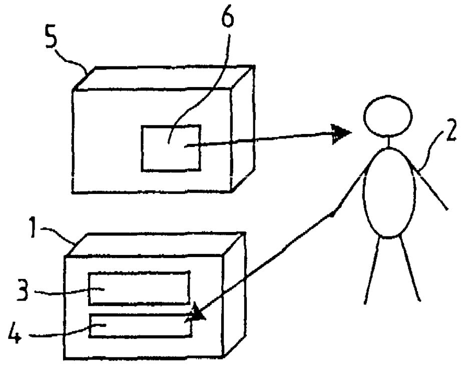
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, 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: METHOD AND SYSTEM FOR BONDING TWO BLUETOOTH DEVICES



(57) Abstract: Method and system for bonding a first Bluetooth device (5, 8) to a second Bluetooth device (1, 15, 22), with both devices placed in a bonding mode, by having the first devcie to generate a random passkey and transmitting it in a manner which is descernible by a user (2) of the devices, or by sensor means (11, 19) of a reader unit (10, 18), or by sensor means (23) of the other device (22). The reader unit (10) may convert a received signal carrying a passkey which is undiscernible by the user (2) into a presentation which is discernible by user (2). Upon discerning the password the user (2) may enter the password in the other device (1) in the usual way. Said other Bluetooth device (15, 22) may have sensor means (16, 23) for sensing a signal carrying a password transmitted by a reader unit (18) or by the Bluetooth device (8).

WO 02/056536 A1

Title: Method for bonding two Bluetooth devices and system suitable for applying the method.

The invention relates to a method for bonding two Bluetooth devices as described in the preamble of claim 1. The invention also relates to a system which is suitable for applying the method as described in the preamble of claim 6.

The Bluetooth technology provides for a short range connection between devices based on 2.4 GHz radio technology. The range is about 10 meters and the devices do not have to be in line of sight to communicate. The maximum bandwidth for data traffic is 1 Mb per second. Bluetooth is operating in the free ISM band, which is also used by many other devices. Bluetooth prevents disturbance by other devices by hopping over 79 frequencies every 1/1600 second.

When a communication cable between two devices is replaced by the use of radio signals for communication there will be a need to prevent eavesdropping and falsifying transmitted messages. Therefore the Bluetooth technology has built-in functionality for authentication and encryption. Authentication is used to prevent unwanted access to data and to prevent falsifying of message originator. Encryption is used to prevent eavesdropping. These two techniques combined with the frequency hopping technique and the limited transmission range for a Bluetooth unit give the technology higher protection against eavesdropping. Dependent on the application which is to be executed the Bluetooth concept provides three levels of security:

1. non-secure; this mode bypasses functionality for authentication and encryption.

2. service-level security; security procedures on this level have not been fully established yet.

3. link-level security; security procedures are initiated before the link set-up upon completion of a Link Manager Protocol (LMP) which is responsible for link set-up between Bluetooth devices.

The link-level security mode is based on the concept of link keys. These keys are secret 128 bit random numbers stored individually for each pair of devices in a Bluetooth connection. Each time two Bluetooth devices communicate the link key is used for authentication and encryption. Both devices contain the same link key which is generated locally in each device based on a passkey which is common for both devices or common information derived from such passkey. The link key is kept secret in each device.

If one wants to use two Bluetooth devices with secure communication between the devices it is necessary to firstly create a trusted relationship between the devices by the user. To that end the user puts the devices in a bonding mode upon which the devices ask the user to enter a passkey, which may be selected arbitrarily by the user. Upon entering the passkey in a device the device will generate a piece of information based on the passkey. The piece of information will be identical for both devices. From then on the two devices are bonded and there is no need to keep the passkey by the user or the devices any longer. In a second stage the passkey based piece of information is used by each device to generate and store a common link key. From that moment on the two devices are paired. The next time the devices get connected the stored link key on both sides will be checked. If the link keys match no request for entering a passkey will be generated. If the link keys do not match the above bonding and pairing procedures must be carried out again.

If the Bluetooth devices which are to be bonded are both equipped with display means and manual input means, in particular a keyboard, there will be no difficulty to enter the passkey by a user of the devices for the bonding procedure.

If one device is not equipped with such an input device the device presently needs to contain a factory programmed passkey. There are two common ways of handling stored passkeys. Firstly the passkeys may be default identical for all manufactured devices of a specific type. Secondly the passkeys may be unique per device.

A drawback of the first solution of handling a factory programmed passkey is that the Bluetooth security is weakened. Since the value of the passkey is essential for creating the link key and the passkey being identical for all devices of the same type a Bluetooth connection between them cannot be considered secure.

A drawback of the second solution is that the manufacturer must maintain a logistic system for handling the many different passkeys, each unique passkey must be communicated to its ultimate user individually, e.g. printed on a box containing a specific Bluetooth device in which the passkey is stored, and the manufacturer must provide a way to restore devices for which the passkey is lost. There must be a support organisation for handling lost passkey requests. Such a logistic and supporting system will be very complex and expensive to maintain.

It is an object of the invention to solve the above mentioned drawbacks.

Therefore the invention provides a method as described in claim 1.

With the method according to claim 1, for entering a passkey in a Bluetooth device, the device needs not to be equipped with a keyboard or such type of physical interface, but any other non-radio communication interface can be used. In particular such non-radio communication interface is part of the device in the first place for normal use of the device. The device may present the randomly generated passkey in several ways, such as by transmission of sound or light.

When applying the method according to the invention the manufacturer may make all Bluetooth devices generic. Still, the devices are able to support Bluetooth encryption in a secure way. There are no logistical costs attached to the method. Since the passkey is uniquely generated every time the device needs to be bonded with another device and on demand by a user of the devices, loosing a passkey is not longer an issue and therefore does not impose costs for retrieving same.

The above mentioned drawbacks are solved also by a system as described in claim 6.

The invention will be described in further detail with reference to the accompanied drawings in which:

fig. 1 shows schematically a system in which a prior art method is applied for entering a passkey into two Bluetooth devices by a user thereof;

figs. 2, 3, 4 and 5 show first to fourth examples respectively of a system according to the invention in which the method according to the invention for entering a passkey into two Bluetooth devices is applied.

The prior art method shown schematically in fig. 1 is suitably for manually entering a passkey into two Bluetooth devices 1 by a user 2. The devices 1 may comprise a display means 3 and an input means 4, such as a keypad.

The arrows shown in fig. 1-5 indicate the entering or transmission of a passkey.

Although indicated as Bluetooth devices, the devices 1 and those to mention may in fact be larger or complexer pieces of equipment containing a pure Bluetooth device integrated therewith. For simplicity the devices as a whole are called Bluetooth device.

The user 2 may choose any suitable passkey arbitrarily. Upon putting the devices 1 in a bonding mode the user 2 may enter the passkey into both devices 1 by using their input means 4. Upon completion thereof each device 1 will use the passkey to generate a link key which will be identical for both devices 1. With every communication session between the devices 1 the devices 1 will check the identity of their link keys by transmitting data which is encrypted by the link key and by analysing a similar received transmission for its validity or identity with the locally stored link key.

The method exemplified by fig. 2 may be applied for providing a common passkey to two Bluetooth devices, such as devices 1, 5, of which one device 5 does not comprise the input means 4 and possibly not the display means 3 of the device 1. Instead, device 5 is provided with some kind of transmission means 6. The transmission means 6 may be an acoustic or optical transducer for transmitting a sound signal or light signal respectively which is discernible by the user 2. The light signal may be of any type, such as light flashes or the display of readable characters.

Bluetooth device 5 contains a random number generator (not shown) for generating a random passkey upon putting the device 5 in bonding mode by user 2. Device 5 will transmit the randomly generated passkey, such that the user 2 can hear, read or otherwise discern the passkey. Then, user 2 may enter the passkey discerned from device 5 into the other device 1 in the same way as with the prior art method shown in fig. 1.

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**