# Privacy Example

# Version 1.5

# September 2018

---------------------------------------------------------------------------------------------------------------------------------

# Disclaimer

The information in this document pertains to information related to Redpine Signals, Inc. products. This information is provided as a service to our customers, and may be used for information purposes only.

Redpine assumes no liabilities or responsibilities for errors or omissions in this document. This document may be changed at any time at Redpine's sole discretion without any prior notice to anyone. Redpine is not committed to updating this document in the future.

# Table of Contents

# 1 Feature Overview

Bluetooth LE supports a feature that reduces the ability to track an LE device over a period of time by changing the Bluetooth device address on a frequent basis, called Privacy of that particular device.

The device address of the remote device referred to as the private address will be resolved by local device in order to connect to that device. The private address is generated by using Identity Resolving Key (IRK) exchange in between devices during SMP bonding procedure. Our local device will add the remote devices in one Resolving list(to maintain remote device identity addresses) along with that IRK's and enable the Resolution, sets privacy mode and connect to the remote device with remote identity address.

## 2 Application Overview

This application demonstrates how to configure device with privacy feature by organizing resolving list and resolution process and how to connect to remote Peripheral device.

### 2.1 Sequence of Events

This Application explains user how to:

- Set a local name to the device
- Scan devices
- Connection to remote device
- SMP level connection
- Exchange of IRK's and store them
- Disconnect with remote device
- Add remote device to resolve list with identity address
- Get resolve list size
- Set resolution enable and time out
- Set privacy mode
- Connect remote device with identity address
- Start Encryption instead of SMP repairing

> **Note**
> If both devices having resolution enable, enhanced connection event will come for any privacy mode. if remote device is without resolution, privacy mode should be device privacy mode.

# 3 Application Setup

The WiSeConnect parts require that the host processor is connected to the WiSeConnect using either SPI, UART or USB host interface. The host processor firmware needs to properly initialize the selected host interface. The Redpine Wireless SAPI framework provides necessary HAL APIs to enable variety of host processors. The WiSeMCU parts offer integrated wireless connectivity and does not require host interface initialization.

## 3.1 WiSeMCU / WiSeConnect  based Setup Requirements

- Windows PC with KEIL or IAR IDE in case of WiSeMCU
- Windows / Linux PC with Host interface(UART/ USB-CDC/ SPI/ USB) in case of WiSeConnect
- Redpine module
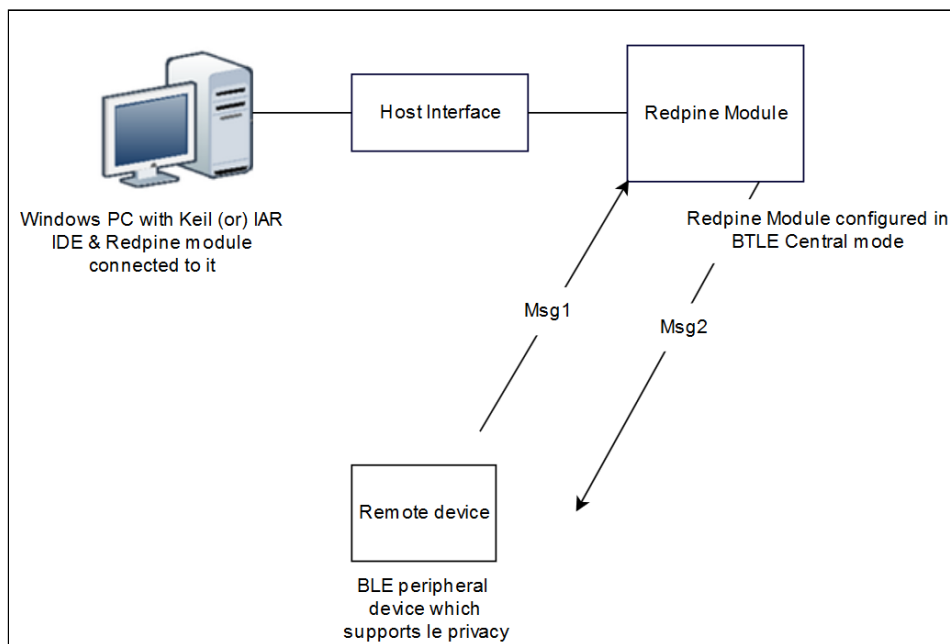- BTLE peripheral device which supports privacy feature(Generally phones with the nRF Connect application

**Figure 1: Setup Diagram**

# 4 Configuration and Execution of the Application

## 4.1 Configuring the Application

1. Open *rsi_ble_le_privacy.c* file and update/modify following macros:
   **RSI_BLE_LOCAL_NAME** refers the name of the Redpine device to appear during scanning by remote devices.

   ```
   #define RSI_BLE_LOCAL_NAME                      "BLE_PRIVACY"
   ```

   RSI_REMOTE_DEVICE_NAME refers the name of the Remote device to which Redpine module initiate connection.

   ```
   #define RSI_REMOTE_DEVICE_NAME                  "REMOTE_DEV"
   ```

   RSI_DEVICE_ROLE refers the role of the Redpine device.

   ```
   #define RSI_DEVICE_ROLE                         "RSI_MASTER"
   ```

   > **Note**
   >
   > RSI_DEVICE_ROLE should be RSI_MASTER

   RSI_DEVICE_ROLE refers the role of the Redpine device.

   ```
   #define RSI_DEVICE_ROLE                         "RSI_MASTER"
   ```

   RSI_DEVICE_ROLE refers the role of the Redpine device.

   ```
   #define RSI_DEVICE_ROLE                         "RSI_MASTER"
   ```

   RSI_BLE_SMP_IO_CAPABILITY refers the IO capability of redpine device for SMP, RSI_BLE_SMP_PASSKEY is smp passkey key from redpine device

   ```
   #define RSI_BLE_SMP_IO_CAPABILITY               0x01
   #define RSI_BLE_SMP_PASSKEY                     0
   ```

Following are the **non-configurable** macros in the application.
Following are the event numbers for connection, Disconnection, and enhanced connection events.

```
#define  RSI_APP_EVENT_ADV_REPORT                  0x00
#define  RSI_BLE_CONN_EVENT                        0x01
#define  RSI_BLE_DISCONN_EVENT                     0x02
#define  RSI_BLE_SMP_REQ_EVENT                     0x03
#define  RSI_BLE_SMP_RESP_EVENT                    0x04
#define  RSI_BLE_SMP_PASSKEY_EVENT                 0x05
#define  RSI_BLE_SMP_FAILED_EVENT                  0x06
#define  RSI_BLE_ENCRYPT_STARTED_EVENT             0x07
#define  RSI_BLE_SMP_PASSKEY_DISPLAY_EVENT         0x08
#define  RSI_BLE_SC_PASSKEY_EVENT                  0x09
#define  RSI_BLE_LTK_REQ_EVENT                     0x0A
#define  RSI_BLE_SECURITY_KEYS_EVENT               0x0B
#define  RSI_BLE_ENHANCE_CONNECTED_EVENT           0x0C
```

**BT_GLOBAL_BUFF_LEN** refers Number of bytes required by the application and the driver

```
#define BT_GLOBAL_BUFF_LEN                         12000
```

**RSI_BLE_DEV_ADDR_TYPE** refers the address type of the remote device

```
#define RSI_BLE_REMOTE_ADDR_TYPE                   LE_PUBLIC_ADDRESS
```

**RSI_BLE_DEV_ADDR_1** refers remote device address which has to connect

```
#define RSI_BLE_REMOTE_ADDR                        "00:15:83:6A:64:17"
```

**RSI_BLE_SET_RESOLVABLE_PRIV_ADDR_TOUT** refers resolution timeout , that is the length of time the Controller uses a Resolvable Private Address before a new resolvable private address is generated and starts being used.

```
#define RSI_BLE_SET_RESOLVABLE_PRIV_ADDR_TOUT      120
```

**RSI_BLE_PROCESS_TYPE** refers the operation to be performed on the resolving list

```
#define RSI_BLE_PROCESS_TYPE                       RSI_BLE_ADD_TO_RESOLVE_LIST
```

valid configurations for the RSI_BLE_PROCESS_TYPE are
RSI_BLE_ADD_TO_RESOLVE_LIST
RSI_BLE_REMOVE_FROM_RESOLVE_LIST
RSI_BLE_CLEAR_RESOLVE_LIST

**RSI_BLE_PRIVACY_MODE** refers the privacy mode of local device

```
#define RSI_BLE_PRIVACY_MODE                       RSI_BLE_DEVICE_PRIVACY_MODE
```

**RSI_BLE_RESOLVING_LIST_SIZE** refers the resolving list size of redpine device

```
#define RSI_BLE_RESOLVING_LIST_SIZE                5
```

2. Open **rsi_ble_config.h** file and update/modify following macros
   **RSI_BLE_DEV_ADDR_RESOLUTION_ENABLE** refers address resolution is enable or not.It should be 1 to enable privacy feature.

```
#define RSI_BLE_DEV_ADDR_RESOLUTION_ENABLE          1
```

**RSI_BLE_ADV_DIR_ADDR_TYPE** refers the address type of remote device which use while advertising.

```
#define RSI_BLE_ADV_DIR_ADDR_TYPE               LE_PUBLIC_ADDRESS
```

**RSI_BLE_ADV_DIR_ADDR** refers to which device the local device will advertise with private address, it should be one of the device in resolve list.

```
#define RSI_BLE_ADV_DIR_ADDR                    "00:15:83:6A:64:17"
```

```
#define RSI_BLE_PWR_INX                         30
#define RSI_BLE_PWR_SAVE_OPTIONS                0
#define RSI_DUTY_CYCLING                        0
```

3. Open **rsi_wlan_config.h** file and update/modify following macros,

```
#define CONCURRENT_MODE                     RSI_DISABLE
#define RSI_FEATURE_BIT_MAP                 FEAT_SECURITY_OPEN
#define RSI_TCP_IP_BYPASS                   RSI_DISABLE
#define RSI_TCP_IP_FEATURE_BIT_MAP          TCP_IP_FEAT_DHCPV4_CLIENT
#define RSI_EXT_CUSTOM_FEATURE_BIT_MAP      EXT_FEAT_256K_MODE
#define RSI_BAND                            RSI_BAND_2P4GHZ
```

> **Note**
> **rsi_wlan_config.h** and **rsi_ble_config.h** files are already set with desired configuration in respective example folders user need not change for each example.

## 4.2 Executing the Application

1. After the program gets executed, Redpine module will be in Scanning state.
2. Advertise remote device,
3. If Redpine module get device with name configured `RSI_BLE_LOCAL_NAME` or bd address with address configured in `RSI_BLE_REMOTE_ADDR` in results ,local device will try to connect with remote device.
4. After connection Redpine device which is in master mode will initiate SMP request
5. Give response from Remote device and passkey
6. After successful SMP connection security keys will exchanged between Remote device and Redpine device.
7. Redpine device will add remote device's IRK's and local IRK's in to resolve list and enable resolution
8. Give disconnect from remote device and keep in advertise mode.
9. Now Redpine module will try to connect to remote device with identity address.
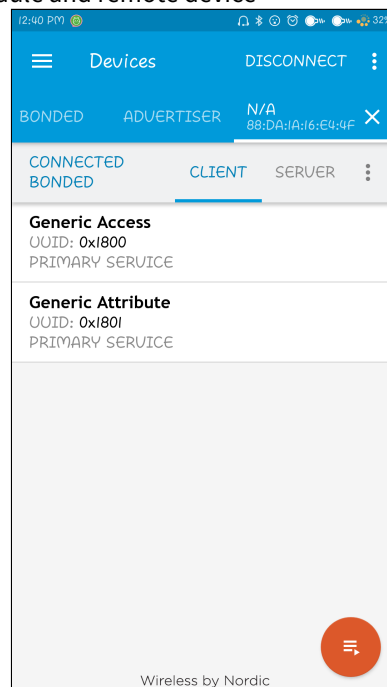
10. After successful connection, Redpine module will give start encryption instead of SMP repairing.
11. Encryption will be enabled on both sides.

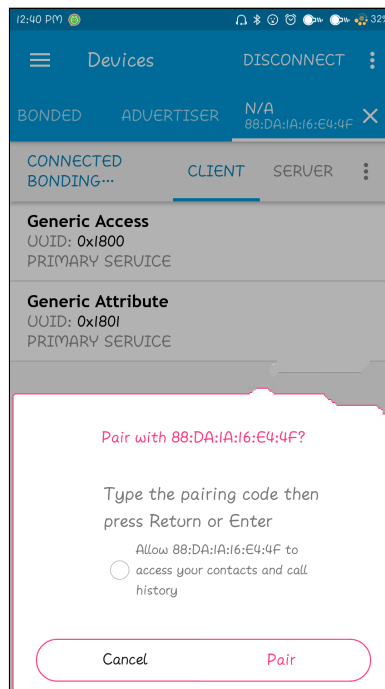Please find following screen shots for reference.

1. Advertise remote device
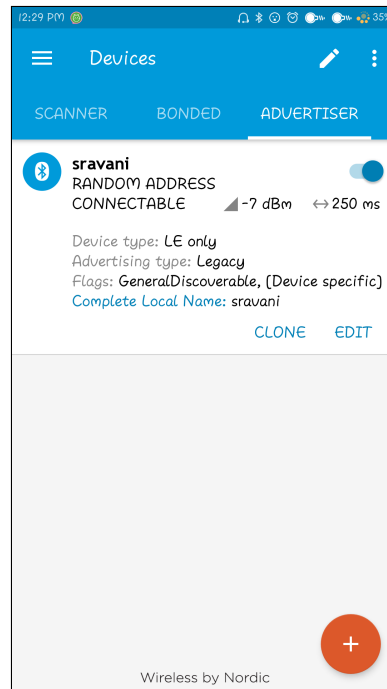


2. Connection in between redpine module and remote device

3. Pairing confirmation



4. Passkey confirmation