

BLUETOOTH PAIRING SYSTEM, METHOD, AND APPARATUS

FIELD OF THE INVENTION

The present invention relates to Bluetooth enabled devices and in one particular form
5 relates to methods securely pairing Bluetooth devices.

BACKGROUND OF THE INVENTION

The Specification of the Bluetooth System (hereafter referred to as the Bluetooth specification) defines a short range wireless communication system. The system uses
10 frequency hopping spread spectrum technology in the unlicensed Industrial, Scientific, and Medical (ISM) 2.4 GHz short-range radio frequency band. Bluetooth is primarily designed for low power short range communications, typically using low-cost transceiver microchips embedded in devices. Devices may be assigned a class based upon the maximum permitted power, which defines an effective transmission range.
15 Class 1 devices have a range of approximately 1m, class 2 devices have a range of approximately 10m, and class 3 devices have a range of approximately 100m. As Bluetooth is a radio frequency based system, communications between devices need not be line of sight. Version 1.2 of the specification provides for data rates of 1MBit/s and version 2.0+EDR provides for a data rate of 3MBit/s. Version 2.1 of the specification
20 was adopted on July 26, 2007, and plans exist for High Speed Bluetooth, the use of ultra wideband technology (allowing data rates of 480 MBit/s) and ultra low power Bluetooth (Wibree). Devices which implement the Bluetooth specification will be referred to as Bluetooth enabled devices.

25 Bluetooth devices are assigned a unique Bluetooth Device Address (BD_ADDR) which is a 48 bit address assigned from the IEEE Registration Authority. The address is comprised of three fields – the lower address part consisting of 24 bits (LAP), the upper address part consisting of 8 bits (UAP), and the non significant address par consisting of 16 bits (NAP). The LAP is company assigned, and the UAP and NAP form a
30 company ID. There are 64 contiguous LAP values reserved for inquiry operations.

All Bluetooth transmissions over the physical channel begin with an access code based upon the LAP of a device address or an inquiry address. The device access code (DAC) is used during paging. Only the Bluetooth device address is required to setup a connection. To establish new connections a paging procedure is used in which a device

5 makes a page scan using the Bluetooth device address of the target. The Bluetooth device address may be obtained from user interactions, or via an Inquiry procedure, in which a device asks for the Bluetooth device addresses of all nearby devices (additional information is also provided). Individual devices can choose whether or not to respond to Inquiry requests.

10

To enable the establishment of a secure connection between two Bluetooth devices, the Bluetooth specification defines Security Mode 3 which is a link level security mode. A bond is created between the devices by creating, exchanging and storing a common link key (K) which is associated with the Bluetooth Device Address of the other device and

15 such devices are said to be bonded or paired. The common link key is used in authentication procedures during the establishment of a secure connection between the two devices, and is also used to generate an encryption key for encrypting data sent over the connection.

20 The Bluetooth specification defines a pairing procedure (LMP-Pairing, also known as simple pairing) which may be performed for the purpose of generating and storing the link key for later use (this is known as bonding), or as part of the procedure for establishing a secure connection between two devices. The pairing procedure involves creating an initialisation key K_{init} in both devices, using this to create a combined link

25 key K_{AB} , and then mutually authenticating the generated combined link key before allowing establishment of a secure connection.

Generation of initialisation is performed by the first device (A) sending a 128 bit random number (IN_RAND) to the second device (B). Each device then creates an

30 initialisation key K_{init} using the Bluetooth Device Address of the first device (BD_ADDR_A), the random number generated by the first device (IN_RAND) and a (typically 4 digit) PIN code known to both devices. After the generation of the

initialisation key, a combined link key (K_{AB}) is generated. Both devices chose a 128 bit random number (LK_RAND_A , LK_RAND_B) which is bitwise xor'ed with the initialisation key K_{init} and then send to the other device. Each device then extracts the other devices random number and a common link key is created based on
 5 (LK_RAND_A , LK_RAND_B , BD_ADDR_A , BD_ADDR_B). Finally mutual authentication step is performed.

In a mutual authentication step, a first device choses a 128 bit random number (AU_RAND_A) as a challenge and sends it to the second device. The second device
 10 creates a 32 bit word $SRES'_A$ using (AU_RAND_A , BD_ADDR_B , K_{AB}) which is sent back to A. A makes it own calculation of $SRES_A$ using the same input, and compares the two numbers. If $SRES_A$ and $SRES'_A$ agree, the process is repeated but with the roles of A and B switched (ie B initiates and A responds). This mutual authentication procedure is also used by two paired devices when they are establishing any future
 15 secure connections (in which case a link key already exists and does not have to be regenerated).

A problem with the pairing procedure is that if a third party eavesdrops on the whole pairing procedure, they can perform brute force calculations through the space of all
 20 available PIN's and obtain the link key. For example a four digit pin can be cracked in 63 milliseconds using a 3GHz Pentium IV processor.

Version 2.1 of the Specification defined Secure Simple Pairing to provide passive eavesdropping protection through the use of public key cryptography system which
 25 makes the task of obtaining the link key a considerably more difficult problem. Devices exchange public keys, and use one of 4 protocols to exchange information which is used to generate a shared key. A link key is then calculated from the derived shared key and publicly exchanged data.

30 Whether pairing is performed according to the more secure Version 2.1 specification, or earlier less secure versions, a problem exists that either device can control when a new link key is generated. In some situations in which devices are issued to users, it may be

desirable that pairing of devices is performed in a controlled or supervised situation, and that further unauthorised (re)pairing is prevented.

SUMMARY OF THE INVENTION

- 5 According to a first aspect of the present invention, there is provided a method for generating a link key in a Bluetooth enabled device, the method including:
- storing a partial link key in a Bluetooth enabled device;
 - providing a secret key to the Bluetooth enabled device;
 - generating a link key based on the stored partial link key and the provided secret
- 10 key; and
- storing the generated link in the Bluetooth enabled device.

According to a second aspect of the present invention, there is provided a Bluetooth enabled device, said device including:

- 15 means for storing a partial link key in a Bluetooth enabled device;
- means for providing a secret key to the Bluetooth enabled device;
 - means for generating a link key based on the stored partial link key and the provided secret key.

- 20 According to a third aspect of the present invention, there is provided a Bluetooth enabled device, said device including:
- a storage component;
 - a user input component; and
 - a link key generator for generating a link key based on a partial link key stored
- 25 in the storage component and a secret key provided via the user input component.

According to a fourth aspect of the present invention, there is provided a method for bonding two Bluetooth enabled devices, the method including:

- storing a link key in a first Bluetooth enabled device;
- 30 storing a partial link key in a second Bluetooth enabled device;
- providing a secret key to the second Bluetooth enabled device;

generating a copy of the link key in the second device using the stored partial link key and the provided secret key.

associating the generated link key in the second device with the Bluetooth device address of the first Bluetooth enabled device (BD_ADDR1); and

5 associating the stored link key in the first device with the Bluetooth device address of the second Bluetooth enabled device (BD_ADDR2).

According to a fifth aspect of the present invention, there is provided a system for bonding two Bluetooth enabled devices, the system including:

10 a first Bluetooth enabled device including a stored a link key;
a second Bluetooth enabled device including a stored partial link key and a link key generator;

wherein the link key generator generates a copy of the link key stored in the first Bluetooth enabled device using the stored partial link key and a secret key provided to
15 the second Bluetooth device, and the generated link key is associated with the Bluetooth device address of the first Bluetooth enabled device (BD_ADDR1), and a secure connection is established between the two devices using the link key.

According to a sixth aspect of the present invention, there is provided a system for
20 providing link keys to a plurality of Bluetooth enabled devices, the system including:

a plurality of Bluetooth enabled devices, wherein a link key is stored in each device, wherein the stored link key is associated with a partial link key and a secret key, and one or more devices may be associated with the same partial link key to form a set of one or more devices sharing the same partial link key;

25 one or more Bluetooth enabled devices, wherein each device includes at least one partial link key and associated look up key, and where each of the at least one partial link key is associated with a set of one or more devices, and the lookup key identifies the set the partial link key is associated with, and each device include a link key generator for generating a link key using a secret key provided to the device and the
30 partial link key associated with a lookup key provided to the device.

According to a seventh aspect of the present invention, there is provided a method for providing link keys to a plurality of Bluetooth enabled devices, the method including:

storing a link key in each of a plurality of Bluetooth enabled devices, wherein the stored link key is associated with a partial link key and a secret key, and one or
5 more devices may be associated with the same partial link key to form a set of one or more devices sharing the same partial link key;

storing at least one partial link key and associated look up key in each of one or more Bluetooth enabled devices, wherein each of the at least one partial link key is associated with a set of one or more devices;

10 providing a secret key and lookup key to one of the one or more Bluetooth enabled devices which stores at least one partial link key and generating and storing a link key using the provided secret key and the partial link key associated with the provided lookup key.

15 According to a eighth aspect of the present invention, there is provided a method for issuing a first and a second Bluetooth enabled device to a user, the system including:

issuing a first Bluetooth enabled device to a user by an issuing authority, wherein the first device includes a link key and a sensor for detecting the status of a third device;

20 issuing a second Bluetooth enabled devices to a user by an issuing authority, wherein the second device includes a partial link key and wireless communications capability;

providing a secret key to the second device;

25 generating a copy of the link key in the second device using the provided secret key and the partial link key;

establishing a secure Bluetooth link between the first and second Bluetooth enabled devices using the link key;

30 sending an initial status report to a supervising authority using the wireless communications capability of the second device, wherein the initial status report includes the status of device detected by the sensor in the first device and device identifiers for the first and second Bluetooth enabled devices;

sending a confirmation report to the supervising authority from the issuing authority, wherein the confirmation report includes the device identifiers for the first and second Bluetooth enabled devices;

5 verifying that the information received by the supervising authority in the initial status report and in the confirmation report is in agreement.

According to a ninth aspect of the present invention, there is provided a method for remotely monitoring the status of a device by a supervising authority using a first Bluetooth device including a link key and a sensor for detecting the status of a third
10 device, and a second Bluetooth enabled devices including a partial link key and wireless communications capability, the method including:

 establishing a secure Bluetooth link between the first and second Bluetooth enabled devices using the link key, wherein the link key was generated in the second device using a secret key provided to the second device and a partial link key stored in
15 the second device;

 sending an initial status report to the supervising authority using the wireless communications capability of the second device, wherein the initial status report includes the status of device detected by the sensor in the first device and device identifiers for the first and second Bluetooth enabled devices;

20 sending a confirmation report to the supervising authority from the issuing authority, wherein the confirmation report includes the device identifiers for the first and second Bluetooth enabled devices;

 verifying that the information received by the supervising authority in the initial status report and in the confirmation report is in agreement;

25 sending one or more status messages to the supervising authority from the second device using the communications capability;

 sending a change of status alert to the supervising authority from the second device using the wireless communications capability when the sensor on the first device detects a change in status of the third device;

30 sending a loss of link alert to the supervising authority from the second device using the wireless communications capability when there is a loss of the Bluetooth link between the first and second devices.

BRIEF DESCRIPTION OF THE DRAWINGS

Various embodiments of the present invention will be discussed with reference to the accompanying drawings wherein:

- 5 FIGURE 1A is a diagram representing the generation of a link key in a Bluetooth enabled device according to an embodiment of the invention;
 FIGURE 1B is a diagram representing the generation of a link key stored in a first device in a second Bluetooth enabled device according to an embodiment of the invention;
- 10 FIGURE 2 is a system for providing link keys to four groups of devices according to an embodiment of the invention;
 FIGURE 3 is a system for remotely monitoring the status of a device according to an embodiment of the invention;
 FIGURE 4 is a flowchart of a method for generating a link key in a Bluetooth enabled
 15 device according to an embodiment of the invention;
 FIGURE 5 is a flowchart of a method for bonding two Bluetooth enabled devices according to an embodiment of the invention;
 FIGURE 6 is a flowchart of a method for providing link keys to a plurality of Bluetooth enabled devices according to an embodiment of the invention;
- 20 FIGURE 7 is a flowchart of a method for issuing a first and a second Bluetooth enabled device to a user according to an embodiment of the invention; and
 FIGURE 8 is a flowchart of a method for remotely monitoring the status of a device according to an embodiment of the invention.

- 25 In the following description, like reference characters designate like or corresponding parts in the drawings.

DETAILED DESCRIPTION OF THE INVENTION

- 30 Referring now to Figure 1A, there is shown a diagram representing the generation of a link key in a Bluetooth enabled device 100 according to an embodiment of the invention. The link key is as 128 bit number as defined in the Bluetooth Specification (ie 128 bit random number), and thus is suitable for performing authentication and

generation of encryption keys for supporting establishment of secure paired connections between devices using the Bluetooth specification.

5 A first Bluetooth enabled device 110 includes a partial link key (PLK) 112 which is stored in a storage component included in the device. Such a component may include a memory, memory card, firmware chip, or other suitable means for storing information. The device also includes a link key generator for generating a link key 114. The link key generator may comprise hardware, software or a combination thereof, and may be implemented within one or more general purpose processors, microprocessors,
10 application specific integrated circuits (ASICs), programmable logic devices (PLDs), field programmable gate arrays (FPGAs), or other electronic units designed to perform the function of generating a link key. The may be generated using known cryptographic methods that use two input numbers, such as the E2 or E3 key generation functions used in the Bluetooth specification.

15

The device receives a secret key 116 via a user input component such as a keypad, a wired connection such as via a USB cable, or over a wireless connection such as a Bluetooth, WiFi, mobile telecommunications link or other radio frequency or IR link. Security of the system is enhanced if the secret key is provided over a non wireless
20 means. The partial link key 112 and secret key 116 are provided to the link key generator 124 which generates a link key 118. The generated link key 118 is stored in the storage component for use in bonding with another Bluetooth enabled device.

The generated link key may be associated with the Bluetooth device address of a second
25 Bluetooth enabled device (BD_ADDR₂) and stored in the storage component. This may replaced a previously stored link key associated with BD_ADDR₂. The device may further include a key generation controller which prevents replacement of the generated link key associated with BD_ADDR₂ if the replacement key was not generated by the link key generator. This may involve disabling the LMP-Pairing procedure or the
30 Secure Simple Pairing procedure in the implementation of the Bluetooth Specification included in the device.

A method may be defined for generating a link key in a Bluetooth enabled device. Figure 4 is a flowchart of a method for generating a link key in a Bluetooth enabled device (400). The method includes storing a partial link key in a Bluetooth enabled device (410), providing a secret key to the Bluetooth enabled device (420), generating a
 5 link key based on the stored partial link key and the provided secret key (430); and storing the generated link in the Bluetooth enabled device (440).

In Figure 1B, a system for bonding two Bluetooth enabled devices is presented (102). The first Bluetooth enabled device presented in Figure 1A may be bonded with a
 10 second Bluetooth enabled device 120 which includes a link key 122 which is loaded into a storage means included in the device (eg flash memory, memory card, firmware chip, etc). The second Bluetooth enabled device may also include a modified implementation of the Bluetooth Specification which disables use of the standard bonding procedure used to generate a link key. The link key 122 has an associated
 15 partial link key and secret key. If the associated partial link key is stored in first device 110, and the associated secret key 116 is provided to the first device using an input means such as keypad, then the link key generated in the first device 118 will be identical to the link key stored in the second device 122. If each device associates the
 20 link key with the Bluetooth device address of the other device, a Bluetooth bond is created between the two devices. Such a bond enables generation of a secure connections between the devices (ie the devices will be able to mutually authenticate the other using the stored (common) link key.

In one exemplary embodiment a method for bonding two Bluetooth enabled devices is
 25 provided. Figure 5 is a flowchart of a method for bonding two Bluetooth enabled devices 500. The method includes storing a link key in a first Bluetooth enabled device 510, storing a partial link key in a second Bluetooth enabled device 520, providing a secret key to the second Bluetooth enabled device 530, generating a copy of the link key in the second device using the stored partial link key and the provided secret key
 30 540, associating the generated link key in the second device with the Bluetooth device address of the first Bluetooth enabled device (BD_ADDR_1) 550; and associating the

stored link key in the first device with the Bluetooth device address of the second Bluetooth enabled device (BD_ADDR₂) 560.

5 In a further modification the first Bluetooth enabled device 110 may include a plurality of partial link keys, wherein each partial link key has an associated lookup key. If this lookup key is provided to device with the secret key then the link key generator may use the lookup key to select the partial link key to be used to generate the link key. Again security is enhanced if the secret key is provided via non wireless means such as via a keypad.

10

In one exemplary embodiment a method for providing link keys to a plurality of Bluetooth enabled devices is provided. Figure 6 is a flowchart of a method for providing link keys to a plurality of Bluetooth enabled devices 600. The method includes storing a link key in each of a plurality of Bluetooth enabled devices, wherein
15 the stored link key is associated with a partial link key and a secret key, and one or more devices may be associated with the same partial link key to form a set of one or more devices sharing the same partial link key 610. At step 620, the method includes storing at least one partial link key and associated look up key in each of one or more Bluetooth enabled devices, wherein each of the at least one partial link key is associated
20 with a set of one or more devices. The final step 630 includes providing a secret key and lookup key to one of the one or more Bluetooth enabled devices which stores at least one partial link key and generating and storing a link key using the provided secret key and the partial link key associated with the provided lookup key.

25 A system for providing link keys to a plurality of Bluetooth enabled devices (200) is illustrated in Figure 2. A plurality of devices 212, 214, 222, 224, 232, and 236 are divided into three sets 210, 220 and 230 of two devices. However the sets may include one device or many devices (indicated by dashed lines 234). Each device includes a preloaded link key. This may be unique link keys 213, 215, 223, 225 stored, or loaded
30 into devices 212, 214, 222, 224. Alternatively two devices in the same set may share the same link key as in set 230 in which devices 232 and 236 each share link key 233. As is

illustrated in Figure 2, some sets may share link keys whilst other sets may use unique link keys.

Each of the link keys in a given set are associated with a partial link key. A further set
5 240 of devices 242 and 243 include Bluetooth enabled devices which store a partial link
key and look up associated with each set. This may stored in the form of a lookup table
243 equivalent data structure may be used, either in hardware, software or a
combination. Each of the devices in set 240 may be bonded with any of the devices in
set 210, 220 or 230 by providing the device with the secret key associated with the
10 device to be bonded, and the lookup key associated with the set the device to be bonded
is part of. This allows the device in set 240 to generate the appropriate link key which is
stored in the device to which it is to be bonded, thus allowing generation of a secure
Bluetooth connection.

15 A key generation controller may also be used to prevent replacement of a generated link
key. The controller may optionally prevent any replacement or just replacement by link
key generated by some other means. The use of the key generation controller may be
activated or disactivated using a password or other instruction to allow an administrator
to control this functionality. Devices may also be modified so that they will only
20 respond to a Bluetooth Device Inquiry from another device, or allow establishment of a
Bluetooth link with another device, if a predetermined portion of Bluetooth device
address (BD_ADDR) of the other device is in a list of approved address portions. This
may for example be based on the lower address part (LAP) of the Bluetooth device
address (BD_ADDR). The LAP is assigned to manufacturers and in this way
25 communication can be restricted to devices from the same manufacturer, or from other
approved manufacturers by storing a list of approved LAP's in the device.

These methods, devices and systems, or variants thereof may be utilised as parts of
larger systems. For example in the case of a security monitoring system, in which
30 officer are issued weapons, a supervising authority may wish to know when the weapon
is removed from the holster or readied for action such as by unclipping a holster clip. In

such a system, a security officer may be issued a Bluetooth enabled mobile phone which is paired to a Bluetooth enabled device for monitoring weapon status.

- In one exemplary embodiment a method for issuing a first and a second Bluetooth enabled device to a user is provided. Figure 7 is a flowchart of a method for issuing a first and a second Bluetooth enabled device to a user 700. The method includes issuing a first Bluetooth enabled device to a user by an issuing authority, wherein the first device includes a link key and a sensor for detecting the status of a third device 710 and issuing a second Bluetooth enabled devices to a user by an issuing authority, wherein the second device includes a partial link key and wireless communications capability; providing a secret key to the second device 720. At step 730 the method continues by generating a copy of the link key in the second device using the provided secret key and the partial link key, and establishing a secure Bluetooth link between the first and second Bluetooth enabled devices using the link key 740. At step 750 the method continues by sending an initial status report to a supervising authority using the wireless communications capability of the second device, wherein the initial status report includes the status of device detected by the sensor in the first device and device identifiers for the first and second Bluetooth enabled devices. At step 760 the method continues by sending a confirmation report to the supervising authority from the issuing authority, wherein the confirmation report includes the device identifiers for the first and second Bluetooth enabled devices, and then verifying that the information received by the supervising authority in the initial status report and in the confirmation report is in agreement 770.
- 25 The confirmation report may include a confirmation of the status of the third device. Further the second device may resends the initial status report until an acknowledgement message is received from the supervising authority.

- In one exemplary embodiment a method for remotely monitoring the status of a device by a supervising authority. Figure 8 is a flowchart of a method for remotely monitoring the status of a device by a supervising authority using a first Bluetooth device including a link key and a sensor for detecting the status of a third device, and a second Bluetooth

enabled devices including a partial link key and wireless communications capability 800. The method includes:

5 establishing a secure Bluetooth link between the first and second Bluetooth enabled devices using the link key, wherein the link key was generated in the second device using a secret key provide to the second device and partial link key stored in the second device 810;

10 sending an initial status report to the supervising authority using the wireless communications capability of the second device, wherein the initial status report includes the status of device detected by the sensor in the first device and device identifiers for the first and second Bluetooth enabled devices 820;

sending a confirmation report to the supervising authority from the issuing authority, wherein the confirmation report includes the device identifiers for the first and second Bluetooth enabled devices 830;

15 verifying that the information received by the supervising authority in the initial status report and in the confirmation report is in agreement 840;

sending one or more status messages to the supervising authority from the second device using the communications capability 850;

20 sending a change of status alert to the supervising authority from the second device using the wireless communications capability when the sensor on the first device detects a change in status of the third device 860;

sending a loss of link alert to the supervising authority from the second device using the wireless communications capability when there is a loss of the Bluetooth link between the first and second devices 870.

25 The second Bluetooth enabled device may resend a previously sent message one or more times if an acknowledgement message is not received from the supervising authority. Also the one or more status messages are sent at regular time intervals until monitoring of the status of the third device is terminated. In one example this could be every 5 minutes. In one example the second Bluetooth enabled device is a mobile
30 telephone. The third device may be is a weapon and the sensor may be a holster sensor which detects removal of a clip for holding the weapon in the holster.

Figure 3 is a system for remotely monitoring the status of a device according to an embodiment of the invention. The issuing authority 320 issues a device from a first set of Bluetooth enabled devices 326 and a device from a second set of Bluetooth enabled devices 324. The first set of Bluetooth enabled devices may be holster monitoring
5 sensors. These could be electromagnetic sensors which detect clipping and unclipping of the holster. The holster could be for a variety of weapons and devices. The second set of Bluetooth enabled devices may for example be mobile telephones and include partial link keys and lookup keys. An application 322 stores secret keys for devices and records pairing of two devices which is sent to a supervising authority 310 over wired
10 or wireless means 342.

The issuing authority may provide the secret key to the second device over a wired connection. The issuing authority could use the application to lookup the secret key associated with the second device (either on the PC device the application, or a server
15 the application is in communication with) , and the application could send the secret key over the wired connection. Alternatively the issuing authority could look up the key using the application and manually enter it into the key pad of the second device. In another alternative a interface device may store the secret key for the second device (temporarily or over an extended period), The interface device may be connected to the
20 second device using a wired connection and send the secret key to the second device over the wired connection upon a suitable instruction. The instruction may be via a button, keypad, or similar input means on the interface device, or an application running on the second device may recognise the interface device and request the secret key.

25 At 330 an officer has been issued a mobile telephone device 332 according to an embodiment of the invention and holster monitoring device 336 according to an embodiment of the invention which also includes a sensor 337 for monitoring the status of a holster clip 338. A secure Bluetooth connection 334 exists between the devices. The mobile telephone sends and receives information to and from the supervising
30 authority using a wireless telephone connection indicated by 344, 340 and 342. When the officer unclips or draws their weapon an alert is sent to the supervising authority who may acknowledge and plan further action. This could include sending the officer

further assistance, or communicating with the officer. If there is a loss of link, such as the holster monitoring device 336 no longer being in Bluetooth communications range with the mobile telephone device 332 then an alert may be sent to the supervising authority who may acknowledge and plan further action such as attempting to contact the officer.

The methods, devices and systems described herein advantageously provide security enhancements to the Bluetooth specification. Devices may be securely bonded, especially in systems where there are a large number of devices to potentially to be bonded to other devices. Reuse of link keys reduces the required memory capacity of the devices. Preloading of link keys, and modification of Bluetooth procedures in the Bluetooth specification such as preventing replacement of generated link keys (such as by disabling standard link key generation means), along with making devices non responsive to devices other than those from the same or other approved manufacturers limits tampering of the system and provides security enhancements. Such enhancements can be deployed for example in a security setting for monitoring the status of security officer's weapons. This example is illustrative only and in no way limiting. Further monitoring of officers using embodiments of the invention may also prevent officers from misusing issued devices.

20

Throughout the specification and the claims that follow, unless the context requires otherwise, the words "comprise" and "include" and variations such as "comprising" and "including" will be understood to imply the inclusion of a stated integer or group of integers, but not the exclusion of any other integer or group of integers.

25

The reference to any prior art in this specification is not, and should not be taken as, an acknowledgement of any form of suggestion that such prior art forms part of the common general knowledge.

It will be appreciated by those skilled in the art that the invention is not restricted in its use to the particular application described. Neither is the present invention restricted in its preferred embodiment with regard to the particular elements and/or features

described or depicted herein. It will be appreciated that various modifications can be made without departing from the principles of the invention. Therefore, the invention should be understood to include all such modifications in its scope.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS

1. A method for generating a link key in a Bluetooth enabled device, the method including:
 - storing a partial link key in a Bluetooth enabled device;
 - providing a secret key to the Bluetooth enabled device;
 - generating a link key based on the stored partial link key and the provided secret key; and
 - storing the generated link in the Bluetooth enabled device.
2. A method as claimed in claim 1, wherein the Bluetooth enabled device includes a user input means, and the secret key is provided via the user input means.
3. A method as claimed in claim 2, wherein the user input means is a keypad, and the secret key is provided via the keypad.
4. A method as claimed in any one of claims 1-3, further including:
 - associating the generated link key with the Bluetooth device address of a second Bluetooth enabled device (BD_ADDR₂).
5. A method as claimed in claim 4, wherein the generated link key replaces a previously stored link key associated with BD_ADDR₂.
6. A method as claimed in claim 5, further including:
 - preventing replacement of the generated link key associated with BD_ADDR₂ if the replacement key was generated by an alternative method to the method of claims 1-5.
7. A Bluetooth enabled device, said device including:
 - means for storing a partial link key in a Bluetooth enabled device;
 - means for providing a secret key to the Bluetooth enabled device;
 - means for generating a link key based on the stored partial link key and the provided secret key.

8. A device as claimed in claim 7, wherein the means for providing a secret key is a keypad.
9. A device as claimed in claim 7 or 8, further including:
means for associating the generated link key with the Bluetooth device address of a second Bluetooth enabled device (BD_ADDR₂).
10. A device as claimed in claim 9, wherein the generated link key replaces a previously stored link key associated with BD_ADDR₂.
11. A device as claimed in claim 10 further including:
means for preventing replacement of the generated link key associated with BD_ADDR₂.if the replacement key was not generated by the means for generating a link key.
12. A Bluetooth enabled device, said device including:
storage component;
a user input component; and
a link key generator for generating a link key based on a partial link key stored in the storage component and a secret key provided via the user input component.
13. A device as claimed in claim 12, wherein the user input component is a keypad.
14. A device as claimed in claim 12 or 13, wherein the generated link key is associated with the Bluetooth device address of a second Bluetooth enabled device (BD_ADDR₂) and stored in the storage component.
15. A device as claimed in claim 14, wherein the generated link key replaces a previously stored link key associated with BD_ADDR₂.
16. A device as claimed in claim 10 further including:

a key generation controller which prevents replacement of the generated link key associated with BD_ADDR₂ if the replacement key was not generated by the link key generator.

17. A method for bonding two Bluetooth enabled devices, the method including:
storing a link key in a first Bluetooth enabled device;
storing a partial link key in a second Bluetooth enabled device;
providing a secret key to the second Bluetooth enabled device;
generating a copy of the link key in the second device using the stored partial link key and the provided secret key.

associating the generated link key in the second device with the Bluetooth device address of the first Bluetooth enabled device (BD_ADDR₁); and

associating the stored link key in the first device with the Bluetooth device address of the second Bluetooth enabled device (BD_ADDR₂).

18. A method as claimed in claim 17, wherein the secret key is provided using non-wireless means.

19. A method as claimed in claim 18, wherein the secret key is provided via a user input means included in the second device.

20. A method as claimed in claim 19, wherein the user input means is a keypad.

21. A method as claimed in any one of claims 17 to 20, wherein the generated link key replaces a previously stored link key associated with BD_ADDR₁.

22. A method as claimed in any one of claims 17 to 21, further including:
disabling generation of a new link key in the first Bluetooth enabled device.

23. A method as claimed in any one of claims 17 to 22, further including:
preventing replacement of the generated link key associated with BD_ADDR₂ if the replacement key was generated by an alternative method to the method of claims 17-22.

24. A system for bonding two Bluetooth enabled devices, the system including:
a first Bluetooth enabled device including a stored a link key;
a second Bluetooth enabled device including a stored partial link key and a link key generator;
wherein the link key generator generates a copy of the link key stored in the first Bluetooth enabled device using the stored partial link key and a secret key provided to the second Bluetooth device, and the generated link key is associated with the Bluetooth device address of the first Bluetooth enabled device (BD_ADDR₁), and a secure connection is established between the two devices using the link key.
25. A system as claimed in claim 24, wherein the secret key is provided using non-wireless means.
26. A system as claimed in claim 25, wherein the secret key is provided via a keypad.
27. A system as claimed in any one of claims 24 to 26, wherein the generated link key replaces a previous link key associated with the first Bluetooth device.
28. A system as claimed in any one of claims 24 to 27, wherein the first Bluetooth enabled device is disabled from generating a new link key.
29. A system as claimed in any one of claims 24to 28, wherein the second Bluetooth enabled device includes a plurality of partial link keys, wherein each partial link key has an associated lookup key, and a lookup key is provided to the second Bluetooth enabled device, and link key generator uses the lookup key to select the partial link key to be used to generate the link key.
30. A system for providing link keys to a plurality of Bluetooth enabled devices, the method including:
a plurality of Bluetooth enabled devices, wherein a link key is stored in each device, wherein the stored link key is associated with a partial link key and a secret key,

and one or more devices may be associated with the same partial link key to form a set of one or more devices sharing the same partial link key;

one or more Bluetooth enabled devices, wherein each device includes at least one partial link key and associated look up key, and where each of the at least one partial link key is associated with a set of one or more devices, and the lookup key identifies the set the partial link key is associated with, and each device include a link key generator for generating a link key using a secret key provided to the device and the partial link key associated with a lookup key provided to the device.

31. A system as claimed in claim 30, wherein a secret key is provided using non-wireless means.

32. A system as claimed in claim 30 or 31, wherein each of the devices in a set also share the same link key.

33. A system as claimed in claim 30 or 31, wherein each of the devices in a set have a unique link key.

34. A system as claimed in any one of claims 30 to 32, wherein the Bluetooth enabled devices are disabled from generating a link key using the link key generator is present or other link key generation means.

35. A system as claimed in claim 30 to 34 wherein each of the devices will only respond to a Bluetooth Device Inquiry from another device, or allow establishment of a Bluetooth link with another device, if a predetermined portion of Bluetooth device address (BD_ADDR) of the other device is in a list of approved address portions.

36. A system as claimed in claim 35 wherein the predetermined portion is the lower address part (LAP) of the Bluetooth device address (BD_ADDR), and the list of approved address portions is a list of approved LAPs.

37. A method for providing link keys to a plurality of Bluetooth enabled devices, the method including:

storing a link key in each of a plurality of Bluetooth enabled devices, wherein the stored link key is associated with a partial link key and a secret key, and one or more devices may be associated with the same partial link key to form a set of one or more devices sharing the same partial link key;

storing at least one partial link key and associated look up key in each of one or more Bluetooth enabled devices, wherein each of the at least one partial link key is associated with a set of one or more devices;

providing a secret key and lookup key to one of the one or more Bluetooth enabled devices which stores at least one partial link key and generating and storing a link key using the provided secret key and the partial link key associated with the provided lookup key.

38. A method as claimed in claim 37, wherein a secret key is provided using non-wireless means.

39. A method as claimed in claim 37 or 38, wherein each of the devices in a set also share the same link key.

40. A method as claimed in claim 37 or 38, wherein each of the devices in a set have a unique link key.

41. A method as claimed in any one of claims 37 to 40, further including:
preventing replacement of a generated link key if the replacement key was generated by an alternative method to the method of claims 37 to 41.

42. A method as claimed in claim 37 to 41 wherein each of the devices will only respond to a Bluetooth Device Inquiry from another device, or allow establishment of a Bluetooth link with another device, if a predetermined portion of Bluetooth device address (BD_ADDR) of the other device is in a list of approved address portions.

43. A method as claimed in claim 42 wherein the predetermined portion is the lower address part (LAP) of the Bluetooth device address (BD_ADDR), and the list of approved address portions is a list of approved LAPs.

44. A method for issuing a first and a second Bluetooth enabled device to a user, the method including:

issuing a first Bluetooth enabled device to a user by an issuing authority, wherein the first device includes a link key and a sensor for detecting the status of a third device;

issuing a second Bluetooth enabled devices to a user by an issuing authority, wherein the second device includes a partial link key and wireless communications capability;

providing a secret key to the second device;

generating a copy of the link key in the second device using the provided secret key and the partial link key;

establishing a secure Bluetooth link between the first and second Bluetooth enabled devices using the link key;

sending an initial status report to a supervising authority using the wireless communications capability of the second device, wherein the initial status report includes the status of device detected by the sensor in the first device and device identifiers for the first and second Bluetooth enabled devices;

sending a confirmation report to the supervising authority from the issuing authority, wherein the confirmation report includes the device identifiers for the first and second Bluetooth enabled devices;

verifying that the information received by the supervising authority in the initial status report and in the confirmation report is in agreement.

45. A method as claimed in claim 44 wherein a secret key is provided using non-wireless means.

46. A method as claimed in claim 44 or 45, wherein the confirmation report includes confirmation of the status of the third device.

47. A method as claimed in any one of claims 44 to 46, wherein the second device resends the initial status report until an acknowledgement message is received from the supervising authority.

48. A method for remotely monitoring the status of a device by a supervising authority using a first Bluetooth device including a link key and a sensor for detecting the status of a third device, and a second Bluetooth enabled devices including a partial link key and wireless communications capability, the method including:

- establishing a secure Bluetooth link between the first and second Bluetooth enabled devices using the link key, wherein the link key was generated in the second device using a secret key provided to the second device and a partial link key stored in the second device;

- sending an initial status report to the supervising authority using the wireless communications capability of the second device, wherein the initial status report includes the status of device detected by the sensor in the first device and device identifiers for the first and second Bluetooth enabled devices;

- sending a confirmation report to the supervising authority from the issuing authority, wherein the confirmation report includes the device identifiers for the first and second Bluetooth enabled devices;

- verifying that the information received by the supervising authority in the initial status report and in the confirmation report is in agreement;

- sending one or more status messages to the supervising authority from the second device using the communications capability;

- sending a change of status alert to the supervising authority from the second device using the wireless communications capability when the sensor on the first device detects a change in status of the third device;

- sending a loss of link alert to the supervising authority from the second device using the wireless communications capability when there is a loss of the Bluetooth link between the first and second devices.

49. A method as claimed in claims 48 wherein the secret key is provided using non-wireless means.

50. A method as claimed in claim 48 or 49, wherein the second Bluetooth enabled device resends a previously sent message one or more times if an acknowledgement message is not received from the supervising authority.

51. A method as claimed in any one of claims 48 to 50, wherein the one or more status messages are sent at regular time intervals until monitoring of the status of the third device is terminated.
52. A method as claimed in any one of claims 48 to 51, wherein the second Bluetooth enabled device is a mobile telephone.
53. A method as claimed in any one of claims 48 to 52, wherein the third device is a weapon.
54. A method as claimed in claim 53, wherein the sensor is a holster sensor which detects removal of a clip for holding the weapon in the holster.