BLUETOOTH SERIAL PORT ADAPTER SECURITY

Document Revision

Document number: 5570572

Release: Oct 21, 2011 14:08

Document version: 7

1 Table of Content

2 Introduction

With the introduction of Bluetooth 2.1+EDR, Simple Pairing was introduced.

The main goals for Simple Pairing are:

1. To simplify the pairing process from the point of view of the end user.
2. To maintain or improve the security in Bluetooth.

This document shortly describes:

- What Simple Pairing is (Section *Bluetooth Specification Simple Pairing*).
- How security is implemented in the Bluetooth 2.1+EDR versions of the connectBlue Serial Port Adapter (Section *Serial Port Adapter Security Modes*).
- Some common user scenarios (Section *Sample Use Cases*).
- How the connectBlue Bluetooth Serial Port Adapter Toolbox can be of some assistance for some of the security modes (Section *Bluetooth Serial Port Adapter Toolbox*).

2.1 Related Documents

- The **Bluetooth Serial Port Adapter Toolbox - Getting Started**, shortly describes how to use the toolbox to configure the Bluetooth serial port adapter.
- The **Bluetooth Serial Port Adapter AT Commands** document contains a short introduction to the concepts of the Serial Port Adapter as well as a description of the AT commands supported.

3 Bluetooth Specification Simple Pairing

Simple Pairing aims to improve protection against *passive eavesdropping*, using an Elliptic Curve Diffie-Hellman (ECDH) public key cryptography. This means about 95 bits of entropy which exceeds the requirements of the Bluetooth SIM Access Profile (profile with strongest security requirements).

Simple Pairing also protects the user from *man-in-the-middle attacks* (active eavesdropping) with a goal of offering a 1 in 1000000 risk that a man-in-the-middle could mount a successful attack. This is a probability that is considered low enough to meet FIPS 140-29 requirements for authentication.

There are three main use cases to consider for Simple Pairing.

1. *Just Works:* Intended for scenarios where at least one device does not have a display or keyboard, such as cell phone - headset. The idea is to enable pairing during only the time that the phone and headset shall be connected. During this time, all pairing attempts will be automatically accepted.
2. *Numeric Comparison:* Intended for scenarios where both sides have a display and possibility to enter yes/no, such as cell phone - PC. A six digit number will be displayed on both sides, and if the number is the same, the pairing attempt is accepted by entering yes on both sides.
3. *Passkey Entry:* Intended for scenarios where one side does only have input capabilities (no output) and the other side has output capabilities, such as keyboard - PC. The device with output capabilites displays a six digit number which is entered on the side with the input capabilities. If the number is correct pairing is successful.

If a Bluetooth 2.1+EDR device tries to pair with a Bluetooth 2.0+EDR (or earlier version) device, the Bluetooth 2.1+EDR device must do pairing according to the Bluetooth 2.0+EDR security (which means no simple pairing). However, two Bluetooth 2.1+EDR devices must apply to the requirements of Simple Pairing and may not use the Bluetooth 2.0+EDR security mechanisms.

4 Serial Port Adapter Security Modes

There are 7 different security modes to support all kinds of use cases regarding the pairing procedure. Each mode is specified for both Bluetooth 2.0+EDR and 2.1+EDR security since both must be supported depending on what the remote device supports. If the remote device supports only Bluetooth 2.0+EDR (or previous versions), a Bluetooth 2.1+EDR device must conform to the Bluetooth 2.0+EDR security algorithms.

All security modes except Security Mode 1 (Security Disabled) for Bluetooth 2.0+EDR devices uses encryption. Hence, security mode 1 (Security Disabled) for Bluetooth 2.1+EDR still uses encryption. The encryption algorithm is a 128-bit cipher called E0.

Security mode 1 and 2 are implemented to keep the same (or similar) behaviour as for previous versions of the Serial Port Adapter.

The Display Only, Display Yes/No and Keyboard Only modes (modes 5, 6 and 7) can only be used when the serial port adapter is in AT or Extended Data mode since it requires user interaction (AT commands and events). The other modes works also in Data mode.

Please note that the Security Mode for the Serial Port Adapter does not directly correspond to the Security Mode of the Bluetooth specification.

4.1 Security Mode 1: Security Disabled

Remote Device - Bluetooth 2.0+EDR

Security is disabled and no link key is generated.

Corresponds to BT 2.0 Security Mode 1 in the Bluetooth specification.

Remote Device - Bluetooth 2.1+EDR (Simple Pairing)

Pairing will be auto accepted without using a passkey and a link key is generated. Since a link key is generated, pairability must be enabled.

Corresponds to BT 2.1 Security Mode 4 Level 1 in the Bluetooth specification.

4.2 Security Mode 2: Bluetooth 2.0+EDR Security

This mode disables Simple Pairing and enforces Bluetooth 2.0+EDR security.

It is included only for backward compatibility and should not be used since pairing between two Bluetooth 2.1+EDR devices must use Simple Pairing.

Please note that according to the Bluetooth specification, Simple Pairing must be used between two Bluetooth 2.1+EDR devices.

Corresponds to BT 2.0 Security Mode 2 in the Bluetooth specification.

4.3 Security Mode 3: Fixed Pin

Remote Device - Bluetooth 2.0+EDR

Fixed pin (AT*AGFP) and Bluetooth 2.0+EDR security is used.

Note that the fixed pin consists of 1 to 16 alphanumerical characters.

Corresponds to BT 2.0 Security Mode 2 in the Bluetooth specification.

Remote Device - Bluetooth 2.1+EDR (Simple Pairing)

In Bluetooth 2.0 versions of the connectBlue Serial Port Adapters, security is managed automatically using the fixed pin code (AT*AGFP). This is not one of the standard use cases described in Simple Pairing. However, if two Bluetooth 2.1+EDR devices both acts as Keyboard Only devices it will still work in a similar manner. Instead of having a user enter the 6 digit numerical passkey, a fixed passkey stored in flash is used (AT*AGFP2).

Note that the passkey consists of 1 to 6 numerical digits.

This security mode is intended for use cases between two connectBlue Bluetooth 2.1+EDR Serial Port Adapters where both are configured for Fixed Pin security.

Pairing will then be automatic (no user interaction) using the stored passkey (AT*AGFP2) and a link key is generated.

Corresponds to BT 2.1 Security Mode 4 Level 3 in the Bluetooth specification.

Note: in Bluetooth 2.0 it is called pin code and in Bluetooth 2.1 it is called passkey.

4.4 Security Mode 4: Just Works

When the Just Works security mode is set, pairability is automatically disabled (see AT*AGPM). This means that pairing will always fail. The idea is to enable pairing only during the time the two devices shall be associated and in a safe environment. In AT mode, pairing is temporarily enabled using the AT*AGPM command. If pairing is enabled and not disabled, it will be disabled at next power on. In Data mode, the "External Connect" button can be pressed for at least 5 seconds to enable pairable for 60 seconds. The LED will blink during the time pairing is enabled. To trigger external connect, the "External Connect" button is pressed for a maximum of 1 seconds.

Remote Device - Bluetooth 2.0+EDR

Fixed pin (AT*AGFP) and Bluetooth 2.0+EDR security is used.

Corresponds to BT 2.0 Security Mode 2 in the Bluetooth specification.

Remote Device - Bluetooth 2.1+EDR (Simple Pairing)

Pairing will be auto accepted without using a passkey and a link key is generated. Please note that if the device is always pairable, this mode is the same as No Security for the Bluetooth 2.1+EDR use case.

Corresponds to BT 2.1 Security Mode 4 Level 2 in the Bluetooth specification.

*Note that when the Just Works security mode is set, pairablility is automatically disabled. If the security mode is then changed to something else, pairability is still disabled and must be enabled using AT*AGPM to pair. Every time the module leaves Data Mode or is reset, pairability is disabled again.*

4.5 Security Mode 5: Display Only

Intended for devices which supports output capabilites and with a remote device that supports input capabilities.

Remote Device - Bluetooth 2.0+EDR

Fixed pin (AT*AGFP) and Bluetooth 2.0+EDR security is used.

Corresponds to BT 2.0 Security Mode 2 in the Bluetooth specification.

Remote Device - Bluetooth 2.1+EDR (Simple Pairing)

The device must be in AT or Extended Data mode.

When pairing is initiated, the User Passkey Display event (*AGUPD) will be sent to the host with a six digit number. The local host shall then display the number so that it can be entered at the remote device.

Corresponds to BT 2.1 Security Mode 4 Level 3 in the Bluetooth specification.

4.6 Security Mode 6: Display Yes/No

Intended for devices with both output and input capabilities and where the remote device supports both output and input capabilities.

Remote Device - Bluetooth 2.0+EDR

Fixed pin (AT*AGFP) and Bluetooth 2.0+EDR security is used.

Corresponds to BT 2.0 Security Mode 2 in the Bluetooth specification.

Remote Device - Bluetooth 2.1+EDR (Simple Pairing)

The device must be in AT or Extended Data mode.

When pairing is initiated, the User Confirmation event (*AGUC) will be sent to the host with a six digit number and the Bluetooth address of the remote device. The host shall then display the number and let the user accept or reject the pairing attempt by calling the User Confirmation command (AT*AGUC).

Corresponds to BT 2.1 Security Mode 4 Level 3 in the Bluetooth specification.

4.7 Security Mode 7: Keyboard Only

Intended for a device with input capabilites and with a remote device that supports output capabilities.

Remote Device - Bluetooth 2.0+EDR

Fixed pin (AT*AGFP) and Bluetooth 2.0+EDR security is used.

Corresponds to BT 2.0 Security Mode 2 in the Bluetooth specification.

Remote Device - Bluetooth 2.1+EDR (Simple Pairing)

The device must be in AT or Extended Data mode.

When pairing is initiated, the User Passkey Entry event (*AGUPE) is sent to the host with the Bluetooth address of the remote device. The User Passkey Entry command (AT*AGUPE) shall then be called with the 6 digit number that is displayed at the remote device.

Corresponds to BT 2.1 Security Mode 4 Level 3 in the Bluetooth specification.

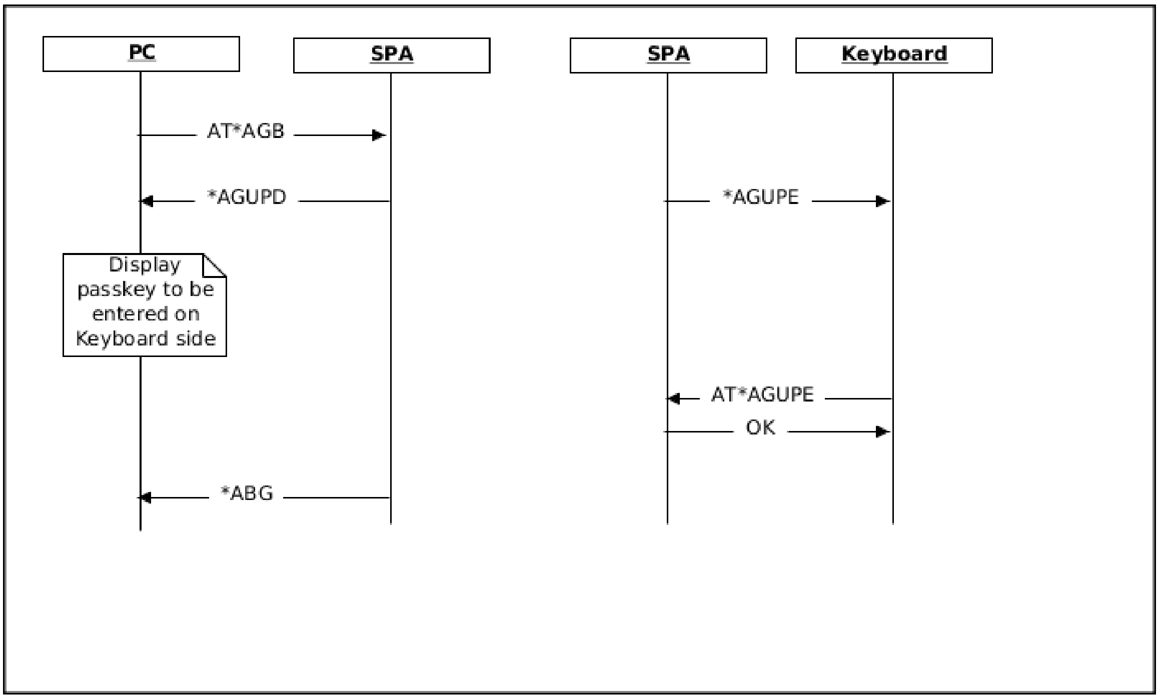
5 Sample Use Cases

5.1 PC - Keyboard

This use case is intended for one device having input capabilites only (e.g. keyboard) and the other device having output capabilites (e.g. PC or Cell Phone). Hence, the keyboard side is configured with security mode 7 (keyboard only) and the PC side is configured for security mode 5 (display only).

In the figure below the Bond command (AT*AGB) is used to initiate paring and the Bond event (*AGB) is sent to inform the result of the pairing attempt. The Bond command (AT*AGB) could be called from either side.

When the PC gets the User Passkey Display event (*AGUPD), it must display the 6 digit number received in the event. At the same time the keyboard side will get the User Passkey Entry event (*AGUPE) to inform the host to insert a 6 digit number using the User Passkey Entry command (AT*AGUPE). If the inserted number is the same as the displayed number, pairing is successful.



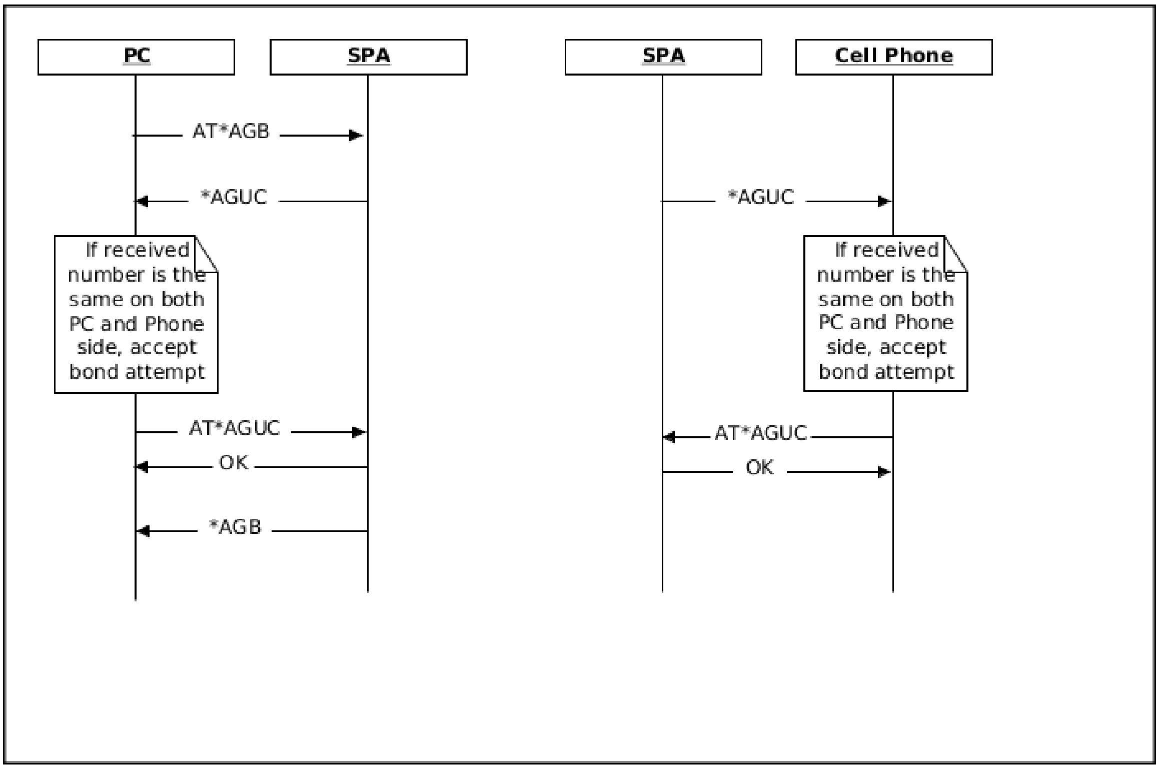
The above sample, describes a case where neither the PC nor the keyboard supports Bluetooth and both sides uses an SPA (Serial Port Adapter) for Bluetooth support. This case can, of course, be seperated into two use cases where either the PC or the keyboard has built-in Bluetooth without the need of a SPA.

5.2 PC - Cell Phone

This use case is intended where both the local and remote device having input capabilites as well as output capabilites (e.g. PC or Cell Phone). Hence, both sides are configured with security mode 6 (Display Yes/No).

In the figure below the Bond command (AT*AGB) is used to initiate paring and the Bond event (*AGB) is sent to inform the result of the pairing attempt. The Bond command (AT*AGB) could be called from either side.

When the PC and Cell Phone gets the User Confirmation event (*AGUC), it must display the 6 digit number and allow for the user to accept/reject pairing. The user input is then sent to the Serial Port Adapter using the User Confirmation command (AT*AGUC). If the user on both sides accepted pairing, it is successful.


PC
SPA
SPA
Cell Phone
AT*AGB
*AGUC
*AGUC
If received number is the same on both PC and Phone side, accept bond attempt
If received number is the same on both PC and Phone side, accept bond attempt
AT*AGUC
OK
AT*AGUC
OK
*AGB

5.3 Cell Phone - Headset

If at least one side does not have any input and output capabilities (e.g. headset) and BT 2.1+EDR security must still be used, the Just Works security mode must be selected (security mode 4).

The Serial Port Adapter disables pairability when this security mode is selected and it must temporarily be enabled while pairing is in progress.

AT Mode

1. Enable Pairable using the Pairable Mode command (AT*AGPM)
2. Initiate pairing by connecting or bonding (AT*AGB)
3. Disable Pariable using the Pairable Mode command (AT*AGPM)

Data Mode

1. Enable Pairable for 60 seconds by pressing the "External Connect" button for at least 5 seconds. The LED will blink when the 5 seconds has elapsed and continously during the time the module is pairable.
2. Initiate pairing by connecting.
3. After 60 seconds pairable will be disabled automatically.

Note that if a Serial Port Adapter is used on both sides, pairing must be enabled on both sides as well, using the "External Connect" button.

5.4 connectBlue Specific

There are two security modes that are specific for the connectBlue BT 2.1+EDR Serial Port Adapters.

- Bluetooth 2.0+EDR Security (Security mode 2): This mode is included for backward compatibility and it enforces BT2.0+EDR security.
- Fixed Pin (Security mode 3): Allows for a fixed pin code between two connectBlue BT 2.1+EDR modules.

5.4.1 Bluetooth 2.0+EDR Security

If a connectBlue BT 2.1+EDR Serial Port Adapter is configured for security mode 2, it uses only the BT 2.0+EDR security mechanisms and not the Simple Pairing mechanism introduced in BT2.1+EDR. This means it will use the fixed pin code set by the AT*AGFP command.

Please note that this is not allowed between two BT 2.1+EDR devices (according to Bluetooth specfication) and should only be used as a last resort for backward compatibility or interoperability problems (until solved).

5.4.2 Fixed Pin

Simple pairing does not support fixed pin codes in the same way as BT 2.0+EDR does.

Therefore, there is a connectBlue specific security mode 3 (Fixed Pin) which allows for fixed passkeys (6 digit number) to be used. Basically, the Serial Port Adapter on both sides takes the role of a keyboard as described in the PC-Keyboard use case. Instead of the user having to enter the passkey, it is read from memory set by the AT*AGFP2 command.

If a number of connectBlue Bluetooth 2.0 and Bluetooth 2.1 moduels are mixed, with security enabled, the recommended configuration is:

- Bluetooth 2.0 modules: Security Mode 2, Bluetooth 2.0+EDR Security using a fixed pin set by AT*AGFP.
- Bluetooth 2.1 modules: Security Mode 3, Fixed Pin using a passkey set by AT*AGFP2.

This means, pairing where at least one module is Bluetooth 2.0 uses the Bluetooth 2.0+EDR security algorithm which means the pin code set by AT*AGFP is used. Pairing between two Bluetooth 2.1 modules uses the Bluetooth 2.1 security algorithm which means the passkey set by AT*AGFP2 is used. Of course the Bluetooth 2.0 fixed pin must be the same between all modules, both Bluetooth 2.0 and 2.1.Hence, when connectBlue Bluetooth 2.1 modules are introduced to replace and work with existing connectBlue 2.0 modules, the Bluetooth 2.1 moduels should be configured with security mode 3 (Fixed Pin). The Bluetooth 2.0 pin code must be selected according to the existing Bluetooth 2.0 module and the Bluetooth 2.1 passkey should be selected for the case where two Bluetooth 2.1 modules are connected.

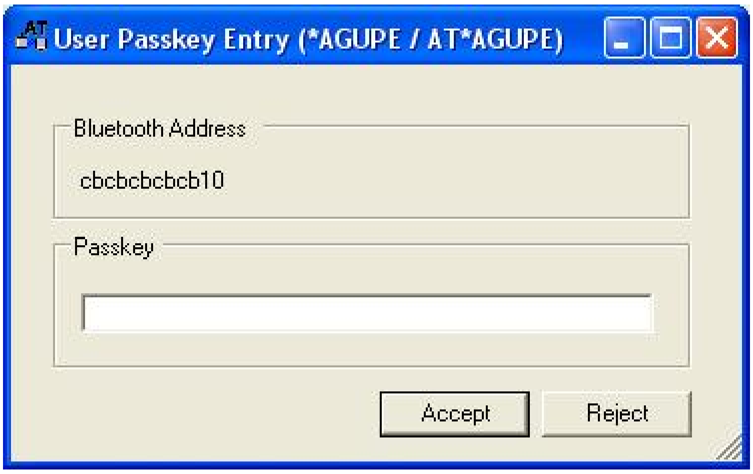
6 Bluetooth Serial Port Adapter Toolbox

The Bluetooth Serial Port Adapter Toolbox version 3.7 or later implements support to set the security mode, fixed pin code (BT 2.0+EDR) and passkey (BT 2.1+EDR) and initiate bonding. Furthermore, if any of the security modes requiring the module to be in AT mode is used (Display Only, Display Yes/No, Keyboard Only), the Toolbox provides some additional support.

Please note that the security tab of the Toolbox must be active for the pop-up windows to be activated!

Keyboard Only

The user may enter the 6 digit number in a pop-up window.



User Passkey Entry (*AGUPE / AT*AGUPE)

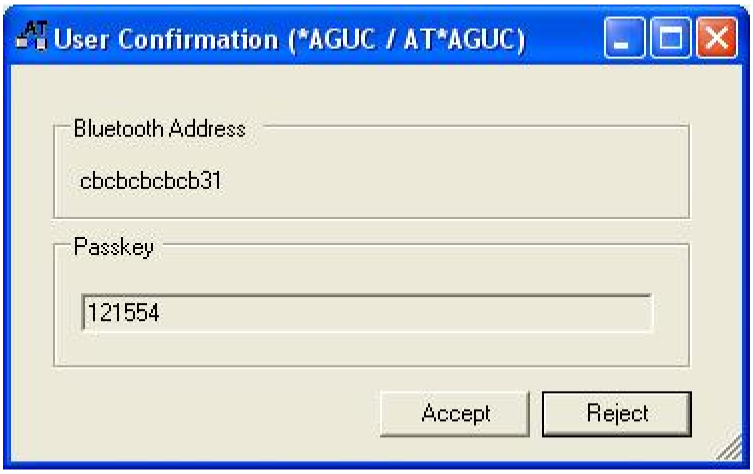
Bluetooth Address

cbcbcbcbcb10

Passkey

Display Yes/No

A pop-up window displays a 6 digit number and the user may accept or reject the pairing attempt.



User Confirmation (*AGUC / AT*AGUC)

Bluetooth Address

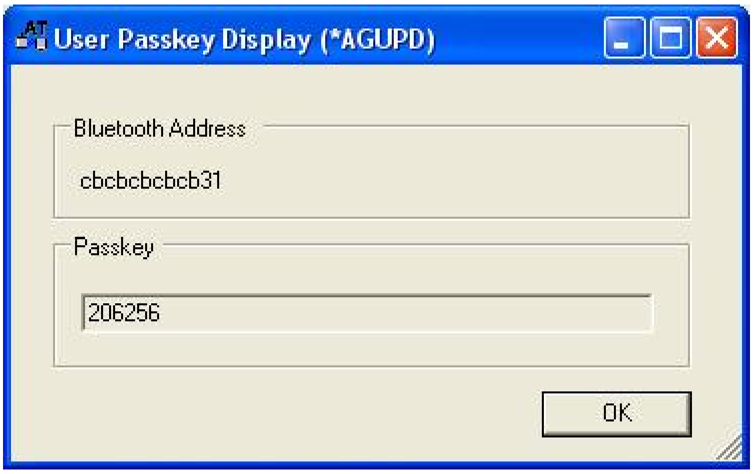
cbcbcbcbcb31

Passkey

121554

Display Only

A pop-up window displays a 6 digit number which may be read or copied.



User Passkey Display (*AGUPD)

Bluetooth Address

cbcbcbcbcb31

Passkey

206256