

u-connectXpress

Bluetooth security

Application note

Abstract

This application note describes the features and supported security modes in u-blox short range stand-alone modules.

Document information

Title	u-connectXpress	
Subtitle	Bluetooth security	
Document type	Application note	
Document number	UBX-16022676	
Revision and date	R08	11-Aug-2023
Disclosure restriction	C1-Public	

This document applies to the following products:

Product name	u-connectXpress software version
ANNA-B112	All
ANNA-B412	All
NINA-B111	4.0.0 or later
NINA-B112	4.0.0 or later
NINA-B221	All
NINA-B222	All
NINA-B311	All
NINA-B312	All
NINA-B316	All
NINA-B410	All
NINA-B416	All
NINA-W151	All
NINA-W152	All
NINA-W156	3.1.0 or later
ODIN-W260	5.0.0 or later
ODIN-W262	5.0.0 or later
ODIN-W263	5.0.0 or later

u-blox or third parties may hold intellectual property rights in the products, names, logos, and designs included in this document. Copying, reproduction, or modification of this document or any part thereof is only permitted with the express written permission of u-blox. Disclosure to third parties is permitted for clearly public documents only.

The information contained herein is provided "as is" and u-blox assumes no liability for its use. No warranty, either express or implied, is given, including but not limited to, with respect to the accuracy, correctness, reliability, and fitness for a particular purpose of the information. This document may be revised by u-blox at any time without notice. For the most recent documents, visit www.u-blox.com.

Copyright © u-blox AG.


Contents

Document information	2
Contents	3
1 Introduction	4
1.1 Documentation.....	4
2 Introduction to secure simple pairing	5
3 Bluetooth LE secure connections	6
3.1 Introduction.....	6
3.2 Payment card industry security requirements	6
4 Security modes	7
4.1 Introduction.....	7
4.2 Bluetooth LE security modes and levels	7
4.2.1 Bluetooth LE security mode 1	7
4.2.2 Bluetooth LE security mode 2	7
4.3 Bluetooth BR/EDR security modes and levels.....	7
4.4 Security mode 1: Security Disabled Auto Accept.....	8
4.5 Security mode 2: Just Works	8
4.6 Security mode 3: Display Only	9
4.7 Security mode 4: Display Yes/No	9
4.8 Security mode 5: Keyboard Only	9
4.9 Security mode 6: Out Of Band	9
4.10 Fixed pin Bluetooth 2.0	10
5 Supported use cases	11
6 Sample use cases	12
6.1 Cellphone and headset pairing	12
6.2 PC and keyboard pairing	12
6.3 PC and cellphone pairing	13
7 Security in s-center	14
Appendix	15
A Known vulnerabilities	15
A.1 CVE-2019-9506, “KNOB” attack	15
A.2 BLESAs vulnerability	15
B Glossary	16
Related documents	17
Revision history	17
Contact	17

1 Introduction

This document describes:

- Secure Simple Pairing
- u-connect security solutions for Bluetooth BR/EDR and Bluetooth Low Energy (LE)
- Bluetooth LE secure connections
- Some common user scenarios
- Bluetooth security in u-blox s-center tool

 The terms pairing and bonding are both used in this document. “Bonding” means that the generated link key is stored by the Bluetooth devices, while “pairing” is only valid for the current connection. u-connectXpress only supports bonding.

1.1 Documentation

- s-center user guide [\[2\]](#): describes how to use s-center for configuring u-blox short range modules
- u-connectXpress user guide [\[9\]](#): describes the use cases supported by each product
- u-connect AT commands manual [\[1\]](#) describes the standard and proprietary AT commands for u-blox modules that support Bluetooth Low Energy, Bluetooth BR/EDR, and Wi-Fi connectivity with u-connectXpress software.
- Product summary – describes the security features supported by:
 - ODIN-W2 [\[3\]](#)
 - NINA-W15 [\[12\]](#)
 - NINA-B1 [\[4\]](#)
 - NINA-B2 [\[5\]](#)
 - NINA-B30 [\[6\]](#)
 - NINA-B31 [\[7\]](#)
 - ANNA-B112 [\[8\]](#)
 - ANNA-B412 [\[16\]](#)

2 Introduction to secure simple pairing

Secure Simple Pairing was introduced in Bluetooth v4.0.

The main goals for Secure Simple Pairing are:

- To simplify the pairing process from the end user's point of view
- To maintain or improve the security in Bluetooth

Secure Simple Pairing aims to improve protection against *passive eavesdropping*, using 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 the strongest security requirements).

Secure Simple Pairing also protects the user from “man-in-the-middle attacks” (active eavesdropping) with a goal of offering a 1 in 1,000,000 risk that any man-in-the-middle could mount a successful attack. This probability is considered low enough to meet the FIPS 140-29 requirements for authentication.

Consider the following three main use cases for Secure Simple Pairing:

1. **Just Works:** Intended for cellphone-to-headset (or similar) pairing scenarios, where one device has neither display nor keyboard. In these instances, the Bluetooth device only allows pairing during the time that the phone and headset are performing the pairing procedure. During this time, all pairing attempts are automatically accepted.
2. **Numeric Comparison:** Intended for cellphone-to-PC (or similar) pairing scenarios, where the two connecting devices both include some interactive mechanism (display, keyboard, switch, or similar) that allows the respective users to confirm either “yes” or “no” to a connection request. To make the connection, a common six-digit confirmation number is displayed for the respective users of both devices. Pairing between the two devices is only completed after the users have confirmed that the numbers match. The pairing is aborted if the numbers do not match.
3. **Passkey Entry:** Intended for keyboard-to-PC (or similar) pairing scenarios, where only one of the connecting devices has input (but no output) capability and the other has output (but no input) capability. The device with output capability displays a six-digit confirmation number that must be confirmed by the user of the device with input capability. The pairing of the two devices is only made after the user has confirmed that the number is correct.

The pairing arrangements for connecting devices that support different Bluetooth versions differ:

- Bluetooth 2.1 (or newer) devices pairing with Bluetooth 2.0 (or earlier) devices must connect in accordance with Bluetooth 2.0 (or earlier) security protocols. This means that Secure Simple Pairing cannot be used.
- Bluetooth 2.1 (or newer) devices connecting with similarly versioned devices must connect in accordance with Secure Simple Pairing protocols and cannot use Bluetooth 2.0 (or earlier) security mechanisms.

3 Bluetooth LE secure connections

3.1 Introduction

Bluetooth Low Energy (LE) Secure Connections is an improved pairing mechanism introduced in Bluetooth v4.2. It uses Elliptic Curve Diffie Hellman (ECDH) encryption for key generation and provides stronger protection against Man-In-The-Middle (MITM) attacks. This encryption method uses public-private key pairs for exchanging the Long Term Key between paired devices.

Low energy secure connections can only be used if both devices support this feature. If only one device supports low energy secure connections, the devices must connect using legacy low energy pairing instead.

In Secure Connections Only Mode, the device rejects both new outgoing and incoming service level connections when the other device does not support low energy secure connections.

Secure connections can be enabled by the following AT command:

```
AT+UBTST=1
```

A device is set in the Secure Connections Only Mode by setting it in FIPS only mode:

```
AT+UBTST=2
```

Low energy secure connections support the following four association models:

- Just works
- Numeric Comparison (only in Low Energy Secure Connections)
- Passkey Entry
- Out of Band (OOB) – not supported by u-connectXpress

In order to use the Numeric comparison association model, the IO capabilities of the involved devices must be matched as specified in [Table 1](#).

Bluetooth Low Energy	Initiator					
	No sec (1)	Just Works (2)	Display Only (3)	Display Y/N (4)	Keyboard Only(5)	Out Of band (6)
Responder	No sec (1)					
	Just Works (2)					
	Display Only (3)					
	Display Y/N (4)			Numeric comparison		
	Keyboard Only (5)					
	Out Of Band (6)					

Table 1: IO Capabilities for numeric comparison

3.2 Payment card industry security requirements

In order to set up a device to be compatible with Payment Card Industry (PCI) security requirements, it is essential to fulfill the following requirements:

- Low Energy Security Mode 1 Level 4 only
- Just Works association model cannot be used.

This means that a u-blox module must be set in the FIPS-only mode (`AT+UBTST=2`) and it is not possible to use the Just Works security mode. See the u-connectXpress user guide [\[9\]](#) and PCI Security Standards Council [\[11\]](#) for more information.

4 Security modes

4.1 Introduction

This chapter provides an overview of the different security modes in u-blox u-connect products, with mapping to the relevant Bluetooth standard. For information describing the general security features included in the Bluetooth standard that are supported by u-connectXpress modules, see [Bluetooth low energy security modes and levels](#) and [Bluetooth BR/EDR security modes and levels](#). Additional security modes supported by these modules are described later in this chapter.

 Note that the Security Modes in u-blox u-connect products do not directly correspond to the Security modes or the Security levels of the Bluetooth specification.

4.2 Bluetooth LE security modes and levels

The security modes and levels described here are in accordance with the Bluetooth standard [10], volume 3, part C, chapter 10.2.

Bluetooth low energy has two Security Modes with different levels.

4.2.1 Bluetooth LE security mode 1

Security mode 1 uses data encryption but no signing of data. It has the following security levels:

1. No security (no authentication and no encryption)
2. Unauthenticated pairing with encryption
3. Authenticated pairing with encryption
4. Authenticated Bluetooth LE Secure Connections pairing with encryption using a 128-bit strength encryption key. See also [Low energy secure connections](#).

All of these security levels are applicable for u-blox u-connect products. Please see the product specification and u-connect AT commands manual [1] for details on each product.

4.2.2 Bluetooth LE security mode 2

Security mode 2 uses data signing. It has two security levels:

1. Unauthenticated pairing with data signing
2. Authenticated pairing with data signing

Bluetooth LE security mode 2 is not used in u-blox products.

4.3 Bluetooth BR/EDR security modes and levels

Different security modes are available for all kinds of use cases involving the pairing procedure. Each mode is specified for Bluetooth v2.0 (or earlier) and v2.1 (or newer) security. This is to comply with the version in the remote device. If the remote device supports only Bluetooth 2.0 (or earlier), a Bluetooth 2.1 (or newer) device must conform to the Bluetooth 2.0 security algorithms.

All security modes (except security modes 1 and 2) for Bluetooth 2.0 devices use encryption. The security modes 1 and 2 (Security Disabled) for Bluetooth 2.1 still use encryption. The encryption algorithm is a 128-bit cipher called E0.

For secure connections, 128-bit equivalent strength for link and encryption keys are required using FIPS approved algorithms (E0 not allowed, SAFER+ not allowed, and P-192 not allowed).

The security modes 1 and 2 are implemented to keep the behavior similar to the previous versions of u-blox Bluetooth products.


The Display Only, Display Yes/No, and Keyboard Only modes (modes 3, 4 and 5) can only be used in the AT or Extended Data mode since it requires user interaction (AT commands and events).

Security level required for service	Link key type required for remote devices	Link key type required for pre-v2.1 remote device	Comments
Level 4 • MITM protection required • Encryption required • User interaction acceptable	Authenticated (P-256 based Secure Simple Pairing and Secure Authentication)	NA	Highest Security Only possible when both devices support Secure Connections
Level 3 • MITM protection required • Encryption required • User interaction acceptable	Authenticated	Combination (16-digit PIN recommended)	High Security
Level 2 • MITM protection not necessary • Encryption desired	Unauthenticated	Combination	Medium Security
Level 1 • MITM protection not necessary • Encryption not necessary • Minimal user interaction desired	Unauthenticated	None	Low Security
Level 0 • MITM protection not necessary • Encryption not necessary • No user interaction desired	None	None	Permitted only for SDP and service data sent via either L2CAP fixed signaling channels or the L2CAP connectionless channel to PSMs that correspond to the service class UUIDs, which are allowed to utilize Level 0

Table 2: Security level mapping to link key requirements, according to the Bluetooth standard

4.4 Security mode 1: Security Disabled Auto Accept

For security modes 1 and 2, pairing is auto-accepted and the link keys are generated without using a passkey. The pairing devices must allow pairing.


 This security mode corresponds to Bluetooth v2.1 Security Mode 4 Level 1 in the Bluetooth specification, which is also shown in [Table 2](#).

4.5 Security mode 2: Just Works

Security mode 2 is the configuration to use when no user interaction can be performed and all possible pairing comparisons should be done.

The I/O capability is set to “no input/no output” and no authentication is required. The Bluetooth device replies to all pairing requests. If the remote device has a higher authentication requirement, the remote device decides whether this is an acceptable bond.


Pairing is initially disabled and needs to be explicitly enabled using switch **SW2**. You set the Just Works configuration with the AT command `AT+UBTPM` or by pressing the “external connect” button for 5 seconds. Pressing the button enables the pairing for 60 seconds during which time signal BLUE (typically connected to an LED) toggles/flashes.

 This security mode corresponds to Bluetooth v2.1 Security Mode 4, Level 2 in the Bluetooth specification, which is also shown in [Table 2](#).

4.6 Security mode 3: Display Only

Security mode 3 suits devices that support output capabilities. It is intended to be used together with remote devices that support input capabilities. MITM protection is required to get a successful bond.


When pairing is initiated, the User Passkey Display event (+UUBTUPD) 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.

 This security mode corresponds to Bluetooth 2.1 Security Mode 4 Level 3 in the Bluetooth specification, which is also shown in [Table 2](#).

4.7 Security mode 4: Display Yes/No

Security mode 4 suits devices with both output and input capabilities. It is intended to be used with remote devices supporting both output and input capabilities. MITM protection is required to get a successful bond.


When pairing is initiated, the User Confirmation event (+UUBTUC) is 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+UBTUC).

 This security mode corresponds to Bluetooth v2.1 Security Mode 4 Level 3 in the Bluetooth specification, which is also shown in [Table 2](#).

4.8 Security mode 5: Keyboard Only

Security mode 5 suits devices with input capabilities. It is intended to be used with remote devices that support output capabilities. MITM protection is required to get a successful bond.

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

 This security mode corresponds to Bluetooth 2.1 Security Mode 4 Level 3 in the Bluetooth specification, which is also shown in [Table 2](#).

4.9 Security mode 6: Out Of Band

Security mode 6 is suitable if both devices can transmit and/or receive data over an out-of-band channel. It is indicated by a one field in the Pairing Request/Response message (OOB Data Flag) if OOB data is available. Both devices must set the OOB flag in order to use OOB pairing.

Before pairing is initiated, a temporary key is initiated on one side, which must serve as an input on the other side.

```
AT+UBTOTK=0
AT+UBTOTK?
+UBTOTK:9A4F4D0377ED71B023BD82C16499609A
```

This key needs to be set on the other side before pairing can be performed.


```
AT+UBTOTK=1,9A4F4D0377ED71B023BD82C16499609A
```

Pairing is possible now using the Bond (AT+UBTB) command. Use NFC as the typical OOB medium.

4.10 Fixed pin Bluetooth 2.0

For backwards compatibility a legacy fixed pin scheme for Bluetooth 2.0 devices is supported.

Instead of having the user enter the pin code during bonding, a fixed passkey stored in flash is used for bonding Bluetooth 2.0 devices.

 `AT+UBTSM` with the Bluetooth 2.0 fixed pin option must be enabled.

The pin code in Bluetooth v2.0 consist of 1 to 16 alphanumerical digits. Pairing is then automatic (with no user interaction required) using the stored passkey (`AT+UBTSM`) and a link key is generated.

5 Supported use cases

Man in the middle protection is required for the security modes 3 (Display Only), 4 (Display Yes/No), and 5 (Keyboard Only). This means it is not possible to pair with devices having security modes 1 (auto accept) or 2 (Just Works) without authentication, which is in accordance with the Bluetooth Core Specification [10]. Table 3 and Table 4 show the combinations where pairing is possible.

When the device is configured with a required MITM protection, the pairing will only be successful if the remote side also requires authentication.

Table 3 shows the association models for Bluetooth BR/EDR. Security modes shown as “MITM” are not supported due to the risk of “Man in the Middle” attacks.

	Bluetooth BR/EDR	Initiator				
		No sec (1)	Just Works (2)	Display Only (3)	Display Y/N (4)	Keyboard Only (5)
Responder	No sec (1)	Yes ¹	Yes ¹	MITM	MITM	MITM
	Just Works (2)	Yes ¹	Yes ¹	MITM	MITM	MITM
	Display Only (3)	MITM	MITM	MITM	MITM	Yes ³
	Display Y/N (4)	MITM	MITM	MITM	Yes ²	Yes ³
	Keyboard Only (5)	MITM	MITM	Yes ⁴	Yes ⁴	Yes ⁵

Table 3: Bluetooth BR/EDR association models

Table 4 shows the association models for Bluetooth Low Energy. Security modes shown as “MITM” are not supported due to the risk of “Man in the Middle” attacks.

	Bluetooth Low Energy	Initiator					
		No sec (1)	Just Works (2)	Display Only (3)	Display Y/N (4)	Keyboard Only (5)	Out Of Band (6)
Responder	No sec (1)	Yes ¹	Yes ¹	MITM	MITM	MITM	MITM
	Just Works (2)	Yes ¹	Yes ¹	MITM	MITM	MITM	MITM
	Display Only (3)	MITM	MITM	MITM	MITM	Yes ³	MITM
	Display Y/N (4)	MITM	MITM	MITM	(MITM) ⁸	Yes ³	MITM
	Keyboard Only (5)	MITM	MITM	Yes ⁴	Yes ⁴	Yes ⁵	Yes ⁷
	Out Of Band (6)	MITM	MITM	MITM	MITM	Yes ⁷	Yes ⁶

Table 4: Bluetooth Low Energy association models

Pairing is possible in the following scenarios:

¹ when both devices have pairing enabled (AT+UBTPM).

² when receiving +UUBTUC event on both initiator and responder and both sides accept the incoming passkey by sending AT+UBTUC.

³ when the initiator receives +UUBTUPE event and accepts it by sending AT+UBTUPE with passkey from the +UUBTUPD event on responder side.

⁴ when the responder receives +UUBTUPE event and accepts it by sending AT+UBTUPE with passkey from the +UUBTUPD event on initiator side.

⁵ when both initiator and responder receive a +UUBTUPE event and both devices send equal random passkey in AT+UBTUPE command.

⁶ when OOB temporary keys match

⁷ when there is a fallback to Just Works association model due to mismatching capabilities; see Bluetooth Core Specification [10], Vol3, Part H, Table 2.7 and 2.8 (v. 5.1). This fallback is not valid in Low Energy Secure Connections mode.

⁸ when Low Energy Secure Connections is enabled. This combination will result in the Numeric Comparison association model, as described in [Bluetooth LE Low energy secure connections](#).

6 Sample use cases

6.1 Cellphone and headset pairing

Just Works is the security mode recommended for having an easy and sufficient security level. When at least one side does not have any input and output capabilities (for example, in the cellphone paired with headset scenario) and Bluetooth 2.1+EDR security must be used, the Just Works security mode (security mode 2) is the only applicable security level.


In this security mode, the u-blox Bluetooth device is invisible for pairing until pairing is enabled.

AT mode

1. Enable pairing using the Pairing Mode command (`AT+UBTPM`)
2. Initiate pairing by connecting or bonding (`AT+UBTB`)
3. Disable pairing using the Pairing Mode command (`AT+UBTPM`)

Data mode

1. Enable pairing 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 continuously during the time when the module has pairing enabled.
2. Initiate pairing by connecting.
3. After 60 seconds, pairing will be disabled automatically.

 Pairing must be enabled on both the initiator and the responder sides.

6.2 PC and keyboard pairing

The "PC paired with keyboard" use case is intended when only one device (like the keyboard) has input capabilities and the other device (like the PC or cellphone) has output capabilities. Hence, the keyboard side is configured with the security mode 5 (keyboard only) and the PC side is configured for the security mode 3 (display only).

Figure 1 shows the pairing sequence between the PC and keyboard, where Bond command (`AT+UBTB`) is used to initiate pairing and the Bond event (`+UUBTB`) is sent to inform the result of the pairing attempt. The Bond command (`AT+UBTB`) can be called from either side.

When the PC gets the User Passkey Display event (`+UUBTUPD`), it must display the six-digit number received in the event. Simultaneously, the keyboard side will get the User Passkey Entry event (`+UUBTUPE`) to inform the host to insert a six-digit number using the User Passkey Entry command (`AT+UBTUPE`). If the inserted number is the same as the displayed number, pairing is successful.

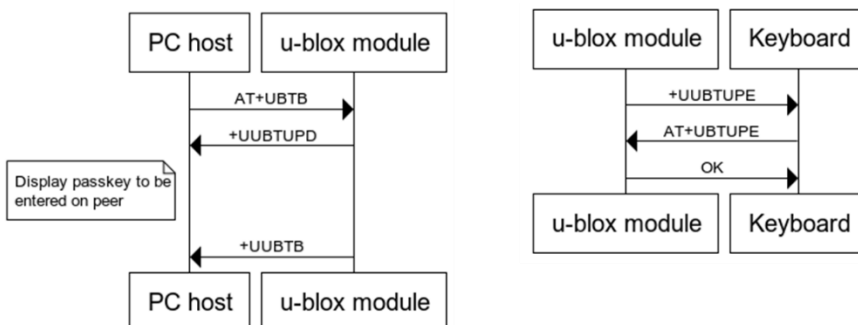


Figure 1: Pairing command sequence between PC and keyboard

The above sample describes a case where neither the PC nor the keyboard supports Bluetooth and both sides use a u-blox Bluetooth module for Bluetooth support. This case can be separated into two use cases where either the PC or the keyboard has built-in Bluetooth without the need of a Bluetooth device.

6.3 PC and cellphone pairing

The PC paired with cellphone use case is intended where both the local and remote device have input capabilities as well as output capabilities (for example, PC or Cellphone). Hence, both sides are configured with the security mode 4 (Display Yes/No).

In the figure below, the Bond command (`AT+UBTB`) is used to initiate pairing and the Bond event (`+UBTB`) is sent to inform the result of the pairing attempt. The Bond command (`AT+UBTB`) could be called from either side. Both devices use a u-blox module each for connectivity.

For both the PC and Cellphone, when it gets the User Confirmation event (`+UUBTUC`), it must display the six-digit number and allow for the user to accept/reject pairing. The user input is then sent to the u-blox Bluetooth device using the User Confirmation command (`AT+UBTUC`). When the users on both sides accept the pairing, it is successful.

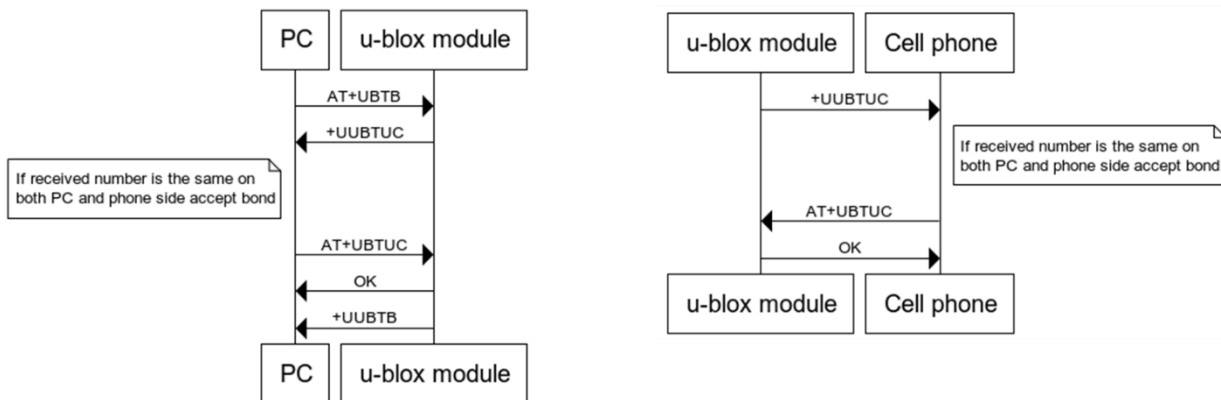


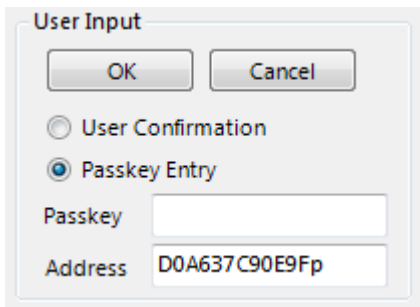
Figure 2: Pairing command sequence between PC and cell phone

7 Security in s-center

s-center implements support to configure the security mode and initiate bonding. For the security modes Display Only, Display Yes/No, and Keyboard Only, s-center provides some additional support.

Keyboard Only

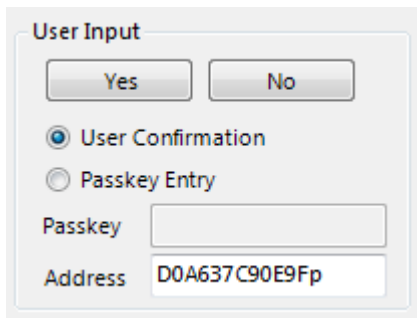
After receiving the keyboard-only event `+UUBTUPE`, the user enters the remote Bluetooth address and the received six-digit passkey number in the window and clicks OK to send the `AT+UBTUPE` command.



The dialog box is titled "User Input". It contains two buttons at the top: "OK" and "Cancel". Below the buttons are two radio button options: "User Confirmation" (unselected) and "Passkey Entry" (selected). Under "Passkey Entry", there are two input fields: "Passkey" (empty) and "Address" (containing the text "D0A637C90E9Fp").

Display Yes/No

After receiving the keyboard-only event `+UUBTUPE`, the user must verify that the passkey is correct. The user enters the remote Bluetooth address and clicks OK to send the `AT+UBTUC` command. The user may accept or reject the pairing attempt.



The dialog box is titled "User Input". It contains two buttons at the top: "Yes" and "No". Below the buttons are two radio button options: "User Confirmation" (selected) and "Passkey Entry" (unselected). Under "User Confirmation", there are two input fields: "Passkey" (empty) and "Address" (containing the text "D0A637C90E9Fp").

Display Only

A six-digit number, which may be read or copied is received in the `+UUBTUPD` event, and should be used on the remote device.

Example: `+UUBTUPD:78A5042F673Dp,209471`

Appendix

A Known vulnerabilities

In the following sub chapters the status of some known issues are listed. See reference [14] for an online list of issues and information on how to report security issues.

A.1 CVE-2019-9506, “KNOB” attack

A Key Negotiation of Bluetooth (KNOB) attack aims to manipulate entropy negotiation. The vulnerability and mitigation for each u-blox module against this kind of attack are shown in Table 5.

Module	Vulnerability	Mitigated
ANNA-B1	No	N/A
NINA-B1	No	N/A
NINA-B2	v1.0.x	v2.1.0 onwards
NINA-B3	No	N/A
NINA-W15	v1.0.x	v2.1.0 onwards
ODIN-W2	v1.0.x – v7.1.x (partly)	ODIN-W2 up to v7.1.x requires a minimum key length of 5 bytes.

Table 5: Module vulnerability and mitigation against KNOB attack

A.2 BLESA vulnerability

The BLESA (Bluetooth Low Energy Spoofing Attack) is an attack that uses some weaknesses in the Bluetooth low energy protocol for reconnecting to previously paired devices. This can, in some cases, allow an attacker to feed a Bluetooth low energy device spoofed values by impersonating a previously paired device.

To ensure that the pairing exchange and subsequent encoding between peer devices is properly maintained, u-connectXpress supports a parameter tag that forces bonding when the security mode is enabled. With this parameter enabled, re-connecting devices are forced to complete the pairing exchange again before the bonding process is initiated. To set this configuration use the command:

```
AT+UBTLECFG=30,1
```

For more information about this and other parameters using this command, see the u-connectXpress AT commands manual [1].


B Glossary

Abbreviation	Definition
BR/EDR	Basic Rate/Enhanced Data Rate
EVK	Evaluation Kit
MITM	Man in the Middle
N/A	Not Applicable
NFC	Near Field Communication
OOB	Out of Band
PCI	Payment Card Industry

Table 6: Explanation of the abbreviations and terms used

Related documents

- [1] u-connectXpress AT commands manual, [UBX-14044127](#)
- [2] s-center user guide, [UBX-16012261](#)
- [3] ODIN-W2 product summary, [UBX-15004332](#)
- [4] NINA-B1 product summary, [UBX-15018552](#)
- [5] NINA-B2 product summary [UBX-17062096](#)
- [6] NINA-B30 product summary, [UBX-17052930](#)
- [7] NINA-B31 product summary, [UBX-17052931](#)
- [8] ANNA-B112 product summary, [UBX-18006008](#)
- [9] u-connectXpress user guide, [UBX-16024251](#)
- [10] Bluetooth Core Specification, <https://www.bluetooth.com/specifications>
- [11] Payment Card Industry Security Standards Council, <https://www.pcisecuritystandards.org/>
- [12] NINA-W15 product summary, [UBX-18052290](#)
- [13] CVE-2019-9506, <https://www.cvedetails.com/cve/CVE-2019-9506/>
- [14] <https://www.u-blox.com/en/report-security-issues>
- [15] NINA-B41 product summary, [UBX-20045962](#)
- [16] ANNA-B412 product summary, [UBX-21025292](#)

 For product change notifications and regular updates of u-blox documentation, register on our website, www.u-blox.com.

Revision history

Revision	Date	Name	Comments
R01	9-Apr-2019	cmag, mape	Initial release.
R02	29-May-2019	mape	Added information about PCI and Numeric Comparison association model (chapter 3).
R03	30-Oct-2019	flun	Added NINA-W15 and NINA-B316 to the list of applicable products (page 2). Added information about CVE-2019-9506 (Appendix A).
R04	6-July-2020	mape	Minor corrections and clarifications throughout document.
R05	3-Dec-2020	mape	OOB association model not supported by LESC. Minor corrections.
R06	4-Feb-2021	flun	Included support for NINA-B41, NINA-W56 and ODIN-W263. Renamed document.
R07	12-Dec-2022	mape	Extended document scope to include ANNA-B412. Clarified pairing and bonding. Updated Fixed pin Bluetooth 2.0 .
R08	11-Aug-2023	mape	Added the appendix Table 5 : Module vulnerability and mitigation against KNOB attack BLESAs vulnerability.

Contact

u-blox AG

Address: Zürcherstrasse 68
8800 Thalwil
Switzerland

For further support and contact information, visit us at www.u-blox.com/support.