BLE Tracker

Firmware Specification

V1.2

Contents

Glossary

Term	Description
BA	Bluetooth Address – A unique 6 byte address similar to a MAC.
BAS	Battery Service – A BLE service for transmitting battery level.
BLE	Bluetooth Low Energy
CRC	Cyclic Redundancy Check – A 16-bit value to check data integrity.
DIS	Device Information Service – A BLE service for transmitting device configuration.
GAP	Generic Application Profile – A BLE topology specification.
GATT	Generic ATTribute profile – A BLE transfer protocol.
LoT	Location of Things
LoTP	LoT Peripheral – The low power BLE tracking device.
LoTC	LoT Central – Any device communicating with the LoTP via BLE.
OTA	Over The Air – An “over the air” upgrade.
RFU	Reserved for Future Use.
TCS	Telstra Custom Service – A BLE service that provides a custom interface for LoT.
UUID	Universally Unique IDentifier.

Table 1: Glossary

1. Introduction

This document specifies the features and behaviours of the Telstra “Location of Things” Bluetooth Low Energy Tracker. This tracker is designed for passive and active BLE tracking using an established infrastructure to locate LoT devices.

Two types of devices are required for tracking, a LoT peripheral and a LoT central device. The BLE tracker is called the LoTP. The LoTP will communicate via the LoTC to the cloud.

The LoTP emit an advertising packet via BLE that any compatible nearby device can detect. The compatible device will then communicate to the cloud the approximate location of the tracker device. Note that this is a unidirectional communication, the compatible device sends no information to the tracker.

When required, the LoTC can connect to the LoTP to collect statistics or play a tune on the LoTP to aid finding the LoTP. The BLE connection consume significant power and so devices should only be connected for brief periods.

The LoTP contains a button. BLE advertising and connection parameters are used to communicate when a button has been pressed to the LoTC/cloud.

The LoTP provides multiple methods so that the LoTC/cloud can authenticate it as a legitimate LoTP.

2. BLE Interface

The Bluetooth interface is divided into a connected interface and an advertising interface. The advertising interface consists of both BLE advertising packets and BLE scan response packets. The connected interface consists of three BLE services: a custom Telstra service, Device Information Service (DAS), and BAttery Service (BAS).

2.1. Advertising Packets

The LoTP is configured to send an advertising packet once every 2570ms; this is not configurable. The advertising packet is updated periodically.

The advertising packet consists of one GAP advertisement element: Manufacturer Specific data (0xFF).

The contents of the element are detailed below.

Name	Start Byte:Bit	Byte:Bit Count	Description
Manufacturer ID	0x00	2	Telstra's Bluetooth manufacturer ID (0x0145)
Advert Revision	0x02:0	0:5	A number that uniquely identifies the format of the rest of the advertisement. (0)
Device Type	0x02:5	0:3	A unique LoTP device type. (0 for Bartlett, 1 for Stone)
Bluetooth Address	0x03	6	The BA of this device.
Notifier	0x09:0	0:1	A value that changes to avoid iOS caching advertisements. (random number)
Button Presses	0x09:1	0:3	Number of times the button has been pressed. (lifetime counter unaffected by factory reset)
Battery Level	0x09:4	0:4	The battery level: 1 (Critical) < 20% 2 (Good) 20% to 80% 3 (High) >=80%
Authentication Data	0x0A	16	Data used to authenticate this device as a genuine LoTP device.

Table 2:Advertising Packet Contents

The manufacturer ID field is a unique ID assigned to Telstra by the Bluetooth SIG.

The button presses field is over the lifetime of the device. Only three bits are allocated for this purpose and so the value is modulo 8.

The authentication data field is used to authenticate this device as a genuine LoTP device when not connected via BLE. See Section 4.3 for details.

Note that bit fields start from low bits first.

2.2. Scan Response Packets

The scan response data provides a small amount of additional data without connecting to the LoTP. This data cannot be acquired in the background of an iOS app and so this data only provides secondary information.

The scan response consists of two elements: Complete Local Name (0x09), and Complete Available 16bit Services (0x03).

The complete local name element is “Telstra LoT”.

The complete available 16-bit services element includes the three BLE Services: the custom Telstra service, DIS and BAS.

2.3. Telstra Custom Service

The TCS is used to provide a custom interface whilst connected via BLE. The following table summarises the characteristics of that service, the BLE access permissions, and the number of bytes of data it expects.

All values are assumed to be Little Endian; this means that the least significant byte is first.

Name	128-bit Characteristic Identification	Read	Write	Notify	Bytes
Authentication	0x0FE6255C-B21B-6F9D-1B09-2496BECA9DC3	✓	✓		16
Buzzer Tune	0xB9A3BB8F-008A-4F03-FF19-CF3E69C1FDE8	✓	✓	✓	1
Buzzer Play Count	0xA20C8F15-02D3-9113-EF55-69E6EBE8441C	✓			4
Buzzer Play Duration	0x84B463DF-5C89-E2FC-D834-55CE4FEAA43E	✓			4
Button Press Count	0x638322B8-03A5-C3B5-A903-7D1B234D431E	✓			4
Total Waking Duration	0x61818723-44A2-E34F-23FB-597B8F1D50B8	✓			4
Connection Count	0x7A19F2CB-82E4-61EE-4BE9-5AAB12C735B2	✓			4
Total Connection Duration	0x5108935B-AF6B-F91F-3592-7E5F766981CB	✓			4
Barris Parameter	0x9BB84F45-9B4F-55E2-048B-8210BBF6F618		✓	✓	1
Read IMEI	0xC5613D00-17F0-4647-A0D7-30D09AD99114	✓			1 - 32
Force Device Check-In	0xFE496040-DE5C-4AE8-ADA5-23029BB47BCB		✓		1

Table 3: Telstra Custom Service Characteristics

2.3.1. Authentication Characteristic

The Authentication Characteristic is used to authenticate this device as a genuine LoTP device whilst connected via BLE. See Section 4.4 for details.

2.3.2. Buzzer Characteristics

The Buzzer Play Count Characteristic keeps track of the number of times a tune has played for in the lifetime of the device. This includes when starting a new tune when one is already playing. It has a maximum value of (2^{16} - 1) or 65535. If it has reached this limit, then playing a new tune will not alter this value.

The Buzzer Play Duration Characteristic keeps track of the total duration of the lifetime of the device that has been spent playing tunes in milliseconds. It has a maximum value of (2^{32} - 1) milliseconds, or around 50 days. Once it has reached that limit, it will increase no further.

2.3.3. Button Press Characteristic

The Button Press Characteristic keeps track of the number of times the button has been pressed in the lifetime of the device. This has a maximum of (2^{32} - 1) or more than 4 billion. If it has reached this limit then pressing the button will not alter this value.

2.3.4. Total Waking Duration Characteristic

The Total Waking Duration Characteristic keeps track of how long the device has been awake for. This includes, but is not limited to when a tune is playing. It has a maximum value of (2^{32} - 1) milliseconds, or around 50 days. Once it has reached that limit, it will increase no further.

2.3.5. Connection Characteristics

The Connection Count Characteristic keeps track of how many times an LoTC has connected to this LoTP via BLE. This count has a maximum of (2^{32} - 1) or more than 4 billion. If it has reached this limit then connecting to this LoTP will not alter this value.

The Total Connection Duration Characteristic keeps track of the total duration of the lifetime of the device that has been spent connected via BLE in milliseconds. It has a maximum value of (2^{32} - 1) milliseconds, or around 50 days. Once it has reached that limit, it will increase no further.

2.4. Device Information Service

The LoTP uses the DIS. It conforms to the BLE standard for this service.

2.5. Battery Service

The LoTP uses the BAS. It conforms to the BLE standard for this service.

3. User Interface

The interface used by LoTP customers consists of a buzzer and a button.

3.1. Buzzer

The LoTP has a piezoelectric speaker used to play tunes. The tunes are part of the enumerated list below. The value is used when interacting with the Buzzer Tune Characteristic of the Telstra Custom Service.

Name	Value	Description
Bip Bip	0x00	Two quick beeps.
Telstra Sting	0x01	A version of the Telstra Sting.

Table 4: Buzzer Tunes

The Bip Bip (Beep Beep) tune is played when the button is pressed. This will interrupt any other playing tune.

The Telstra Tune will play when attempting to locate the LoTP.

3.2. Button

The button is used to provide user interaction. The buzzer will play a tune when the button is pressed. The action perform is executed by the LoTC. If the LoTC is notified by the Button Press Count field of the Manufacturer Specific element of the advertising packet when not connected via BLE. The LoTC is notified by the Button Press Characteristic in the Telstra Custom Service when connected via BLE.

4. Authentication and Security

4.1. Keys and Encryption

All data is encrypted using AES256 in a single 16-byte block. As only one block is ever encoded at one time, no mode of operation is specified.

There is a single 256-bit key used for the entire LoT project; this key will be referred to as the Project Key. Each device will have its own 256-bit key; this key will be referred to as the Device Key. A 256-bit key is used for OTA operations; this key will be referred to as the OTA Key.

4.2. CRC

Data in LoT is validated using CRCs. Specifically, using 16-bit CRCs with a polynomial of 0xA001 and initial value of 0xFFFF. This is the same CRCs that are used by Modbus.

Note that if a 16-bit CRC is stored at the end of the data it is calculated from in little endian format, then the CRC of (the entire data with the CRC appended) will always have the value 0x0000. For this reason, CRCs will always be stored in little endian format after the data which they are calculated on.

4.3. Advertising Authentication

There is a 128-bit block of data in the Manufacturer Specific element of the advertising packet of the LoTP used for authentication. It is encrypted using the Device Key and is updated on a regular basis. Below is a summary of the contents of the authentication block when decrypted. All values are assumed to be Little Endian; this means that the least significant byte is first.

Name	Start Byte	Byte Count	Description
Second Tick	0x00	4	The runtime of the device in seconds.
RFU	0x04	8	Not presently used.
Salt	0x0C	2	Randomised value.
CRC	0x0E	2	CRC of the rest of the packet.

Table 5: Advertising Authentication Block

The Second Tick element is how long the device has been running in seconds. It can be used to detect replay attacks.

The RFU element is not presently used and is presently set to zero.

The Salt element is a randomised value used to increase security.

The CRC element is a 16-bit CRC calculated from the other 14 bytes. It is stored such that the CRC of the entire authentication block has a CRC of 0x0000.

4.4. Telstra Service Authentication

The Telstra Custom Service has an Authentication Characteristic used to ensure that a LoTP is genuine. It a challenge/response characteristic where a certain value is written to the characteristic and the response read from the characteristic is compared to an expected value. The process is outlined below.

1. The LoTC create a 16-byte value with 14 bytes of random data and 2 bytes of zeroes.
2. The LoTC encrypts the 16 bytes using the Project Key.
3. The LoTC writes the encrypted value to the Authentication Characteristic.
4. The LoTP decrypts the value and checks that the last 2 bytes are set to zero.
5. The LoTP fills the last two bytes with a CRC of the previous 14 bytes such that the CRC of the entire 16 bytes is equal to 0x0000.
6. The LoTP encrypts the result with its Device Key.
7. The LoTC/Cloud reads the Authentication Characteristic and decrypts the result.
8. If the CRC of the decrypted 16 bytes is zero, the LoTP is authenticated.

A. Appendix

A.1. Custom Advertisement Example

N/A

A.2. Authentication Characteristic Example

The following is an example of the procedure illustrated in Section 4.4. It uses the default project and device keys.

1. LoTC creates a 16-byte value.

```
Value = [0xe8, 0x2d, 0xd8, 0x4a, 0x47, 0xc9, 0xa5, 0xc7, 0xc3, 0x54, 0x33, 0xe5, 0xe3,
0xda, 0x00, 0x00]
```

2. LoTC encrypts the 16-byte value using the project key.

```
Encypt = [0x5c, 0xce, 0x6a, 0x63, 0x3c, 0x05, 0x09, 0xc6, 0x79, 0xea, 0x65, 0x18, 0x3e,
0xdc, 0x69, 0x94]
```

3. LoTC writes the encrypted value to the Authentication Characteristic
4. LoTP decrypts the value and checks that the last 2 bytes are set to zero.
5. LoTP fills the last two bytes with a CRC of the previous 14 bytes.

```
Value = [0xe8, 0x2d, 0xd8, 0x4a, 0x47, 0xc9, 0xa5, 0xc7, 0xc3, 0x54, 0x33, 0xe5, 0xe3,
0xda, 0x7b, 0x8b]
```

6. LoTP encrypts the result with its Device Key

```
Encrypt = [0xc3, 0x03, 0x10, 0x67, 0x27, 0x6b, 0xd8, 0x1d, 0x3e, 0x1d, 0x78, 0x5b,
0x13, 0xd2, 0x2e, 0x72]
```

7. The LoTC/Cloud reads the Authentication Characteristic and decrypts the result.
8. If the CRC of the decrypted 16 bytes is zero and the first 14 bytes match the initial value, the LoTP is authenticated.

A.3. Development Keys

This project uses 3 keys during development: Project Key, Device Key, and OTA Key. The project key and device key should change during commissioning. The production OTA key should be determined by vendor.

Name	Value	Description
Device Clear	0x21	Remove all current Safe Devices.
Device Add	0x22	Payload is the Safe Device BA.
Device Remove	0x23	Payload is the Safe Device BA.
Pause Duration Get	0x30	Get the duration used to pause application state machine operation.
Pause Duration Set	0x31	Set the pause duration.
Passive Scan Period Get	0x32	Get the period of safe device/zone scans.
Passive Scan Period Set	0x32	Set the period of safe device/zone scans.
Upload Period Get	0x33	Get the delay between uploads.
Upload Period Set	0x34	Set the delay between uploads.

Key	Default Value
Project Key	0x589A45CB24513B4352820A532C0F42F7E28D30254AABDA4BD7215007FDC6FC97
Device Key	0x5A0D4541A40E93A5A90780BCEA5C57D148C8282541474BCE4F0F188EF5545855
OTA Key	0x4CA814D84BF31457E92608F95FB4DDF22BBF4E5EF0E2822C21C7E80A81ECDA56

Table 15: Development Security Keys

A.4 Additional Parameters

The following table contains the additional parameters their values.

Name	Value	Description
IMEI	0x00	IMEI for Customer Subscription association in the backend
Version	0x01	The firmware version of the ESP.
Charge State	0x02	Charging status: 0, not charging; 1, charging; 2, charge complete.
Accelerometer	0x03	Returns error code of accelerometer self-test. Zero indicates success.
Battery Voltage	0x04	The current battery voltage in millivolts.
BT MAC	0x05	MAC Address of the BLE Interface
Wi-Fi Station MAC	0x06	MAC Address of the Wi-Fi Station Interface