TraceTogether Token

Technical Write-up

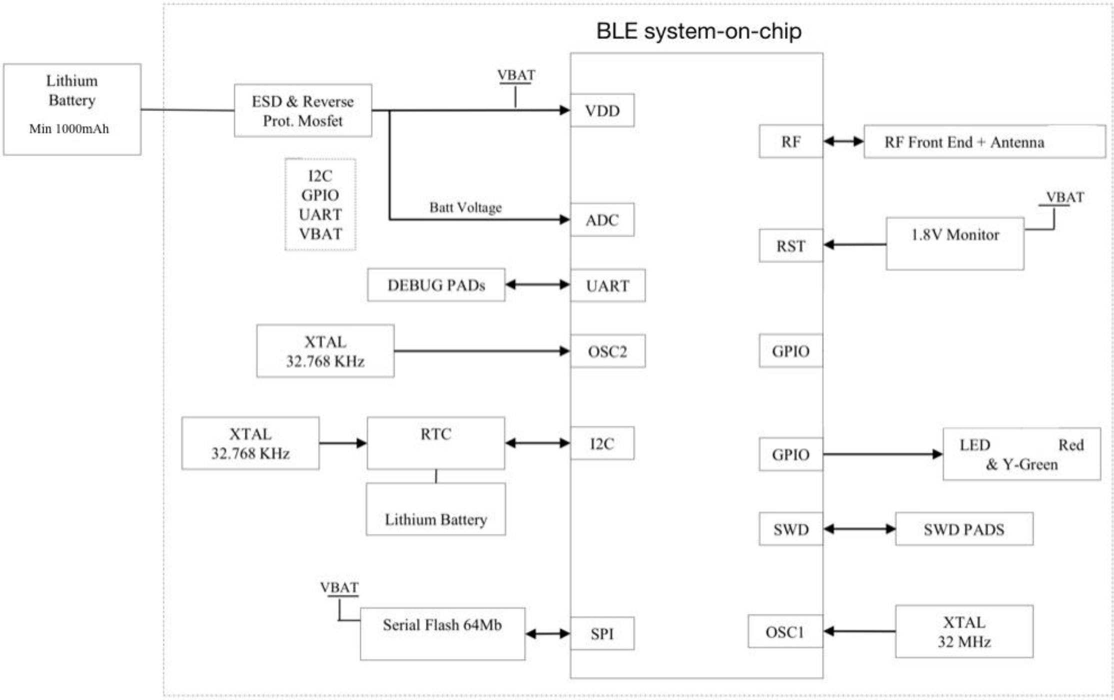
Yang Boon Quek, Director, Sensors and IoT
Government Technology Agency of Singapore

1 Introduction

TraceTogether is Singapore's national deployment of a Bluetooth-based digital contact tracing system to manage the COVID-19 pandemic. The TraceTogether Programme comprises a smartphone app and a portable device (token) of the same name, developed by the Government Technology Agency of Singapore (GovTech) in collaboration with the Ministry of Health. The TraceTogether Token is developed to facilitate greater participation in contact tracing by population segments that include the elderly and children, as well as those who do not have smartphones. This Technical Write-up shares the design and protocol of the TraceTogether Token to enable interoperability of third-party Devices (3PD) within the TraceTogether Programme.

2 Hardware

System Block Diagram

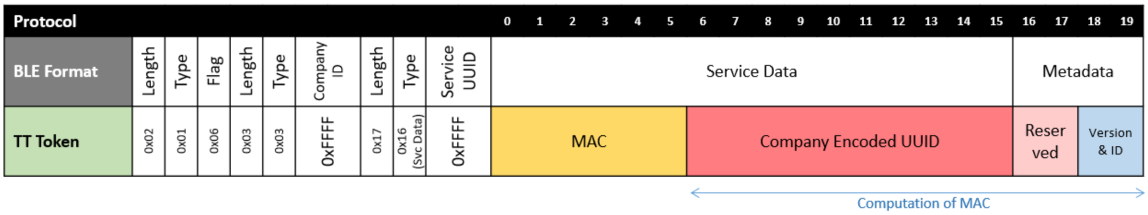


Hardware specifications

- Bluetooth 5 certified wireless microprocessor chip based on a minimum of 32 bit ARM-M4 Cortex with 1MB flash memory.
- Flash memory of at least 64Mb for data storage
- Real time clock (RTC)
- Single use battery or rechargeable Li-ion battery with minimum capacity of 1000mAh
- If rechargeable Li-ion battery is used, battery power management IC and Micro USB for battery charging.
- 2 Led's (Green and Red)
- Debug and SWD breakout pins

3 BlueTrace Lite Protocol

3.1 Interoperability Technical Details: Packet Structure



Protocol										0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
BLE Format	Length	Type	Flag	Length	Type	Company ID	Length	Type	Service UUID	Service Data																Metadata			
TT Token	0x02	0x01	0x06	0x03	0x03	0xFFFF	0x17	0x16 (Svc Data)	0xFFFF	MAC						Company Encoded UUID										Reserved		Version & ID	

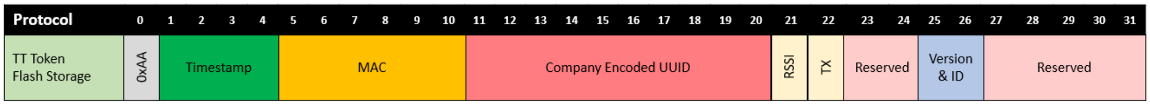
Computation of MAC

- **Licensing:**
  - GovTech will assign a Company ID (Version & ID, Byte 18 and 19) for each company interoperating with TTT
  - 1 x 16 bytes Global Replay Protection Key (RPK) will be provided to each Company

- **Operations:**
  - To transmit a packet, Company shall perform encryption using AES-CTR with the RPK on Company Encoded UUID + Company ID. The encryption output is Message Authentication Code (MAC) and form part of the packet to be transmitted.
  - On receiving the logged data, Company shall perform encryption using AES-CTR with the RPK on Company Encoded UUID + Company ID and compare to the MAC received. Logged data is only saved if the comparison is identical.

3.2 Storage packet to flash memory

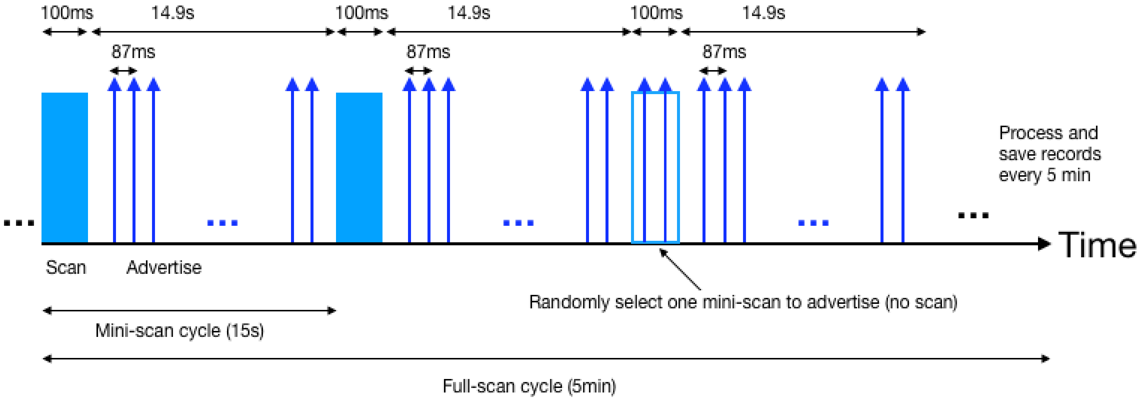
When TraceTogether Token scan the packet advertised by another TraceTogether Token, the receiving Token will then record the data in the flash memory in the following format. Subsequently, if there is a need to contact trace, this record can then be extracted using BLE GATT connection.



Protocol	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
TT Token Flash Storage	0xAA	Timestamp				MAC						Company Encoded UUID										RSSI	TX	Reserved		Version & ID		Reserved				

3.3 Advertise and Scan protocol

The BlueTrace Lite's Advertise and Scan protocol comprises a 5-min Full-scan cycle, which further comprises 20 Mini-scan cycles as shown in the figure below. To enable detection of another token with synchronised timing, the protocol requires a randomly selected Mini-scan cycle in each Full-scan cycle to continue advertising (with 87-ms intervals) in place of the scan period. The 5-min Full-scan cycle is repeated indefinitely.



Scanned packets are checked for unique IDs and stored in internal flash after every Mini-scan cycle. After every Mini-scan, store only unique IDs in internal flash; if a repeat ID is scanned, store the maximum RSSI value and increase nRp (number of repeats) by 1.

At the end of a Full-scan cycle, the scanned packets are sorted according to max RSSI (nRp is only used for reference). Discard all packets below a RSSI threshold of -74dBm. Only the highest 30 records are saved to external flash memory. A maximum of 30 records are saved every 5 mins.

4 Interoperability within TraceTogether Programme

The information shared in this document allows interested parties to understand the technical details behind the TraceTogether Token, and possibly build their own variant of the tokens. These self-built tokens however, are unable to interoperable with the TraceTogether Token, and by extension the TraceTogether App, as there is a still a need to perform security key exchanges for MAC authentication, as well as the need to establish data pipes for sending of contact tracing details between Government and the 3rd Party Device (3PD) providers.

Interested parties who wish to build devices that are able to interoperate with the TraceTogether Token and be part of Singapore Digital Contact Tracing ecosystem (i.e. TraceTogether Programme) can do so by signing a licensing agreement with GovTech. The licensing agreement will spell out the obligation, terms and conditions with regards to joining the TraceTogether Programme.

Upon signing of the agreement, the licensees will be provided the necessary security keys for data exchange, and the technical assistance necessary to test for the interoperability. Interested parties who wish to apply for the interoperability license shall be a registered company with Singapore Accounting and Corporate Regulatory Authority (ACRA)[1].

Interested parties who wish to find out more about interoperability with the TraceTogether Tokens can write to info@tech.gov.sg.

GOVTECH
SINGAPORE

[1] For information in registering a company in Singapore, please go to www.gobusiness.gov.sg.