USER MANUAL

Product Name	**02500**
Version	**A**
Date	**2019.06.14**

SQL Technologies
4400 North Point Parkway, Suite 265
Alpharetta, GA 30022
Phone: 770-754-4711

1. Description

AcSiP Technology Corp. introduces a low-cost and low-power consumption IoT module. This stand-alone module is an operating system designed for wearable or internet of things (IoT) devices with smart connection and cloud application/services.

MD026 is a highly integrated SIP module which features an application processor, a low power 1x1 dual-band Wi-Fi subsystem, a Bluetooth subsystem, and a Power Management Unit. The application processor subsystem contains an ARM Cortex-M4F MCU, which has many peripherals, including UART, I2C, SPI, I2S, PWM, IrDA, and auxiliary ADC. 02500 also includes embedded SRAM/ROM and an external 4MB serial flash.

The Wi-Fi subsystem contains the 802.11a/b/g/n radio, baseband, and MAC that are designed to meet both the low power and high throughput application. It also contains a 32-bit RISC CPU that could fully offload the application processor.

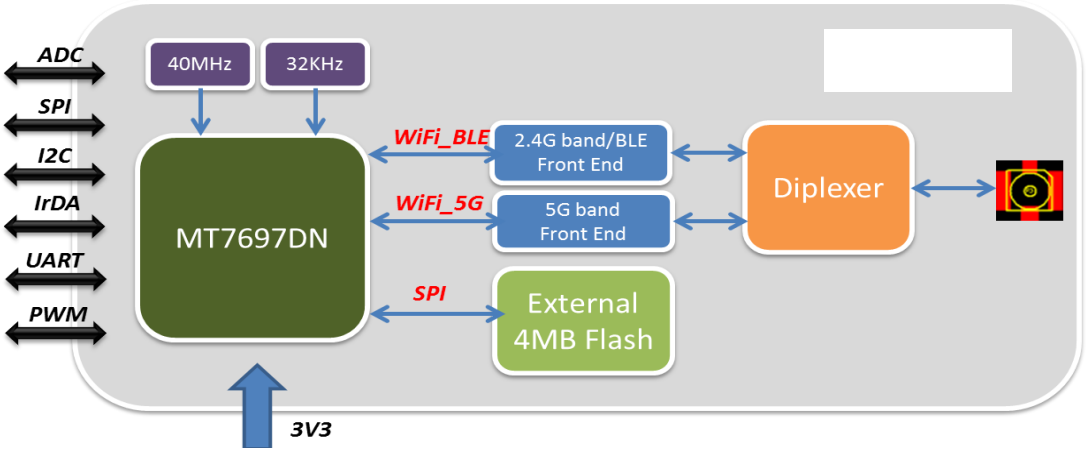
The Bluetooth subsystem contains the Bluetooth radio, baseband, link controller. It also uses the same 32-bit RISC CPU for the Bluetooth protocols.

1.1. Platform Features

General

- ARM Cortex M4 MCU with FPU with up to 192MHz clock speed
- 352KB SRAM / 64KB boot / 4MB Flash
- Supports external serial flash with Quad Peripheral Interface (QPI) mode
- Supports eXecute In Place (XIP) on flash
- 32KB cache in XIP mode
- Hardware crypto engines including AES, DES/3DES, SHA2 for network security
- Two UART interfaces with hardware flow control and one UART for debug, all multiplexed with GPIO
- One SPI slave interface multiplexed with GPIO
- Two I2C master interface multiplexed with GPIO
- One I2S interface multiplexed with GPIO
- Four channel 12-bit ADC multiplexed with GPIO
- Dedicated high-performance 32-bit RISC CPU N9 up to 160MHz clock speed
- IEEE 802.11 a/b/g/n compliant
- Supports 20MHz,40MHz bandwidth in 2.4/5GHz
- Dual-band 1T1R mode with data rate up to 150Mbps
- Supports STBC, LDPC
- Greenfield, mixed mode, legacy modes support
- IEEE 802.11 d/e/h/i/k/r/w support
- Security support for WFA WPA/WPA2 personal, WPS2.0, WAPI
- Supports 802.11w protected managed frames
- QoS support of WFA WMM, WMM PS
- Integrated LNA, PA, and T/R switch
- Optional external LNA and PA support.
- RX diversity support with additional RX input
- Bluetooth 4.2 Low Energy (LE)

2. Block Diagram

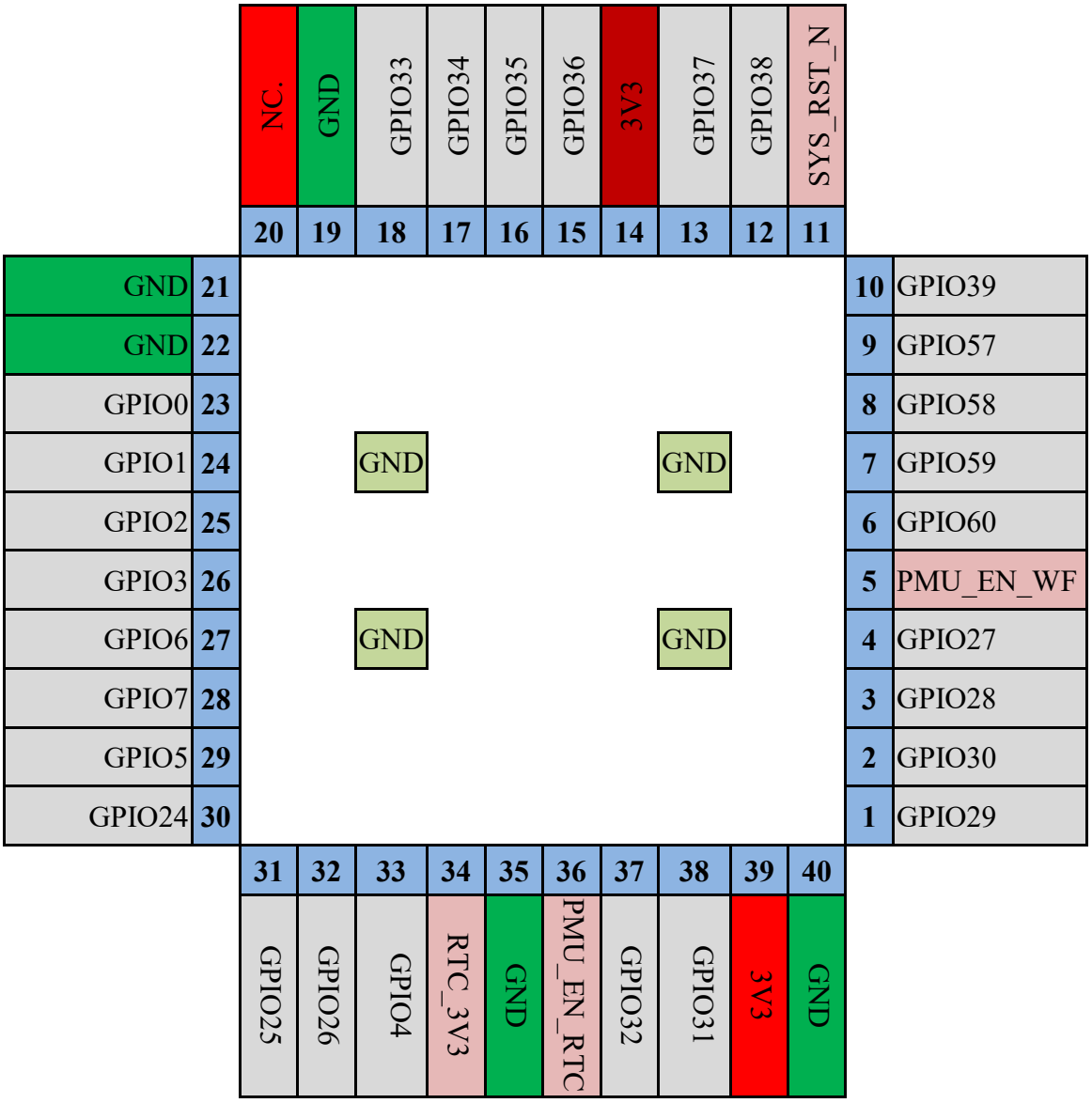


2.1. Specification

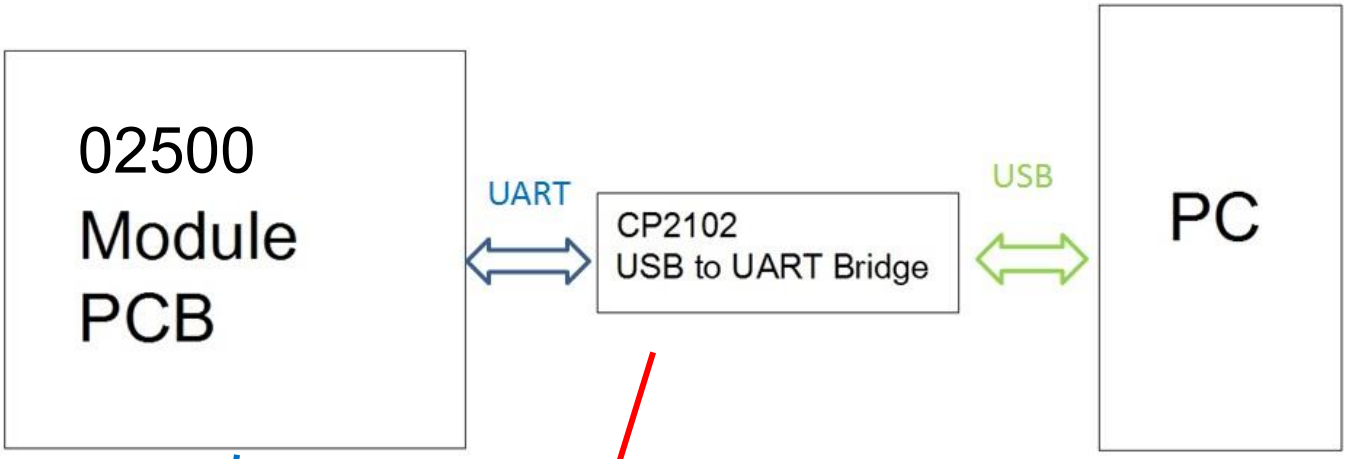
02500	
Chipset	MT7697D
Core	ARM Cortex-M4 MCU
FPU Clock Speed	192MHz
SRAM	352KB
External Flash	4MB
Antenna connector	MHF4 series: 20449-001E
Support 5G Band(MHz)	5150~5250(Band1)、5725~5850(Band4)
Operation Condition	
Temperature	Operating : -40℃ ~ +85℃ Storage : -40℃ ~ +105℃
Humidity	Operating : 10 ~ 95% (Non-Condensing) Storage : 5 ~ 95% (Non-Condensing)
Mechanical Information	
Dimension	18mm X 18mm X 1.7mm (Typ.)
Package	LGA 44Pin – Stamp hole type

3.Pin Definition

3.1 Detailed Pin Description

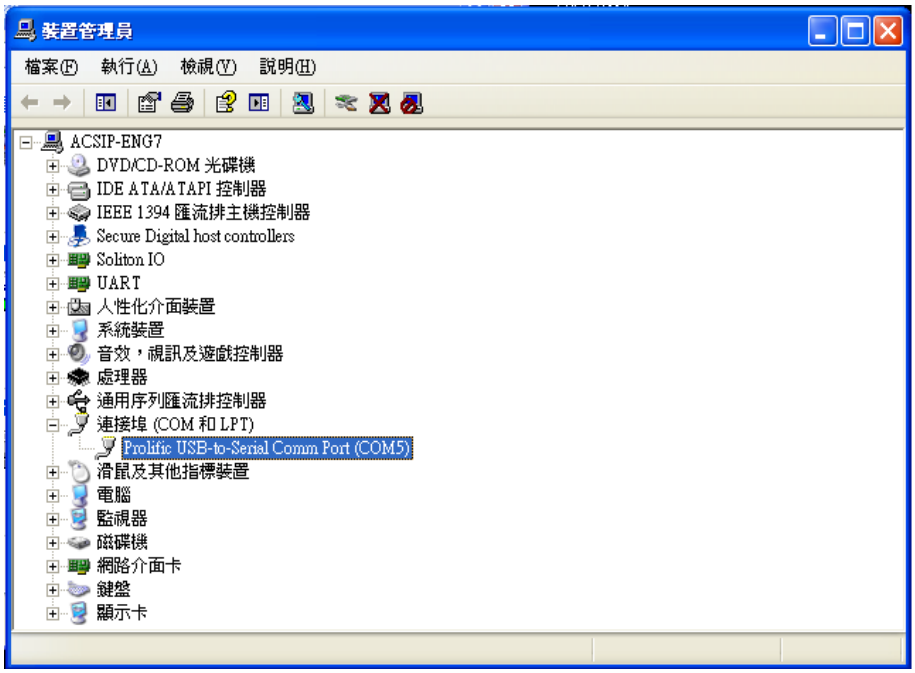


Operating Block

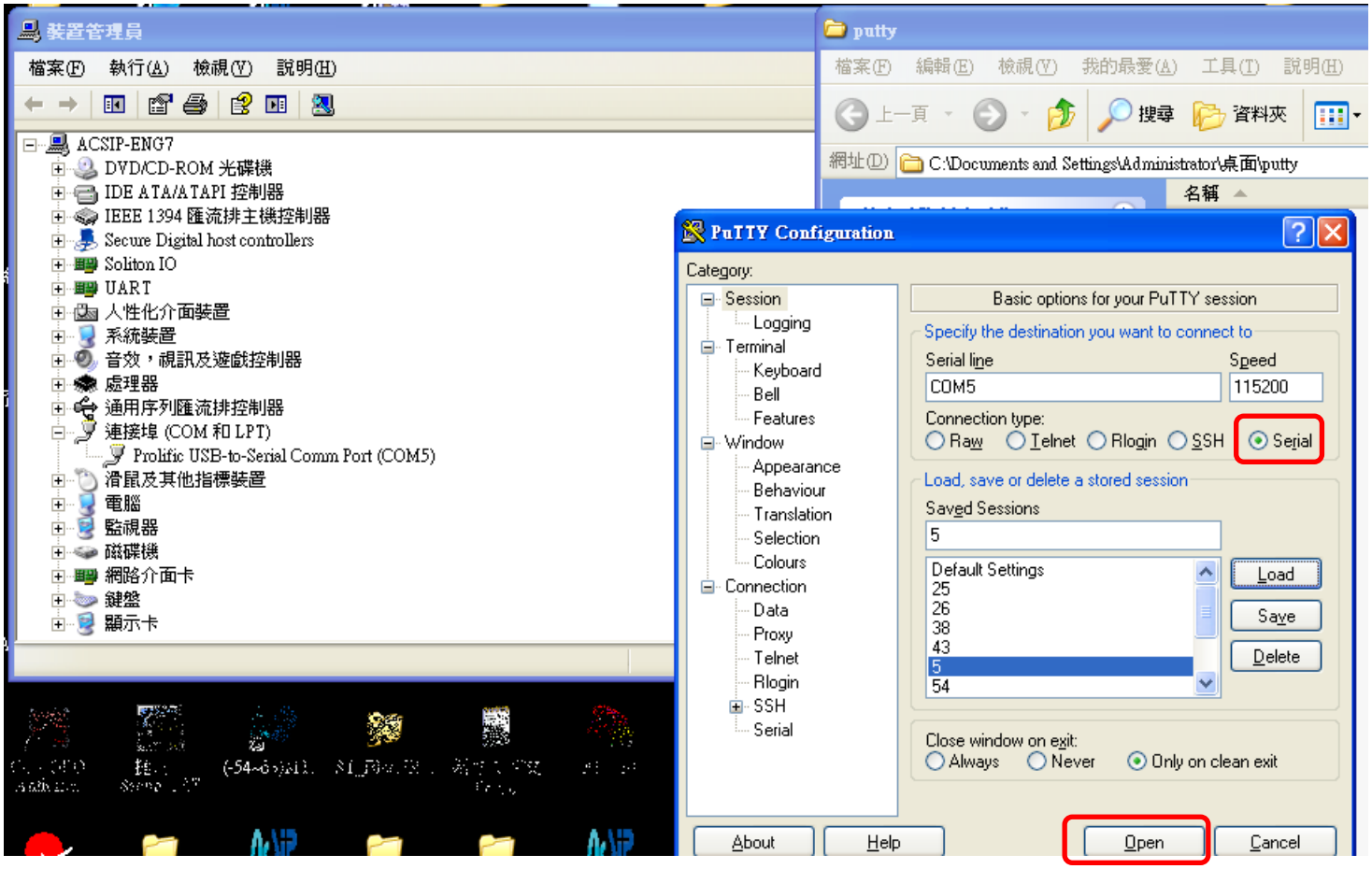


2.4GHz. 5GHz

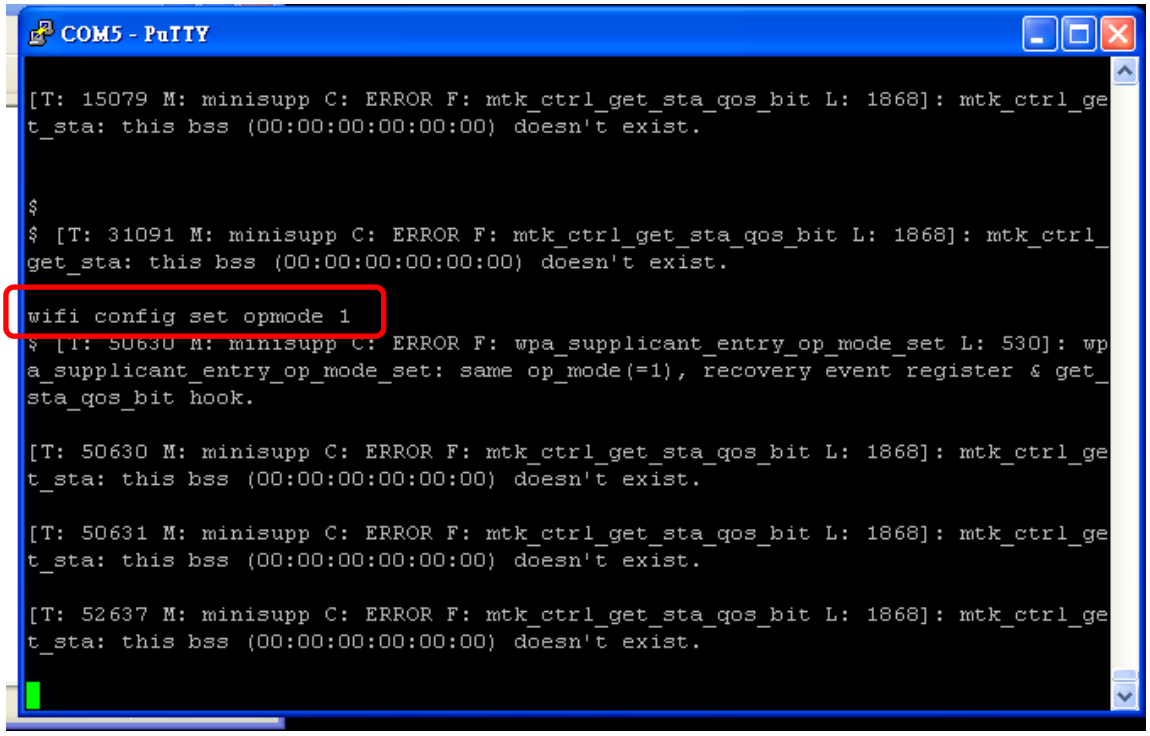
Dual-Band Antenna



PuTTY Program



Command



Software operating

Connect the board to PC with a serial port cable.

- Build the example project and download the binary file to the MT7687.
- Reboot the HDK, the console will show "FreeRTOS Running" message to indicate the HDK is booting up.
- Use '?' and enter to query the available command line options.

  Note that the command line options are still under development and subject to change without notice.
- Below are two examples to demonstrate the Wi-Fi station and Wi-Fi access point modes of MT7687.
- Example 1. Wi-Fi station mode.
  - Find your Wi-Fi access point settings:

    Before connecting to a Wi-Fi access point, the following information needs to be collected:

    1. What is the SSID of your Wi-Fi access point?
    2. What is the authentication mode of your Wi-Fi access point?

       In general, it is WPA PSK or WPA2 PSK. If you want to use different settings, please read the table 'Table 1. Supported AuthMode(s)' at the bottom of this example.

3. What is the password of your Wi-Fi access point?

4. What is the encryption mode of your Wi-Fi access point?

In general, AES or TKIP is used. If you want to use different settings, please read the table 'Table 2. Supported EncrypType(s)' at the bottom of this example.

- Once you have this information, use the following commands to configure the HDK. This example assumes you want to use either WPA PSK or WPA2 PSK, your packets are encrypted with TKIP or AES, the access point SSID is 'myhome' (length 6), and the password of WPA or WPA2 is '12345678' (length 8).

```
config write STA AuthMode 9
config write STA EncrypType 8
config write STA Ssid myhome
config write STA SsidLen 6
config write STA WpaPsk 12345678
config write STA WpaPskLen 8
config write common OpMode 1
```

press the reset button on the LinkIt 7687 HDK to restart the system.

- Boot up with the new configuration.

If everything is correct, similar messages will be shown in the console to notify your HDK has received an IP address.

```
**********************
DHCP got IP:10.10.10.101
**********************
```

- PING from the LinkIt 7687 HDK (SDK v3.1.0)

If the IP address is fetched and the network is operating, the LinkIt 7687 can ping other devices/computer on the network with the following command in the console.

```
f 11 10.10.10.254 3 64
```

The ping stops after sending three packets to 10.10.10.254.

The ping usage is: f 11 <ip address> <times> <ping packet length>

- Wi-Fi configuration options for AuthMode and EncrypType.

```
+---+-----------------------------------+
| 0 | open, no security                 |
+---+-----------------------------------+
| 4 | WPA PSK                           |
+---+-----------------------------------+
| 7 | WPA2 PSK                          |
+---+-----------------------------------+
| 9 | Support both WPA and WPA2 PSK     |
+---+-----------------------------------+
```

Table 1. Supported AuthMode(s)

```
+---+-----------------------+
| 0 | WEP                   |
+---+-----------------------+
| 1 | No encryption         |
+---+-----------------------+
| 4 | TKIP                  |
```

```
+---+-----------------------+
| 6 | AES                   |
+---+-----------------------+
| 8 | Support TKIP and AES  |
+---+-----------------------+
```

Table 2. Supported EncrypType(s)

- Example 2. Wi-Fi access point mode.
  - Decide Wi-Fi access point settings:
    - SSID
    - Authentication Mode
    - Encryption Type.
    - Password

    You need the above settings before proceeding.
  - Once the information is collected, use the following commands to configure the LinkIt 7687 HDK. This example assumes WPA2 PSK is used for authentication, AES for encryption, 'iot_ap' (length 6) for the SSID, and the password of WPA2 as '87654321' (length 8).

```
config write AP Ssid iot_ap
config write AP SsidLen 6
config write AP AuthMode 7
config write AP EncrypType 6
config write AP WpaPsk 87654321
config write AP WpaPskLen 8
config write common OpMode 2
```

press reset button on the LinkIt 7687 HDK to restart the system.

- Use a handheld device or a laptop computer to connect to the access point 'iot_ap'. In the MT7687 console, the IP address assigned to the cellphone or laptop is shown as below.

```
[DHCPD:DBG]lease_ip:10.10.10.2
```

BLE mode

Use the command 'ble ?' and enter to query the available Bluetooth command line options.

- Input the command "ble gap start_scan 0 0024 0011 1 0" in the serial tool to scan for the nearby Bluetooth enabled devices.

- 0, passive scan.

- 0024, scan interval (36 * 0.625 ms). Two bytes long HEX value.

- 0011, scan window (17 * 0.625 ms). Two bytes long HEX value.

- 1, own address type, 1 means random address.

- 0, filter policy.

A similar log is written to the output:

@code

Find a device A,

```
[I][APP] BT_GAP_LE_ADVERTISING_REPORT_IND Success
[I][APP] ==========================================
[I][APP] Address:        [RANDOM] 73-2c-d4-3f-d3-b2
[I][APP] Event Type:     ADV_IND
[I][APP] AD Flags:       LE General Discoverable Mode
[I][APP] RAW DATA=0x02011a14ff4c000100000000040000000000000000000000
[I][APP] ==========================================
```

Find a device B,

```
[I][APP] ==========================================
[I][APP] Address:        [RANDOM] ff-76-f0-01-a4-1a
[I][APP] Event Type:     ADV_IND
[I][APP] Complete Name: WeLoop B08 DEF4D4
[I][APP] AD Flags:       LE Limited Discoverable Mode
[I][APP] RAW DATA=0x120957654c6f6f702042303820444546344434031934120201050303e7fe
[I][APP] ==========================================
```

@endcode

- Connect the device with the command "ble gap connect 1 732cd43fd3b2".

- 1, random address, based on the [RANDOM] tag. 0, public address based on the [PUBLIC] tag.

- 732cd43fd3b2: remote device address.

The output log indicates the connection is established with a remote device.

```
@code
[I][APP] BT_GAP_LE_CONNECT_IND Success
[I][APP] connection handle=0x0200
[I][APP] role=Master
[I][APP] peer address:[RANDOM] 73-2c-d4-3f-d3-b2
@endcode
```

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This device is intended only for OEM integrators under the following conditions:

1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and

2) The transmitter module may not be co-located with any other transmitter or antenna.

As long as **2** conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed

IMPORTANT NOTE: In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

End Product Labeling

The product can be kept as far as possible from the user body or set the device to lower output power if such function is available. The final end product must be labeled in a visible area with the following: “Contains FCC ID: **2ATHJ02500**”. The grantee's FCC ID can be used only when all FCC compliance requirements are met.

Manual Information To the End User

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user’s manual of the end product which integrates this module.

The end user manual shall include all required regulatory information/warning as show in this manual.