

## Chapter 6: Bluetooth® LE centrals

This chapter introduces you to the central side of the Bluetooth® LE connection. By the end of this chapter you will be able to create a Bluetooth® LE central that finds the right Bluetooth® LE peripheral, connects to it, reads, writes and enables/handles notifications. It will also be able to perform the GATT service discovery procedure to find the handles of the services, characteristics, and descriptors on the GATT server.

### Table of contents

<b>6.1</b>	<b>GAP Roles, the observer and the central .....</b>	<b>2</b>
<b>6.2</b>	<b>Configurator for central devices.....</b>	<b>2</b>
<b>6.3</b>	<b>Scanning .....</b>	<b>4</b>
<b>6.4</b>	<b>Connecting, pairing and encrypting.....</b>	<b>7</b>
<b>6.5</b>	<b>Attribute protocol &amp; more GATT procedures .....</b>	<b>9</b>
6.5.1	GATT client read .....	10
6.5.2	GATT client write and write command.....	11
6.5.3	GATT client notify and indicate .....	12
6.5.4	GATT group.....	12
6.5.5	GATT client read by group type .....	13
6.5.6	GATT client find by type value .....	14
6.5.7	GATT client read by type.....	14
6.5.8	GATT client find information .....	14
<b>6.6</b>	<b>Service discovery .....</b>	<b>15</b>
6.6.1	Service discovery algorithm .....	15
6.6.2	Service discovery implementation.....	15
<b>6.7</b>	<b>Running a GATT Server.....</b>	<b>17</b>
<b>6.8</b>	<b>Exercises .....</b>	<b>18</b>
	Exercise 1: Make an observer .....	18
	Exercise 2: Parse the device name and list only your peripheral.....	20
	Exercise 3: Connect to your peripheral and turn LED ON/OFF.....	21
	Exercise 4: Add commands to enable/disable notifications .....	24
	Exercise 5: Implement service discovery .....	26

### Document conventions

Convention	Usage	Example
Courier New	Displays code and text commands	CY_ISR_PROTO (MyISR) ; make build
<i>Italics</i>	Displays file names and paths	sourcefile.hex
[bracketed, bold]	Displays keyboard commands in procedures	[Enter] or [Ctrl] [C]
Menu > Selection	Represents menu paths	File > New Project > Clone
<b>Bold</b>	Displays GUI commands, menu paths and selections, and icon names in procedures	Click the <b>Debugger</b> icon, and then click <b>Next</b> .

## 6.1 GAP Roles, the observer and the central

In the previous chapters the focus has been on Bluetooth® LE peripherals. Instead of dividing the world into peripheral and central, it would have been more technically correct to say that Bluetooth® Low Energy has four GAP device roles:

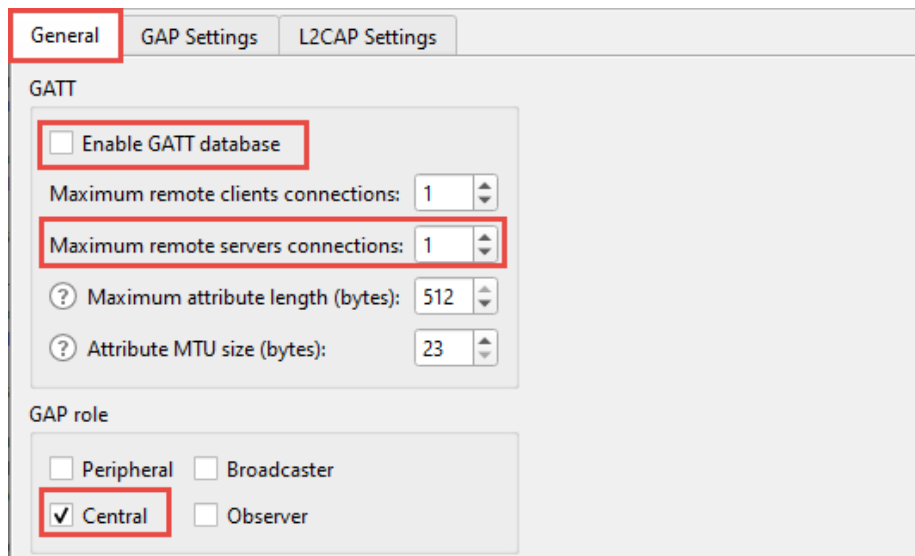
- **Broadcaster:** A device that only advertises (e.g. beacon)
- **Peripheral:** A device that can advertise and be connected to
- **Observer:** A device that passively listens to advertisers (e.g. beacon scanner)
- **Central:** A device that can listen to advertisers and create a connection to a peripheral

So, the previous chapters were really focused on broadcasters and peripherals. But what about the central side of a connection? The answer to that question is the focus of this chapter.

## 6.2 Configurator for central devices

In previous chapters, we used the Bluetooth® configurator to setup a peripheral but it also allows you to specify settings for a central. Role selection is done on the **General** tab as seen below. You can select one or more roles at a time. You can also enable or disable the GATT database.

The GATT server is usually the peripheral, so the GATT database will often be disabled on the server.

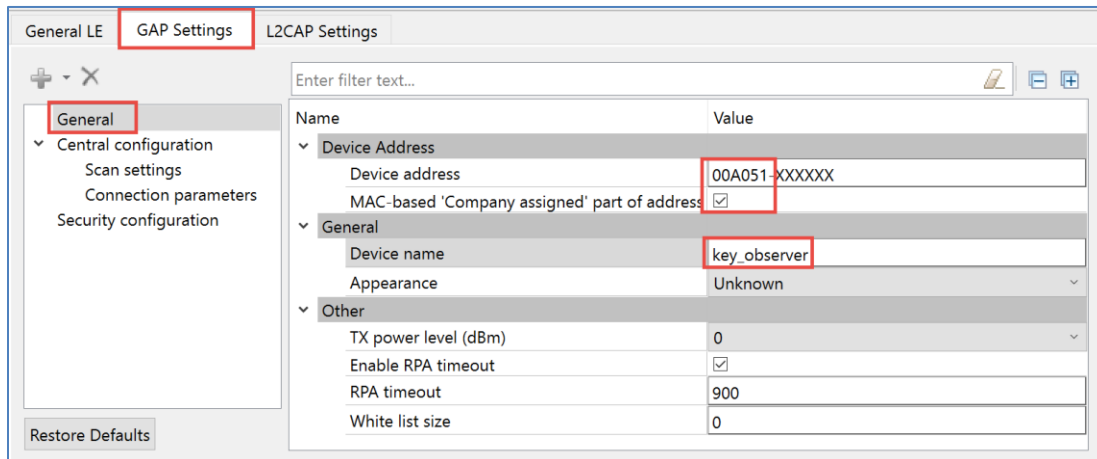


The screenshot shows the 'General' tab of the Bluetooth configurator. The 'GATT' section has a checkbox for 'Enable GATT database' which is unchecked. Below it are four spinners: 'Maximum remote clients connections' (set to 1), 'Maximum remote servers connections' (set to 1), 'Maximum attribute length (bytes)' (set to 512), and 'Attribute MTU size (bytes)' (set to 23). The 'GAP role' section has four checkboxes: 'Peripheral', 'Broadcaster', 'Central' (which is checked), and 'Observer'.

**Note:** The value for **Maximum remote servers connections** must be set to a number larger than 0. If not, your device will not be able to connect to a GATT server.

**Note:** When you disable the GATT database, the **GATT Settings** tab goes away.

On the **GAP Settings** tab, you will still see the **General** section for device name, address, RPA settings, and so on, but now there is a section for **Central configuration** that allows you to select **Scan settings** and **Connection parameters**.



General LE **GAP Settings** L2CAP Settings

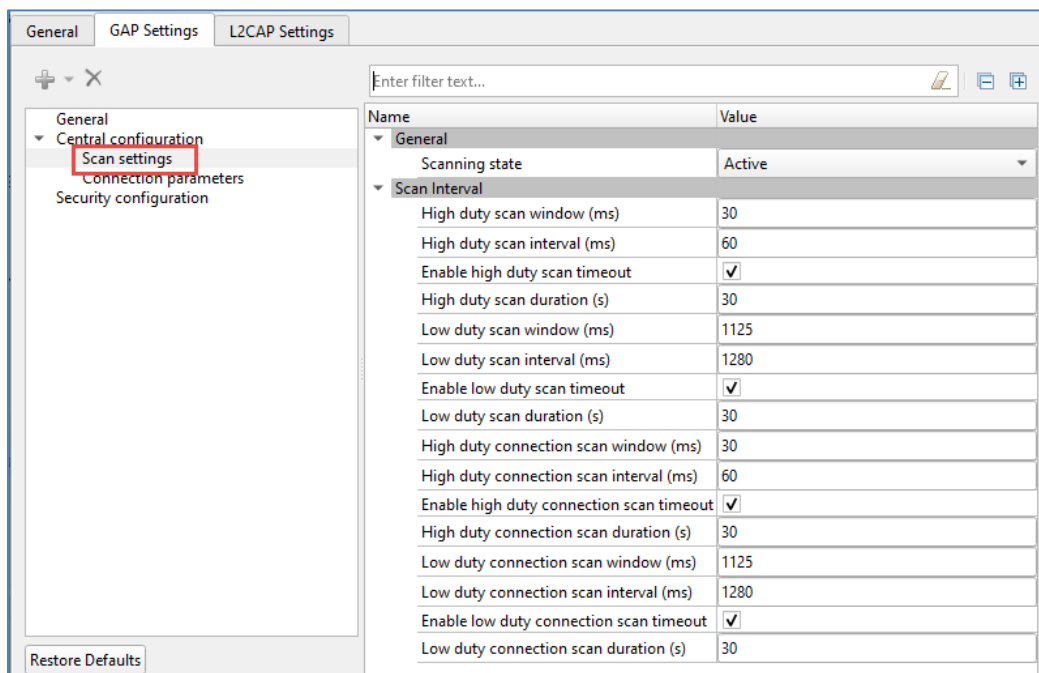
General

- Central configuration
  - Scan settings
  - Connection parameters
  - Security configuration

Restore Defaults

Name	Value
Device Address	00A051-XXXXXX
Device address	00A051-XXXXXX
MAC-based 'Company assigned' part of address	<input checked="" type="checkbox"/>
General	
Device name	key_observer
Appearance	Unknown
Other	
TX power level (dBm)	0
Enable RPA timeout	<input checked="" type="checkbox"/>
RPA timeout	900
White list size	0

**Note:** The first three bytes of the **Device Address** were changed from 00A050 to 00A051. That's necessary because the last three bytes are based on the MAC address of the computer used to build the application. If the value for the part wasn't changed, you would get the same address for the peripheral and the central (assuming you used the same computer to build both).



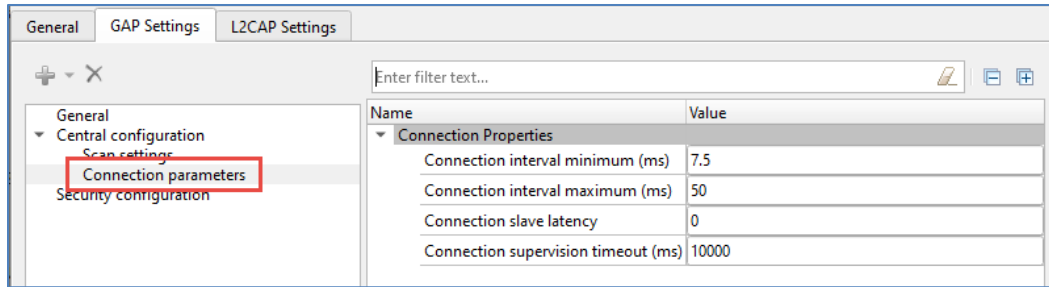
General **GAP Settings** L2CAP Settings

General

- Central configuration
  - Scan settings**
  - Connection parameters
  - Security configuration

Restore Defaults

Name	Value
General	
Scanning state	Active
Scan Interval	
High duty scan window (ms)	30
High duty scan interval (ms)	60
Enable high duty scan timeout	<input checked="" type="checkbox"/>
High duty scan duration (s)	30
Low duty scan window (ms)	1125
Low duty scan interval (ms)	1280
Enable low duty scan timeout	<input checked="" type="checkbox"/>
Low duty scan duration (s)	30
High duty connection scan window (ms)	30
High duty connection scan interval (ms)	60
Enable high duty connection scan timeout	<input checked="" type="checkbox"/>
High duty connection scan duration (s)	30
Low duty connection scan window (ms)	1125
Low duty connection scan interval (ms)	1280
Enable low duty connection scan timeout	<input checked="" type="checkbox"/>
Low duty connection scan duration (s)	30



## 6.3 Scanning

In the previous chapters you learned how to create different peripherals that advertise their existence and some data. How does a central find this information? And how does it use that information to get connected?

First, you must put the central into scanning mode. You do this with a simple call to `wiced_bt_ble_scan`. This function takes three arguments.

1. The first argument is a `wiced_bt_ble_scan_type_t` which tells the controller to either turn off, scan fast (high duty) or scan slowly (low duty).

```
enum wiced_bt_ble_scan_type_e
{
    BTM_BLE_SCAN_TYPE_NONE,           /**< Stop scanning */
    BTM_BLE_SCAN_TYPE_HIGH_DUTY,      /**< High duty cycle scan */
    BTM_BLE_SCAN_TYPE_LOW_DUTY        /**< Low duty cycle scan */
};
typedef uint8_t wiced_bt_ble_scan_type_t;
```

The actual values of scan high and low duty are set in the Bluetooth® configurator, as you saw earlier.

2. The next argument is a `wiced_bool_t` that tells the scanner to filter or not. If you enable the filter, the scanner will only call you back one time for each unique BD ADDR that it hears even if the advertising packet changes.
3. The final argument is a function pointer to a callback function that looks like this:

```
void myScanCallback(wiced_bt_ble_scan_results_t *p_scan_result, uint8_t *p_adv_data);
```

For example, you may start high duty cycle scanning with filtering like this:

```
wiced_bt_ble_scan( BTM_BLE_SCAN_TYPE_HIGH_DUTY, WICED_TRUE, myScanCallback );
```

Each time that your central hears an advertisement, it will call your callback with a pointer to a scan result structure with information about the device it just heard, and a pointer to the raw advertising data. The scan result structure simply has the Bluetooth® Device Address, the address type, what type of advertisement packet, the RSSI and a flag like this:

```
/** LE inquiry result type */
typedef struct
{
    wiced_bt_device_address_t    remote_bd_addr;           /**< Device address */
    uint8_t                     ble_addr_type;             /**< LE Address type */
    wiced_bt_dev_ble_evt_type_t ble_evt_type;             /**< Scan result event type */
    int8_t                      rssi;
    uint8_t                     flag;
} wiced_bt_ble_scan_results_t;
```

In your scan callback function you must first check the scan result to make sure it was due to a device being found and not something else like a scan off event. For example:

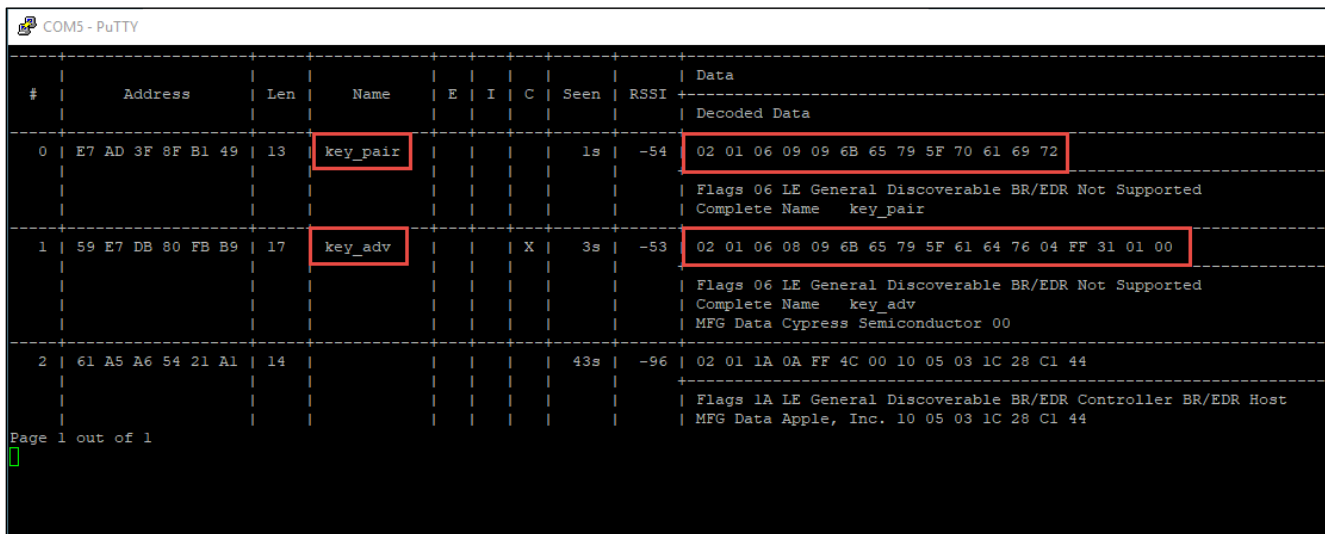
```
void myScanCallback( wiced_bt_ble_scan_results_t *p_scan_result, uint8_t *p_adv_data )
{
    if(p_scan_result->remote_bd_addr != NULL && p_scan_result != NULL)
    {
        /* All scan callback processing goes here. */
    }
}
```

Once you have verified that the scan result is not NULL, you can parse the advertising data to decide what to do next. The `btstack` library provides you a function called `wiced_bt_ble_check_advertising_data` which can help you find information in the packet. Recall that every advertising packet is broken up into fields that each have a type. The `wiced_bt_ble_check_advertising_data` function will search the advertising packet looking for a field that you specify and then, if it finds that field, will return a pointer to the field and the length (via a pointer). For example, you might have this inside the callback function to search for a service UUID:

```
uint8_t len;
uint8_t *findServiceUUID = wiced_bt_ble_check_advertising_data(p_adv_data,
    BTM_BLE_ADVERT_TYPE_128SRV_COMPLETE, &len);
```

After making this call, `findServiceUUID` will either be 0 (it didn't find the field) or will be a pointer to the bytes that make up the service UUID. In addition, `len` will either be 0 or it will be the number of bytes in that field. Remember that the enumeration `wiced_bt_ble_advert_type_e` in the file `mtb_shared/btstack/<version>/wiced_include/wiced_bt_ble.h` has a list of the legal advertising field types.

So, now what? Consider the two cases in the following screenshot from an Advertising Scanner application. In this case you can see that there are two different devices advertising, one named "key\_pair" and one named "key\_adv". You can see the raw bytes of the advertising packet and the decode of those bytes.



#	Address	Len	Name	E	I	C	Seen	RSSI	Data
0	E7 AD 3F 8F B1 49	13	key_pair				1s	-54	02 01 06 09 09 6B 65 79 5F 70 61 69 72 Flags 06 LE General Discoverable BR/EDR Not Supported Complete Name key_pair
1	59 E7 DB 80 FB B9	17	key_adv			X	3s	-53	02 01 06 08 09 6B 65 79 5F 61 64 76 04 FF 31 01 00 Flags 06 LE General Discoverable BR/EDR Not Supported Complete Name key_adv MFG Data Cypress Semiconductor 00
2	61 A5 A6 54 21 A1	14					43s	-96	02 01 1A 0A FF 4C 00 10 05 03 1C 28 C1 44 Flags 1A LE General Discoverable BR/EDR Controller BR/EDR Host MFG Data Apple, Inc. 10 05 03 1C 28 C1 44

Page 1 out of 1

If you were looking for a device named `key_pair` you could do something like this:

```
uint8_t len;
uint8_t * p_name = wiced_bt_ble_check_advertising_data( p_adv_data,
BTM_BLE_ADVERT_TYPE_NAME_COMPLETE, &len );

if( p_name && ( len == strlen("key_pair") ) && ! memcmp( "key_pair", p_name, len ) )
{
    WICED_BT_TRACE("Found Matching Device with BD Address: [%B]",
p_scan_result->remote_bd_addr );
}
```

If you were looking for a device that was advertising the "PSOC" service UUID you might do the following. Notice that the UUIDs are stored little endian in the advertising packet. This UUID is the one that the template peripheral application has – I just copied over the macro from the *GeneratedSource/cycfg\_gatt\_db.h* file. If you created your own application, it would have a different (random) UUID unless you manually enter this value in the configurator.

```
#define __UUID_SERVICE_PSOC      0x90, 0x86, 0x13, 0xFE, 0x44, 0x99, 0x07, 0x93, 0x67, 0x4B, 0x3F,
                                0x63, 0xFF, 0x8A, 0x9E, 0x9D

static const uint8_t serviceUUID[]={ __UUID_SERVICE_PSOC };

uint8_t *findServiceUUID = wiced_bt_ble_check_advertising_data(p_adv_data,
BTM_BLE_ADVERT_TYPE_128SRV_COMPLETE,&len);

if(findServiceUUID && (memcmp(findServiceUUID,serviceUUID,len) == 0))
{
    WICED_BT_TRACE("Host = %B Found Service UUID\r\n ", p_scan_result->remote_bd_addr);
}
```

**Note:** *The first argument to the "if" function is there to make sure we have a valid (non-null) pointer returned from the advertising packet.*

There are several functions which can be useful in comparing data for when you want to identify a specific device such as (note that you must include *string.h* to get access to `memcmp`):

1. `memcmp(uint8_t *p1, uint8_t *p2, int size)` allows you to compare two blocks of memory. It returns 0 if the two blocks of memory are the same.
2. If you have two variables of type `wiced_bt_uuid_t` you can compare them with the `wiced_bt_util_uuid_cmp` function. Like the functions above, it returns 0 if the two UUIDs match.

```
int wiced_bt_util_uuid_cmp(wiced_bt_uuid_t *p_uuid1, wiced_bt_uuid_t *p_uuid2);
```

## 6.4 Connecting, pairing and encrypting

Now that you have found a device that you are interested in what next? First you need to register a GATT event callback. This looks exactly like it does on the peripheral side. Note that you don't need to initialize the GATT database because the central doesn't contain the database – it's on the peripheral.

```
wiced_bt_gatt_register(app_bt_gatt_callback);
```

To make a connection you just call `wiced_bt_gatt_le_connect`:

```
wiced_bool_t wiced_bt_gatt_le_connect(wiced_bt_device_address_t bd_addr,  
                                       wiced_bt_ble_address_type_t bd_addr_type,  
                                       wiced_bt_ble_conn_mode_t conn_mode,  
                                       wiced_bool_t is_direct);
```

The `bd_addr` and `bd_addr_type` are passed in to the callback as part of the scan result. The `conn_mode` is an enumeration with three possible values which determines how fast the connection is established (and how much power is consumed to establish the connection):

```
enum wiced_bt_ble_conn_mode_e  
{  
    BLE_CONN_MODE_OFF,                /*< Stop initiating */  
    BLE_CONN_MODE_LOW_DUTY,           /*< slow connection scan parameter */  
    BLE_CONN_MODE_HIGH_DUTY           /*< fast connection scan parameter */  
};
```

The final argument should be set to `WICED_TRUE`.

When the connection has been made, the GATT callback that you registered with `wiced_bt_gatt_register` will be called with the event `GATT_CONNECTION_STATUS_EVT`. The parameter passed to you will be of type `wiced_bt_gatt_connection_status_t` which contains a bunch of information about the connection.

```
typedef struct  
{  
    uint8_t          *bd_addr;    /*< Remote device address */  
    wiced_bt_ble_address_type_t addr_type; /*< Remote device address type */  
    uint16_t         conn_id;     /*< ID of the connection */  
    wiced_bool_t     connected;    /*< TRUE/FALSE connected/disconnected */  
    wiced_bt_gatt_disconn_reason_t reason; /*< Reason code (see @link  
                                       wiced_bt_gatt_disconn_reason_e  
                                       wiced_bt_gatt_disconn_reason_t @endlink) */  
    wiced_bt_transport_t transport; /*< Transport type of the connection */  
    uint8_t          link_role;    /*< Link role on this connection */  
} wiced_bt_gatt_connection_status_t;
```

Typically, you would save the `conn_id` so that you can perform reads and writes to the peripheral. If you were going to support multiple connections, you might make a table of connection ID / Bluetooth® address tuples.

Once connected, the central can initiate pairing (if the devices were not previously bonded). The function is `wiced_bt_dev_sec_bond`:

```
wiced_result_t wiced_bt_dev_sec_bond(wiced_bt_device_address_t bd_addr,  
                                       wiced_bt_ble_address_type_t bd_addr_type,  
                                       wiced_bt_transport_t transport,  
                                       uint8_t pin_len,  
                                       uint8_t *p_pin);
```

The transport can be either `BT_TRANSPORT_BR_EDR` (for Classic) or `BT_TRANSPORT_LE` (for Bluetooth® LE). The last two arguments are only for legacy pairing modes, so just use 0 for `pin_len` and `NULL` for `p_pin`.

Remember that some characteristic values can only be read or written once the device is paired. This is determined by the GATT characteristic permissions (e.g. LEGATTDB\_PERM\_AUTH\_READABLE or LEGATTDB\_PERM\_AUTH\_WRITABLE).

If you previously saved bonding information on both the peripheral and client, then you don't need to initiate pairing on subsequent connections. In that case instead of `wiced_bt_dev_sec_bond` you just need to enable encryption by calling `wiced_bt_dev_set_encryption`:

```
wiced_result_t wiced_bt_dev_set_encryption (wiced_bt_device_address_t bd_addr,
                                             wiced_bt_transport_t transport,
                                             void *p_ref_data);
```

The transport is again either `BT_TRANSPORT_BR_EDR` (for Classic) or `BT_TRANSPORT_LE` (for Bluetooth® LE). The last argument is a pointer to an enumeration of type `wiced_bt_ble_sec_action_type_t` which returns the encryption status. The enumeration is:

```
/** LE encryption method */
enum
{
    BTM_BLE_SEC_NONE,           /**< No encryption */
    BTM_BLE_SEC_ENCRYPT,        /**< encrypt the link using current key */
    BTM_BLE_SEC_ENCRYPT_NO_MITM, /**< encryption without MITM */
    BTM_BLE_SEC_ENCRYPT_MITM    /**< encryption with MITM*/
};
typedef uint8_t wiced_bt_ble_sec_action_type_t;
```

To summarize, the client would typically do something like this after making a connection:

```
/* Check for existing data in KV store for a bonded device */
kv_rslt = mtb_kvstore_read(&kvstore_obj, "kv_link_keys", NULL, NULL);

if (kv_rslt == CY_RSLT_SUCCESS) /* Bonding data exists, so read it in */
{
    data_size = sizeof(link_keys);
    mtb_kvstore_read(&kvstore_obj, "kv_link_keys", (uint8_t *)&link_keys, &data_size);

    if (memcmp(link_keys.bd_addr, p_peer_info->peer_addr, sizeof(wiced_bt_device_address_t))==0)
    {
        isBonded = WICED_TRUE; // We found keys for the Peripheral's BD Address
    }
}

if ( isBonded ) /* Device is bonded so just need to enable encryption */
{
    status = wiced_bt_dev_set_encryption( p_peer_info->peer_addr,
                                           p_peer_info->transport,
                                           &encryption_type );
    WICED_BT_TRACE( "wiced_bt_dev_set_encryption %d \n", status );
}
else /* Device not bonded so we need to pair */
{
    status = wiced_bt_dev_sec_bond( p_peer_info->peer_addr,
                                    p_peer_info->addr_type,
                                    p_peer_info->transport, 0, NULL );
    WICED_BT_TRACE( "wiced_bt_dev_sec_bond %d \n", status );
}
```

When you want to disconnect, just call `wiced_bt_gatt_disconnect` with the connection ID as a parameter. Note that the connect function has "le" in the name but the disconnection function does not!



## 6.5 Attribute protocol & more GATT procedures

In the previous chapters you saw the peripheral side of several GATT Procedures. Specifically, read, write, notify, and indicate. Moreover, in those chapters you learned how to create firmware to respond to those requests. You will recall that each of those GATT procedures are mapped into one or more attribute requests. Here is a list of all the attribute requests with the original request and the applicable response.

Note that the request can be initiated by either the client or server depending on the operation. For example, a write is initiated by the GATT client while a notification is initiated by the GATT server.

Bluetooth® Spec * Chap Ref	Request	Request Data	Bluetooth® Spec * Chap Ref	Response	Response Data
			3.4.1.1 N/A	Error Response	Request Op Code in Error Attribute Handle in Error Error Code
3.4.2.1 N/A	Exchange MTU	Client Rx MTU	3.4.2.2 N/A	Exchange MTU response	Server Rx MTU
3.4.3.1 6.5.8	Find Information	Starting Handle Ending Handle	3.4.3.2 6.5.8	Find Information Response	Handles Attribute Type UUIDs
3.4.3.3 6.5.6	Find by Type Value	Starting Handle Ending Handle Attribute Type Attribute Value	3.4.3.4 4D.4.60	Find by Type Value Response	Start Handle End of Group Handle
3.4.4.1 0	Read by Type	Starting Handle Ending Handle Attribute Type UUID	3.4.4.2 0	Read by Type Response	Handle Value Pairs
3.4.4.3 6.5.1	Read	Handle	3.4.4.4 4A	Read Response	Handle, Value
3.4.4.5 N/A	Read Blob	Handle, Offset	3.4.4.6 N/A	Read Blob Response	Handle, Data
3.4.4.7 N/A	Read Multiple	Handles	3.4.4.8 N/A	Read Multiple Response	One response with all values concatenated
3.4.4.9 0	Read by Group Type	Starting Handle Ending Handle Attribute Group Type UUID	3.4.4.10 0	Read by Group Type Response	For each match: Handle, Value Handle of last Attribute in Group
3.4.5.1 6.5.2	Write	Handle, Value	3.4.5.2 4A	Write Response	Response code 0x1E Or Error Response
3.4.5.3 6.5.2	Write Command	Handle, Value	There is no Server response to a Write.		
3.4.5.4 N/A	Signed Write Command	Handle, Value, Signature	3.4.5.2 4A	Write Response	Response code 0x1E Or Error Response
3.4.6.1 N/A	Prepare Write	Handle Offset Value	3.4.6.2 N/A	Prepare Write Response	Handle Offset Value

Bluetooth® Spec * Chap Ref	Request	Request Data	Bluetooth® Spec * Chap Ref	Response	Response Data
3.4.6.3 N/A	Execute Write	Flags (0-cancel, 1-write)	3.4.6.4 N/A	Execute Write Response	Response code 0x19 Or Error Response
3.4.7.1 4B	Notification	Handle, Value	There is no Client response to a Notification, but you can read about what happens on the Client side in 0		
3.4.7.2 4B	Indication	Handle, Value	3.4.7.3 0	Handle Value Confirmation	Response code 0x1E Or Error Response

\* Bluetooth® spec references are from Volume 3, Part F (Attribute Protocol). Additional details on the GATT procedures that use the ATT protocols can be found in Volume 3, Part G (Generic Attribute Profile).

This leads us to some obvious questions: What happens with read, write and notify on the GATT client side of a connection? And what about these other operations?

## 6.5.1 GATT client read

To initiate a read of the value of a characteristic you use the following function:

```
wiced_bt_gatt_client_send_read_handle(uint16_t conn_id, uint16_t handle,
                                       uint16_t offset, uint8_t * p_read_buf, uint16_t len,
                                       wiced_bt_gatt_auth_req_t auth_req);
```

The arguments are:

- conn\_id: The connection ID for the sever that you want to read from.
- handle: The handle for the attribute that you want to read. This will normally be a characteristic's value handle.
- offset: The offset to start the read from. This will normally be 0.
- p\_read\_buf: A pointer to a buffer where you want the stack will store the return value.
- len: The length of the p\_read\_buf. If the value from the attribute that you are reading won't fit in this buffer, you will get an error code from the stack.
- auth\_req: Authentication requirements – the possible values are:

```
enum wiced_bt_gatt_auth_req_e {
    GATT_AUTH_REQ_NONE = 0, /* No Authentication Required */
    GATT_AUTH_REQ_NO_MITM = 1, /* Unauthenticated encryption (No MITM) */
    GATT_AUTH_REQ_MITM = 2, /* Authenticated encryption (MITM) */
    GATT_AUTH_REQ_SIGNED_NO_MITM = 3, /* Signed Data (No MITM) */
    GATT_AUTH_REQ_SIGNED_MITM = 4 /* Signed Data (MITM) */
};
```

**Note:** The connection must have at least the requested level of authentication for the read to succeed. For example, if you select `GATT_AUTH_REQ_MITM` the connection must be encrypted and must have MITM protection. Likewise, if you select `GATT_AUTH_REQ_NO_MITM` the connection must be encrypted and MITM protection is allowed but not required. If you select `GATT_AUTH_REQ_NONE` than the request will succeed no matter what the connection encryption or MITM status is.

The `wiced_bt_gatt_client_send_read_handle` function call causes the Stack to send a read request to the GATT server. After some time, you will get a callback in your GATT event handler with the event code `GATT_OPERATION_CPLT_EVENT`.

This event is used to handle many of the responses from a GATT server. So, once you get the event callback you should verify that it was the read operation of the correct characteristic that caused the event. You should also verify that the operation was successful. If both of these are true, then you can read the value from the buffer that you provided.

Everything you need to know is passed into the GATT event callback by the stack using a parameter that is a structure of type `wiced_bt_gatt_event_data`. For example, if I assign that parameter to `p_event_data`, and I want to print the value of the characteristic whose handle is "myHandle", you could use this:

```
case GATT_OPERATION_CPLT_EVT:
    if (p_event_data->operation_complete.status == WICED_BT_GATT_SUCCESS)
    {
        if (p_event_data->operation_complete.op == GATTC_OPTYPE_READ_HANDLE)
        {
            if (p_event_data->operation_complete.response_data.handle ==
                myHandle)
            {
                /* Read the value from the buffer that was provided in
                 * the wiced_bt_gatt_client_send_read_handle function */
            }
        }
    }
    else
    {
        printf("GATT operation failed with status: %d\n",
            p_event_data->operation_complete.status);
    }
    break;
```

The possible values for the status can be found in the enumeration `wiced_bt_gatt_status_e` and the possible values for the operation type can be found in `wiced_bt_gatt_optype_e`.

## 6.5.2 GATT client write and write command

In order to send a GATT write all you need to do is make a structure of type `wiced_bt_gatt_write_hdr_t`, setup the handle, offset, length, and authorization then call `wiced_bt_gatt_client_send_write` with a pointer to the data that you want to send. Here is an example:

```
/* Set up write parameters */
wiced_bt_gatt_write_hdr_t write_params;
write_params.handle = myHandle;
write_params.offset = 0;
write_params.len = sizeof(val);
write_params.auth_req = GATT_AUTH_REQ_NONE;

/* Send the write command */
wiced_bt_gatt_client_send_write ( connection_id, GATT_CMD_WRITE,
                                &write_params, &val, NULL);
```

The second argument to `wiced_bt_gatt_client_send_write` function can either be `GATT_CMD_WRITE` (no response requested) or `GATT_REQ_WRITE` (response requested).

**Note:** *The characteristic on the server must have the properties and permissions set for the type of write that you are doing (e.g. Write and/or Write Without Response).*

If you asked for a write with response (i.e. `GATT_REQ_WRITE`), sometime after you call `wiced_bt_gatt_client_send_write` you will get a GATT callback with the event code `GATT_OPERATION_CPLT_EVT`. You can then figure out if the write was successful by checking the response code. The codes are defined in the `wiced_bt_gatt_status_e` enumeration. A successful write will result in one of the following codes depending on whether the connection is encrypted and has MITM protection:

```
WICED_BT_GATT_ENCRYPTED_MITM      = WICED_BT_GATT_SUCCESS,  /**< Encrypted MITM */
WICED_BT_GATT_ENCRYPTED_NO_MITM   = 0x878E,                /**< Encrypted No MITM */
WICED_BT_GATT_NOT_ENCRYPTED       = 0x878F,                /**< Not Encrypted */
```

Don't forget the you can only issue one Read/Write at a time and that you cannot send the next Read/Write until the last one is finished.

### 6.5.3 GATT client notify and indicate

To register for notifications and indications, the client just needs to write to the CCCD for the characteristic of interest.

For a CCCD, the LSB (bit 0) is set to 1 for notifications, and bit 1 is set to 1 for Indications. That is:

```
/** characteristic descriptor: client configuration value */
enum wiced_bt_gatt_client_char_config_e
{
    GATT_CLIENT_CONFIG_NONE          = 0x0000,          /**< No notifications or indications */
    GATT_CLIENT_CONFIG_NOTIFICATION = 0x0001,          /**< Send notifications */
    GATT_CLIENT_CONFIG_INDICATION   = 0x0002           /**< Send indications */
};
```

When the GATT server initiates a notify or an indicate you will get a GATT callback with the event code set as `GATT_OPERATION_CPLT_EVT`. You will see that the operation value is `GATTC_OPTYPE_NOTIFICATION` or `GATTC_OPTYPE_INDICATION`. In the case of indicate you can return `WICED_BT_GATT_SUCCESS` which means the stack will return a handle value confirmation to the client, or you can return something other than `WICED_BT_GATT_SUCCESS` in which case the stack sends an error response with the code that you choose from the `wiced_bt_gatt_status_e` enumeration.

### 6.5.4 GATT group

There is one last GATT concept that needs to be introduced to understand the next set of GATT procedures. That is the group. A group is a range of handles starting at a service, service include or a characteristic, and ending at the last handle that is associated with the group. To put it another way, a group is all of the rows in the GATT database that logically belong together. For instance, in the GATT database below, the service group for <<Generic Access>> starts at handle 0x0001 and ends at 0x0005.

## 6.5.5 GATT client read by group type

The GATT client "Read by Group Type" request takes as input a search starting handle, search ending handle and group type. It outputs a list of tuples with the group start handle, group end handle, and value. This request can only be used for a "Grouping Type" meaning, <<Service>>, <<Included Service>> and <<Characteristic>>.

Note that anything inside double angle brackets << >> indicates a Bluetooth® SIG defined UUID. For example, <<Primary Service>> is defined by the SIG to be 0x2800.

Consider this GATT database for a peripheral with a Service called "PSoC" that contains two characteristics; Button Count and LED (which happens to be the application you will control from your central device in this chapter's exercises).

Handle	Type	Value
0x0001	<<Primary Service>>	<<Generic Access>>
0x0002	<<Characteristic>>	0x02, 0x03, <<Device Name>>
0x0003	<<Device Name>>	key_per
0x0004	<<Characteristic>>	0x02, 0x05, <<Appearance>>
0x0005	<<Appearance>>	0x00
0x0006	<<Primary Service>>	<<Generic Attribute>>
0x0007	<<Primary Service>>	__UUID_SERVICE_PSoC
0x0008	<<Characteristic>>	0x0A, 0x09, __UUID_CHARACTERISTIC_PSoC_LED
0x0009	__UUID_CHARACTERISTIC_PSoC_LED	RGB LED value
0x000A	<<Characteristic>>	0x1A, 0x0B, __UUID_CHARACTERISTIC_PSoC_BUTTON_COUNT
0x000B	__UUID_CHARACTERISTIC_PSoC_BUTTON_COUNT	Button Count Value
0x000C	<<CCCD>>	0x0000 (notify off) or 0x0001 (notify on)

Remember that the type and values for different attributes are:

Attribute	Type	Value
Service	<<Primary Service>> or <<Secondary Service>>	Service UUID
Characteristic	<<Characteristic>>	Properties, Handle to the Value, Characteristic UUID
Characteristic Value	Characteristic UUID	Characteristic Value

In the database above if you input search start handle=0x0001, search end handle=0xFFFF and group type = <<Service>> you would get as output:

Group Start Handle	Group End Handle	UUID
0x0001	0x0005	<<Generic Access>>
0x0006	0x0006	<<Generic Attribute>>
0x0007	0x000C	__UUID_SERVICE_PSoC

In words, you receive a list of all the service UUIDs with the start handle and end handle of each service group.

## 6.5.6 GATT client find by type value

The GATT client "Find by Type Value" request takes as input the search starting handle, search ending handle, attribute type and attribute value. It then searches the attribute database and returns the starting and ending handles of the group that match that attribute type and attribute value. This function was put into GATT specifically to find the range of handles for a specific service.

Consider the example above. If your input to the "Find by Type Value" was starting handle 0x0001, ending handle 0xFFFF, type <<Service>> and value \_\_UUID\_SERVICE\_PSOC, the output would be:

Group Start Handle	Group End Handle
0x0007	0x000C

This function cannot be used to search for a specific characteristic because the attribute value of a characteristic declaration cannot be known a-priori. This is because the characteristic properties and characteristic value attribute handle (which are part of the attribute value) are not known up front. As a reminder, here is the characteristic declaration:

Attribute Handle	Attribute Types	Attribute Value			Attribute Permissions
0xNNNN	0x2803–UUID for «Characteristic»	Characteristic Properties	Characteristic Value Attribute Handle	Characteristic UUID	Read Only, No Authentication, No Authorization

## 6.5.7 GATT client read by type

The GATT client "Read by Type" request takes as input the search starting handle, search ending handle and attribute type. It outputs a list of handle value pairs. In the example above if you entered the search starting handle 0x0007, search ending handle 0x000C and type <<Characteristic>>, you would get as output:

Characteristic Handle	Value Handle	UUID	GATT Permission
0x0008	0x0009	__UUID_CHARACTERISTIC_PSOC_LED	0x0A
0x000A	0x000C	__UUID_CHARACTERISTIC_PSOC_BUTTON_COUNT	0x0A

In words, you get back a list of the characteristic handles, the handles of the values, the UUIDs, and the GATT permissions.

## 6.5.8 GATT client find information

The input to the GATT client "Find Information" request is simply a search starting handle and a search ending handle. The GATT server responds with a list of every handle in that range, and the attribute type of the handle. Notice that this is the only GATT procedure that returns the attribute type.

If you execute a GATT client "Find Information" with the handle range set to 0x0005 > 0x0005 you will get a response of:

Handle	Attribute Type
0x0005	<<Appearance>>

In words, the attribute type that is associated with the characteristic handle 0x0005.

## 6.6 Service discovery

Given that all transactions between the GATT client and GATT server use the handle instead of the UUID, one huge question left unanswered is how do you find the handles for the different services, characteristics and descriptors on the GATT server?

A very, very bad answer to that question is that you hard-code the handles into the GATT client (although some devices with custom applications do just that).

A much better answer is that you do service discovery. The phrase service discovery includes discovering all the attributes of a device including services, characteristics and descriptors. This is done using the GATT procedures that were introduced in sections just above: "Read by Group Type", "Find by Type Value", "Read by Type" and "Find Information".

### 6.6.1 Service discovery algorithm

The steps in the service discovery algorithm are:

1. Do one of the following:
  - a. Discover all the services using "Read by Group Type" which gives you the UUID and start and end handles of all the service groups.
  - b. Discover one specific service by using "Find by Type Value" which gives you the start and end handles of the specified service group.
2. For each service group discover all the characteristics using "Read by Type" with the handle range of the service group or groups that you discovered in step (1). This gives you the characteristic handles, characteristic value handles, UUIDs, and permissions of each characteristic.
3. Using the characteristic handles from (2) you can then calculate the start and end handle ranges of each of the descriptors for each characteristic.
  - a. The range for a given characteristic starts at the next handle after the characteristic's value handle and ends either at the end of the service group (if it's the last characteristic in the service group) or just before the next characteristic handle (if it isn't the last characteristic in the service group).
4. Using the ranges from (3) discover the descriptors using the GATT procedure "Find Information". This gives you the attribute type of each descriptor.

### 6.6.2 Service discovery implementation

The btstack library has a service discovery API that can discover services, characteristics and descriptors:

```
wiced_bt_gatt_status_t wiced_bt_gatt_client_send_discover (uint16_t conn_id,
                                                         wiced_bt_gatt_discovery_type_t discovery_type,
                                                         wiced_bt_gatt_discovery_param_t *p_discovery_param );
```

The discovery type is an enumeration (note that GATT\_DISCOVER\_MAX is not a legal parameter):

```
enum wiced_bt_gatt_discovery_type_e
{
    GATT_DISCOVER_SERVICES_ALL = 1,           /**< discover all services */
    GATT_DISCOVER_SERVICES_BY_UUID,          /**< discover service by UUID */
    GATT_DISCOVER_INCLUDED_SERVICES,         /**< discover an included svc within a svc */
    GATT_DISCOVER_CHARACTERISTICS,           /**< discover characteristics of a service*/
}
```

```
GATT_DISCOVER_CHARACTERISTIC_DESCRIPTOR, /**< discover characteristic descriptors */
GATT_DISCOVER_MAX                      /* maximum discovery types */
};
```

The discovery parameter contains:

```
typedef struct
{
    wiced_bt_uuid_t uuid;           /**< Service or Characteristic UUID */
    uint16_t s_handle;             /**< Start handle for range to search */
    uint16_t e_handle;             /**< End handle for range to search */
} wiced_bt_gatt_discovery_param_t;
```

The UUID entry in the discovery parameter structure is itself a structure that allows you to specify a 2, 4, or 16byte UUID (i.e. 16, 32, or 128 bits):

```
/** UUID Type */
typedef struct
{
    #define LEN_UUID_16      2      /**< 2 Byte UUID */
    #define LEN_UUID_32      4      /**< 4 Byte UUID */
    #define LEN_UUID_128     16     /**< 16 Byte UUID */

    uint8_t len;                /**< UUID length */

    /** UUID Data */
    union
    {
        uint16_t uuid16; /**< 16-bit UUID */
        uint32_t uuid32; /**< 32-bit UUID */
        uint8_t  uuid128[MAX_UUID_SIZE]; /**< 128-bit UUID */
    } uu;
} wiced_bt_uuid_t;
```

After you call `wiced_bt_gatt_send_discover`, the stack will issue the correct GATT Procedure. Then, each time the GATT server responds with some information you will get a GATT callback with the event type set to `GATT_DISCOVERY_RESULT_EVT`.

The result is provided in the `discovery_result` entry in the event data structure. It contains the connection ID, type of discovery that the result came from, and the data itself. You can work your way through this structure to find out what you need to know about the server. For example, to find the service start and end handles after running `GATT_DISCOVER_SERVICES_BY_UUID` you could do this:

```
if( p_event_data->discovery_result.discovery_type == GATT_DISCOVER_SERVICES_BY_UUID )
{
    serviceStartHandle = p_event_data->discovery_result.discovery_data.group_value.s_handle;
    serviceEndHandle = p_event_data->discovery_result.discovery_data.group_value.e_handle;
}
```

When the discovery is complete you will get one more GATT callbacks with the event type set to `GATT_DISCOVERY_CPLT_EVT`.

Your firmware would typically be a state machine that would sequence through the service, characteristic and descriptor discoveries as the `GATT_DISCOVERY_CPLT_EVT` is completed.



---

## 6.7 Running a GATT Server

Although somewhat uncommon, there is no reason why a Bluetooth® LE central cannot run a GATT server. In other words, all combinations of GAP peripheral/central and GATT server/client are legal. An example of this might be a TV that has a Bluetooth® LE remote control. Recall that the device that needs to save power is always the peripheral, in this case the remote control. However, the TV is the thing being controlled, so it would have the GATT database remembering things like channel, volume, etc.

The firmware that you write on a central to run a GATT database is EXACTLY the same as on a peripheral.

## 6.8 Exercises

The exercises in this chapter require two kits - a peripheral and a central. You can use another CY8CKIT-062S2-43012, CY8CPROTO-062-4343W or CY8CPROTO-062S2-43439 as the peripheral.

The peripheral application is a combination of the exercises from previous chapters. It advertises the device name and the service UUID. It uses high-duty advertising and it never times out. The RGB LED can be written to using a characteristic that can be read and written without authentication. The characteristic takes a value from 0 (off) to 7 (white). A button counter characteristic, which is incremented by pressing the user button 1 on the peripheral, requires pairing before the central can read it or enable notifications.

*Note: If you are using a CY8CPROTO-062-4343W or CY8CPROTO-062S2-43439 kit for the peripheral, they do not have an RGB LED. For those kits, the user LED will turn off for a value of 0 and will turn on for any other value of the LED characteristic from 1 to 7.*

### Exercise 1: Make an observer

In this exercise you will first program the peripheral and then you will build an observer that will listen to all the Bluetooth® LE devices that are advertising and will print out the BD Address of each device that it finds.

#### Create/Test peripheral



1. Make sure only the kit that you intend to use as a peripheral is plugged into your computer.



2. Create a new ModusToolbox™ application for the BSP you are using as the peripheral.

On the application template page, use the **Browse** button to start from the template found in *Templates/ch06\_ex01\_peripheral*. Keep the same name.



3. Use the Bluetooth® configurator to change the device name to `<inits>_per`.

*Note: Because the advertising packet is limited to 31 bytes, the name you use must be 8 characters or less.*



4. Review the GATT properties and permissions for the characteristics and CCCD for this application. This will be important when we read/write the values in later exercises. They are:

**LED:** read and write authentication are not required, write and write without response are both supported

**BUTTON\_COUNT:** read authentication is required

**CCCD:** read and write authentication are required, write is supported, but write without response is not supported



5. Open a UART terminal to the central if it isn't already open, then build the application and program it to the kit.



6. Use AIROC™ Connect to test the application:

- i. Write a number between 0 and 7 to the LED characteristic to control the RGB LED (for the CY8CKIT-062S2-43012) or to turn on/off CYBSP\_USER\_LED (for the CY8CPROTO-062-4343W or CY8CPROTO-062S2-43439).

- ii. Enable notifications and press the button on the kit to receive notifications.



1. Disconnect from the kit and close the UART window.

- ☐ 2. Unplug the peripheral kit so that you don't accidentally re-program it with the central application.

*Note: You should not need to re-program this kit again and so, if possible, plug it into a USB charger instead of your computer.*

### Create/Test observer

- ☐ 1. Plug the kit that you are going to use for the observer into your computer.
- ☐ 2. Create a new ModusToolbox™ application for the BSP you are using for the central.

On the application template page, use the **Browse** button to start from the template found in *Templates/ch06\_ex01\_observer*. Keep the same name.

*Note: The template sets the PSoC™ 6 **System > Power > System Idle Power Mode** to **CPU Sleep** because the UART used as a user interface in later exercises will not function in Deep Sleep.*

- ☐ 3. Open the Bluetooth® configurator and set it up for an observer as shown in section 6.2.

*Note: Be sure to change the first part of the **Device Address** from 00A050 to 00A051 so that your observer and peripheral will not have the same address.*

- ☐ 4. In main.c create a function declaration and a callback function to process the scanned advertising packets. The function should look like this:

```
void scanCallback( wiced_bt_ble_scan_results_t *p_scan_result, uint8_t *p_adv_data )
{
    if (p_scan_result->remote_bd_addr != NULL && p_scan_result != NULL)
    {
        printf("Host = ");
        print_bd_address(p_scan_result->remote_bd_addr);
    }
}
```

*Note: The template has TODO comments where changes are required.*

- ☐ 5. Add a call to `wiced_bt_ble_scan` in the `BTM_ENABLED` event with a function pointer to the callback function you created in the previous step.

Enable filtering so that each new device only shows up once – otherwise you will see a LOT of packets from all the existing devices.

- ☐ 6. Open a UART terminal, then build the application and program it to the kit.

- ☐ 7. Once the application starts, you should see a list of devices that are advertising. When high duty scanning times out, you will get a similar list for low duty scanning. Scanning will stop after the low duty timeout.

## Exercise 2: Parse the device name and list only your peripheral

In this exercise you will extend the previous exercise so that it examines the advertising packet to find the device name. It will only print out the address of your device instead of all devices that are found.

- ☐ 1. If your peripheral is plugged into your computer, unplug it so that you don't accidentally re-program it.
- ☐ 2. Create a new ModusToolbox™ application for the BSP you are using for the central.

On the application template page, use the **Browse** button to start from the previous completed exercise. If you did not complete that exercise, the solution can be found in *Projects/key\_ch06\_ex01\_observer*. Name the new application *ch06\_ex02\_mydev*.

- ☐ 3. Use the Bluetooth® configurator to change the device name to `<init>_mydev`.

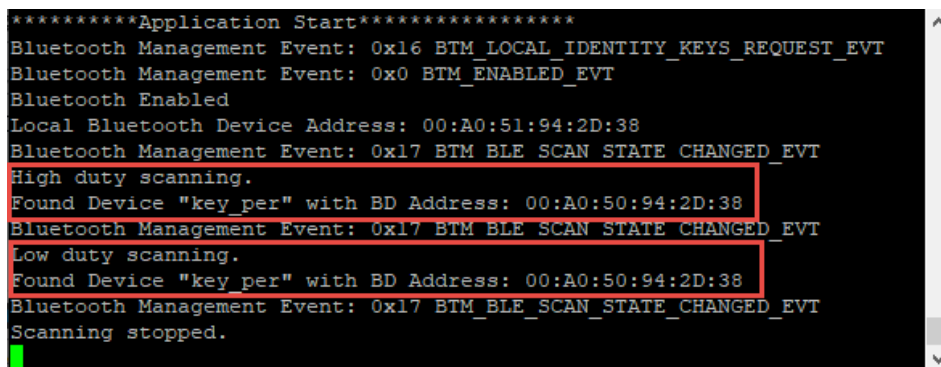
*Note:* This step isn't strictly necessary since the central never advertises its name, but we will update it for consistency.

- ☐ 4. Update the scanner callback function so that it looks at the advertising packet. Find and print out the device name and address only for devices that match your peripheral's device Name.

*Note:* Use the function `wiced_bt_ble_check_advertising_data` to look at the advertising packet and find fields of type `BTM_BLE_ADVERT_TYPE_NAME_COMPLETE`. If there is a field that matches it will return a pointer to those bytes and a length.

*Note:* Use `memcmp` to see if the field contents match the name you are looking for.

- ☐ 5. Open a UART terminal to the central if it isn't already open, then build the application and program it to the kit.
- ☐ 6. Plug your peripheral back in (if necessary).
- ☐ 7. On the UART terminal for the central, you should see a result just for your device.



```
*****Application Start*****
Bluetooth Management Event: 0x16 BTM_LOCAL_IDENTITY_KEYS_REQUEST_EVT
Bluetooth Management Event: 0x0 BTM_ENABLED_EVT
Bluetooth Enabled
Local Bluetooth Device Address: 00:A0:51:94:2D:38
Bluetooth Management Event: 0x17 BTM_BLE_SCAN_STATE_CHANGED_EVT
High duty scanning.
Found Device "key_per" with BD Address: 00:A0:50:94:2D:38
Bluetooth Management Event: 0x17 BTM_BLE_SCAN_STATE_CHANGED_EVT
Low duty scanning.
Found Device "key_per" with BD Address: 00:A0:50:94:2D:38
Bluetooth Management Event: 0x17 BTM_BLE_SCAN_STATE_CHANGED_EVT
Scanning stopped.
```

*Note:* The *retarget-io* library on the central is configured with flow control. This is necessary for the CYW920829M2EVK-02 kit to operate properly when using the UART for input. Therefore, you must keep a UART terminal open to prevent the Tx buffer from filling up, which may cause the firmware to hang.

*Note:* The peripheral is not configured with flow control so a UART terminal is optional for the peripheral.

## Exercise 3: Connect to your peripheral and turn LED ON/OFF

In this exercise, you will modify the previous exercise to connect to your peripheral once it is located. We will decide the device to connect to by matching to your peripheral's device name.

*Note: In real-world applications, it would be more common to search for a service UUID or manufacturer data instead of the device name, depending on what the peripheral provides.*

Once connected, you will be able to send values to the LED characteristic to turn the LED off/on. You will also be able to read the current state of the LED from the peripheral.

To simplify the application, you will hard-code the handle. However, in the upcoming exercises you will add service discovery.

Since there are a lot of additions to be made, we will do them in f parts and will test each one along the way.

### Use UART interface to start/stop scanning

- ☐ 1. If your peripheral is plugged into your computer, unplug it so that you don't accidentally re-program it.
- ☐ 2. Create a new ModusToolbox™ application for the BSP you are using for the central.
- ☐ On the application template page, use the **Browse** button to start from the previous completed exercise. If you did not complete that exercise, the solution can be found in *Projects/key\_ch06\_ex02\_mydev*. Name the new application *ch06\_ex03\_connect*.
- ☐ 3. Use the Bluetooth® configurator to change the device name to `<inits>_connect`.
- ☐ 4. The template that you started with already has a UART with a receive interrupt and a task to handle character input. Change the value for `#define UART_ENABLE` in *main.c* to `true` to enable it.
- ☐ 5. Review the interrupt service routine (`rx_cback`) and UART task (`uart_task`) to understand how they work.
- ☐ 6. Update the UART task to start scanning (lower case **s**) and stop scanning (upper case **S**).
- ☐ 7. Remove the call to `wiced_bt_ble_scan` from the `BTM_ENABLED_EVT` event.
- ☐ 8. Open a UART terminal to the central if it isn't already open, then build the application and program it to the kit.
- ☐ 9. Plug your peripheral back in (if necessary).
- ☐ 10. Verify that the keyboard interface works by typing **s** in the UART terminal to start scanning and then **S** to stop scanning. Type **?** to see the help message.

### Add GATT connect/disconnect functionality

- ☐ 1. If your peripheral is plugged into your computer, unplug it so that you don't accidentally re-program it.
- ☐ 2. Update your scan callback function to connect to the Peripheral when it finds one that it recognizes by calling `wiced_bt_gatt_le_connect`.

*Note: Use the Device Name of your peripheral here so that it will only connect to your device.*

- ☐ 3. After making the connection, turn off scanning.
- ☐ 4. Add a **d** command to the UART interface to call the disconnect function.

*Note: Remember that the disconnect function does not have "le" in its name.*

*Note: Don't forget to add the new command to the help message.*

- ☐ 5. Open a UART terminal to the central if it isn't already open, then build the application and program it to the kit.
- ☐ 6. Plug your peripheral back in (if necessary).
- ☐ 7. Test the following:
  - a. Start scanning and connect (**s**)
  - b. Verify that the peripheral is found and the central connects to it
  - c. Disconnect (**d**)

### Add LED control functionality

- ☐ 1. If your peripheral is plugged into your computer, unplug it so that you don't accidentally re-program it.
- ☐ 2. Create a new global `uint16_t` variable called `ledHandle`.

Hard-code its initial value to the handle of the LED characteristic's Value from the peripheral. You won't change the variable in this exercise, but in a future one you will find the handle via a service discovery.

*Note: Make sure you use the handle for the characteristic's value, not the characteristic declaration.*

*Note: The easiest way to find the handle number is to open the file `GeneratedSource/cycfg_gatt_db.h` from the peripheral application. The characteristic handles have the prefix `HDLC`.*

- ☐ 3. Create a new function to write a GATT attribute. It will take the connection ID, handle, offset, authorization required, length of the data to write, and a pointer to the value to write.

If there is no connection or the handle is 0 then the function should just return. Otherwise, setup the write parameter structure and then call `wiced_bt_gatt_client_send_write` to send the value to the peripheral.

*Note: For now, the handle will never be 0 since we hard-coded it, but this will be useful once we add service discovery.*

*Note: The LED characteristic on the server allows both "write" and "write with response" commands. Use write with response (`GATT_REQ_WRITE`) in the `wiced_bt_gatt_client_send_write` function call so that the same function will work to write the CCCD value in later exercises (which requires write with response).*

*Note: The `GATT_OPERATON_CPLT_EVT` already prints out a message when a GATT operation is successful. For simplicity, we won't do any other checking specific to write responses.*

- ☐ 4. In the UART interface, call the function you created when values from 0 – 7 are entered.

*Note: The case is already provided for you, but don't forget to add a help message.*

*Note: Since we are not pairing yet, use `GATT_AUTH_REQ_NONE` for the authorization required. Recall that the LED characteristic on the server does not require authentication for read or write so this will work.*

- ☐ 5. Open a UART terminal to the central if it isn't already open, then build the application and program it to the kit.
- ☐ 6. Plug your peripheral back in (if necessary).
- ☐ 7. Test the following:
  - a. Start scanning and connect (**s**)
  - b. Verify that the peripheral is found and the central connects to it
  - c. Change the LED color by typing values from **0** to **7**
  - d. Disconnect (**d**)

#### Add LED read functionality

- ☐ 1. If your peripheral is plugged into your computer, unplug it so that you don't accidentally re-program it.
- ☐ 2. Create a new global `uint16_t` variable called `ledStatus`.
- ☐ 3. Add a UART command (**r**) to read the value of the LED from the peripheral and print it to the terminal.

*Note: Use `GATT_AUTH_REQ_NONE` as the required authorization so that the value can be read without pairing first.*

*Note: Don't forget to add the new command to the help message.*

- ☐ 4. The GATT event callback function already has a case for `GATT_OPERATON_CPLT_EVT` and it checks if the command was successful or not. Add nested `if` statements to check the operation type and the handle whose value was read and print out the value of the LED if the event was a read of that characteristic.
- ☐ 5. Open a UART terminal to the central if it isn't already open, then build the application and program it to the kit.
- ☐ 6. Plug your peripheral back in (if necessary).
- ☐ 7. Test the following:
  - a. Start scanning and connect (**s**)
  - b. Verify that the peripheral is found and the central connects to it
  - c. Change the LED color by typing values from **0** to **7** and verify each value after writing it by typing **r**.
  - d. Disconnect (**d**)

## Exercise 4: Add commands to enable/disable notifications

In this exercise, you will enhance the previous exercise to allow the CCCD to be turned on/off so that notifications for the button characteristic can be enabled/disabled. You will print out messages when notifications are received.

- ☐ 1. If your peripheral is plugged into your computer, unplug it so that you don't accidentally re-program it.
- ☐ 2. Create a new ModusToolbox™ application for the BSP you are using for the central.
- ☐ 3. On the application template page, use the **Browse** button to start from the previous completed exercise. If you did not complete that exercise, the solution can be found in *Projects/key\_ch06\_ex03\_connect*. Name the new application *ch06\_ex04\_connect\_notify*.
- ☐ 4. Use the Bluetooth® configurator to change the device name to `<init>_connect_notify`.
- ☐ 5. In the GATT connect event handler, initiate pairing by calling `wiced_bt_dev_sec_bond` for the connected case.

*Note:* This is necessary because the CCCD permissions for your Peripheral are set such that it cannot be read or written unless the devices are paired first.

*Note:* This must be done after the connection is established so that's why it is inside the GATT connect event handler.

- ☐ 6. Add a new `uint16_t` global variable called `cccdHandle` to hold the handle of the CCCD and one called `buttonCountHandle` to hold the handle of the button count characteristic's value.

Hard-code its initial value to the handle of the button counter characteristic's CCCD from the peripheral. You won't change the variable in this exercise, but in a future one you will find the handle via a service discovery.

*Note:* The easiest way to find the handle number is to open the file *GeneratedSource/cycfg\_gatt\_db.h* from the peripheral application. The characteristic descriptor handles have the prefix `HDLD`.

- ☐ 7. Add cases in the UART to set (n) and unset (N) to set and unset the CCCD using the same attribute write function you created to write to the LED.

*Note:* Remember that the CCCD value is 2 bytes so the write length must be 2.

Use `GATT_AUTH_REQ_NO_MITM` for the required authorization so that pairing is required to write the CCCD but MITM protection is not required. This is necessary because both the peripheral and client have their pairing IO capabilities set to `BTM_IO_CAPABILITIES_NONE` which means that MITM protection can't be achieved. If you were to set the authorization to require MITM, the client would attempt to pair again (and would fail).

- ☐ 8. In the `GATT_OPERATION_CPLT_EVT`, if the operation was successful, check to see if the operation was `GATT_OPTYPE_NOTIFICATION`. If it was, print out the notification value that was received.

*Note:* The operation type can be found in:  
`p_event_data->operation_complete.op`

*Note:* The data is provided as a `uint8_t` pointer in:  
`p_event_data->operation_complete.response_data.att_value.p_data`  
The length of the data is provided in:  
`p_event_data->operation_complete.response_data.att_value.len`



- 
- ☐ 9. Open a UART terminal to the central if it isn't already open, then build the application and program it to the kit.
  - ☐ 10. Plug your peripheral back in (if necessary).
  - ☐ 11. Test the following:
    - a. Start Scanning and connect (**s**)
    - b. Verify that the connection is made
    - c. Press the button on the peripheral. Notifications are not enabled so you should not see a response.
    - d. Enable Notifications (**n**)
    - e. Press the button on the peripheral. You should see a response in the UART.
    - f. Disable Notifications (**N**)
    - g. Press the button on the peripheral. You should not see a response.
    - h. Disconnect (**d**)

## Exercise 5: Implement service discovery

In this exercise, instead of hardcoding the handles for the LED and Button CCCD, you will modify the previous exercise to do a service discovery. Instead of triggering the whole process with a state machine, you will use keyboard commands to launch each stage.

The three stages are:

- 'q'= Service discovery with the UUID of the service to get the start and end handles for the service group.
- 'w'= Characteristic discovery with the range of handles from step 1 to discover all characteristic handles and characteristic value handles.
- 'e' = Descriptor discovery of the button characteristic to find the CCCD handle.



1. If your peripheral is plugged into your computer, unplug it so that you don't accidentally re-program it.



2. Create a new ModusToolbox™ application for the BSP you are using for the central.

On the application template page, use the **Browse** button to start from the previous completed exercise. If you did not complete that exercise, the solution can be found in *Projects/key\_ch06\_ex04\_connect\_notify*. Name the new application *ch06\_ex05\_discover*.



3. Use the Bluetooth® configurator to change the device name to `<init>_discover`.



4. Open the file *GeneratedSource/cycfg\_gatt\_db.h* from the peripheral application and copy over the macros for the following into the *main.c* file for use in this exercise:

```
__UUID_SERVICE_PSOC
__UUID_CHARACTERISTIC_PSOC_LED
__UUID_CHARACTERISTIC_PSOC_BUTTON_COUNT
__UUID_DESCRIPTOR_CLIENT_CHARACTERISTIC_CONFIGURATION
```

*Note: This guarantees that the Central uses the same UUIDs that are used in the Peripheral.*

### Global Variables



5. Create variables to save the start and end handles of the "PSOC" service group and create a variable to hold the "PSOC" Service UUID.

```
static const uint8_t serviceUUID[] = { __UUID_SERVICE_PSOC};
static uint16_t serviceStartHandle = 0x0001;
static uint16_t serviceEndHandle = 0xFFFF;
```



6. Define a new structure type to manage the discovered handles of the characteristics:

```
typedef struct {
uint16_t startHandle;
uint16_t endHandle;
uint16_t valHandle;
uint16_t cccdHandle;
} charHandle_t;
```



7. Create a `charHandle_t` structure for the LED and the button counter characteristic groups and variables with the characteristic UUIDs to search for.

```
static const uint8_t ledUUID[] = { __UUID_CHARACTERISTIC_PSOC_LED };  
static charHandle_t ledChar;  
static const uint8_t counterUUID[] = { __UUID_CHARACTERISTIC_PSOC_BUTTON_COUNT };  
static charHandle_t counterChar;
```



8. Create an array of `charHandle_t` to temporarily hold the characteristic handles while they are discovered.

*Note:* When you discover the characteristics, you won't know what order they will occur in, so you need to save the handles temporarily to calculate the end of group handles.

```
#define MAX_CHARS_DISCOVERED (10)  
static charHandle_t charHandles[MAX_CHARS_DISCOVERED];  
static uint32_t charHandleCount;
```

### Service Discovery (q)



9. Add a function to launch the service discovery called `startServiceDiscovery`.

This function will be called when the user presses **q**. Instead of finding all the UUIDs you will turn on the filter for just the "PSoC" Service UUID.

- Setup a structure of type `wiced_bt_gatt_discovery_param_t` with the starting and ending handles set to `0x0001` and `0xFFFF`. This covers all possible handle values.
- Set the UUID to be the UUID of the "PSoC" service.

*Note:* The "PSoC" Service uses a 128-bit UUID so you will need something like this:

```
discovery_param.uuid.len = LEN_UUID_128;  
memcpy( &discovery_param.uuid.uu.uuid128, serviceUUID, LEN_UUID_128 );
```

- Use `memcpy` to copy the service UUID into the `wiced_bt_gatt_discovery_param_t` structure.
- Set the discovery type to `GATT_DISCOVER_SERVICES_BY_UUID` and call the `wiced_bt_gatt_send_discover` function.



10. Add the case `GATT_DISCOVERY_RESULT_EVT` to the GATT event handler.

If the discovery type is `GATT_DISCOVER_SERVICES_BY_UUID` then update the `serviceStart` and `serviceEnd` handles with the returned start and end handles (remember you can use `GATT_DISCOVERY_RESULT_SERVICE_START_HANDLE` and `GATT_DISCOVERY_RESULT_SERVICE_END_HANDLE`).

### Characteristic Discovery (w)



11. Add a function to launch the Characteristic discovery called `startCharacteristicDiscovery` when the user presses **w**.

- Set the global variable `charHandleCount` to 0. This must be done here so that each time a new characteristic discovery is started the variable that keeps track of how many characteristics have been found is reset.

- b. Setup a structure of type `wiced_bt_gatt_discovery_param_t` with the start and end handles to the range you discovered in the previous step (i.e. the service group start/end handles).

*Note:* Use `serviceStartHandle + 1` for the search start handle since we already know the first handle must be the service UUID.

- c. Call `wiced_bt_gatt_send_discover` with the discovery type set to `GATT_DISCOVER_CHARACTERISTICS`.



12. In the `GATT_DISCOVERY_RESULT_EVT` of the GATT event handler add an `if` statement for the characteristic result.

- a. Inside the `if`, save the `startHandle` and `valueHandle` in the `charHandles` array. Set the `endHandle` to the end of the service group (assume that this new characteristic is the last one in the service). If this is not the first characteristic that you found, then re-set the previous characteristic's end handle now that you know it wasn't the last one. It will be just before the new start handle. For example:

```
if( charHandleCount != 0 )
{
    charHandles[charHandleCount-1].endHandle =
        charHandles[charHandleCount].startHandle-1;
}
charHandleCount += 1;
```

*Note:* The point is to assume that the current characteristic ends at the end of the service group. But, if you find another characteristic, then you know that the end of the previous characteristic's end handle is the start of the new characteristic minus 1.

- b. Check if the characteristic is the LED or button counter characteristic based on the UUID. If it is one of those, then copy the start and value handles in the appropriate structure that you created (`ledChar` or `counterChar`). The end handles will not be done until characteristic discovery is complete because we won't know the true end handles until then. We'll add that next.



13. Add a case for the `GATT_DISCOVERY_CPLT_EVT` to get the LED and button counter end handles from the temporary array once characteristic discovery has finished.

You should first check to see if it is a characteristic discovery that just completed. If it is, copy the LED and button counter `endHandle` from the `charHandles` array. Your code could look something like this:

```
// Once all characteristics are discovered... you need to setup the end handles
if( p_event_data->discovery_complete.discovery_type ==
    GATT_DISCOVER_CHARACTERISTICS )
{
    for( int i=0; i<charHandleCount; i++ )
    {
        if( charHandles[i].startHandle == ledChar.startHandle )
            ledChar.endHandle = charHandles[i].endHandle;
        if( charHandles[i].startHandle == counterChar.startHandle )
            counterChar.endHandle = charHandles[i].endHandle;
    }
}
```

### Descriptor Discovery (e)

- ☐ 14. Add a function to launch the Descriptor discovery called `startDescriptorDiscovery` when the user presses **e**.

The purpose of this function is to find the CCCD handle for the button counter characteristic.

*Note: Rather than make a generic descriptor discovery function, we will just look at the button counter characteristic since that's the only characteristic that we want to control notifications on.*

- a. It will need to search for all descriptors in the button counter characteristic's group.

*Note: Since you know the first 2 attributes in the characteristic group are the characteristic declaration and the characteristic value, you can use the counter value handle + 1 for the start of the search space and the end handle for the end of the search space.*

- b. Once the parameters are setup, launch `wiced_bt_gatt_send_discover` with `GATT_DISCOVER_CHARACTERISTIC_DESCRIPTOR`.

- ☐ 15. In the `GATT_DISCOVERY_RESULT_EVT` of the GATT event handler add an `if` statement for the descriptor result.

If the descriptor UUID is `__UUID_DESCRIPTOR_CLIENT_CHARACTERISTIC_CONFIGURATION`, save the CCCD handle.

- ☐ 16. Add the commands for 'q', 'w', and 'e' to call your three new functions to the UART task. Also add those keys to the help message.

### Use Discovered Handles

- ☐ 17. Remove the 3 variables that have the hard-coded handle values for the LED value, button count value, and CCCD value (`ledHandle`, `buttonCountHandle` and `cccdHandle`) so that we can see that service discovery works.

- ☐ 18. In the places where the old variables are used, change the code to use the `valHandle` or `cccdHandle` element from the appropriate `charHandle_t` structure (`ledChar` or `counterChar`).

### Testing

- ☐ 19. Open a UART terminal to the central if it isn't already open, then build the application and program it to the kit.

- ☐ 20. Plug your peripheral back in (if necessary).

- ☐ 21. Test the following:

- ☐ a. Start scanning and connect (**s**)
- ☐ b. Try to control the LED (**0...7**) and notice that nothing happens because the handles have not been discovered yet
- ☐ c. Discover the "PSoC" Service (**q**)
- ☐ d. Discover the LED and counter characteristics (**w**)
- ☐ e. Discover the button CCCD (**e**)

- ☐ f. Control the LED (**0...7**)
- ☐ g. Turn on notifications (**n**)
- ☐ h. Press the button on the peripheral to observe the notification
- ☐ i. Turn off notifications (**N**)
- ☐ j. Press the button on the peripheral to observe notifications are disabled
- ☐ k. Disconnect (**d**)

#### Trademarks

All referenced product or service names and trademarks are the property of their respective owners.

**Published by**  
**Infineon Technologies AG**  
**81726 Munich, Germany**

**© 2024 Infineon Technologies AG.**  
**All Rights Reserved.**

#### IMPORTANT NOTICE

The information given in this document shall in no event be regarded as a guarantee of conditions or characteristics ("Beschaffenhheitsgarantie").

With respect to any examples, hints or any typical values stated herein and/or any information regarding the application of the product, Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party.

In addition, any information given in this document is subject to customer's compliance with its obligations stated in this document and any applicable legal requirements, norms and standards concerning customer's products and any use of the product of Infineon Technologies in customer's applications.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office ([www.infineon.com](http://www.infineon.com)).

#### WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.