S

# u-connectXpress Bluetooth Security

## Security in u-blox short range modules

Application Note


### Abstract

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



**www.u-blox.com**
UBX-16022676 - R01

# Document Information

| | | |
|---|---|---|
| **Title** | **u-connectXpress Bluetooth Security** | |
| **Subtitle** | Security in u-blox short range modules | |
| **Document type** | Application Note | |
| **Document number** | UBX-16022676 | |
| **Revision and date** | R01 | 9-Apr-2019 |
| **Disclosure Restriction** | | |

This document applies to the following products:

| Product name | Type number | Firmware version | PCN reference |
|---|---|---|---|
| ODIN-W2 | ODIN-W26x | 5.0.0 or later | N/A |
| NINA-B1 | NINA-B1xx | 4.0.0 or later | N/A |
| NINA-B2 | NINA-B2xx | 1.0.0 or later | N/A |
| NINA-B3 | NINA-B3xx | 1.0.0 or later | N/A |
| ANNA-B112 | ANNA-B112 | 1.0.0 or later | N/A |

# Contents

# 1 Introduction

This document describes:

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

To see which features are applicable for each product, refer to the Product Summary document for the product in question.

## 1.1 Documentation

- The s-center user guide [2] describes how to use s-center to configure the u-blox short range modules.
- The u-connect AT Commands Manual [1] contains a description of the supported AT commands.
- The product summary for each applicable product describes which security features are applicable for each product.
  - ODIN-W2 product summary [3]
  - NINA-B1 product summary [4]
  - NINA-B2 product summary [5]
  - NINA-B30 product summary [6]
  - NINA-B31 product summary [7]
  - ANNA-B112 product summary [8]

# 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 1000000 risk that a man-in-the-middle could mount a successful attack. This is a probability that 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 scenarios where at least one device does not have a display or keyboard, such as cellphone to headset pairing. The idea is to enable pairing only during the time that the phone and headset shall be paired. 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 cellphone to PC pairing. A six-digit number will be displayed on both sides, and if the same number is displayed, the pairing attempt is accepted by entering yes on both sides.
3. **Passkey Entry:** Intended for scenarios where one side only has input capabilities (no output) and the other side has output capabilities, such as keyboard to PC pairing. The device with output capabilities 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 (or newer) device tries to pair with a Bluetooth 2.0 (or earlier) device, the Bluetooth 2.1 (or newer) device must do pairing according to the Bluetooth 2.0 (or earlier) security (which means no Secure Simple Pairing will be used). However, two Bluetooth 2.1 (or newer) devices must apply to the requirements of Secure Simple Pairing and may not use the Bluetooth 2.0 (or earlier) security mechanisms.

# 3 Low energy secure connections

Low energy secure connection 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 by using public-private key pairs for exchanging the Long Term Key used for encrypting the communication.

Low energy secure connections can be used only if both devices support this feature. If only one device supports low energy secure connection, they can fall back to low energy legacy pairing.

A device may also be in a Secure Connections Only mode. In Secure Connections Only mode, the device will reject 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 for low energy secure connections, not implemented)
- Passkey Entry
- Out of Band (OOB)

# 4 Security modes

## 4.1 Introduction

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.

This chapter provides an overview of the different security modes in u-blox u-connect products, and a mapping to the Bluetooth standard. Sections 4.2 and 4.3 give an introduction to the security features of the Bluetooth standard while the sections that follow describe the security modes used in u-blox u-connect products.

## 4.2 Bluetooth low energy security modes and levels

The security modes and levels described here are according to the Bluetooth standard (reference [9]), volume 3, part C, chapter 10.2.

Bluetooth low energy has two Security Modes with different levels.

### 4.2.1 Low energy security mode 1

Low energy security mode 1 uses data encryption but no signing of data. It has the following security modes:

1. No security (No authentication and no encryption)
2. Unauthenticated pairing with encryption
3. Authenticated pairing with encryption
4. Authenticated Bluetooth low energy Secure Connections pairing with encryption using a 128-bit strength encryption key (see chapter 3 for more information).

All of these security levels are applicable for u-blox u-connect products.

### 4.2.2 Low energy security mode 2

Low energy security mode 2 uses data signing. It has two security modes:

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

Low energy security mode 2 is not used in u-blox products.

## 4.3 Bluetooth BR/EDR security modes and levels

Different security modes are available to support all kinds of use cases regarding 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).

☞ 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.

| 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<br>• MITM protection required<br>• Encryption required<br>• User interaction acceptable | Authenticated (P-256 based Secure Simple Pairing and Secure Authentication) | NA | Highest Security<br>Only possible when both devices support Secure Connections |
| Level 3<br>• MITM protection required<br>• Encryption required<br>• User interaction acceptable | Authenticated | Combination (16-digit PIN recommended) | High Security |
| Level 2<br>• MITM protection not necessary<br>• Encryption desired | Unauthenticated | Combination | Medium Security |
| Level 1<br>• MITM protection not necessary<br>• Encryption not necessary1<br>• Minimal user interaction desired | Unauthenticated | None | Low Security |
| Level 0<br>• MITM protection not necessary<br>• Encryption not necessary<br>• 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 1: 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 will be auto accepted and the link keys are generated without using a passkey; the pairing devices must allow pairing.

☞ This corresponds to Bluetooth v2.1 Security Mode 4 Level 1 in the Bluetooth specification, which is also shown in Table 1.

## 4.5 Security mode 2: Just Works

Just Works is the configuration to use when no user interaction can be done 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 will reply to all pairing requests and if the remote device has a higher authentication requirement, the remote device takes the decision whether this is an acceptable bond.

Pairing is initially disabled and needs to be explicitly enabled when using the Just Works method. This is done by AT+UBTPM or by using the “external connect” button for 5 seconds; the device will have pairing enabled for 60 seconds and the LED will blink during this period.

☞ This corresponds to Bluetooth v2.1 Security Mode 4 Level 2 in the Bluetooth specification, which is also shown in Table 1.

## 4.6 Security mode 3: Display Only

The 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 corresponds to Bluetooth 2.1 Security Mode 4 Level 3 in the Bluetooth specification, which is also shown in Table 1.

## 4.7 Security mode 4: Display Yes/No

The 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) 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+UBTUC).

☞ This corresponds to Bluetooth v2.1 Security Mode 4 Level 3 in the Bluetooth specification, which is also shown in Table 1.

## 4.8 Security mode 5: Keyboard Only

The 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 corresponds to Bluetooth 2.1 Security Mode 4 Level 3 in the Bluetooth specification, which is also shown in Table 1.

## 4.9 Security mode 6: Out Of Band

The 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

Two Bluetooth 2.1+EDR devices acting as Keyboard Only devices will work similarly to the Bluetooth 2.0 pairing using a fixed pin. Instead of having a user enter the six-digit numerical passkey, a fixed passkey stored in flash is used (AT+UBTSM with the Bluetooth 2.0 fixed pin option must be enabled).

The passkey consists of 1 to 6 numerical digits.

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

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

☞ This corresponds to Bluetooth v2.1 Security Mode 4 Level 3 in the Bluetooth specification, which is also shown in Table 1Table 1: Security Level mapping to link key requirements.

☞ In Bluetooth v2.0, it is called a pin code, while in Bluetooth 2.1, it is called a passkey.

# 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 ([9]).

Table 2 and Table 3 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.

☞ In the two tables below, “MITM” means not supported due to Man in the Middle attack risk.

| 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 2: Bluetooth BR/EDR association models**

| 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 | 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 3: Bluetooth low energy association models**

[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 [9], Vol3, Part H, Table 2.7 and 2.8 (v. 5.1).

# 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.

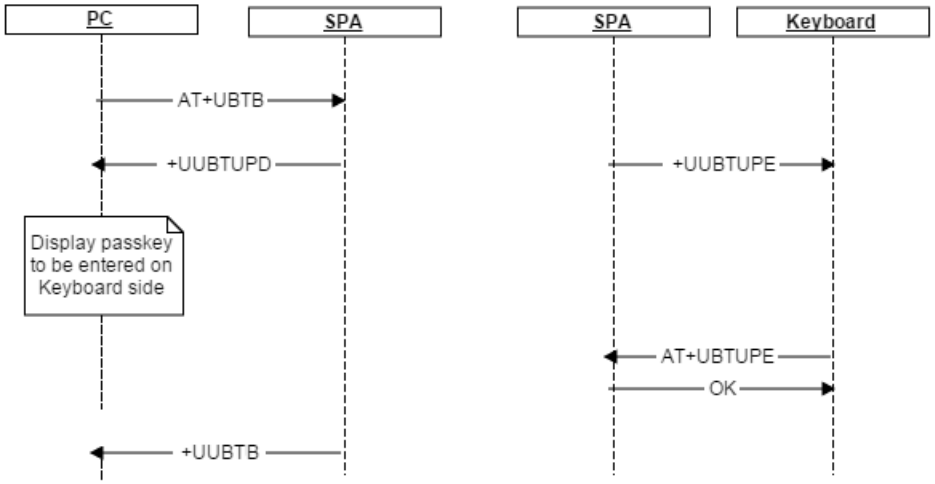
☞ Pairing must be enabled on both the initiator and the responder sides.

## 6.2 PC and keyboard pairing

The PC paired with keyboard use case is intended when only one device has input capabilities (for example, the keyboard) and the other device has output capabilities (for example, the PC or cellphone). 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).

In the figure below, the 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.



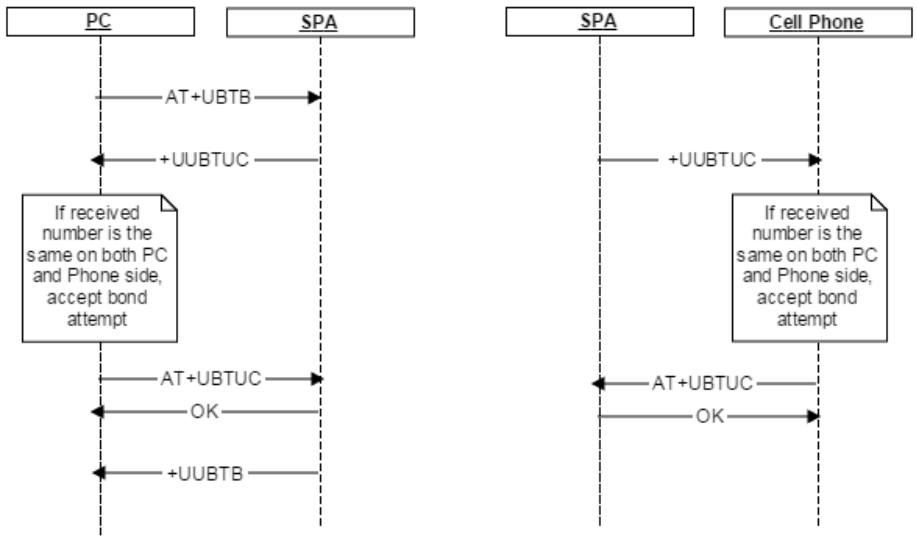

The above sample describes a case where neither the PC nor the keyboard supports Bluetooth and both sides use a u-blox Bluetooth device for Bluetooth support. This case can be separated into two use cases where either the PC or the keyboard has built-in Bluetooth without the need of a Bluetooth device.

## 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.

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.

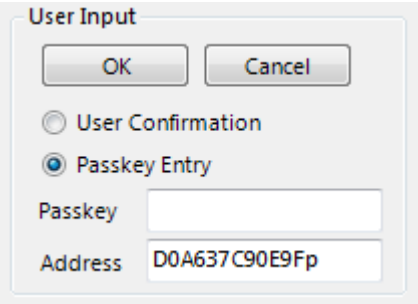


# 7 Security in s-center

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.

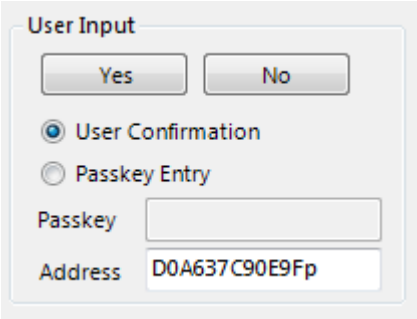
## Keyboard Only

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.




## 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.




## 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 Glossary

| Abbreviation | Definition |
|---|---|
| BR/EDR | Basic Rate/Enhanced Data Rate |
| EVK | Evaluation Kit |
| NFC | Near Field Communication |
| OOB | Out of Band |
| MITM | Man in the Middle |

**Table 4: Explanation of the abbreviations and terms used**

# Related documents

[1] u-blox Short Range Modules AT Commands Manual, Document No. UBX-14044127
[2] s-center User Guide, Document No. UBX-16012261
[3] ODIN-W2 product summary, Document No. UBX-15004332
[4] NINA-B1 product summary, Document No. UBX-15018552
[5] NINA-B2 product summary, Document No. UBX-17062096
[6] NINA-B30 product summary, Document No. UBX-17052930
[7] NINA-B31 product summary, Document No. UBX-17052931
[8] ANNA-B112 product summary, Document No. UBX-18006008
[9] Bluetooth Core Specification, https://www.bluetooth.com/specifications

☞ For regular updates to u-blox documentation and to receive product change notifications, register on our homepage (www.u-blox.com).

# Revision history

| Revision | Date | Name | Comments |
|---|---|---|---|
| R01 | 9-Apr-2019 | cmag, mape | Initial release. |

# Contact

For complete contact information, visit us at www.u-blox.com.

**u-blox Offices**


**North, Central and South America**

**u-blox America, Inc.**

Phone: +1 703 483 3180
E-mail: info_us@u-blox.com

**Regional Office West Coast:**

Phone: +1 408 573 3640
E-mail: info_us@u-blox.com

**Technical Support:**

Phone: +1 703 483 3185
E-mail: support@u-blox.com

**Headquarters**
**Europe, Middle East, Africa**

**u-blox AG**

Phone: +41 44 722 74 44
E-mail: info@u-blox.com
Support: support@u-blox.com

**Asia, Australia, Pacific**

**u-blox Singapore Pte. Ltd.**

Phone: +65 6734 3811
E-mail: info_ap@u-blox.com
Support: support_ap@u-blox.com

**Regional Office Australia:**

Phone: +61 2 8448 2016
E-mail: info_anz@u-blox.com
Support: support_ap@u-blox.com

**Regional Office China (Beijing):**

Phone: +86 10 68 133 545
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

**Regional Office China (Chongqing):**

Phone: +86 23 6815 1588
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

**Regional Office China (Shanghai):**

Phone: +86 21 6090 4832
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

**Regional Office China (Shenzhen):**

Phone: +86 755 8627 1083
E-mail: info_cn@u-blox.com
Support: support_cn@u-blox.com

**Regional Office India:**

Phone: +91 80 405 092 00
E-mail: info_in@u-blox.com
Support: support_in@u-blox.com

**Regional Office Japan (Osaka):**

Phone: +81 6 6941 3660
E-mail: info_jp@u-blox.com
Support: support_jp@u-blox.com

**Regional Office Japan (Tokyo):**

Phone: +81 3 5775 3850
E-mail: info_jp@u-blox.com
Support: support_jp@u-blox.com

**Regional Office Korea:**

Phone: +82 2 542 0861
E-mail: info_kr@u-blox.com
Support: support_kr@u-blox.com

**Regional Office Taiwan:**

Phone: +886 2 2657 1090
E-mail: info_tw@u-blox.com
Support: support_tw@u-blox.com