



## Chapter 4C: BLE Low Power, Beacons, and OTA

This chapter covers more advanced topics such as low power modes, scan response packets, beacons, and OTA firmware upgrade.

<b>4C.1 LOW POWER .....</b>	<b>2</b>
4C.1.1 POWER MODE OVERVIEW .....	2
4C.1.2 WICED LOW-POWER CODE .....	6
4C.1.3 PROGRAMMING IN LOW POWER MODE .....	11
<b>4C.2 ADVERTISING PACKETS .....</b>	<b>12</b>
4C.2.1 USING THE ADVERTISING PACKET TO GET CONNECTED .....	12
4C.2.2 BEACONS .....	13
<b>4C.3 SCAN RESPONSE PACKETS .....</b>	<b>17</b>
<b>4C.4 OTA (OVER THE AIR) UPGRADE .....</b>	<b>18</b>
4C.4.1 INTRODUCTION .....	18
4C.4.2 DESIGN AND ARCHITECTURE .....	19
4C.4.3 APPLICATIONS FOR LOADING NEW FIRMWARE .....	21
4C.4.4 OTA FIRMWARE .....	24
4C.4.5 SECURE OTA .....	31
<b>4C.5 EXERCISES .....</b>	<b>33</b>
EXERCISE 4C.1 BLE LOW POWER (EPDS) .....	33
EXERCISE 4C.2 (ADVANCED) EDDYSTONE URL BEACON .....	35
EXERCISE 4C.3 (ADVANCED) USE MULTI-ADVERTISING ON A BEACON .....	37
EXERCISE 4C.4 (ADVANCED) ADVERTISE MANUFACTURING DATA AND USE SCAN RESPONSE FOR THE UUID .....	39
EXERCISE 4C.5 (ADVANCED) OTA FIRMWARE UPGRADE (NON-SECURE) .....	40
EXERCISE 4C.6 (ADVANCED) OTA FIRMWARE UPGRADE (SECURE) .....	42



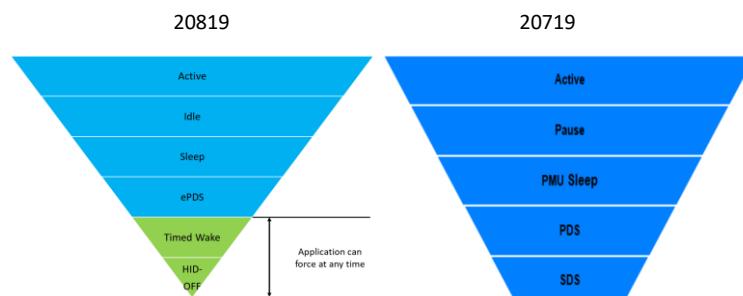
## 4C.1 Low Power

### 4C.1.1 Power Mode Overview

You will get a chance to experiment with Low Power in [Exercise 4C.1](#).

WICED Bluetooth devices support different power modes. However, it is important to note that not all the devices support every mode. The following figures show the modes from highest to lowest power for the 20819 and 20719 families.

Further details can be found in application notes [CYW20819 Low-Power Guidelines \(AN225270\)](#) and [CYW20706 and CYW20719 Low-Power Modes](#).



The following table provides additional details of each of the WICED Power Modes:

Mode	Family	Description
Active	Both	Active mode is the normal operating mode in which all peripherals are available, and the CPU is active.
Idle Pause	20819 20719	In this mode, the CPU is in Wait for Interrupt (WFI) and the HCLK, which is the high frequency clock derived from the main crystal oscillator, is running at a lower clock speed. Other clocks are active, and the state of the entire chip is retained. Idle/Pause mode is chosen when the other lower power modes are not possible. Any configured interrupt can wake the device.
Sleep	Both	In this mode, the CPU is in WFI and the HCLK is not running. The PMU determines if other clocks can be turned off and does so accordingly. The state of the entire chip is retained, the internal LDOs run at a lower voltage (voltage is managed by the PMU), and SRAM is retained. Wake can be from various sources such as GPIO, timer, or BT activity.
Power Down Sleep (PDS)	20719	This mode is an extension of the PMU Sleep wherein most of the peripherals such as UART and SPI are turned OFF. The entire memory is retained, and on wakeup the execution resumes from where it was paused.
Shut Down Sleep (SDS)	20719	Everything is turned OFF except LHL GPIOs, RTC, and LPO. The device can come out of this mode either due to Bluetooth activity, an LHL interrupt, or a timer. This mode makes use of micro-Bluetooth Core Scheduler ( $\mu$ BCS), which is a compressed scheduler different from the regular BCS. Before going into this mode, the application can store some bytes of data into the Always-On RAM (AON). When the device comes out of this mode, the data from AON is restored.



Mode	Family	Description
		After waking from SDS, the application will start from the beginning (fastboot) and must restore its state based on information stored in AON. In the SDS mode, a single Bluetooth task with no data activity, such as a BLE connection or BLE advertisement can be performed. If there is data activity during these tasks, the system will undergo full boot and normal BCS will be called.
Enhanced Power Down Sleep (ePDS)	20819	The entire device is OFF except for RTC, LPO, and a comparator to wake the device. The entire SRAM memory is retained. The device enters this state through WFI but exits through a reset vector. Before entering this mode, the PMU stores the CPU state and some register values (including the program counter) in SRAM, which are restored after wakeup so that the CPU starts executing from where it stopped. It can wake up using a GPIO, a timer, or BT activity.
Timed-Wake	20819	The device can enter this mode asynchronously, that is, the application can force the device into this mode at any time without asking permission from other blocks. LHL, RTC, and LPO are the only active blocks. The only wakeup sources are a timer or an LHL interrupt. SRAM is not retained. The device starts executing from reset; therefore, the wakeup time is the same as that of power on reset.
HID-OFF	20819	This mode is like Timed-Wake, but in HID-OFF mode even the LPO and RTC are turned OFF. The only wakeup source is an LHL interrupt. SRAM is not retained. The device starts executing from reset; therefore, the wakeup time is the same as that of power on reset.

The power domains on the chip (and the peripherals they supply) are managed by the PMU as described in the following table:

S. No	Power Domain	Peripherals	Operational Power Modes
1	VDDC	SRAM, Patch RAM PWM (20719)	PWM: If ACLK is used, then the hardware block can operate until the PMU enters Sleep. If LHL clock is used, then the hardware block can operate until the PMU enters SDS.
2	VDDCP (20819)	PWM (20819)	PWM is switched OFF in ePDS mode but can work in higher power modes.
2	VDDCG	I2C, SPI, PUART, WDT, ARM GPIO, Dual Input 32-bit Timer, flash, ROM	The hardware blocks can operate until the PMU enters Sleep (20719) or ePDS (20819)
3	VBAT/LHL	LHL GPIO, Analog PMU, RTC	The hardware blocks can operate until the PMU enters SDS (20719) or HID-Off (20819)
4	VBAT/LHL	Aux ADC	The Aux ADC can operate until the PMU enters Sleep (20719) or ePDS (29819).

### PMU Mode Transitions

The Bluetooth device contains a Power Management Unit (PMU) which is responsible for all power mode transitions except Timed-Wake and HID-OFF. The firmware can control whether PDS or SDS (20719) or ePDS (20819) are allowed but it cannot prevent Pause/Idle or Sleep. It is up to the PMU to determine which sleep mode to enter depending on scheduled events. For example, if the firmware allows SDS, the PMU may decide to go into PDS instead of SDS because of an event scheduled for a short



time in the future. In that case, going to SDS would not be beneficial because there is time (and power) required to shut down and re-initialize the system. The PMU can transition to Idle/Pause or Sleep any time.

In the firmware, you configure sleep by providing wake sources and by providing a sleep permit handler callback function that the PMU will call whenever it wants to go to PDS or SDS (20719) or ePDS (20819). In the callback function, you can disallow or allow the requested low power mode transition. For the 20719, you can choose to only allow PDS or allow both PDS and SDS depending on your firmware's requirements.

In ePDS/PDS mode, the device will wake every time a BLE event must be serviced. For example, during advertising, the device will wake every time a new advertising packet needs to be sent. Once a connection has been established, the device will wake for each connection interval.

In SDS mode, the micro-Bluetooth Core Scheduler ( $\mu$ BCS) is used to service BLE events such as sending advertising packets and keeping the connection alive, so it does not need to wake for these events. During a connection, the device will typically only wake when data needs to be sent over the link, such as due to a timer that sends data periodically or due to a GPIO interrupt indicating a change.

Using RPA (i.e. the RPA refresh timeout is set to something other than `WICED_BT_CFG_DEFAULT_RANDOM_ADDRESS_NEVER_CHANGE`) causes the firmware to wake frequently (about twice per second). This will cause increased power consumption. Therefore, RPA should not be used in power critical applications.

#### **Additional SDS Mode Details (Advanced)(20719 family only)**

A global variable can be set in different sections of the firmware so that whenever the callback is called the appropriate sleep state will be allowed. In general, for a GAP Peripheral:

1. SDS can be used while advertising or with one connection with no pending activities.
  - a. SDS will be entered while advertising only if the timeout for that advertising type is set to 0. If not, the system will only enter PDS. For example, if the high duty cycle timeout is 30 seconds and the low duty cycle timeout is 0 then the device will use PDS during high duty cycle advertising (for 30 seconds) and will use SDS during low duty cycle advertising.
  - b. If SDS is entered while advertising, a connection request will have to be sent twice to initiate a connection. However, this may be worthwhile in applications where advertising continues for a long time.
2. SDS should not be used while pairing (i.e. encryption) is being negotiated.

For a GAP Central, SDS should not be used.

Upon wake from SDS, the device re-initializes from application\_start. The boot type can be determined as initial power up or reset (cold boot) or wake from SDS (fast boot). Differences required between cold and fast boot are handled by using the boot type.



SDS mode will not be entered if you have any active application threads. Therefore, if you have threads they must include an RTOS delay with ALLOW\_THREAD\_TO\_SLEEP as the second parameter so that the thread will sleep.

Variables are not retained in SDS unless they are stored in Always On (AON) RAM. There are 256 bytes of AON RAM available to the application. This will be discussed in more detail in a minute.

For SDS, the connection interval should be set to 100ms or longer. Otherwise, SDS will not save significant power because the system will wake frequently.

Using RPA (i.e. the RPA refresh timeout is set to something other than WICED\_BT\_CFG\_DEFAULT\_RANDOM\_ADDRESS\_NEVER\_CHANGE) causes an additional issue in SDS. During advertising, the address will change every time a fast boot occurs. Since this happens about twice per second if RPA is enabled, it is very difficult to connect because the address will change before you can connect to the device.

HCI UART and other BT pins such as host and dev wake are powered down in SDS.

It can be difficult to achieve lower power using SDS than with PDS – much depends on how frequent the system must wakeup due to the overhead in re-initializing everything on every wakeup.

### Wake Times

Approximate wake times for various modes are as follows:

Mode	Typical Wake Time (ms)
Active	N/A
Idle/Pause	ISR service time – almost instantaneous
Sleep	0.5 – 2
PDS	
SDS	10
ePDS	2
Timed Wake	Same as POR – a few hundred ms
HID Off	Same as POR – a few hundred ms

### Current Consumption

The exact current consumption depends on the firmware, but the approximate values to be expected are as follows:

Mode	Typical Current ( $\mu$ A)
Active	>50 (very FW dependent - often much higher)
Idle/Pause	
PDS	<20
SDS	<10
ePDS	~10 with no BLE
Timed Wake	~3
HID Off	~3



#### 4C.1.2 WICED Low-Power Code

To use low power modes in the firmware, the following steps are required:

1. Add sleep header files
2. Setup sleep configuration
3. Create a sleep permit handler callback function
4. Update connection parameters on a GATT connection
5. Create wakeup events (GPIO interrupts, timers, threads, etc.)
6. Update Advertising Settings
7. Update BT Address Setting

The following additional steps are required only when SDS is used on the 20719 family:

8. Update sleep permission variables at appropriate locations
9. Configure AON variables
10. Determine boot type and perform system initialization based on the boot type

#### Sleep Header Files

The header file `wiced_sleep.h` contains the API related to low power operation. That header file must be included in the source code to call the sleep API functions. You should also include `wiced_bt_i2c.h` so that we will be able to update the connection parameters in the firmware.

#### Sleep Configuration

The function `wiced_sleep_configure` is used to enable low power operation of the device. The parameter passed to this function is a pointer to a structure of type `wiced_sleep_config_t` that contains the sleep configuration information. The structure is defined like this:

```
/** Sleep configuration parameters */
typedef struct
{
    wiced_sleep_mode_type_t      sleep_mode;          /**< Requested sleep mode */
    wiced_sleep_wake_type_t     host_wake_mode;       /**< Active level for host wake */
    wiced_sleep_wake_type_t     device_wake_mode;     /**< Active level for device wake */
    uint8_t                     device_wake_source;   /**< Device wake source(s). GPIO mandatory for
                                                WICED_SLEEP_MODE_TRANSPORT */
    uint32_t                    device_wake_gpio_num;  /**< GPIO# to wake the device, mandatory for
                                                WICED_SLEEP_MODE_TRANSPORT */
    wiced_sleep_allow_check_callback sleep_permit_handler; /**< Call back to be called by sleep framework
                                                to poll for sleep permission */
}wiced_sleep_config_t;
```

In the firmware, you need to: (1) declare a global variable of type `wiced_sleep_config_t`; (2) initialize all the elements of the structure just after stack initialization; and (3) call `wiced_sleep_configure`.

The elements in the structure are:

**sleep\_mode:** This can be either `WICED_SLEEP_MODE_NO_TRANSPORT` or `WICED_SLEEP_MODE_TRANSPORT`. If you select the former, the device will enter sleep only if no host is connected (i.e. HCI UART CTS line not asserted). If you select the latter, the device will enter sleep only when an external HCI host is connected (i.e. HCI UART CTS line is asserted). If



the device is being used stand-alone without an external HCI host, you should choose *WICED\_SLEEP\_MODE\_NO\_TRANSPORT*. Note that in ModusToolbox 2.0 hosted operation is not supported and so this element is always *WICED\_SLEEP\_MODE\_NO\_TRANSPORT*.

**host\_wake\_mode:** This can be either *WICED\_SLEEP\_WAKE\_ACTIVE\_LOW* or *WICED\_SLEEP\_WAKE\_ACTIVE\_HIGH* depending on the polarity of the interrupt to wake the host (if a host is connected). This only applies if sleep\_mode is *WICED\_SLEEP\_MODE\_TRANSPORT*. The Host Wake function is on a dedicated device pin, but it can be multiplexed into other IOs (this multiplexing feature is not currently supported in the API).

**device\_wake\_mode:** This can be either *WICED\_SLEEP\_WAKE\_ACTIVE\_LOW* or *WICED\_SLEEP\_WAKE\_ACTIVE\_HIGH* depending on the polarity of the interrupt for the host to wake the device (if a host is connected). This only applies if sleep\_mode is *WICED\_SLEEP\_MODE\_TRANSPORT*. The Device Wake function is on a dedicated device pin, but it can be multiplexed into other IOs (this multiplexing feature is not currently supported in the API). This pin is not available on the 20719 40-pin package, but the *device\_wake\_source* pin can be used for this purpose.

**device\_wake\_source:** The wake source can be keyscan, quadrature sensor, GPIO, or a combination of those. For example, you may want to use an interrupt from a sensor as a GPIO wake source so that the device wakes whenever new sensor data is available.

```
/** Wake sources */
#define WICED_SLEEP_WAKE_SOURCE_KEYSCAN  (1<<0)  /**< Enable wake from keyscan */
#define WICED_SLEEP_WAKE_SOURCE_QUAD    (1<<1)  /**< Enable wake from quadrature sensor */
#define WICED_SLEEP_WAKE_SOURCE_GPIO    (1<<2)  /**< Enable wake from GPIO */
```

**device\_wake\_gpio\_num:** This entry specifies which GPIO is used to wake the device from sleep. This only applies if *device\_wake\_source* includes GPIO.

**sleep\_permit\_handler:** This element requires you to provide a function pointer for callback function that will be called by the PMU to request sleep permission and when sleep is entered. This function will be described next.

### Sleep Permit Handler Callback Function

The sleep permit handler callback function takes one argument of type *wiced\_sleep\_poll\_type\_t* which specifies the reason for the callback (*WICED\_SLEEP\_POLL\_SLEEP\_PERMISSION* or *WICED\_SLEEP\_POLL\_TIME\_TO\_SLEEP*) and it returns a *uint32\_t*.

For a *WICED\_SLEEP\_POLL\_SLEEP\_PERMISSION* callback, the return value must be one of the following based on the device and the requirements of the firmware:

- *WICED\_SLEEP\_NOT\_ALLOWED* – The application can return this value if it does not want the device to enter Sleep mode.
- *WICED\_SLEEP\_ALLOWED\_WITHOUT\_SHUTDOWN* -The application can return this value if low power is allowed. This will always be the return value for the 20819 when sleep is allowed. For the 20719, this value should be returned if the firmware wishes to allow PDS but not SDS.



- *WICED\_SLEEP\_ALLOWED\_WITH\_SHUTDOWN* – This return value is only used for the 20719. When this value is returned, the device can enter any of the low power modes including SDS.

For a *WICED\_SLEEP\_POLL\_TIME\_TO\_SLEEP* callback, you must return the maximum time that the system should be allowed to sleep. This is typically set to *WICED\_SLEEP\_MAX\_TIME\_TO\_SLEEP* but may also be returned as 0 if you don't want the system to go to sleep at that time. If you want to wake at a specific time, it is better to use a timer. You should not depend on this parameter as a wake source.

Remember that the PMU makes the final decision – it polls the firmware and each peripheral to see which type of sleep is allowed and how long sleep will be possible, and then decides which mode makes sense.

### Connection Parameter Update

The connection interval, latency and timeout are typically chosen by the Central. However, upon a connection, the Peripheral may request to update those values. The Central may or may not agree to the request. To reduce power consumption, it is recommended that the connection interval be set to 100ms or more once a GATT connection is established. In addition, the timeout should be set appropriately based on the connection interval, latency, and other application requirements.

An L2CAP function is used to request new values for the connection interval and timeout. This is done in the GATT connection callback when the connection state is "connected" (i.e. when the connection comes up). The function takes the BD\_ADDR, the min and max intervals in units of 1.25ms, latency in number of connection intervals that can be missed, and the timeout in units of 10ms.

To request new connection parameters, use the following function:

```
wiced_bt_l2cap_update_ble_conn_params (
    wiced_bt_device_address_t rem_bdRa, // BD_ADDR of remote device
    uint16_t min_int, // Min connection interval in units of 1.25ms
    uint16_t max_int, // Max connection interval in units of 1.25ms
    uint16_t latency, // Latency - number of connection intervals
    uint16_t timeout); // Timeout in units of 10ms
```

### Advertising Settings

In ePDS/PDS mode, the device will wake every time a new advertising packet needs to be sent. Therefore, slower advertising will result in lower power. There is also a timer that runs to schedule advertising timeouts, so power will be lower during advertising if the timeout is set to 0 which doesn't require a timer.

### BT Address Settings

There is a timer that is used to track resolvable private addresses (RPA). This will cause the firmware to wake frequently during advertising. Therefore, RPA should not be used in power critical applications.



## Wakeup Events

The firmware may need events that cause it to wake periodically or on specific events. For example, you may need to read a sensor value every few seconds or respond to user input such as a button press.

For periodic wakeup, you can either use a timer or you can use threads with delays that allow the thread to sleep (i.e. ALLOW\_THREAD\_TO\_SLEEP). The device will not enter sleep unless all threads and timers are in a sleep state.

As previously discussed, during sleep configuration the device wake source may be configured. If that source is set to GPIO then the specified GPIO interrupt will wake up the system. However, you will not get a GPIO interrupt handler callback unless you register the callback function using `wiced_hal_gpio_register_pin_for_interrupt`. Note that while the GPIO configuration (set using `wiced_hal_gpio_configure_pin`) is retained during SDS, the callback registration is NOT retained so you need to register the callback during both cold and fast boot.

## Sleep Permission Variable Update (Advanced)(20719 with SDS only)

One or more global variables may be used to keep track of the sleep type allowed. These variables are used in the sleep permit handler callback function to determine what value to return. For example, one possibility would be to:

1. Start out with sleep disabled
2. Allow either PDS or SDS during advertisement
  - a. This depends on how long advertising is expected to last and if it is acceptable to have to send 2 connection requests.
3. Allow only PDS once a GATT connect happens (to allow pairing/encryption)
  - a. Another option is to initiate the pairing request from the device immediately after connection so that the device can go to SDS sooner.
4. Switch between SDS and PDS once encryption of the link has completed (BTM\_ENCRYPTION\_STATUS\_EVT with WICED\_SUCCESS) depending on firmware requirements for activity.

There are other possible flows depending on the firmware's requirements.

If you are not using SDS, then you can always return `WICED_SLEEP_ALLOWED_WITHOUT_SHUTDOWN` from the sleep permit handler callback function for the poll sleep permission case unless your firmware needs to stay awake at certain times for other reasons. In that case, you won't need any sleep permission variables.

## AON Variable Configuration (Advanced)(20719 with SDS only)

During SDS, variables are not retained unless they are stored in Always On (AON) RAM or NVRAM. The AON RAM space is limited to 256 bytes for the user application.

For example, you should store whether the device is connected or not so that when fast boot occurs you will be able to determine if the device was connected when it went to sleep. You may also need to store



the advertising type or sensor values so that you can determine if they have changed from when the device went to sleep (e.g. to determine if a notification should be sent). To store values in AON RAM, use *PLACE\_IN\_ALWAYS\_ON\_RAM* when declaring the variable. For example:

```
PLACE_IN_ALWAYS_ON_RAM uint16_t connection_id;
```



### Determine Boot Type and Perform System Initialization (Advanced)(20719 with SDS only)

The function `wiced_sleep_get_boot_mode` is called in the `application_start` function to determine whether the chip is starting up for the first time (cold boot) or coming out of SDS (fast boot). It returns a variable of type `wiced_sleep_boot_type_t` which can be `WICED_SLEEP_COLD_BOOT` or `WICED_SLEEP_FAST_BOOT`. Settings such as GPIO configuration are retained during SDS so they only need to be configured for a cold boot.

For a fast boot, it is important to check to see if the device was already connected when it went into SDS. If it is already connected, then advertisements should not be started, and you may need to read values from NVRAM or restore GATT array values. Typically, NVRAM is only used if bonding information is being saved. If not, you can store GATT array values that need to be saved during SDS in AON RAM.

#### Timed-Wake and HID-Off Configuration

There is a single API function called `wiced_sleep_enter_hid_off` that is used to enter either Timed-Wake or HID-Off modes. This function should only be called when there is no Bluetooth activity. The function prototype is:

```
wiced_result_t wiced_sleep_enter_hid_off( uint32_t wakeup_time,
                                         uint32_t wake_gpio_pin,
                                         wiced_sleep_wake_type_t wake_active_mode );
```

The arguments are:

- `wakeup_time`: Wakeup time in milliseconds. Set this parameter to 0 if the application only wants to wake on a GPIO.
- `wake_gpio_pin`: The LHL pin used to wake the device. This should be set to `WICED_HAL_GPIO_PIN_UNUSED` if the application only wants to wake at a specified time.
- `wake_active_mode`: The polarity of the GPIO. This can be either `WICED_GPIO_ACTIVE_HIGH` or `WICED_GPIO_ACTIVE_LOW`.

#### 4C.1.3 Programming in Low Power Mode

When the device is asleep it is not listening for HCI commands which are needed to get the device in the correct mode for programming, so it may be difficult to program new firmware. To circumvent this issue, the kit has a "recovery" mode. To enter recovery mode:

- a. Press and hold the recovery button on the base board (left button)
- b. Press and release the reset button (center button)
- c. Release the recovery button
- d. Program as normal



## 4C.2 Advertising Packets

There are two main uses of the advertising packet:

- Identifying a Peripheral with some recognizable data so that a Central knows if it wants to connect and talk to it.
- Sending out data (e.g. beacon data).

### 4C.2.1 Using the Advertising Packet to Get Connected

If you turn on the CySmart scanner, you will find that there are likely a bunch of unknown devices that are advertising around you. For instance, as I sit here right now I can see that there are quite a few Bluetooth LE devices around me that I have no idea what they are.

BLE Devices																															
Pull down to refresh...																															
<table border="1"><thead><tr><th>Unknown Peripheral</th><th>RSSI</th></tr></thead><tbody><tr><td>No Services</td><td>-71 dBm</td></tr><tr><td>ARHMBLaaptop</td><td>RSSI</td></tr><tr><td>No Services</td><td>-89 dBm</td></tr><tr><td>Switch-091799</td><td>RSSI</td></tr><tr><td>1 Service Advertised</td><td>-81 dBm</td></tr><tr><td>Unknown Peripheral</td><td>RSSI</td></tr><tr><td>No Services</td><td>-92 dBm</td></tr><tr><td>Living Room</td><td>RSSI</td></tr><tr><td>No Services</td><td>-69 dBm</td></tr><tr><td>Nest Cam</td><td>RSSI</td></tr><tr><td>1 Service Advertised</td><td>-92 dBm</td></tr><tr><td>iHome iWBT400 app</td><td>RSSI</td></tr><tr><td>1 Service Advertised</td><td>-76 dBm</td></tr><tr><td>N04NK</td><td>RSSI</td></tr></tbody></table>		Unknown Peripheral	RSSI	No Services	-71 dBm	ARHMBLaaptop	RSSI	No Services	-89 dBm	Switch-091799	RSSI	1 Service Advertised	-81 dBm	Unknown Peripheral	RSSI	No Services	-92 dBm	Living Room	RSSI	No Services	-69 dBm	Nest Cam	RSSI	1 Service Advertised	-92 dBm	iHome iWBT400 app	RSSI	1 Service Advertised	-76 dBm	N04NK	RSSI
Unknown Peripheral	RSSI																														
No Services	-71 dBm																														
ARHMBLaaptop	RSSI																														
No Services	-89 dBm																														
Switch-091799	RSSI																														
1 Service Advertised	-81 dBm																														
Unknown Peripheral	RSSI																														
No Services	-92 dBm																														
Living Room	RSSI																														
No Services	-69 dBm																														
Nest Cam	RSSI																														
1 Service Advertised	-92 dBm																														
iHome iWBT400 app	RSSI																														
1 Service Advertised	-76 dBm																														
N04NK	RSSI																														

When a Central wants to connect to a Peripheral, how does it know what Peripheral to talk to? There are two answers to that question.

First, it may advertise a service that the Central knows about (because it is defined by the Bluetooth SIG or is custom to your company). As we talked in the previous chapter you can customize the Advertising packet with information. In the picture above, you can see that some of the devices are advertising that they support 1 service. To do that they add a field of one of these types to the advertising packet along with the UUID of the Service:

```
BTM_BLE_ADVERT_TYPE_16SRV_PARTIAL      = 0x02,          /*< List of supported services - 16 bit UUIDs (partial)
BTM_BLE_ADVERT_TYPE_16SRV_COMPLETE      = 0x03,          /*< List of supported services - 16 bit UUIDs (complete)
BTM_BLE_ADVERT_TYPE_32SRV_PARTIAL       = 0x04,          /*< List of supported services - 32 bit UUIDs (partial)
BTM_BLE_ADVERT_TYPE_32SRV_COMPLETE      = 0x05,          /*< List of supported services - 32 bit UUIDs (complete)
BTM_BLE_ADVERT_TYPE_128SRV_PARTIAL      = 0x06,          /*< List of supported services - 128 bit UUIDs (partial)
BTM_BLE_ADVERT_TYPE_128SRV_COMPLETE     = 0x07,          /*< List of supported services - 128 bit UUIDs (complete)
```



The other scheme that is commonly used is to advertise "Manufacturer's Specific Data". This data has two parts:

- A two-byte manufacturer code as specified by the Bluetooth SIG (e.g. Cypress = 0x0131).
- The actual data which is typically a Product ID that is unique for each product that the company makes.

The way that this works is that you would write a Central application that has a table of known Peripheral Product IDs that it knows how to talk to. Then the Peripherals would advertise their Manufacturer code and Product ID in the Manufacturers Data Field. When a Central sees something that it knows how to talk to, it can make the connection.

#### 4C.2.2 Beacons

BLE Beacons are devices that are intended to send out data using advertising packets. Often, they will allow connections for configuration of the beacon but not for normal use.

Beacons can be used for lots of different purposes such as providing location (especially in large indoor spaces without GPS coverage (like Shinjuku station in Tokyo - <https://allabout-japan.com/en/article/2074>), or links to web sites with geographically relevant information (like a website with sale information for a store that you are currently standing in).

There are (of course) two popular types of beacon: iBeacon, which is defined by Apple, and Eddystone which is defined by Google. Each of these will be discussed in a minute.

#### Multi-Advertisement

Beacons can send out multiple advertisement packets to provide different types of data simultaneously. In many cases, a beacon may send out both iBeacon and Eddystone advertisement packets so that it will appear as both types of beacon. Each advertising instance can have unique parameters if desired.

To do multiple advertisements, you use the following three functions. The functions are all linked to each other using a parameter called "adv\_instance". This can be any integer from 1 to 16 that uniquely identifies each advertising instance.

#### wiced\_set\_multi\_advertisement\_params

This function sets advertisement parameters for each instance such as advertising type, advertising interval, advertising address (if a unique address is desired), etc. Its arguments are:

- advertising\_interval\_min      Same as for standard advertising
- advertising\_interval\_max      Same as for standard advertising
- advertising\_type                Same as for standard advertising
- own\_address\_type              Type of address for this advertising instance – see wiced\_bt\_ble\_address\_type\_t
- own\_address                    Address if unique for this instance (otherwise use NULL)
- peer\_address\_type             Type of address for the peer (only for directed adv)



- peer\_address Address if unique for this instance (otherwise use NULL)
- advertising\_channel\_map List of advertising channels to use (can use 37, 38, 39, or a combination)
- advertising\_filter\_policy Filter policy – see wiced\_bt\_ble\_advert\_filter\_policy\_t
- adv\_instance A unique number used by wiced\_start\_multi\_advertisements
- transmit\_power Transmit power in dB - can use MULTI\_ADV\_TX\_POWER\_MIN or MULTI\_ADV\_TX\_POWER\_MAX

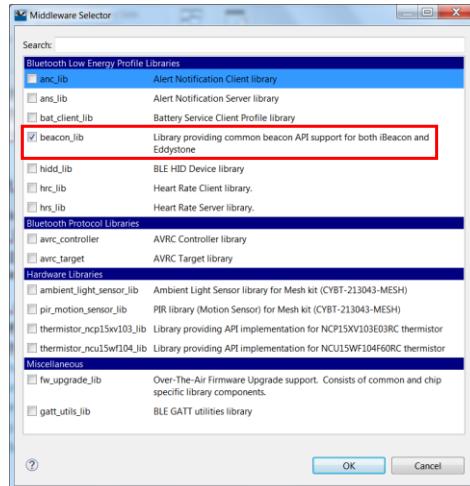
#### wiced\_set\_multi\_advertisement\_data

This function sets advertisement data for multi-advertisement packets. It is analogous to `wiced_bt_ble_set_raw_advertisement_data` but the advertising data is sent as a flat array instead of a structure of advertising elements. Therefore, the procedure to setup the advertising packet will be a bit different as you will see in the exercises. Its arguments are:

- p\_data Pointer to an advertising data array
- data\_len Length of the advertising data array
- adv\_instance Number of the instance specified above

The Bluetooth SDK includes a middleware library called `beacon.lib` that includes a number of functions to help format packets correctly before calling `wiced_set_multi_advertisement_data()`. To create an Eddystone UID (described later) packet, for example, you would use the `wiced_bt_eddystone_set_data_for_url()` function from this library.

To add the library to your application, right-click on the project name and select ModusToolbox Middleware selector or click on "Select Middleware" from the Quick Panel. In the dialog, you simply select the desired library and press OK. The library is added to the project under the libraries folder.





### wiced\_start\_multi\_advertisements

This function starts advertisements using the parameters specified above. It is analogous to wiced\_bt\_start\_advertisements. Its arguments are:

- advertising\_enable                           MULTI\_ADVERT\_START or MULTI\_ADVERT\_STOP
- adv\_instance                                  Number of the instance specified above

### iBeacon

iBeacon is an Advertising Packet format defined by Apple. The iBeacon information is embedded in the Manufacturer section of the advertising packet. It simply contains:

- Apple's manufacturing ID
- Beacon type (2-bytes)
- Proximity UUID (16-bytes)
- Major number (2-bytes)
- Minor number (2-bytes)
- Measured Power (1-bytes)

Because the packet uses the Apple company ID you need to register with Apple to use iBeacon.

The measured power allows you to calibrate each iBeacon as you install it so that it can be used for indoor location measurement.

### Eddystone

You will use this in [Exercise 4C.2](#) and [Exercise 4C.3](#).

Eddystone is a Google protocol specification that defines a Bluetooth low energy (BLE) Advertising message format for proximity beacon messages. It describes several different frame types that may be used individually or in combinations to create beacons that can be used for a variety of applications.

There are currently four types of Eddystone Frames:

- UID – A unique beacon ID for use in mapping functions
- URL – An HTTP URL in a compressed format
- TLM – Telemetry information about the beacon such as battery voltage, device temperature, counts of packet broadcasts
- EID – Ephemeral ID packets which broadcast a randomly changing number

TLM frames do not show up as a separate beacon but rather are associated with other frames from the same device. For example, you may have a beacon that broadcasts UID frames, URL frames, and TLM frames. In a beacon scanner, that will appear as a UID&TLM beacon and a URL&TLM beacon.



The Advertising Packet has the following fields:

- Flags
  - Type: *BTM\_BLE\_ADVERT\_TYPE\_FLAG* (0x01)
  - Value: *BTM\_BLE\_GENERAL\_DISCOVERABLE\_FLAG* / *BTM\_BLE\_BREDR\_NOT\_SUPPORTED*
- 16-bit Eddystone Service UUID
  - Type: *BTM\_BLE\_ADVERT\_TYPE\_16SRV\_COMPLETE* (0x03)
  - Value: 0xFEAA
- Service Data
  - Type: *BTM\_BLE\_ADVERT\_TYPE\_SERVICE\_DATA* (0x16)
  - Value: The Eddystone Service UUID (0xFEAA), the Eddystone frame type, then the actual data. Frame types are:
    - UID – 0x00
    - URL – 0x10
    - TLM – 0x20
    - EID – 0x30

The data required depends on the frame type. For example, a UID frame has: 1 byte of Tx power of the beacon at 0 m and a 16-byte beacon ID consisting of 10-byte namespace, and 6-byte instance.

In the project `snip.ble.eddystone` there is an example of this type of beacon. The example uses multi-advertising so that it will appear as multiple beacons at once on different advertising channels. One beacon sends UID frames, one sends URL frames, and one sends EID frames (there is an option to send TLM frames as well). This is useful if you want to send multiple types of data at once. It is also useful if you want a single device to operate as both an iBeacon and an Eddystone beacon at the same time.

If you are using Eddystone to send a URL, it is limited to 15 characters excluding a prefix (`http://`, `https://`, `http://www.`, or `https://www.`) and a suffix (`.com`, `.com/`, `.org`, `.org/`, `.edu`, `.edu/`, etc.). If you need to create a shorter URL for a site, use a web browser to go to <https://goo.gl>. That site will allow you to create a short URL.

You can find the detailed spec at <https://github.com/google/eddystone>.

Note, there is a middleware library of Eddystone helper functions that can be accessed by including "beacon\_lib" in your application. Once the middleware library is added, you also need to include "wiced\_bt\_beacon.h" in your application.



### 4C.3 Scan Response Packets

You will use this in [Exercise 4C.4](#)

Once a Central finds a Peripheral and wants to know more about it, the Central can look for scan response data. For a peripheral, the scan response packet looks just like an advertising packet except that the Flags field is not required. Like the advertising packet, the scan response packet is limited to 31 bytes.

In WICED, you set up the scan response packet array of advertising elements the same way as you do for the advertising packet. You then call the function `wiced_bt_ble_set_raw_scan_response_data` to pass that information to the Stack. That function takes the same arguments as `wiced_bt_ble_set_raw_advertisement_data` – that is, the number of advertising elements in the array, and a pointer to the array.

When you start advertising with an advertising type other than `_NONCONN_` then the Central will be able to read your scan response data. For example, `_DISCOVERABLE_` will allow the scan response to be read but will not allow connections and `_UNDIRECTED_` will allow the scan response to be read and will allow connections.



## 4C.4 OTA (Over the Air) Upgrade

### 4C.4.1 Introduction

The firmware upgrade feature allows an external device to use the Bluetooth link to transfer and install a newer firmware version to devices that support OTA. This section describes the functionality of the Firmware Upgrade library used in various sample applications.

For 20819 devices, there may not enough on-chip flash to fit two copies of the application firmware that are required during OTA, so it is sometimes required to have external flash. In that case, the OTA process uses the external flash during OTA.

The library is split into two parts. The over the air (OTA) firmware upgrade module of the library provides a simple implementation of the GATT procedures to interact with the device performing the upgrade. The firmware upgrade HAL module of the library provides support for storing data in the non-volatile memory and switching the device to use the new firmware when the upgrade is completed. The embedded application may use the OTA module functions (which in turn use the HAL module functions), or the application may choose to use the HAL module functions directly.

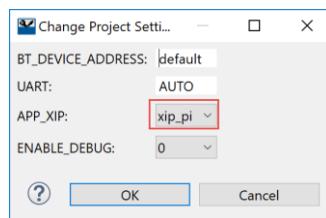
The library contains functionality to support secure and non-secure versions of the upgrade. In the non-secure version, a simple CRC32 verification is performed to validate that all bytes that have been sent from the device performing the upgrade are correctly saved in the serial flash of the device. The secure version of the upgrade validates that the image is correctly signed and has correct production information in the header. This ensures that unknown firmware is not uploaded to your device.



#### 4C.4.2 Design and Architecture

##### Position Independent Applications

If there is enough space in the flash memory to both the old and new application, then the APP\_XIP option should be set to "xip\_pi". This means that the application is built to be "position independent". This allows the new application to be loaded into a different area in flash than the old application as explained below.



In the case of xip\_pi, the flash memory is organized into two partitions for the failsafe upgrade capability. During the startup operation the boot code of the chip checks the first partition and if a valid image is found, assumes that the first partition is active and then starts executing the code in the first partition. If the first partition does not contain a valid image, the boot code checks the second partition and then starts execution of the code in the second partition if a valid image is found there. If neither partition is valid, the boot code enters download mode and waits for the code to be downloaded over HCI UART. The addresses of the partitions are programmed in a file with extension "btp" located in the platform directory of the SDK.

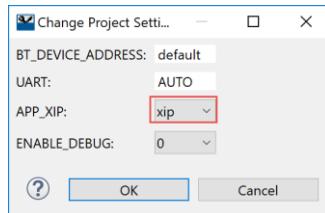
The firmware upgrade process stores received data in the inactive partition. When the download procedure is completed and the received image is verified and activated, the currently active partition is invalidated, and then the chip is restarted. After the chip reboots, the previously inactive partition becomes active. If for some reason the download or the verification step is interrupted, the valid partition remains valid and the chip is not restarted. This guarantees the failsafe procedure.

During an OTA upgrade the device performing the procedure (Downloader) pushes chunks of the new image to the device being upgraded. The embedded application receives the image and stores it in the external or on-chip flash. When all the data has been transferred, the Downloader sends a command to verify the image and passes a 32-bit CRC checksum. The embedded app reads the image from the flash and verifies the image as follows. For the non-secure download, the library calculates the CRC and verifies that it matches received CRC. For the secure download case, the library performs ECDSA verification and verifies that the Product Information stored in the new image is consistent with the Product Information of the firmware currently being executed on the device. If verification succeeds, the embedded application invalidates the active partition and restarts the chip. The simple CRC check can be easily replaced with crypto signature verification if desired, without changing the download algorithm described in this document.



### Non-Position Independent Applications

If on-chip flash is used for the application but the old and new applications can't both fit in the on-chip flash simultaneously, then it is necessary to use external flash temporarily during OTA upgrade to store the new image. In this case, the application is built to go in a specific location by setting the APP\_XIP option to "xip".



The new application is stored in external flash during OTA upgrade. Once the new application is validated, it is copied into internal flash thereby replacing the old application.

### OTA Support Plan

Support for OTA on the 20819 is still evolving. The state of things as it stands and the plan of record for the 20819 device is:

BT_20819A1 SDK Version	XIP Support	XIP_PI Support
1.0	No	Yes (only if optional patch libs not used)
1.1	Yes	Yes (only if optional patch libs not used)
1.2	Yes	No
1.3	Yes	Yes



#### 4C.4.3 Applications for Loading New Firmware

The ModusToolbox installation contains two peer applications that can be used to transmit new firmware over BLE – one for Android and one for Windows. The source code and pre-compiled executables (.apk for Android and .exe for Windows) are provided for both applications. The Windows executable is provided for 32-bit (x86) and 64-bit (x64) architectures but it will only work on Windows 10 or later since BLE is not natively supported in earlier versions.

These peer applications can be found in the ModusToolbox installation folder (the default install folder in Windows is C:\Users\<user\_name>\ModusToolbox\_1.1) at:

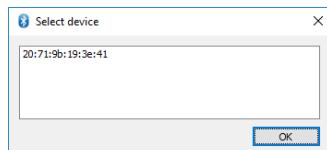
```
libraries\bt_20819A1-1.0\components\BT-SDK\common\peer_apps\ota_firmware_upgrade\Windows\WsOtaUpgrade\Release  
libraries\bt_20819A1-1.0\components\BT-SDK\common\peer_apps\ota_firmware_upgrade\Android\LeOTAAppl\app\build\outputs\apk
```

##### Windows

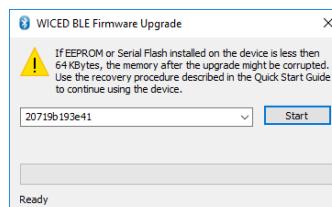
To use the Windows peer application, you must first copy the \*.bin file from the Debug directory of the WICED application into the same folder as the Windows peer application. Then run the application with the \*.bin file provided as an argument. For example, from a command or PowerShell window:

```
.\WsOtaUpgrade.exe ex05_ota- mainapp_download.ota.bin
```

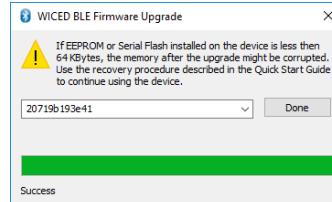
You will get a window that looks like the following. Select the device you want to update and click "OK".



On the next window, verify that the device type is correct and click "Start".



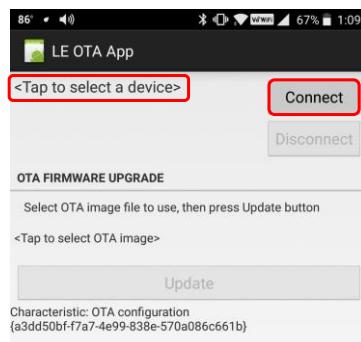
If the update worked, the window will show "Success" at the bottom. Click "Done" to close the window.



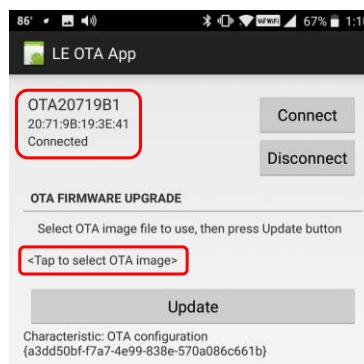
### Android

To use the Android app:

1. Install the app-debug.apk file on your Android device if you have not already done so.
2. Copy the \*.bin file from the Debug directory onto the device in a location where you can find it.
3. Run the app called *LE OTA App*. The startup screen will look like this:

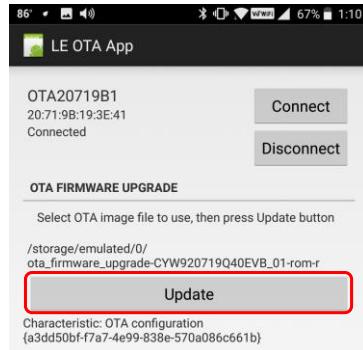


4. Tap where it says <Tap to select a device> and choose your device from the list.
5. Tap on the "Connect" button. Once connected, the screen will look like this:

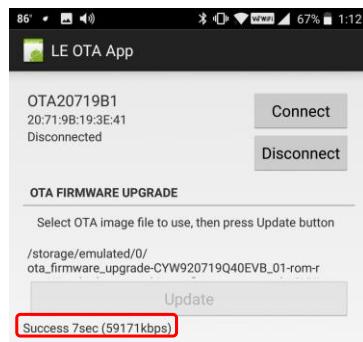




6. Tap where it says <Tap to select OTA Image>, navigate to where you saved the \*.bin file on your device and select it. Once the file is selected, the screen will look like this:



7. Tap the Update button. Once the update is done, you should see "Success" at the bottom of the screen. Disconnect from the device and close the app.





#### 4C.4.4 OTA Firmware

You will use this in [Exercise 4C.5](#)

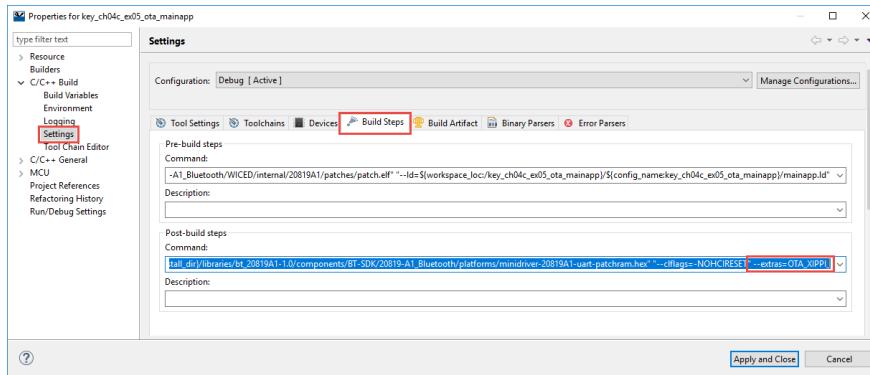
In the firmware, OTA requires the following:

##### Modus.mk

The modus.mk file used to create the application must have the following line in order to setup the proper build settings:

```
DOTA_FW_UPGRADE=1
```

Note: what this does it to modify the project build settings post-build steps command. The difference is shown below.

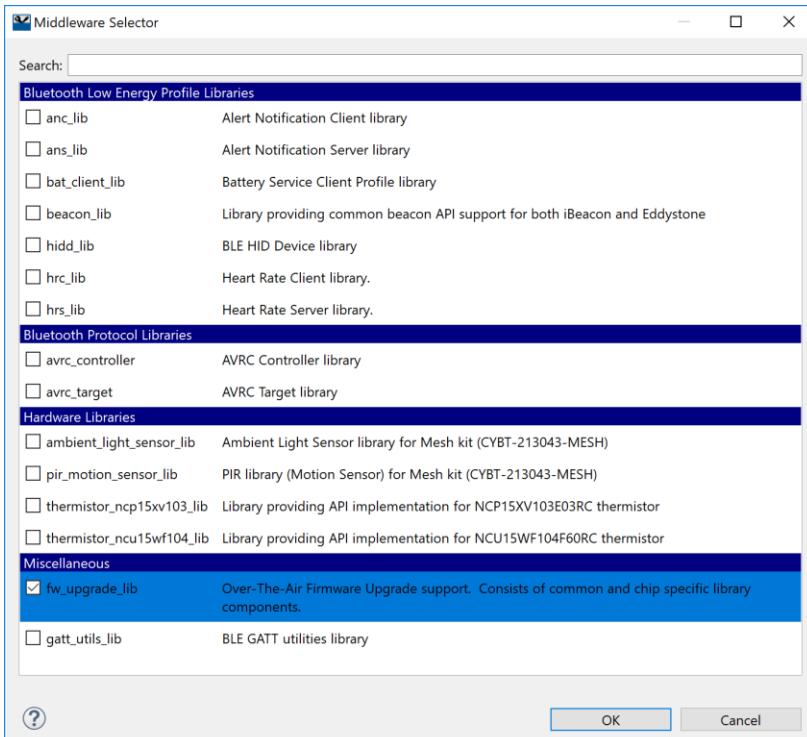


This setting is what causes the OTA .bin file to be generated by the build. That's the file that you will send over the air to update the firmware.



## Library

To get the OTA library included in the project, run the Middleware Selector and add the fw\_upgrade\_lib to the application.



Once that's done, include the following header files at the top of your main .c file:

```
#include "wiced_bt_ota_firmware_upgrade.h"
```



## BLE OTA Service (Non-Secure)

The GATT database must have a Primary Service for OTA. This is a custom Service that is defined by Cypress with two Characteristics, one of which has a CCCD. You must add the OTA Service to your device with the correct names and UUIDs for the Service and the Characteristics as shown below.

Name	Value
Service properties	
UUID	AE5D1E47-5C13-43A0-8635-82AD38A1381F
General	
Service declaration	Primary
Included Services	
Modus	

The UUID for the Service must match exactly those shown in the figure above because that is the Service UUID that has been chosen by Cypress. In addition, the name must match exactly for our template firmware to work. The values (for easy copy/paste) are:

- Service Name: OTA\_FW\_UPGRADE
- Service UUID: AE5D1E47-5C13-43A0-8635-82AD38A1381F

The 128-bit UUID for the Service can be found in the SDK file wiced\_bt\_ota\_firmware\_upgrade.h. Note that the values are reversed because the values are specified little endian in the code.

```
#define UUID_OTA_FW_UPGRADE_SERVICE 0x1f, 0x38, 0xa1, 0x38, 0xad, 0x82,  
0x35, 0x86, 0xa0, 0x43, 0x13, 0x5c,  
0x47, 0x1e, 0x5d, 0xae
```



The configurations for the OTA Service Characteristics are shown below. Note that we have turned on Variable Length in both characteristics and have left the name and value fields unchanged. This is because the OTA update service uses the GATT connection to send data, but it isn't actually stored in the GATT database – it is consumed directly by the OTA library functions.

GATT	
Server	
Generic Access	Characteristic properties
Device Name	UUID A3DD50BF-F7A7-4E99-838E-570A086C661B
Appearance	
Generic Attribute	
Modus	Fields
Counter	New field
Client Characteristic Configuration	Name New field
Characteristic User Description	Value
OTA_FW_UPGRADE	Format utf8s
CONTROL_POINT	Length 0
Client Characteristic Configuration	
DATA	
	Properties
	Read <input type="checkbox"/>
	Write <input checked="" type="checkbox"/>
	WriteWithoutResponse <input type="checkbox"/>
	Signed Write <input type="checkbox"/>
	Reliable Write <input type="checkbox"/>
	Notify <input checked="" type="checkbox"/>
	Indicate <input checked="" type="checkbox"/>
	Writable Auxiliaries <input type="checkbox"/>
	Broadcast <input type="checkbox"/>
	Permission
	Write
	Variable Length <input checked="" type="checkbox"/>
	Write <input checked="" type="checkbox"/>

The values shown above are:

- Name: CONTROL\_POINT
- UUID: A3DD50BF-F7A7-4E99-838E-570A086C661B

GATT	
Server	
Generic Access	Characteristic properties
Device Name	UUID A2E86C7A-D961-4091-B74F-2409E72EFE26
Appearance	
Generic Attribute	
Modus	Fields
Counter	New field
Client Characteristic Configuration	Name New field
Characteristic User Description	Value
OTA_FW_UPGRADE	Format utf8s
CONTROL_POINT	Length 0
Client Characteristic Configuration	
DATA	
	Properties
	Read <input type="checkbox"/>
	Write <input checked="" type="checkbox"/>
	WriteWithoutResponse <input type="checkbox"/>
	Signed Write <input type="checkbox"/>
	Reliable Write <input type="checkbox"/>
	Notify <input type="checkbox"/>
	Indicate <input type="checkbox"/>
	Writable Auxiliaries <input type="checkbox"/>
	Broadcast <input type="checkbox"/>
	Permission
	Write
	Variable Length <input checked="" type="checkbox"/>
	Write <input checked="" type="checkbox"/>

The values shown above are:

- Name: DATA
- UUID: A2E86C7A-D961-4091-B74F-2409E72EFE26



The Control Point Characteristic has Notify and Indicate enabled so it needs a CCCD. For the CCCD, we turned off "Write (authenticated)" so that OTA can be done without pairing first. If you want to require pairing before allowing OTA, then enable that check box. In that case, you would ideally want to enable Write (authenticated) for the two characteristics as well but that can't currently be done in the configurator.

Name	Value
<b>Descriptor properties</b>	
UUID	2902
Description	The Client Characteristic Configuration descriptor defines how the characteristic may be configured by a specific client.
<b>Fields</b>	
<b>Properties</b>	
Format	16bit
<b>BitField</b>	
Item 0	Notifications disabled
Item 1	Indications disabled
<b>Permission</b>	
<b>Read</b>	
Read	<input checked="" type="checkbox"/>
Read (authenticated)	<input type="checkbox"/>
<b>Write</b>	
Variable Length	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>
Write (no response)	<input type="checkbox"/>
<b>Write (authenticated)</b>	<input checked="" type="checkbox"/>
Write (reliable)	<input type="checkbox"/>

Currently the library expects names for the handles that cannot be created by the configurator due to naming conventions. Therefore, it is necessary to do a bit of hacking once you save the Configurator setup to get it to work properly. The steps are:

1. Open the file cycfg\_gatt\_db.h from the GeneratedSource folder.
  2. Add the following include at the top of the file:
- ```
#include "wiced_bt_ota_firmware_upgrade.h"
```
3. Replace the lines that define the handles for the OTA service and characteristics with the following. This just maps the handle names to the ones used in the OTA library functions.

```
/* Service OTA FW UPGRADE */
#define HDS_OTA_FW_UPGRADE
/* Characteristic CONTROL_POINT */
#define HDLC_OTA_FW_UPGRADE_CONTROL_POINT
#define HDLC_OTA_FW_UPGRADE_CONTROL_POINT_VALUE
/* Descriptor Client Characteristic Configuration */
#define HDLD_OTA_FW_UPGRADE_CONTROL_POINT_CLIENT_CHAR_CONFIG
/* Characteristic DATA */
#define HDLC_OTA_FW_UPGRADE_DATA
#define HDLC_OTA_FW_UPGRADE_DATA_VALUE
HANDLE_OTA_FW_UPGRADE_SERVICE
HANDLE_OTA_FW_UPGRADE_CHARACTERISTIC_CONTROL_POINT
HANDLE_OTA_FW_UPGRADE_CONTROL_POINT_
HANDLE_OTA_FW_UPGRADE_CLIENT_CONFIGURATION_DESCRIPTOR
HANDLE_OTA_FW_UPGRADE_CHARACTERISTIC_DATA
HANDLE_OTA_FW_UPGRADE_DATA
```

Remember, this file will be overridden if you update anything in the Bluetooth Configurator so be careful!



## Initialization

During the application initialization (typically just after initializing the GATT database with `wiced_bt_gatt_db_init`), the following function call must be made:

```
/* Initialize OTA (non-secure) */
wiced_ota_fw_upgrade_init(NULL, NULL, NULL);
```

## GATT Connect Event

In the GATT connection status event, it is necessary to pass the connection status information to the OTA library by calling the following (`conn` is a pointer of type `wiced_bt_gatt_connection_status_t` to the event connection status).

```
wiced_ota_fw_upgrade_connection_status_event(p_conn);
```

This should be called on both a connection and disconnection.

## GATT Attribute Request Event

Several of the `GATT_ATTRIBUTE_REQUEST_EVT` events - namely `GATTS_REQ_TYPE_READ`, `GATTS_REQ_TYPE_WRITE`, `GATTS_REQ_TYPE_PREP_WRITE` and `GATTS_REQ_TYPE_CONF` - must call the appropriate OTA function. Note that OTA has its own library functions to handle these events, so they must be called for OTA events instead of the normal application code that is called for normal application functionality.

Namely the following functions must be called:

For `GATTS_REQ_TYPE_READ` to a handle for one of the OTA characteristics or descriptors:

```
result = wiced_ota_fw_upgrade_read_handler(p_attr->conn_id, &(p_attr->data.read_req));
```

For `GATTS_REQ_TYPE_WRITE` or `GATTS_REQ_TYPE_PREP_WRITE` to a handle for one of the OTA characteristics or descriptors:

```
result = wiced_ota_fw_upgrade_write_handler(p_attr->conn_id, &(p_attr->data.write_req));
```

For `GATTS_REQ_TYPE_CONF` to a handle for one of the OTA characteristics or descriptors:

```
result = wiced_ota_fw_upgrade_indication_cfm_handler(p_attr->conn_id, p_attr->data.handle);
```

This functionality has already been added for you in the template. Review the `GATT_ATTRIBUTE_REQUEST_EVT` case to understand what was added.

In addition, code has been added to the read condition to handle reads of the device name and appearance characteristics.



## Buffer Pool Sizes

The large buffer pool must be at least the max MTU size plus 12. Both are defined in `app_bt_cfg.c`. Verify that the buffer pools are large enough in your application.

## Disabling of PUART

For some reason, the PUART sometimes interferes with the OTA process when using the Windows peer app and may cause the update to fail. If this is the case, you can disable the debug UART in the GATT write handler before calling the OTA library write handler function. The code in the template contains that line of code but you can comment it out if you want to see additional debug messages during OTA.

## XIP for Large Applications

If your application is too large to use position independent mapping (i.e. if it used more than  $\frac{1}{2}$  of the internal flash) the following must also be done to perform OTA upgrade using external flash with a non-position independent application.

Open the application settings and change:

- a. APP\_XIP: xip
- b. OTA\_FW\_UPGRADE: 1
- c. OTA\_UPGRADE\_STORE: external\_flash

Note: the above options will likely change in BT SDK 1.3.



#### 4C.4.5 Secure OTA

You will use this in [Exercise 4C.6](#)

To use secure OTA firmware upgrade, we must create a key pair (public/private) and make a few changes in the firmware. The changes are shown in detail below.

##### BLE OTA Service (Secure)

In the OTA BLE Service description in the GATT database, change the UUID for the service to the UUID for secure OTA. The UUID is:

Secure OTA Service: C7261110-F425-447A-A1BD-9D7246768BD8

The Characteristic UUIDs remain unchanged.

Note: remember that if you use the Bluetooth Configurator to make the change above it will overwrite the changes you made earlier for the handle names.

##### Key Generation

Tools are provided in the WICED SDK to create, sign, and verify random keys. Executables for Windows can be found in:

<ModusToolbox\_Insall\_Dir>/tools/wiced-tools-1.0/BT/ecdsa256/bin

The steps are:

1. Double-click on ecdsa\_genkey.exe from Windows explorer to run the program. This will generate random keys. Note that if you re-run the program, it will overwrite any existing key files. The files created are:
  - a. ecdsa256\_key.pri.bin
  - b. ecdsa256\_key.pub.bin
  - c. ecdsa256\_key\_plus.pub.bin
  - d. ecdsa256\_pub.c
2. Copy the file ecdsa256\_pub.c to the application folder.
  - a. Note: You may want to add it to the CY\_APP\_SOURCE list in the modus.mk file to keep it synchronized for command line operation.
3. The OTA file will be signed once it is generated below.



## Header files and Global Variables

Add the following header files to the main application C file:

```
#include "bt_types.h"
#include "p_256_multprecision.h"
#include "p_256_ecc_pp.h"
```

Add an external global variable declaration of type "Point" for the public key that is defined in ecdsa256\_pub.c. For example:

```
extern Point ecdsa256_public_key;
```

## Initialization

In the firmware initialization section, change the first argument to the OTA init function from NULL to a pointer to a public key that was generated earlier. For example:

```
/* Initialize OTA (secure) */
wiced_ota_fw_upgrade_init(&ecdsa256_public_key, NULL, NULL);
```

## Build Firmware and Sign OTA Image

After building the firmware as usual, follow these steps to convert the output file to a signed output file:

1. Once the firmware is built, copy the bin file from the Debug folder for the application to the <ModusToolbox\_Install\_Dir>/tools/wiced-tools-1.0/BT/ecdsa256/bin folder.
2. Open a command terminal or power shell window (shift-right-click in the folder from Windows explorer) and enter the command:

```
.\ecdsa_sign.exe .\mainapp_download.ota.bin
```

This will produce a file called mainapp\_download.ota.bin.signed.

3. Load the signed file into the device using the preferred OTA tool (i.e. Windows or Android).



## 4C.5 Exercises

### Exercise 4C.1 BLE Low Power (ePDS)

#### Introduction

In this exercise, you will program and analyze a project that implements low power using ePDS. The project is based on the exercise that stores BLE bonding information in NVRAM (ch04b/ex03\_bond). This material is covered in [4C.1](#).

#### Project Creation

1. Use the template in folder “templates/CYW920819EVB/ch04c\_ex01\_lp” to create a project called **ch04c\_ex01\_lp**.
2. Launch the Change Applications Settings dialog and set BT\_DEVICE\_ADDRESS = random.
3. Open the Device and Bluetooth configurators, change the name of the device to *<init>\_lp*, then save and close the configurators.
4. Review the file app.c to familiarize yourself with the way sleep is configured.

**Commented [GL1]:** Maybe we should have them do the sleep configuration and write the callback function?

#### Testing

1. Program the project onto the kit.
  - a. Hint: If your device is in low power mode you will have to put it into Recovery mode first to program it. To enter Recovery mode:
    - i. Press and hold the recovery button on the base board (left button)
    - ii. Press and release the reset button (center button)
    - iii. Release the recovery button
2. Open a UART terminal window. This will allow you to see sleep events and to determine how often the device wakes up and goes back to sleep during different operations.
  - a. Hint: You may see strange (non-ASCII) characters in the UART window when the device wakes from sleep. This is because the PUART was left active during ePDS. If the debug print was removed from the low power sleep callback function, you would not see these characters. In a real-life low power application, the PUART would not be left active but we want to see what's going on.
3. Open the PC CySmart app. Start scanning and then stop once your device appears.
4. Observe the UART while the device is in high duty cycle and low duty cycle advertising.
5. Connect to the device in CySmart. You will see a notification asking to confirm the connection parameters. Select ‘Yes’.
6. Observe the UART once the connection is established.
7. Discover all attributes in the GATT database, and Pair with the device.
  - a. Hint: attribute discovery and paring will take longer (~5 to 10 sec) since they each take multiple wakeup cycles to complete.
8. Observe the UART when pairing completes.
9. Enable all notifications.
10. Press and release the button repeatedly so that notifications are sent.



11. Observe the UART while notifications are being sent.
12. Disconnect and clear the Device Information from the Device List in CySmart.

#### Questions

1. Which lines in the code are used to configure and initialize sleep?
2. When in the code is sleep configured (i.e. after which event)?
3. What is used as a wakeup source?
4. What is the name of the sleep permit handler function?
5. When are the connection interval min, max, latency, and timeout values updated in the code and what values are used?



## Exercise 4C.2 (Advanced) Eddystone URL Beacon

### Introduction

In this exercise, you will create an Eddystone beacon that will advertise the URL for <https://www.cypress.com>. From your phone you will be able to scan for the beacon (using a beacon scanner app) and then directly connect to the advertised website. This material is covered in Eddystone.

### Project Creation

1. Create a new application called **ch04b\_ex02\_eddy** using the modus.mk file in templates/CYW920819EVB/ch04b\_ex02\_eddy. This is a very simple application with no GATT support. All it does is advertise.
2. The beacon\_lib library is already added as middleware and wiced\_bt\_beacon.h is included in app.c in the template.
3. Launch the Change Applications Settings dialog and set BT\_DEVICE\_ADDRESS = random.
4. In app\_set\_advertisement\_data() create an advertising packet with three elements.
  - a. BTM\_BLE\_ADVERT\_TYPE\_FLAG
    - i. This is the same element you have used in chapter 4A.
  - b. BTM\_BLE\_ADVERT\_TYPE\_16SRV\_COMPLETE
    - i. Two-byte Eddystone Service UUID (0xFEAA). Note that this is little-endian so the LSB must be the first element in the array.
  - c. BTM\_BLE\_ADVERT\_TYPE\_SERVICE\_DATA
    - i. Eddystone Service UUID (again little-endian).
    - ii. Eddystone frame type for URL (see EDDYSTONE\_FRAME\_TYPE\_URL in wiced\_bt\_beacon.h).
    - iii. Transmit power (use 0xFO)
    - iv. URL Scheme Prefix (see EDDYSTONE\_URL\_SCHEME\_1 in wiced\_bt\_beacon.h)
    - v. Data (the URL itself as a list of characters)
      1. Hint: 'c', 'y', 'p', 'r', 'e', 's', 's'
    - vi. Eddystone suffix for .com (see the Eddystone website).
5. In app\_bt\_cfg.c, change the value of wiced\_bt\_cfg\_settings.ble\_advert\_cfg.high\_duty\_duration to 0, which indicates to the stack that advertising should never time out.
6. Build and program the kit.



### Testing

1. On your phone, install a beacon scanner app. For Android, there is an app called "Beacon Scanner" written by Nicolas Bridoux that works well (although it does not recognize EID frames). Similar apps exist for iOS.
2. Look for your Bluetooth Device address in the UART terminal window to find the correct beacon in the list.
  - a. Note: In iOS the Bluetooth Device address can't be identified (Apple doesn't allow it) so you will not be able to identify your specific device.
3. Open the URL for [www.cypress.com](http://www.cypress.com) from the beacon app.
4. If you don't see your device in the beacon app it most likely means your packet isn't correct. Using the CySmart PC application, scan for your device and look at its advertising packet to determine what's wrong.



### Exercise 4C.3 (Advanced) Use Multi-Advertising on a Beacon

#### Introduction

In this exercise you will use multi-advertising to send UID, URL and TLM frames to the listening devices. This material is covered in Eddystone.

#### Project Creation

1. Create a new application called **ch04b\_ex03\_multi** using the modus.mk file in templates/CYW920819EVB/ch04b\_ex03\_multi. This template already changes the advertising timeout, so you will not need to edit app\_bt\_cfg.c again.
2. The beacon\_lib library is already added as middleware and wiced\_bt\_beacon.h is included in app.c in the template.
3. Launch the Change Applications Settings dialog and set BT\_DEVICE\_ADDRESS = random.
4. The code in app\_set\_advertisement\_data() shows how to set up the URL advertising using multi-advertising. It uses the library function wiced\_bt\_eddystone\_set\_data\_for\_url() which is included in the beacon\_lib middleware library.
5. Find the global that defines the advertising parameters and speed up the advertising rate by changing the value of adv\_int\_max from BTM\_BLE\_ADVERT\_INTERVAL\_MAX (0x4000) to 100.
6. Create a global array for the new packet (e.g. tlm\_packet[]) which will look similar to the url\_packet array.
7. Make a copy of the four lines of code that create the URL packet and edit them to create a TLM packet.
  - a. Instead of wiced\_bt\_eddystone\_set\_data\_for\_url(), call the function for TLM (unencrypted).
  - b. Hint: Use 0 for the vbatt, temp, adv\_cnt and sec\_cnt arguments.
  - c. Hint: You can re-use the packet\_len argument.
  - d. Hint: Use the provided #define BEACON\_EDDYSTONE\_TLM to set up the second packet.
8. Repeat the above two steps for a UID packet.
  - a. Start by creating another packet array (e.g. uid\_packet).
  - b. Make another copy of the four lines of code and edit them to create a UID packet.
    - i. Instead of wiced\_bt\_eddystone\_set\_data\_for\_url(), call the function for UID.  
Hint: Use 0 for the ranging data argument.
    - ii. Modify the bytes in the provided uid\_namespace and uid\_instance arrays so that you will be able to pick out your beacon in the app.  
Hint: The namespace is 10 bytes and the instance is 6 bytes.
9. The template includes a timer that fires every 100ms. Use the provided callback function to increment the "seconds" parameter in the TLM advertising packet.



Note: the parameter is actually tenths of a second even though some scanner apps say seconds.

Hint: In the callback just reuse two lines of code from app\_set\_advertisement\_data() to re-generate the packet and re-set the advertising data.

Hint: Provide the tenths variable value in when you generate the packet instead of a value of 0. Remember that the value needs to be sent little endian – you can use the macro SWAP\_ENDIAN\_32(tenths) to do the swapping for you.

## Testing

1. Build and program the application to your kit.
2. On your phone, open the beacon scanner app.
3. Look for your Bluetooth Device address in the UART terminal window to find the correct beacons in the list.
4. You should see two beacons with your address: one that shows URL and TLM information and the other that shows UID and TLM information. Notice how the TLM Uptime value increases every second.
5. It should look something like this:





## Exercise 4C.4 (Advanced) Advertise Manufacturing Data and use Scan Response for the UUID

### Introduction

In this project, you will take a project that advertises the manufacturer ID for Cypress and a product ID of 0x2A and you will add a scan response packet that sends the Service UUID for the Modus Service. This material is covered in [0](#)

### Project Creation

1. Create a new application called **ch04c\_ex04\_scan** using the modus.mk file in templates/CYW920819EVB/ch04c\_ex04\_scan. This template is a solution to exercise ch04b/ex02\_ntfy.
2. Launch the Change Applications Settings dialog and set BT\_DEVICE\_ADDRESS = random.
3. Open the Device and Bluetooth configurators, change the name of the device to <inits>\_scan, then save and close the configurators.
4. Copy the app\_set\_advertisement\_data function to a new function called app\_set\_scan\_response\_data.
  - a. Hint: Don't forget to add function prototype at the top of the file.
5. Update the scan response packet to send the 128-bit service UUID.
  - a. Hint: there is a macro for the service UUID in cycfg\_gatt\_db.h that you can use in the array that you set up.
  - b. Hint: Remember, the Scan response packet doesn't have flags.
6. At the end of your new function, call the function to set the raw scan response data instead of the raw advertisement data.
7. Call your new function before starting advertising.

### Testing

1. Build and program the project to your kit.
2. Using the CySmart mobile app, scan for devices and note that it reports "1 Service Advertised".
  - a. Note: This feature is only on the iOS version of CySmart. It shows services advertised instead of the Bluetooth Device Address
3. Open the PC version of CySmart and scan for your device. Stop scanning once you see it.
4. Click on your device and examine the Advertisement data packet to verify it is as expected.

Click the tab above the Advertisement data that says Scan response data and verify it is as expected.



## Exercise 4C.5 (Advanced) OTA Firmware Upgrade (Non-Secure)

### Introduction

In this exercise, you will modify a project that counts button presses to add OTA firmware upgrade capability. Once OTA support is added, you will modify the project to decrement the count instead of incrementing and you will upload the new firmware using OTA. This material is covered in [4C.4.4](#).

### Project Creation

1. Create a new application from templates/CYW920819EVB/ch04c\_ex05\_ota.
  - a. Hint: The template is just the solution project for ch04b\_ex02\_pair that counts button presses with OTA\_FW\_UPGRADE=1 added to the modus.mk file to get the build settings updated for OTA.
2. Launch the Change Applications Settings dialog and set BT\_DEVICE\_ADDRESS = random.
3. Open the Middleware selector and enable "fw\_upgrade\_lib".
4. Use the Bluetooth Configurator to:
  - a. Change the device name to <inits>\_ota.
  - b. Add the OTA Service and Characteristics as shown in BLE OTA Service (Non-Secure).
5. Save and close the Configurators.
6. Edit cycfg\_gatt\_db.h:
  - a. Add `#include "wiced_bt_ota_firmware_upgrade.h"`
  - b. Replace the Service and Characteristic handle defines with the ones provided in the BLE OTA Service (Non-Secure) section of this document.
7. Edit app.c:
  - a. Add `#include "wiced_bt_ota_firmware_upgrade.h"`
  - b. Add `wiced_ota_fw_upgrade_init(NULL, NULL, NULL)` after the GATT database is initialized.
  - c. Add `wiced_ota_fw_upgrade_connection_status_event(p_conn)` in the GATT connection status event (for both connect and disconnect events).
  - d. Review the GATT Attribute Request Event handler code to understand how OTA GATT attribute request events are passed to the library.

### Testing

1. Build the project and program it to your kit.
2. Look at the PUART window during initialization and write down your kit's Bluetooth Device Address. You will need this to identify the correct device when you perform OTA upgrade.
3. Use CySmart to make sure the project functions as expected. Press the button and notice that the counter characteristic increases each time the button is pressed
  - a. Hint: The Service with a single Characteristic is the Counter Service and the Service with two Characteristics is the OTA Service.
4. Disconnect from the kit in CySmart.
5. Unplug the kit from your computer. This will ensure that OTA is used instead of regular programming to update the firmware.



6. Update the project so that each button press decrements the value instead of incrementing it.  
Build the project without programming.
  - a. Hint: In Quick Panel, use the link "Build ch04c\_ex05\_ota Application".
7. Connect your kit directly to a power outlet using a USB charger.
8. Use OTA to update your kit. You can use either the Windows or the Android app.
  - a. Hint: The Windows application only works on Windows 10 or later since earlier versions of Windows do not support BLE.
  - b. Hint: Don't forget to copy over the \*.bin file from the Debug folder every time you rebuild the project so that you are updating the latest firmware.
  - c. Hint: If the OTA process fails on Windows, try resetting the kit and trying again. If that still fails, try using the Android version since it is more robust.
9. Once OTA upgrade is done, reset the kit then connect using CySmart and verify that the new firmware functionality is working.



## Exercise 4C.6 (Advanced) OTA Firmware Upgrade (Secure)

### Introduction

In this exercise, you will update the previous OTA exercise to use Secure OTA firmware upgrade. This material is covered in [4C.4.5](#).

### Project Creation

1. Create a new application from templates/CYW920819EVB/ch04c\_ex06\_ota\_sec.
  - a. Hint: The template is just the solution project for ch04c\_ex05\_ota but without the manual edits to the cycfh\_gatt\_db.h file.
2. Launch the Change Applications Settings dialog and set BT\_DEVICE\_ADDRESS = random.
3. Use the Bluetooth Configurator to:
  - a. Change the name to <inits>\_otas.
  - b. Change the OTA Service UUID to the one for Secure OTA.
    - i. Hint: The Secure OTA UUID is: C7261110-F425-447A-A1BD-9D7246768BD8
4. Save and close the configurators.
5. Re-do the edits to cycfg\_gatt\_db.h (add the include and replace the defines for the OTA Service and Characteristic handles).
6. Generate keys and update app.c as described in the BLE OTA Service (Secure) section of this manual.

### Testing

1. Build the project and program it to your kit.
2. Use CySmart to make sure the project functions as expected.
3. Disconnect from the kit in CySmart.
4. Unplug the kit from your computer. This will ensure that OTA is used instead of regular programming to update the firmware.
5. Make the same change as the previous exercise to count down instead of up on each button press.
6. Build the project.
7. Connect your kit directly to a power outlet using a USB charger.
8. Use OTA to update your kit. You can use either the Windows or the Android app.
  - a. Hint: Don't forget that every time you re-build the project you must sign the bin file and copy the resulting \*.bin.signed to the Windows OTA folder or Android device. Remember, instructions on signing the file are in Build Firmware and Sign OTA Image
  - b. Hint: If the OTA process fails on Windows, try resetting the kit and trying again. If that still fails, try using the Android version since it is more robust.
9. Once OTA upgrade is done, connect to the kit using CySmart and verify that the new firmware functionality is working.
10. Try doing OTA with the unsigned image. Notice that it will fail after loading the image. The original firmware will be retained in this case.