TraceTogether or TrackTogether?

An investigation into Singapore's COVID-19 contact tracing system and its implications on privacy

Presented by: Joyce Ng (quatumcatgirl/bitowl.online)

What will be covered

- Technical Implementation and Reverse Engineering
- Policy analysis

COVID-19 is here to stay

THE STRAITS TIMES SINGAPORE LOG IN SUBSCRIBE PDF

Covid-19 cases in S'pore top 56,000 in first week of December, people urged to wear masks in crowded places

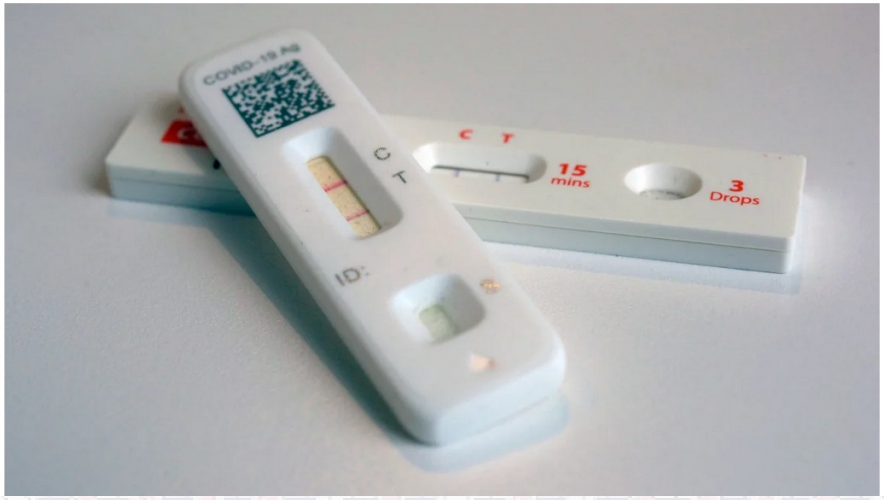
The health ministry said it will update figures daily from Dec 19. ST PHOTO: DESMOND WEE

CNN health Life, But Better Fitness Food Sleep Mindfulness Relationships

Covid-19 variant JN.1 is now the leading cause of infections in the US. Here's what you need to know

By Amanda Musa, CNN

2 minute read · Updated 9:37 PM EST, Sat December 23, 2023



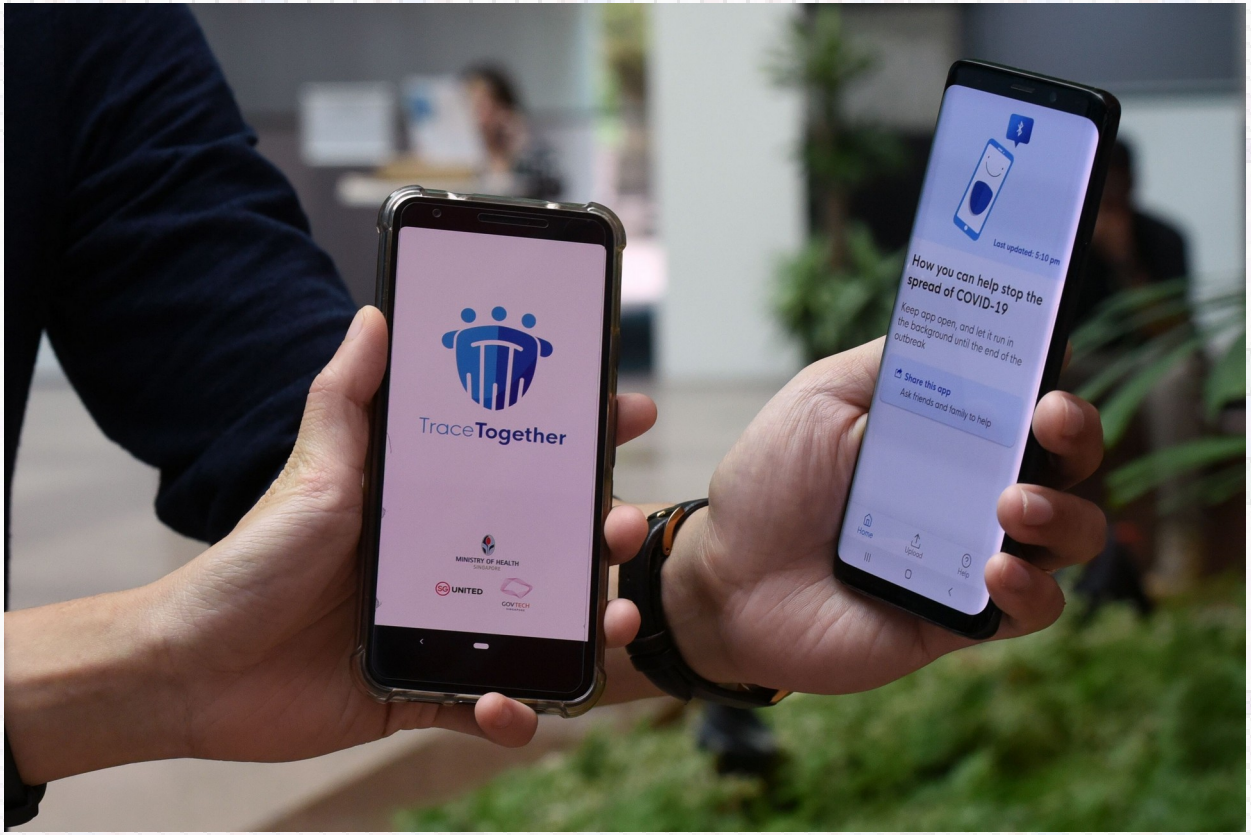
Contact Tracing

Contact tracing is an important tool in epidemiology

Contact Tracing

Digital contact tracing tools developed to combat COVID-19

Contact Tracing - TraceTogether

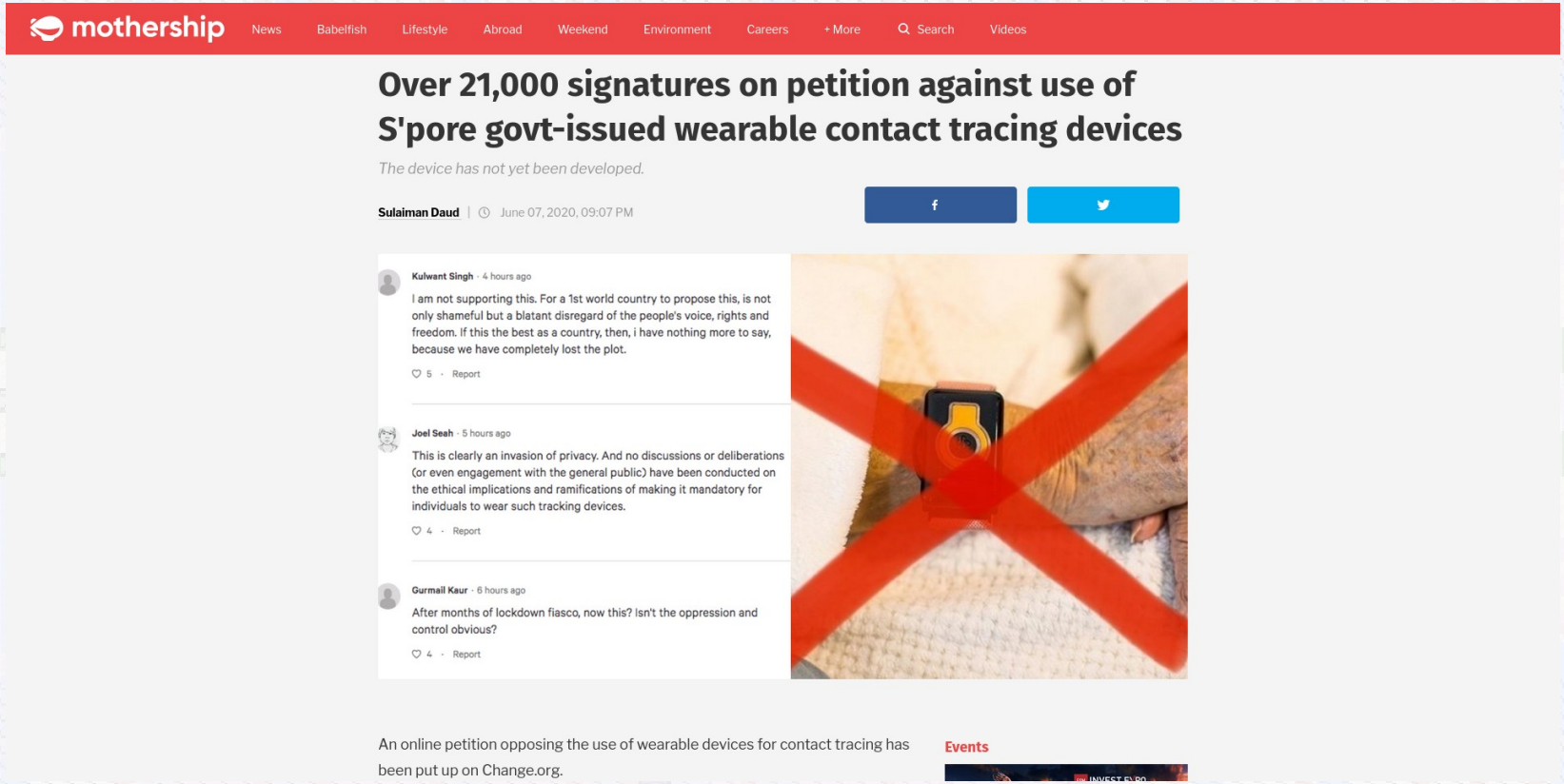


TraceTogether is Singapore’s centralized contact tracing system

Contact Tracing - TraceTogether

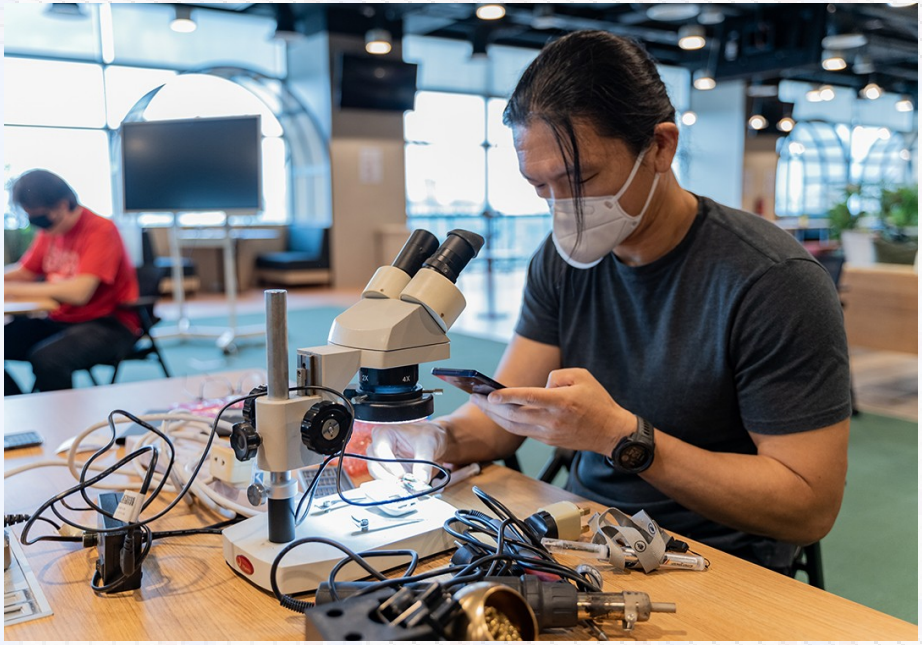
Hardware tokens were also made for those without smartphones

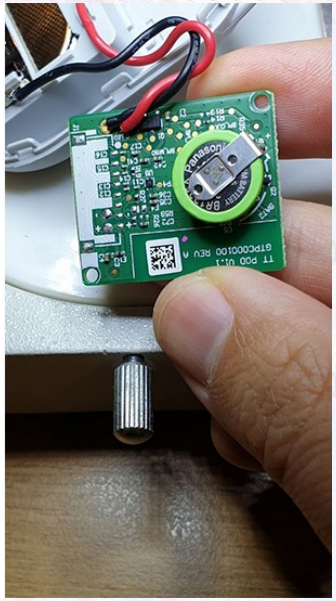
Contact Tracing - TraceTogether



Naturally, Singaporeans had concerns about TraceTogether

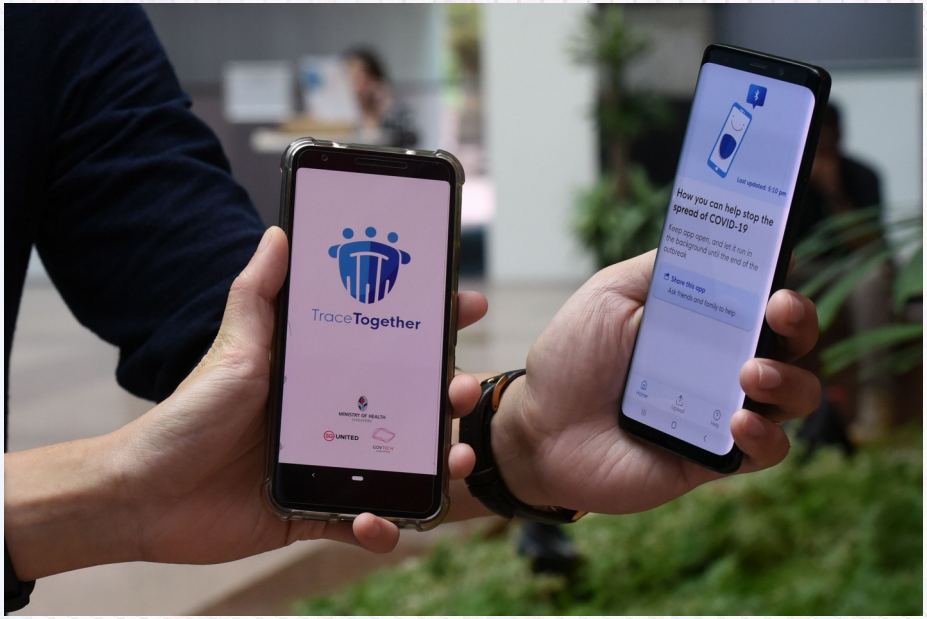
Contact Tracing - TraceTogether





So they ran a teardown session and invited hackers like bunnie

Contact Tracing - TraceTogether



Can people trust centralized contact tracing systems like TraceTogether?

Contact Tracing – Models and Protocols

Centralized:

- BlueTrace (Used in TraceTogether and COVIDSafe)
- Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT)

Decentralized:

- Exposure Notification
- Decentralized Privacy-Preserving Proximity Tracing (DP-3T)
- Temporary Contact Numbers (TCN) Protocol

BlueTrace - Overview

BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders

Jason Bay, Joel Kek, Alvin Tan, Chai Sheng Hau, Lai Yongquan, Janice Tan, Tang Anh Quy
Government Technology Agency
Singapore

ABSTRACT

TraceTogether is the first national deployment of a Bluetooth-based contact tracing system in the world. It was developed by Singapore's Government Technology Agency and the Ministry of Health to help the country better respond to epidemics.

Following its release, more than 50 governments have expressed interest in adopting or adapting TraceTogether for their countries. Responding to this interest, we are releasing an overview of **BlueTrace**, the privacy-preserving protocol that underpins TraceTogether, as well as **OpenTrace**, a reference implementation.

tracking users. The user's encounter history is stored locally on their user's device; none of this data can be directly accessed by the health authority.

If a user is infected or is the subject of contact tracing, they will be asked to share their encounter history with the relevant health authority with the use of a PIN. (A verification code may optionally be provided, to authenticate the health authority official's request.) Only the health authority has the ability to decrypt the shared encounter history to obtain and use personally-identifiable information to filter for close contacts and contact potentially infected users.

BlueTrace is designed to supplement manual con-

Implementation details published in GovTech whitepaper

BlueTrace - Overview

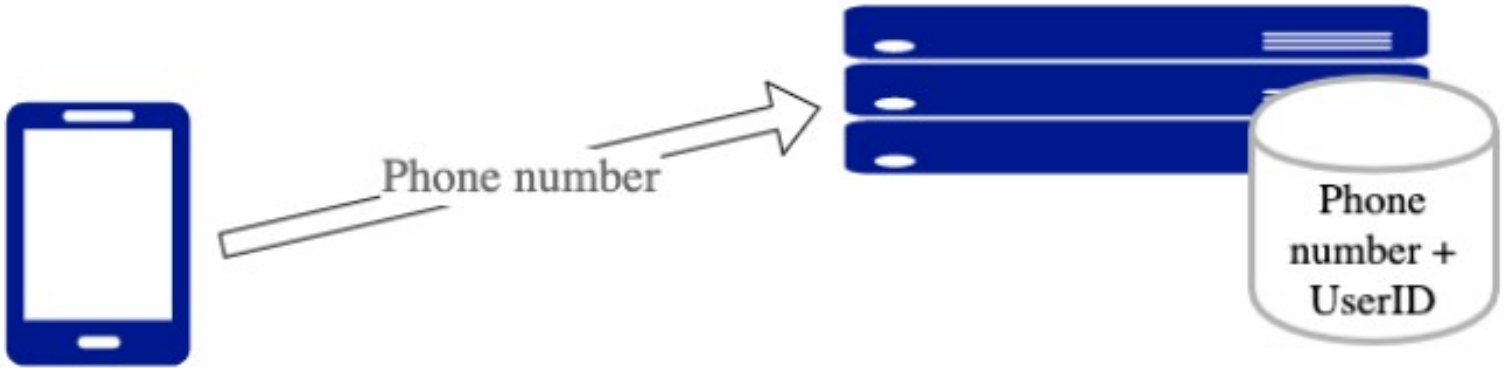


Figure 1: User registration

BlueTrace - Overview

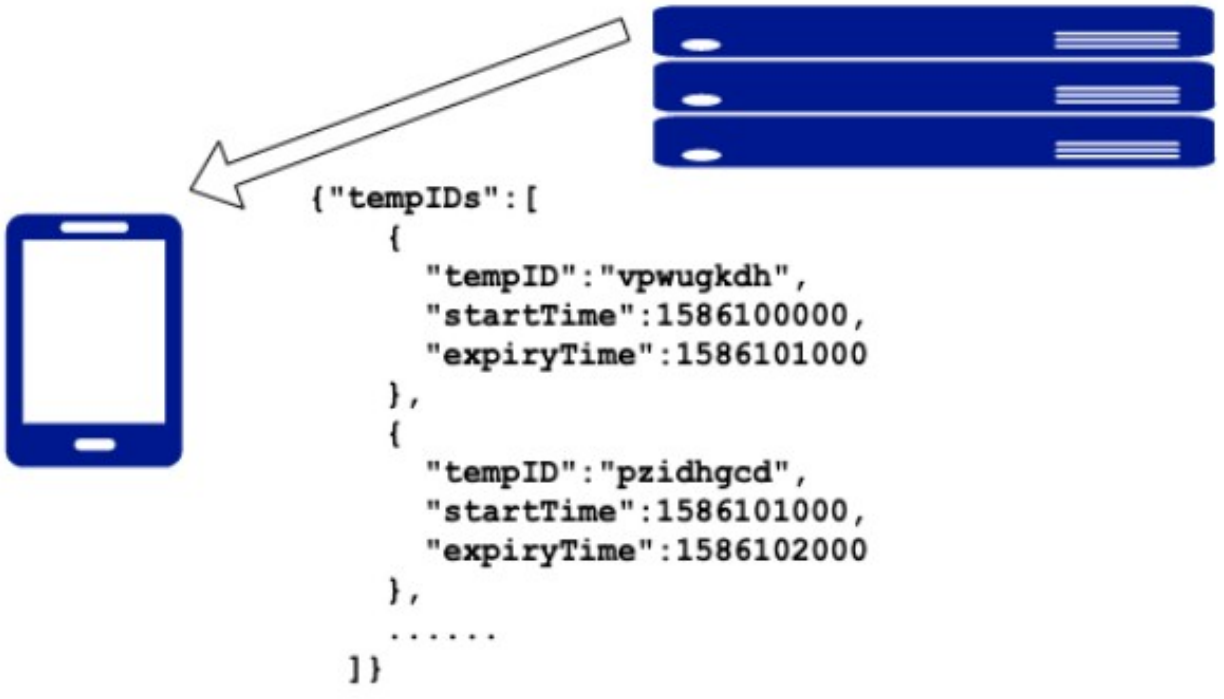


Figure 3: TempIDs sent to device

Batch of TempIDs obtained from server, rotated regularly (every 15 mins)

BlueTrace - Overview

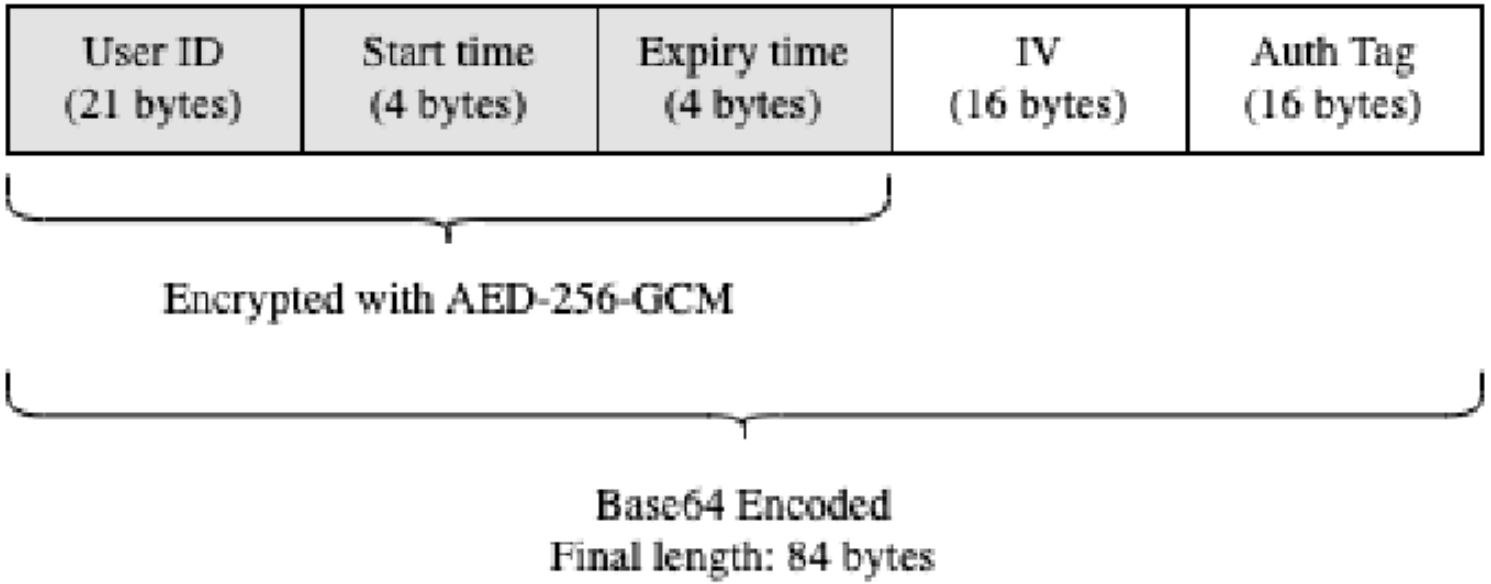


Figure 2: Format of TempID

TempID format

BlueTrace - Overview

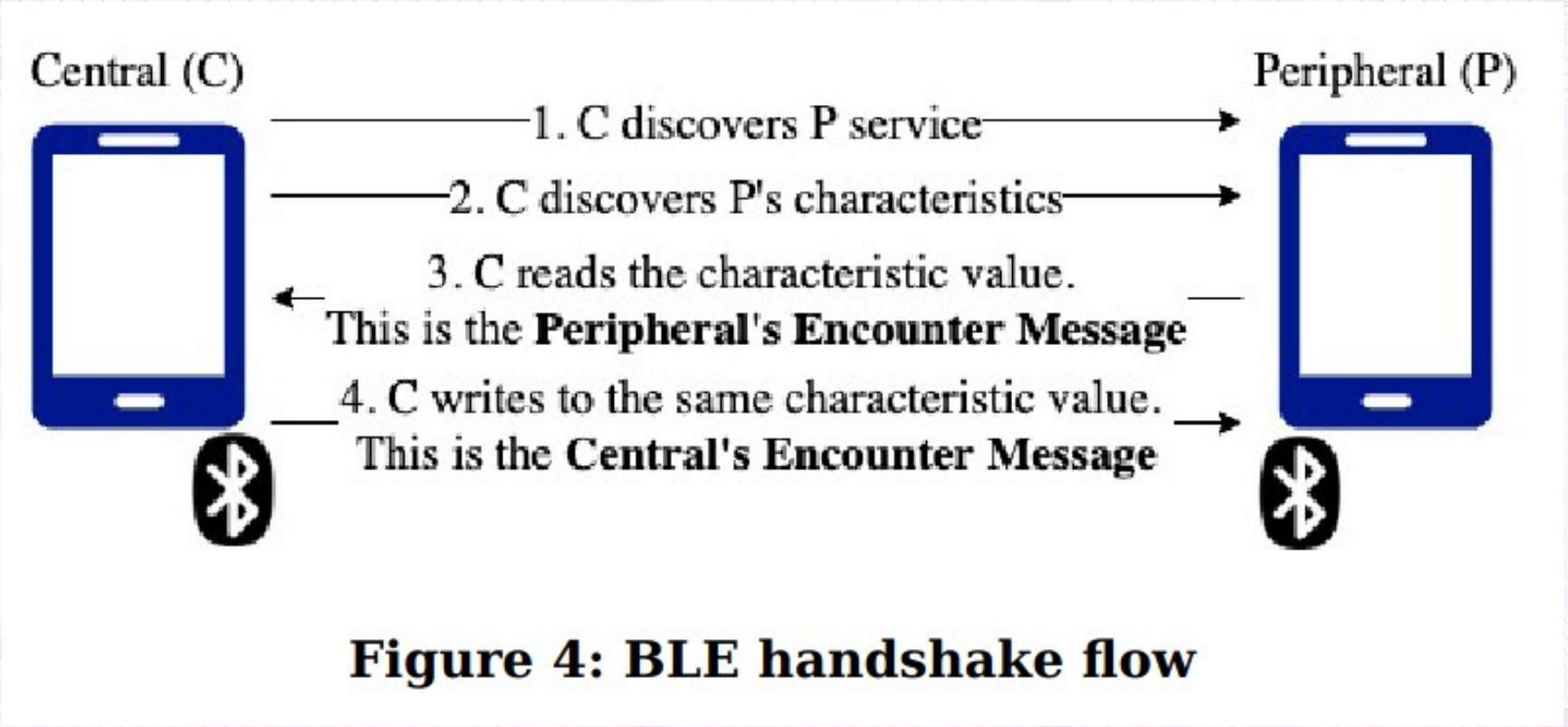


Figure 4: BLE handshake flow

BLE handshake between devices

BlueTrace - Overview

```
{
  // TempID of the Central
  "id": "Fj5jfbTtDySw8JoVsCmeul0wsoIcJKRPV0
      HtEFUlNvNg6C3wyGj8R1utPbw+Iz8tqAdpbxR1
      nSvr+ILXPG==",
  // Device model of the Central, to
      calibrate distance estimates
  "mc": "iPhone X",
  // Received Signal Strength Indicator (
      RSSI) as measured by the Central of
      the Peripheral
  "rs": -60,
  // Organisation code indicating the
      country and health authority with
      which the Central is enrolled
  "o": "SG_MOH",
  // Version of the BlueTrace protocol that
      the Central is running
  "v": 2
}
```

Exposure Notification - Overview

Advertising[1] Payload

The Exposure Notification Service payload shall be ordered as shown below and shall not include other data types.

Flags			Complete 16-bit Service UUID			Service Data - 16 bit UUID				
Length	**Type**	**Flags**	**Length**	**Type**	**Service UUID**	**Length**	**Type**	**Service Data**		
0x02	0x01 (Flag)	0x1A	0x03	0x03 (Complete 16-bit Service UUID)	0xFD6F (Exposure Notification Service)	0x17	0x16 (Service Data - 16 bit UUID)	0xFD6F (Exposure Notification Service)	**16 bytes** **Rolling Proximity Identifier**	**4 bytes** **Associated Encrypted Metadata**

Payload format – taken from EN Bluetooth Specification Document

Exposure Notification - Overview

The Exposure Notification Service payload has four sections:

1. Flags Section — Bluetooth Low Energy general discoverable mode (bit 1) shall be set to 1.
2. Complete 16-bit Service UUID Section — The UUID is 0xFD6F, and shall precede the Service Data section.
3. Service Data 16-bit UUID Section — This section shall have two different sections in its payload:
    a. A 16 byte Rolling Proximity Identifier.
    b. A 4 byte Associated Encrypted Metadata that contains the following (LSB first):
        i. Byte 0 — Versioning.
            - Bits 7:6 — Major version (01).
            - Bits 5:4 — Minor version (00).
            - Bits 3:0 — Reserved for future use.
        ii. Byte 1 — Transmit power level.
            - This is the measured radiated transmit power of Bluetooth Advertisement packets, and is used to improve distance approximation. The range of this field shall be -127 to +127 dBm.
        iii. Byte 2 — Reserved for future use.
        iv. Byte 3 — Reserved for future use.

Exposure Notification - Privacy

Maintaining user privacy is an essential requirement in the design of this specification. The protocol maintains privacy by the following means:

- The Exposure Notification Bluetooth Specification does not use location for proximity detection. It strictly uses Bluetooth beaconing to detect proximity.
- A user's Rolling Proximity Identifier changes on average every 15 minutes, and needs the Temporary Exposure Key to be correlated to a contact. This behavior reduces the risk of privacy loss from broadcasting the identifiers.
- Proximity identifiers obtained from other devices are processed exclusively on device.
- Users decide whether to contribute to exposure notification.
- If diagnosed with COVID-19, users must provide their consent to share Diagnosis Keys with the server.
- Users have transparency into their participation in exposure notification.

TraceTogether Implementation – App

BlueTrace | BlueTraceV2 | BuildConfig | LogRecordDao | LogRecordDao_Impl | LogWorker

```
16      public static final long BLACKLIST_DURATION = 100000;
17      public static final String BLE_SSID = "B82AB3FC-1595-4F6A-80F0-FE094CC218F9";
18      public static final long BTL_MAX_SCAN_INTERVAL = 59000;
19      public static final long BTL_MIN_SCAN_INTERVAL = 59000;
20      public static final long BTL_SCAN_DURATION = 1000;
21      public static final String BT_LITE_SSID = "0000FFFF-0000-1000-8000-00805F9B34FB";
22      public static final String BUILD_TYPE = "release";
23      public static final String CHECK_FOR_SYMPTOMS_URL = "https://sgcovidcheck.gov.sg/";
24      public static final long CONNECTION_TIMEOUT = 6000;
25      public static final String COVID_TEST_RECORDS_URL = "https://eservices.healthhub.sg/covid/records";
26      public static final String COVID_TEST_RESULT_FOOTNOTE_TROUBLESHOOT_URL = "https://support.tracetogether.gov.sg/hc/en-
27      public static final boolean DEBUG = false;
28      public static final String FIN_START_WITH = "Invalid parameter: FIN has to start with F or G";
29      public static final String FIREBASE_REGION = "asia-east2";
30      public static final String FIREBASE_UPLOAD_BUCKET = "govtech-tracer-app";
31      public static final String FIREBASE_UPLOAD_LOGS_BUCKET = "govtech-tracer-log";
32      public static final String GDS_LOGO_URL = "https://hive.tech.gov.sg";
33      public static final String GITHASH = "e4e9f5672";
34      public static final long HEALTH_CHECK_INTERVAL = 900000;
35      public static final String HOW_POSSIBLE_EXPOSURE_DETERMINED_URL = "https://support.tracetogether.gov.sg/hc/en-sg/arti
36      public static final String HUAWEI_APP_GALLERY_URL = "appmarket://details?id=sg.gov.tech.bluetrace";
37      public static final String[] ID_NUMBER_VALIDATION_WHITELIST = new String[0];
38      public static final String ID_VALIDATION_FAILED = "ID validation failed";
39      public static final String IOS_BACKGROUND_UUID = "AQEAAAAAAAAAAAAAAAAAAA==";
40      public static final float LATEST_UPDATE = 2.1f;
41      public static final int LOG_PURGE_DAYS = 14;
42      public static final long MAX_QUEUE_TIME = 7000;
43      public static final long MAX_SCAN_INTERVAL = 59000;
44      public static final int MIN_RSSI = -95;
45      public static final long MIN_SCAN_INTERVAL = 59000;
46      public static final String NEARBY_DEVICE_PERMISSION_EXPLAIN_URL = "https://support.tracetogether.gov.sg/hc/en-sg/arti
47      public static final int NO_OF_DAYS_FOR_HISTORY = 25;
```

TraceTogether Implementation – App

uildConfig | LogRecordDao | LogRecordDao_Impl | TempIDManager | TemporaryID | ExportData

```
/* loaded from: classes3.dex */
public final class LogRecordDao_Impl implements LogRecordDao {
    private final RoomDatabase __db;
    private final EntityInsertionAdapter<LogRecord> __insertionAdapterOfLogRecord;
    private final SharedSQLiteStatement __preparedStmtOfNukeDb;
    private final SharedSQLiteStatement __preparedStmtOfPurgeOldRecords;

    public LogRecordDao_Impl(RoomDatabase roomDatabase) {
        this.__db = roomDatabase;
        this.__insertionAdapterOfLogRecord = new EntityInsertionAdapter<LogRecord>(roomDatabase) { // from class: sg.gov
            @Override // androidx.room.SharedSQLiteStatement
            public String createQuery() {
                return "INSERT OR IGNORE INTO `log_table` (`level`,`type`,`tag`,`message`,`metaData`,`id`,`time`) VALUES
            }

            public void bind(SupportSQLiteStatement supportSQLiteStatement, LogRecord logRecord) {
                if (logRecord.getLevel() == null) {
                    supportSQLiteStatement.bindNull(1);
                } else {
                    supportSQLiteStatement.bindString(1, logRecord.getLevel());
                }
                if (logRecord.getType() == null) {
                    supportSQLiteStatement.bindNull(2);
                } else {
                    supportSQLiteStatement.bindString(2, logRecord.getType());
                }
                if (logRecord.getTag() == null) {
                    supportSQLiteStatement.bindNull(3);
                } else {
                    supportSQLiteStatement.bindString(3, logRecord.getTag());
                }
                if (logRecord.getMessage() == null) {
```

TraceTogether Implementation – App

uildConfig | LogRecordDao | LogRecordDao_Impl | TempIDManager | TemporaryID | ExportData

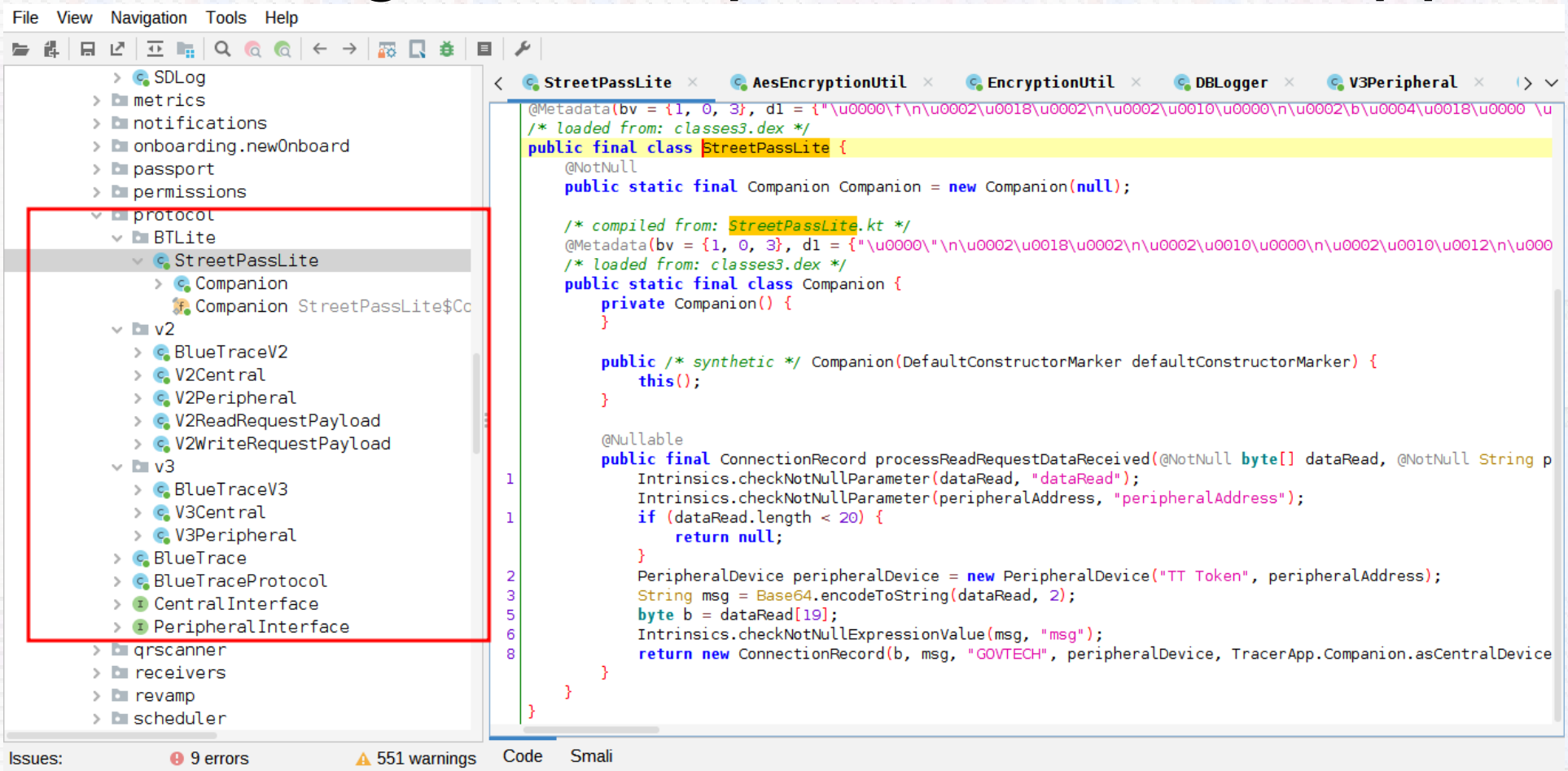
```
    public final boolean needToUpdate(@NotNull Context context) {
1       Intrinsics.checkNotNullParameter(context, "context");
1       long nextFetchTimeInMillis = Preference.INSTANCE.getNextFetchTimeInMillis(context);
2       long currentTimeMillis = System.currentTimeMillis();
        boolean z = currentTimeMillis >= nextFetchTimeInMillis;
3       CentralLog.Companion companion = CentralLog.Companion;
5       companion.i(TAG, "Need to update and fetch TemporaryIDs? " + nextFetchTimeInMillis + " vs " + currentTimeMillis
        return z;
    }

    @NotNull
    public final ApiResponseModel<TempIdModel> onTempIdResponse(@NotNull ApiResponseModel<TempIdModel> result) {
1       Intrinsics.checkNotNullParameter(result, "result");
1       TempIdModel result2 = result.getResult();
        if (result2 == null) {
            return result;
        }
2       CentralLog.Companion companion = CentralLog.Companion;
        companion.i(TAG, Intrinsics.stringPlus("Result from getTempID: ", result));
3       List<TempIdModel.TempID> tempIDs = result2.getTempIDs();
4       List<TempIdModel.TempID> shortTempIDs = result2.getShortTempIDs();
5       boolean isValidTempIds = isValidTempIds(tempIDs);
6       boolean isValidTempIds2 = isValidTempIds(shortTempIDs);
7       companion.i(TAG, Intrinsics.stringPlus("Result from tempIDs: ", tempIDs));
8       companion.i(TAG, Intrinsics.stringPlus("Result from short tempIDs: ", shortTempIDs));
9       if (!result.isSuccess() || !isValidTempIds || !isValidTempIds2) {
27          result.setSuccess(false);
        } else {
10          companion.w(TAG, "Retrieved Temporary IDs from Server");
11          Gson create = new GsonBuilder().disableHtmlEscaping().create();
            Intrinsics.checkNotNullExpressionValue(create, "GsonBuilder().disableHtmlEscaping().create()");
```

TraceTogether Implementation – App

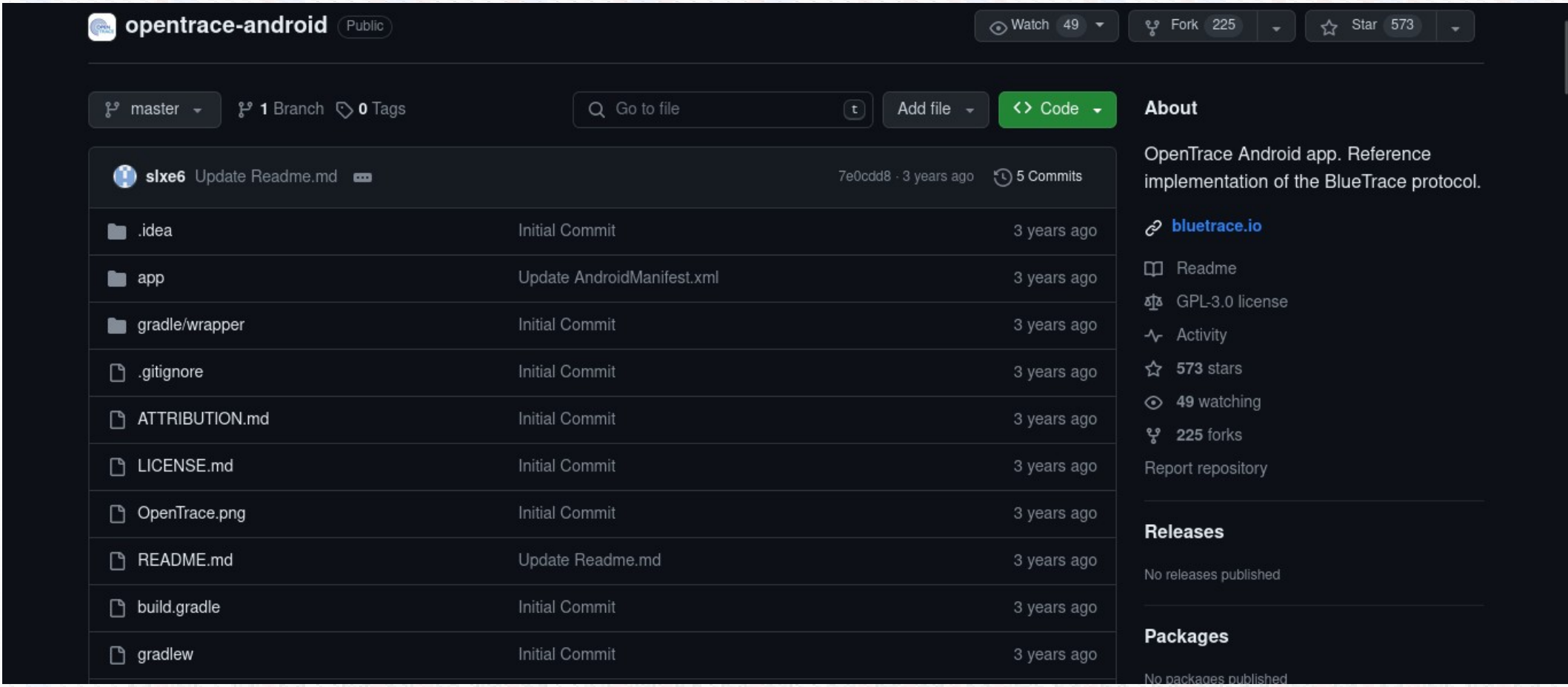
Kt | BLEScanner | BlueTraceProtocol | BlueTraceV3 | StreetPassLite | AesEncryptionUtil

```
    @Nullable
11  public final byte[] encryptWithAesGcm(@NotNull byte[] key, @NotNull String plainText) {
12      Intrinsics.checkNotNullParameter(key, "key");
        Intrinsics.checkNotNullParameter(plainText, "plainText");
        try {
            byte[] bArr = new byte[12];
13          new SecureRandom().nextBytes(bArr);
14          Cipher instance = Cipher.getInstance(AES_GCM_NOPADDING);
16          instance.init(1, new SecretKeySpec(key, "AES"), new GCMParameterSpec(128, bArr));
17          byte[] bytes = plainText.getBytes(Charsets.UTF_8);
            Intrinsics.checkNotNullExpressionValue(bytes, "(this as java.lang.String).getBytes(charset)");
            byte[] cipherMessage = instance.doFinal(bytes);
18          byte[] iv = instance.getIV();
            Intrinsics.checkNotNullExpressionValue(iv, "cipher.iv");
            Intrinsics.checkNotNullExpressionValue(cipherMessage, "cipherMessage");
            return wrapCipherMessageWithIV(iv, cipherMessage);
        } catch (Throwable th) {
19          StringBuilder sb = new StringBuilder();
            sb.append((Object) AesEncryptionUtil.class.getSimpleName());
            sb.append(" -> ");
            new Object() { // from class: sg.gov.tech.bluetrace.encryption.AesEncryptionUtil$encryptWithAesGcm$loggerTAG
            };
            Method enclosingMethod = AesEncryptionUtil$encryptWithAesGcm$loggerTAG$2.class.getEnclosingMethod();
            sb.append((Object) (enclosingMethod == null ? null : enclosingMethod.getName()));
            sb.append("(before M)");
            String sb2 = sb.toString();
20          DBLogger dBLogger = DBLogger.INSTANCE;
23          dBLogger.e(DBLogger.LogType.ENCRYPTION, sb2, "Cannot encrypt with AES", dBLogger.getStackTraceInJSONArrayStr
24          CentralLog.Companion.e("AsymmetricEncrypt", Intrinsics.stringPlus("Cannot encrypt with AES:", th));
            return null;
        }
```

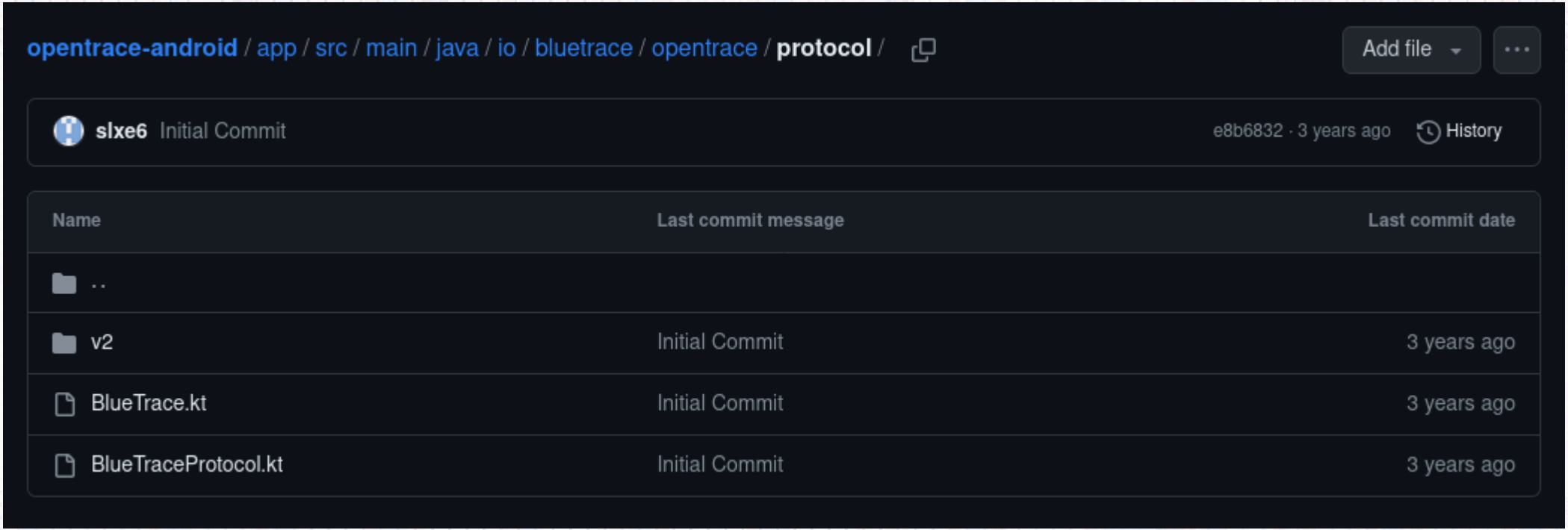
TraceTogether Implementation – App



TraceTogether Implementation – App



TraceTogether Implementation – App



TraceTogether Implementation – Token

TraceTogether Token

Technical Write-up

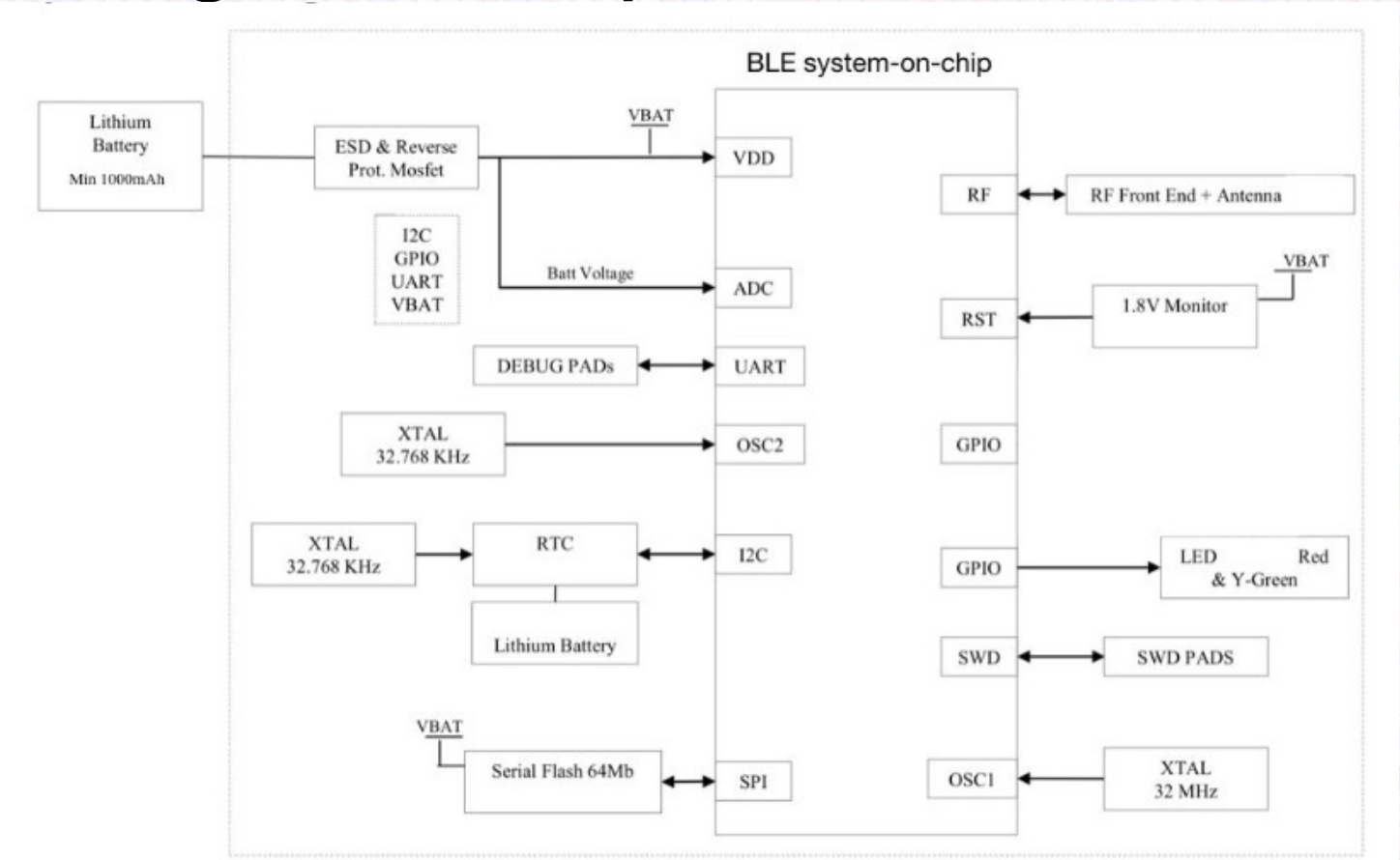
Yang Boon Quek, Director, Sensors and IoT
Government Technology Agency of Singapore

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.

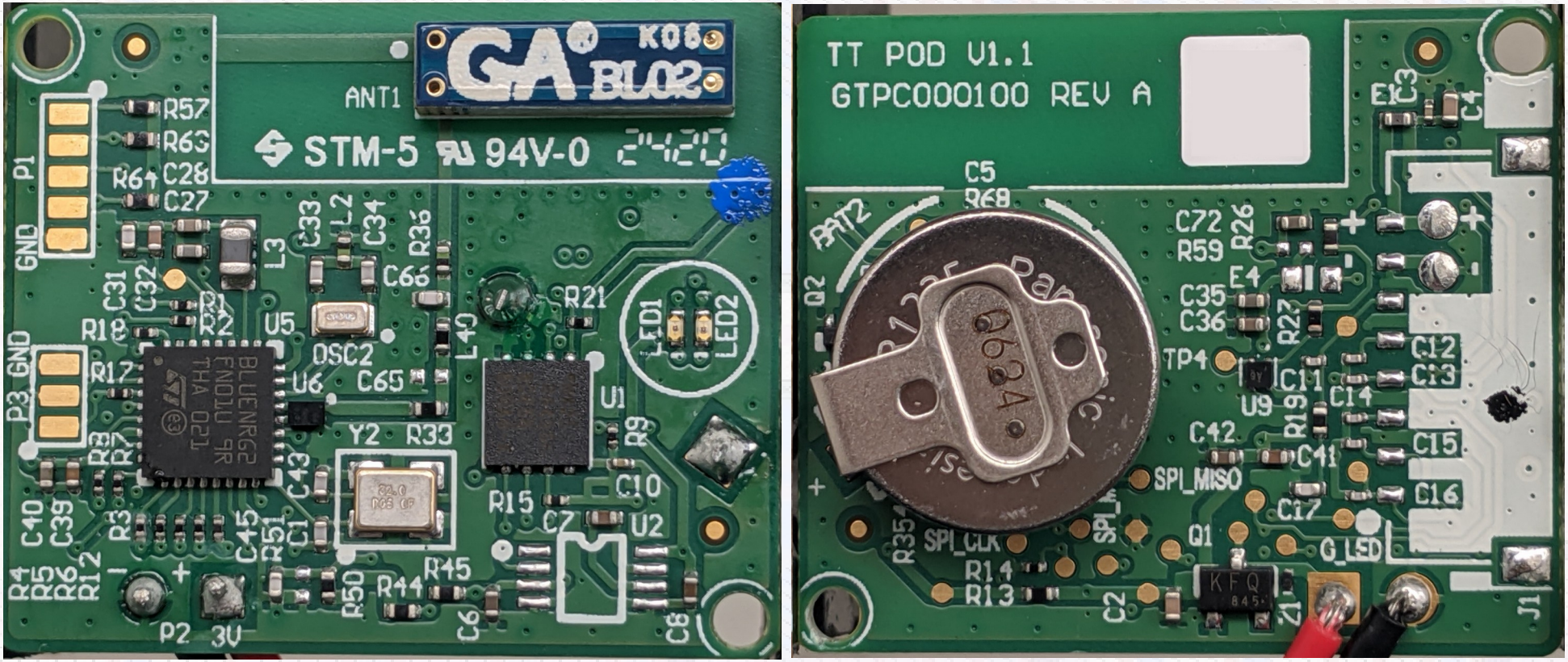
Implementation details published in Technical Writeup Document

TraceTogether Implementation – Token



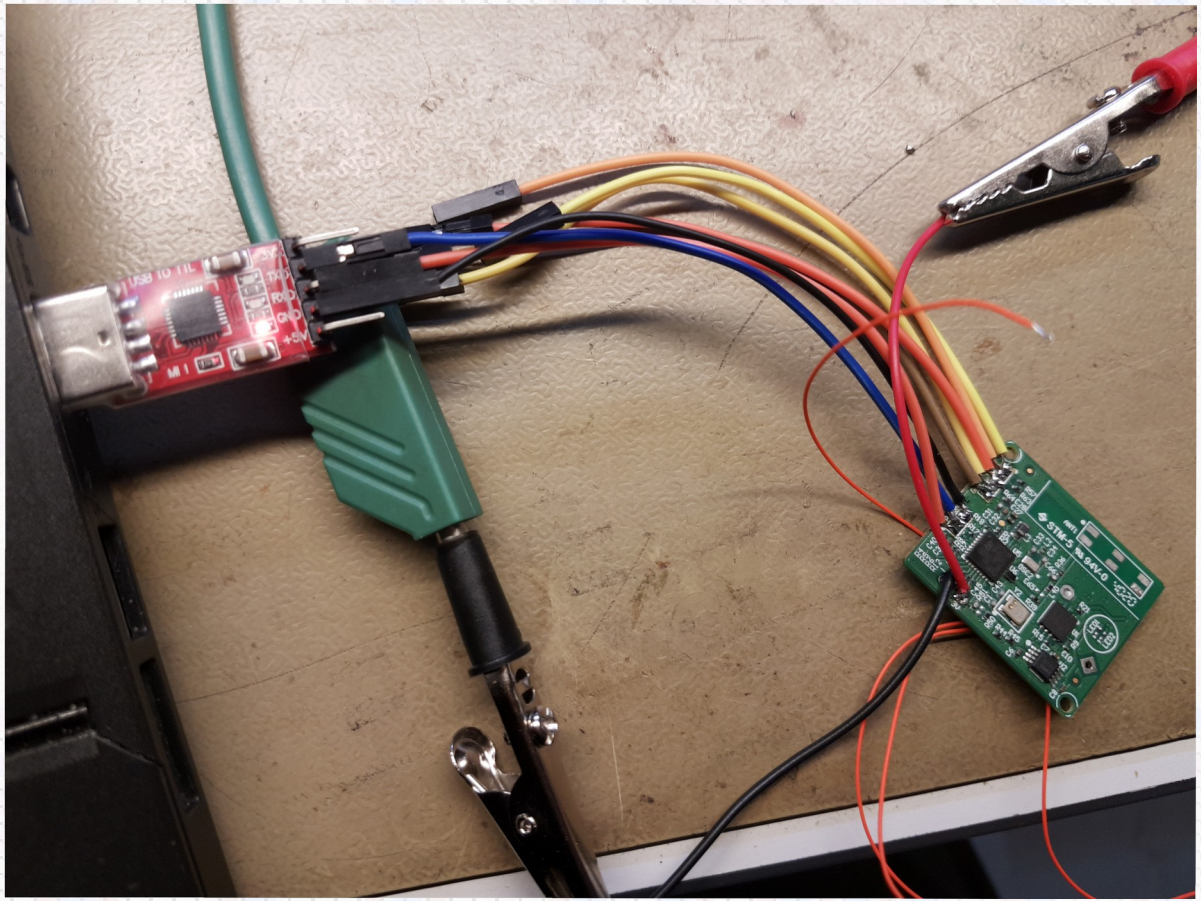
Implementation Block Diagram as per writeup document

TraceTogether Implementation – Token



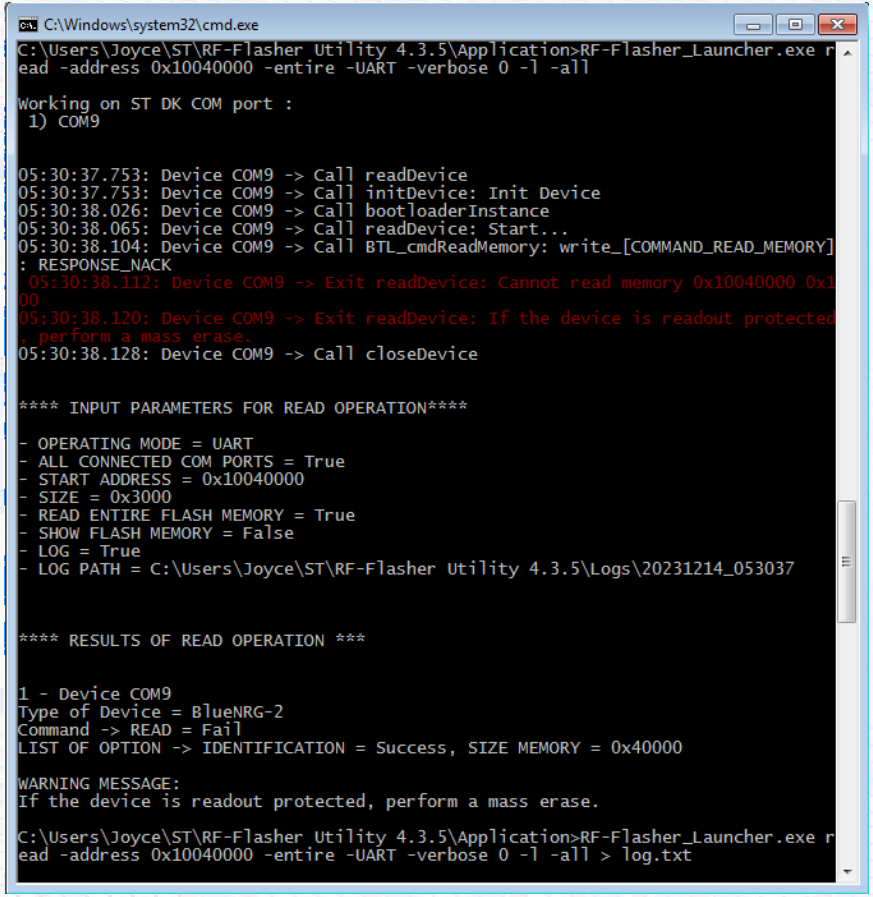
TraceTogether Pod V1.1 Rev A/B (Credit: Roland Turner)

TraceTogether Implementation – Token



SWD Disabled, use UART and put into bootloader mode

TraceTogether Implementation – Token



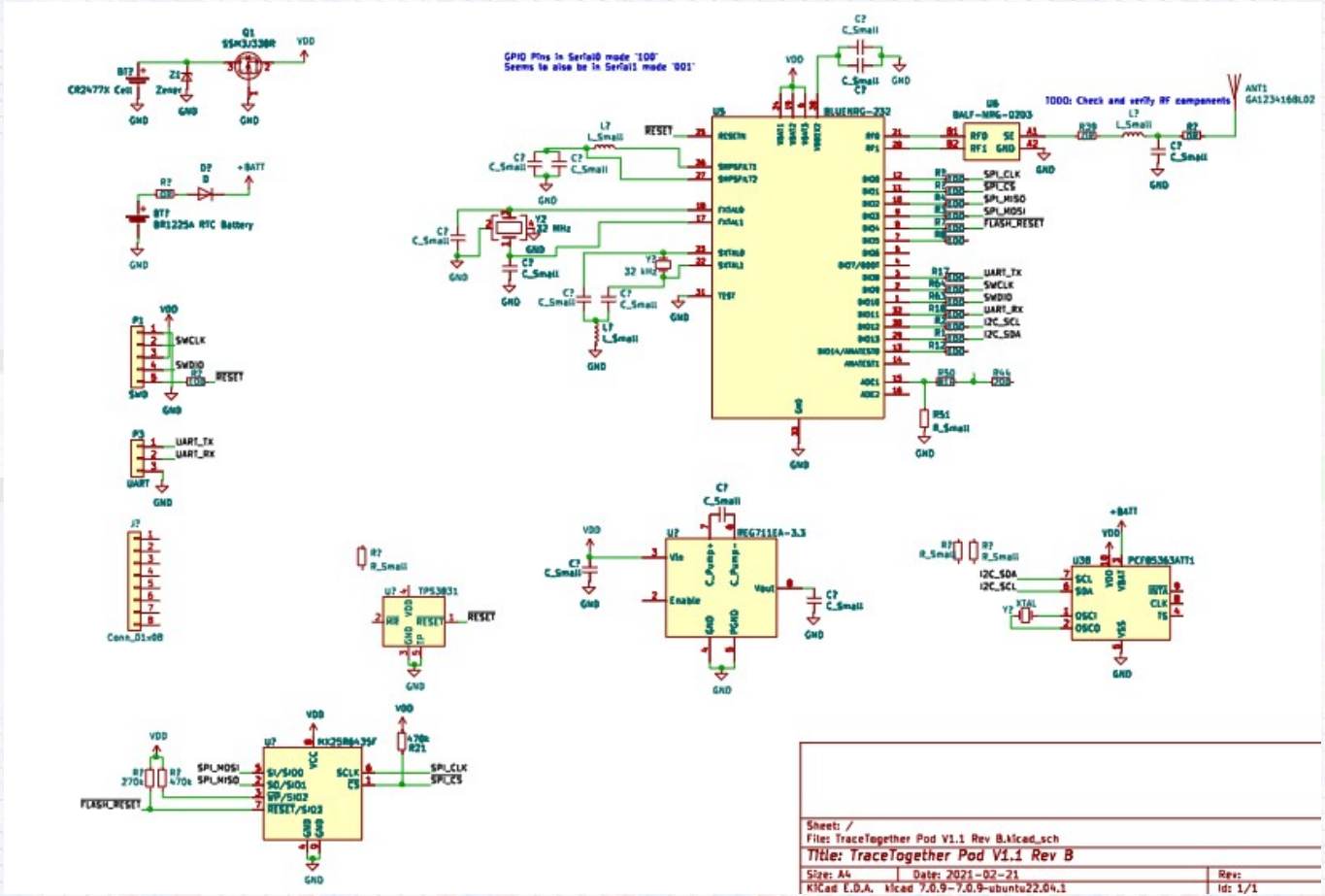
Read failed; Readout Protection likely enabled

TraceTogether Implementation – Token

TraceTogether Pod V1.1 Rev A/B - Main Components:

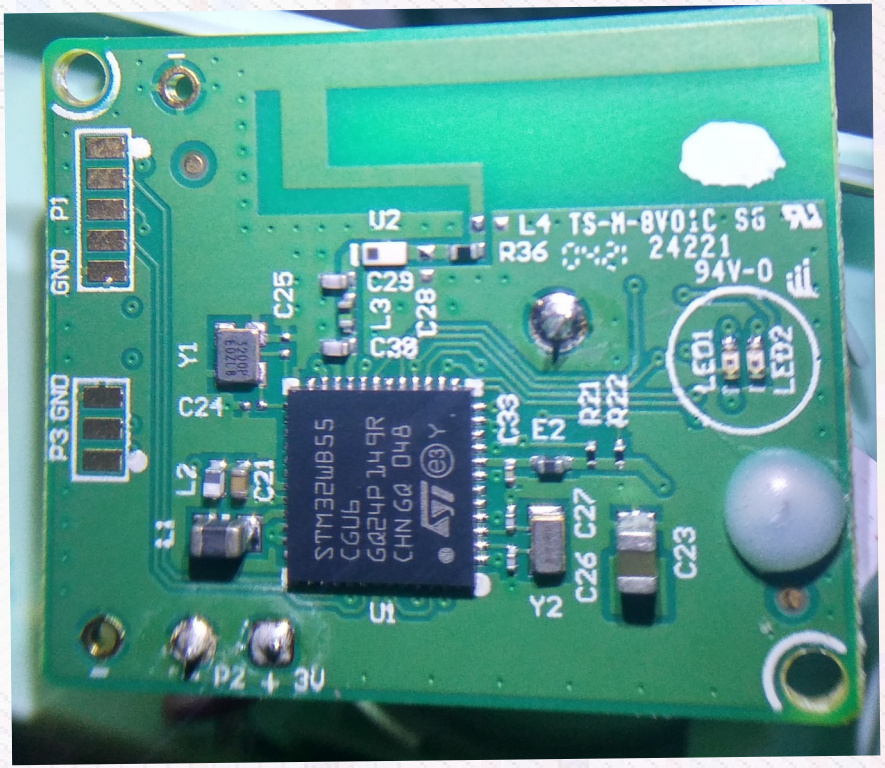
U1: MX25R6435F 64Mbits Serial NOR Flash memory
U2: REG711EA-3.3 Switched Cap DC/DC Converter (for driving LEDs?)
U5: ST Microelectronics BLUENRG-232 Bluetooth SoC
U9: TPS3831 Ultralow Power, Supply Voltage Monitor
U38(?): PCF85363ATT1 I2C Real Time Clock

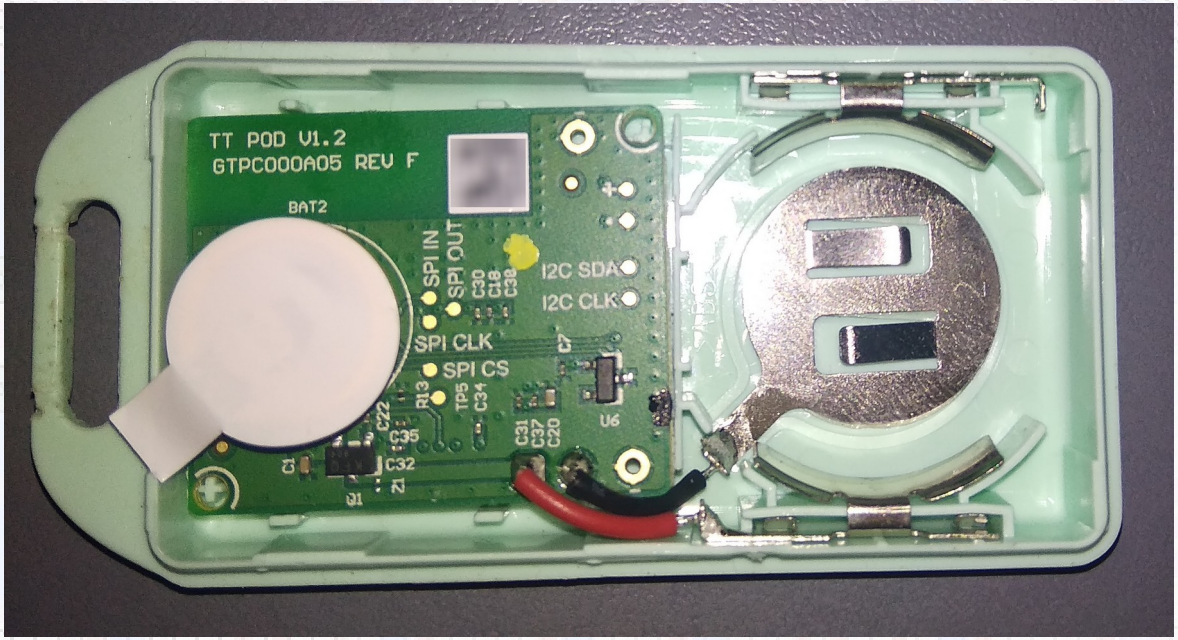
TraceTogether Implementation – Token



TraceTogether Pod V1.1 Rev A/B – Recreated Schematic

TraceTogether Implementation – Token





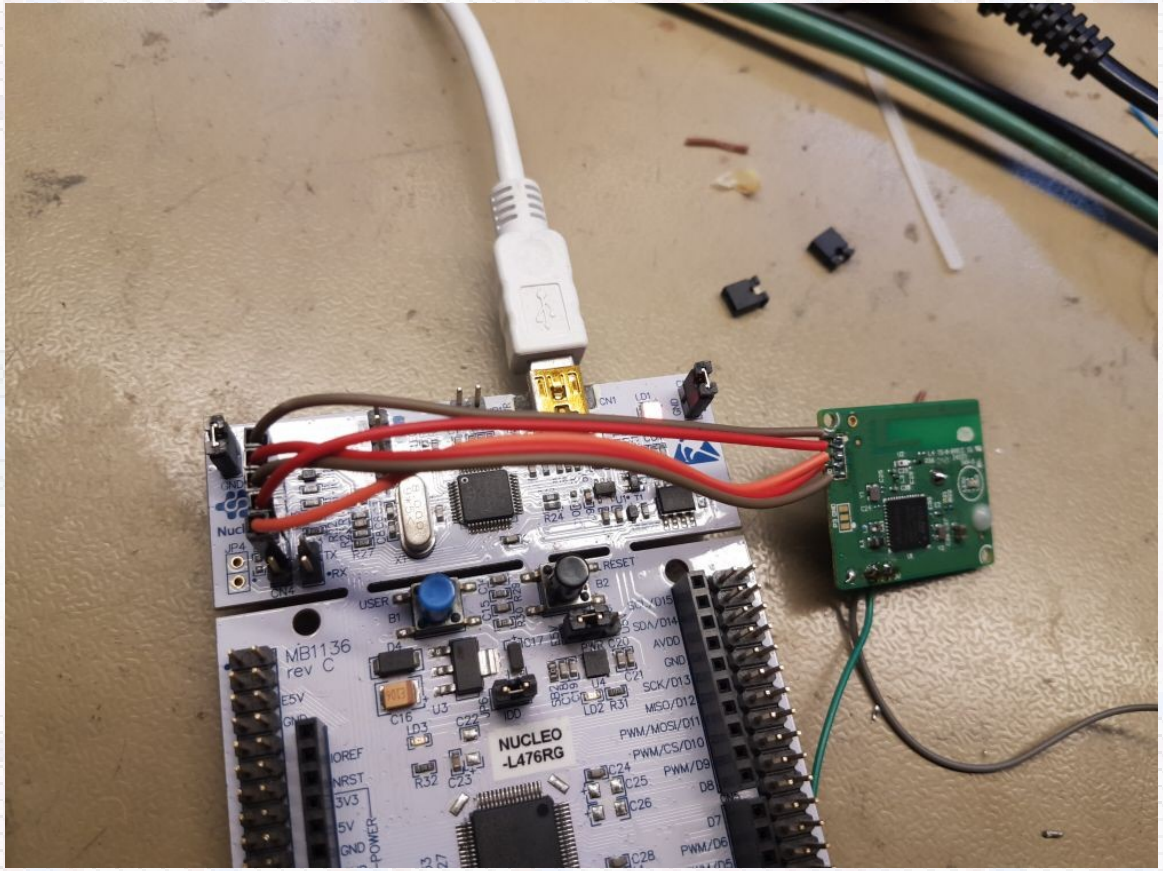
TraceTogether Pod V1.2 Rev F – A lot simpler!

TraceTogether Implementation – Token

TraceTogether Pod V1.2 Rev F - Main Components:

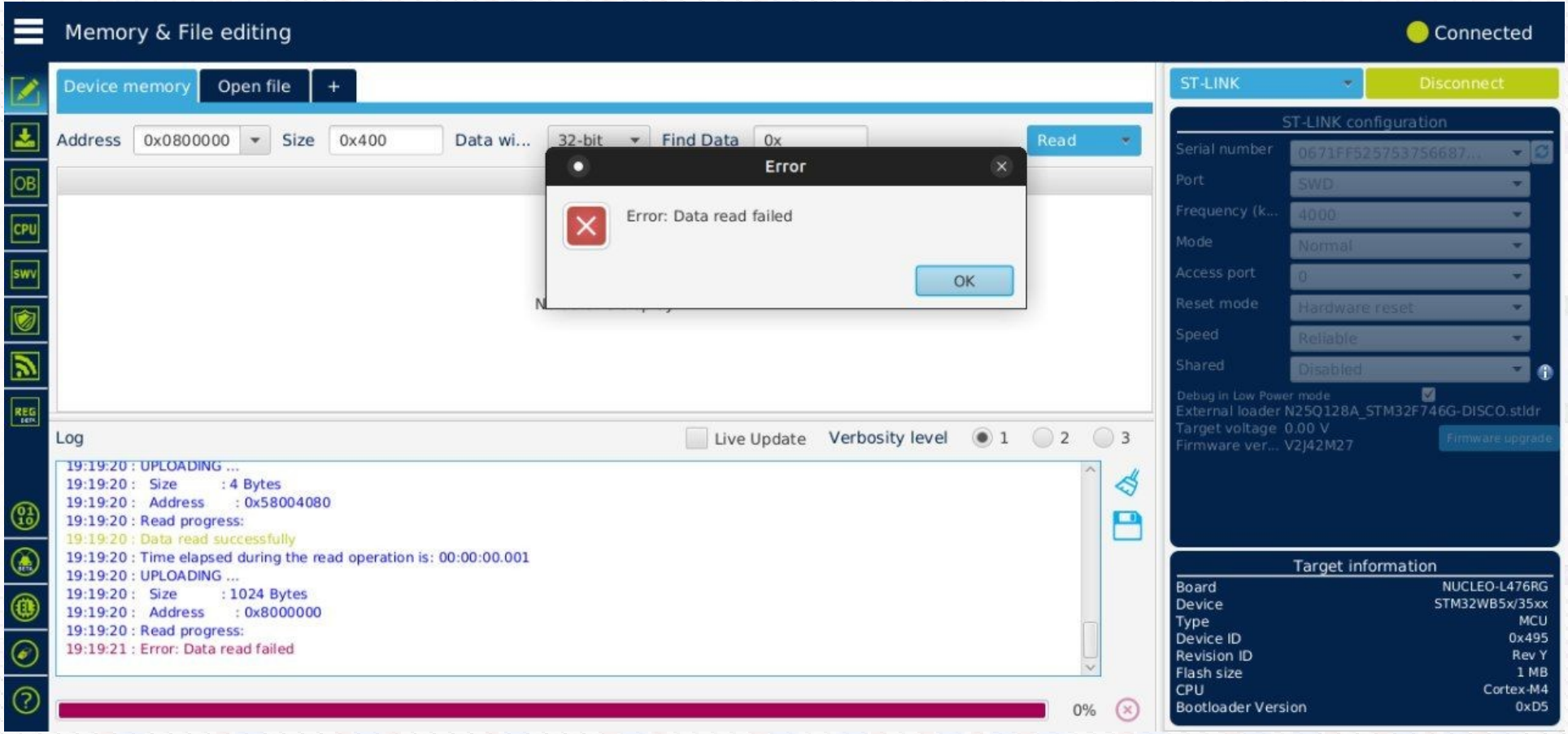
U1: ST Microelectronics STM32WB55CG MCU with BLE 5.4
U6: DRV5032 Ultra-Low-Power Digital-Switch Hall Effect Sensor
U?: GD25WQ64E 64Mbits Serial NOR Flash memory

TraceTogether Implementation – Token



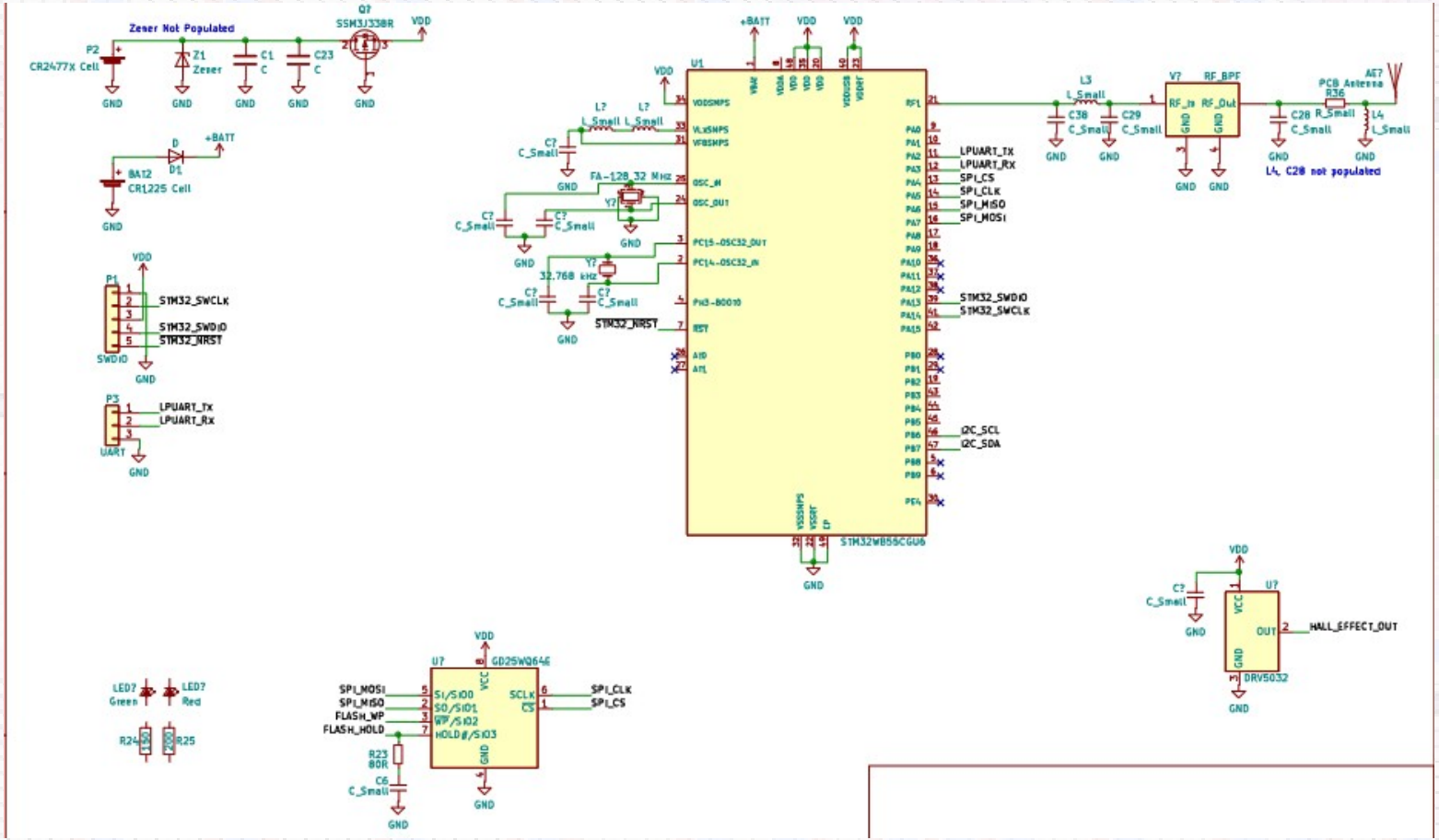
Hook the token to a ST-Link...

TraceTogether Implementation – Token



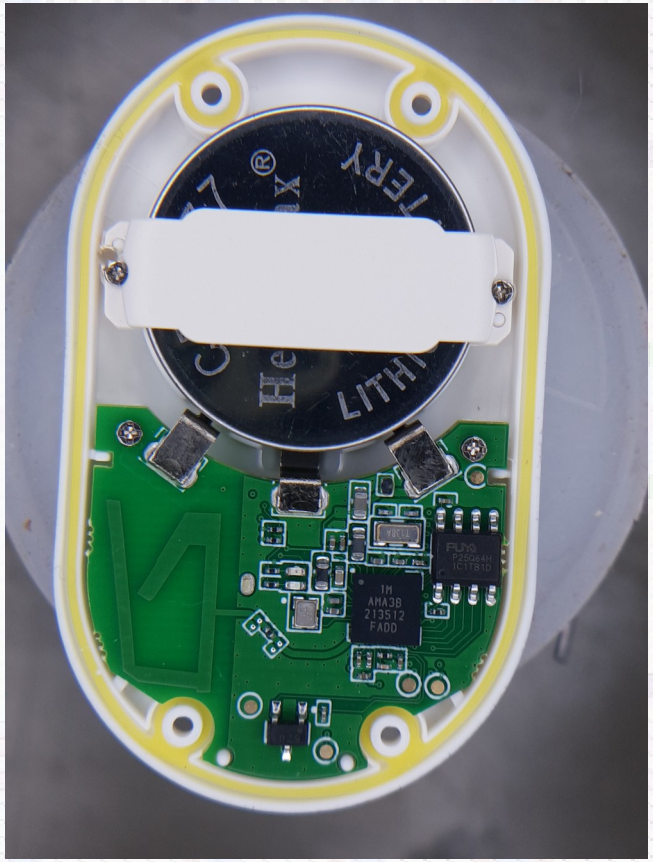
Readout Protection likely enabled too :(

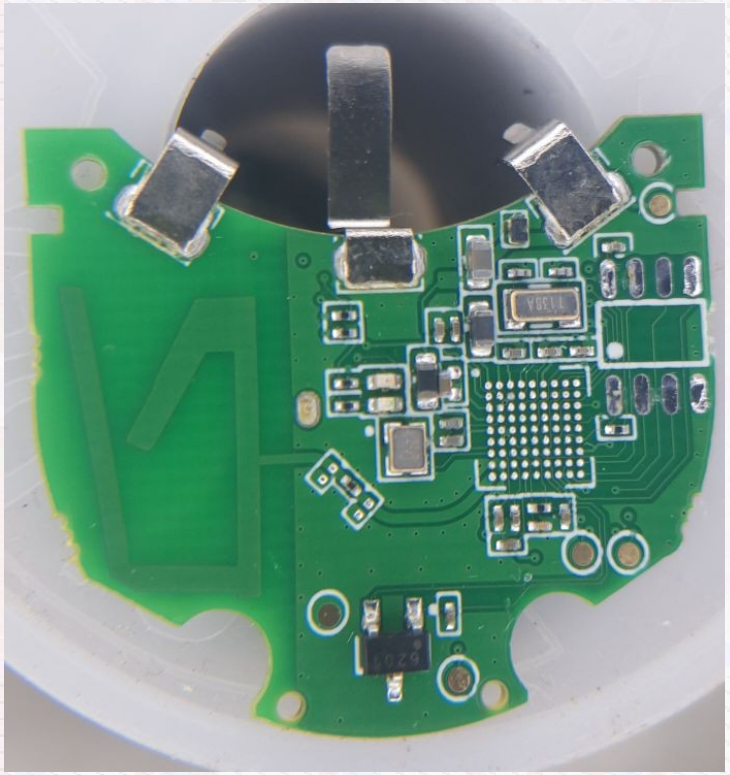
TraceTogether Implementation – Token

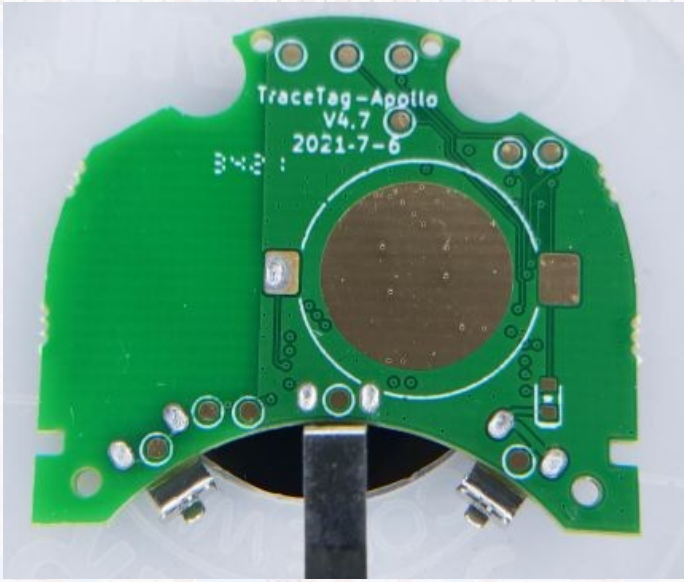


TraceTogether Pod V1.2 Rev F – Recreated Schematic

TraceTogether Implementation – Token







TraceTag-Apollo V4.7 – Even simpler!

TraceTogether Implementation – Token

TraceTag-Apollo v4.7 - Main Components:

MCU: Ambiq Apollo 3 AMA3B1KK-KBR
SPI Flash Memory: Puya P25Q64H 64Mbit Serial Flash
Hall Effect Sensor: CC6201

TraceTogether Implementation – Token

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

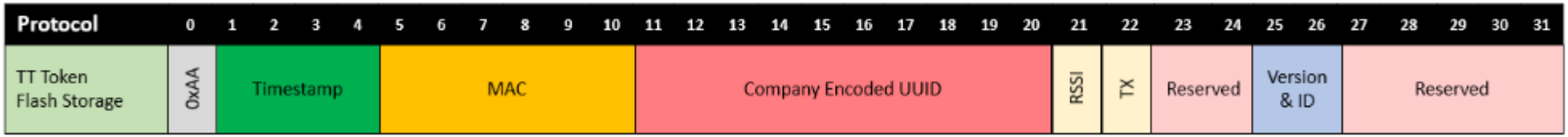
- **Licensing:**
  - GovTech will assign a Company ID (Version & ID, Byte 18 and 19) for each company interoperating with TTT
  - 1 x 16 bytes Global Replay Protection Key (RPK) will be provided to each Company

BlueTrace Lite – Packet Structure

TraceTogether Implementation – Token

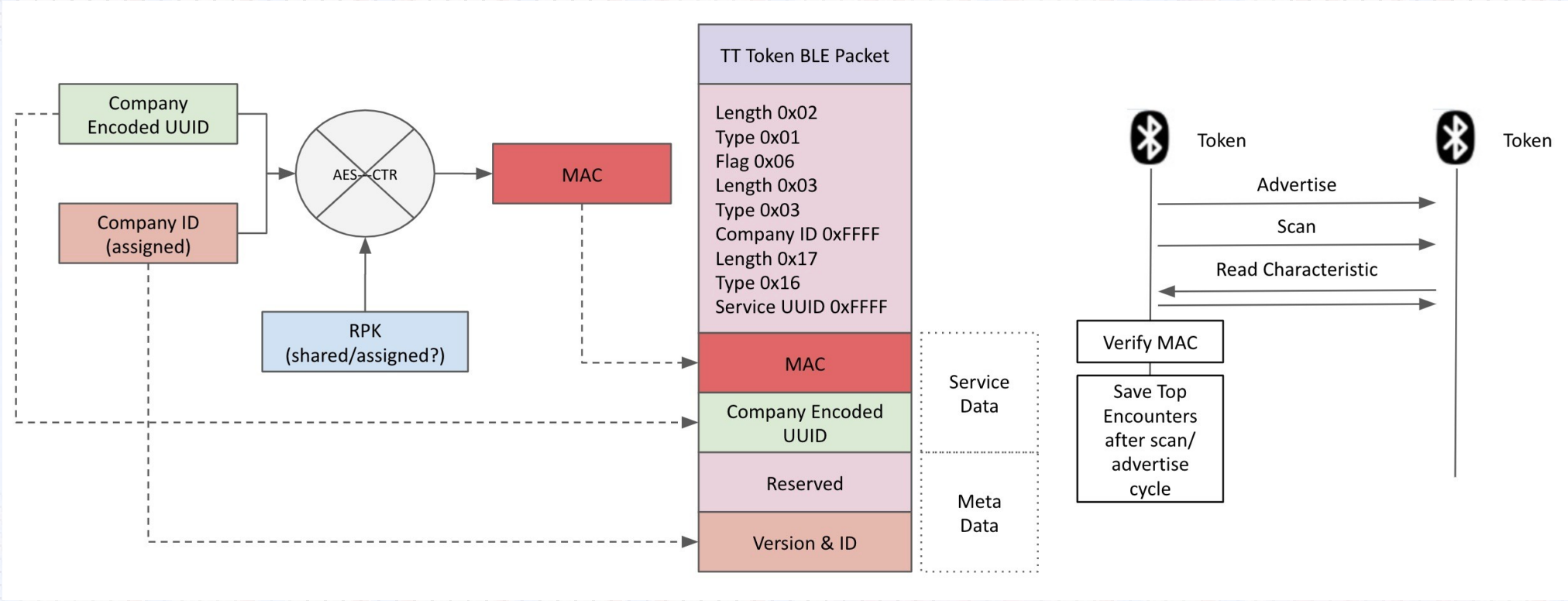
3.2 Storage packet to flash memory

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.



Flash Storage – Packet Format

TraceTogether Implementation – Token



BlueTrace Lite Flow (Diagram Credit: Paul Gallagher (tardate))

TraceTogether Implementation – Token

```
Device : 963F1840-DA74-4EF6-B542-A913DB98E6CD - RSSI : -52 DeviceName : n/a
  --> serviceData : [FFFF: <b8dfb789 55b6d6a9 09cded68 6b081ce7 7fbb3833>]
  --> TTToken : seems like this might be one: Version = 0x38 ID = 0x33
  --> TTToken : companyEncryptedUUID = 0xD6A909CDED686B081CE7
  --> TTToken : MAC = 0xB8DFB78955B6
Device : 963F1840-DA74-4EF6-B542-A913DB98E6CD - RSSI : -52 DeviceName : n/a
Device : 45DD3008-0EF7-4C72-AF68-839B8B4E45E0 - RSSI : -85 DeviceName : n/a
  --> serviceData : [FFFF: <daa96da7 dcfb4b09 9f314835 5fa81600 559f3820>]
  --> TTToken : seems like this might be one: Version = 0x38 ID = 0x20
  --> TTToken : companyEncryptedUUID = 0x4B099F3148355FA81600
  --> TTToken : MAC = 0xDAA96DA7DCFB
Device : 45DD3008-0EF7-4C72-AF68-839B8B4E45E0 - RSSI : -85 DeviceName : n/a
Device : 31631232-B67A-4C60-8E1B-26701E64C7C5 - RSSI : -69 DeviceName : n/a
Device : 31631232-B67A-4C60-8E1B-26701E64C7C5 - RSSI : -86 DeviceName : n/a
Device : 52817F59-FC26-40D1-B030-B138068A5D4E - RSSI : -62 DeviceName : n/a
  --> serviceData : [FFFF: <da652a96 857c81ad 9529c91a 9e8d23ff 7e713833>]
  --> TTToken : seems like this might be one: Version = 0x38 ID = 0x33
  --> TTToken : companyEncryptedUUID = 0x81AD9529C91A9E8D23FF
  --> TTToken : MAC = 0xDA652A96857C
```

TTScan tool output (Credit: Paul Gallagher (tardate))

TraceTogether Implementation – Token

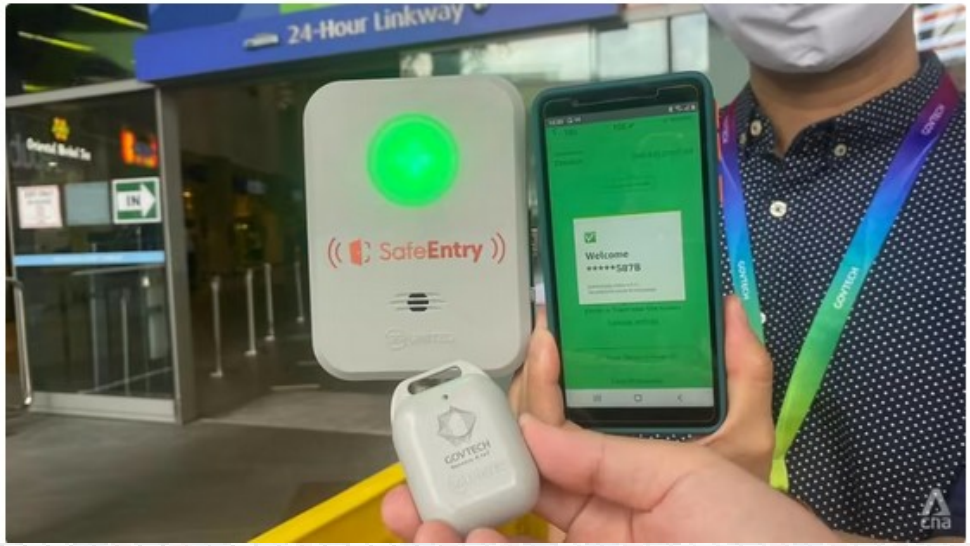
So, everything looks fine and dandy here right?

TraceTogether – Gateway Introduced

cna
Best News Website or Mobile Service • WAN-IFRA Digital Media Awards Worldwide 2022

Singapore

New SafeEntry Gateways to be set up at malls, cinemas, supermarkets and more public places



Ang Hwee Min
@HweeMinCNA

16 Mar 2021 11:39AM
(Updated: 16 Mar 2021 11:15PM)

TraceTogether – Made Mandatory

Singapore

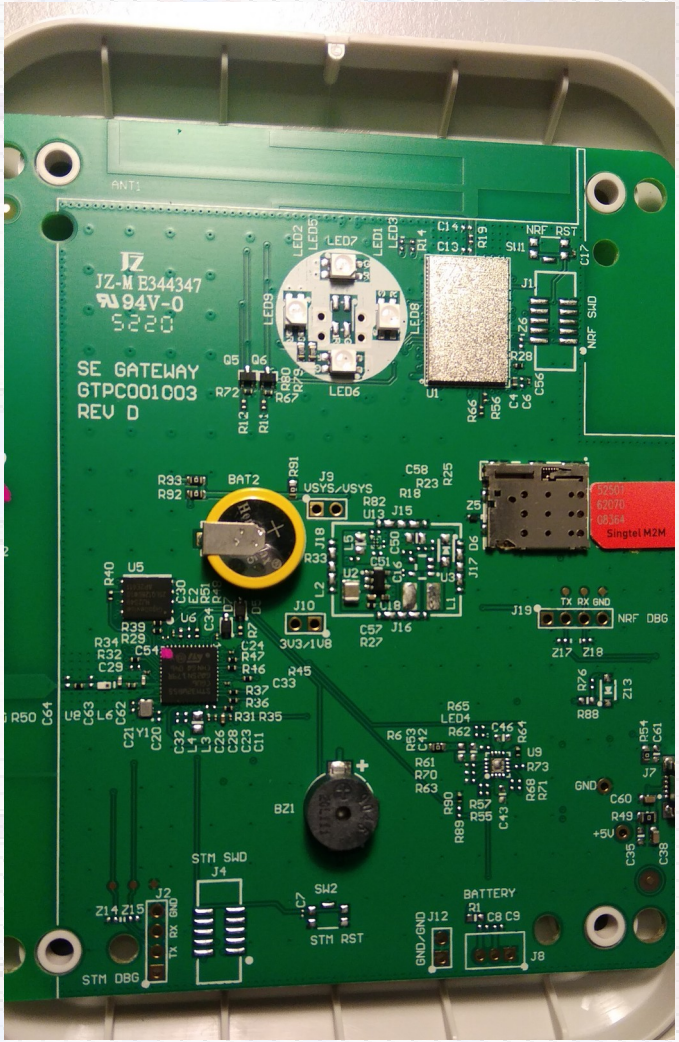
Mandatory TraceTogether-only SafeEntry brought forward to May 17

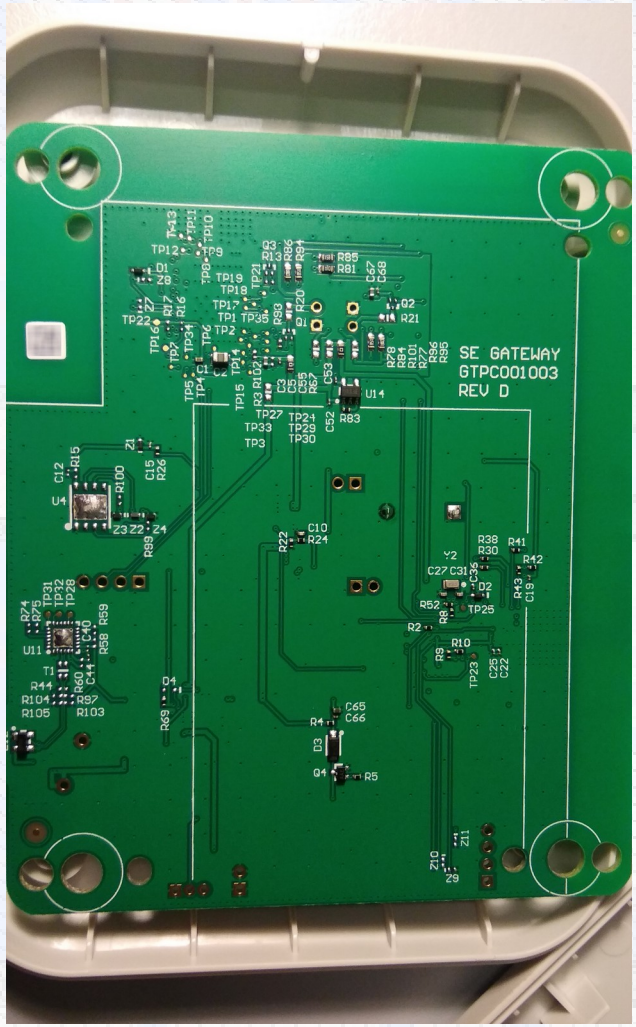
Low Zoey

04 May 2021 07:28PM
(Updated: 11 May 2021 12:29AM)

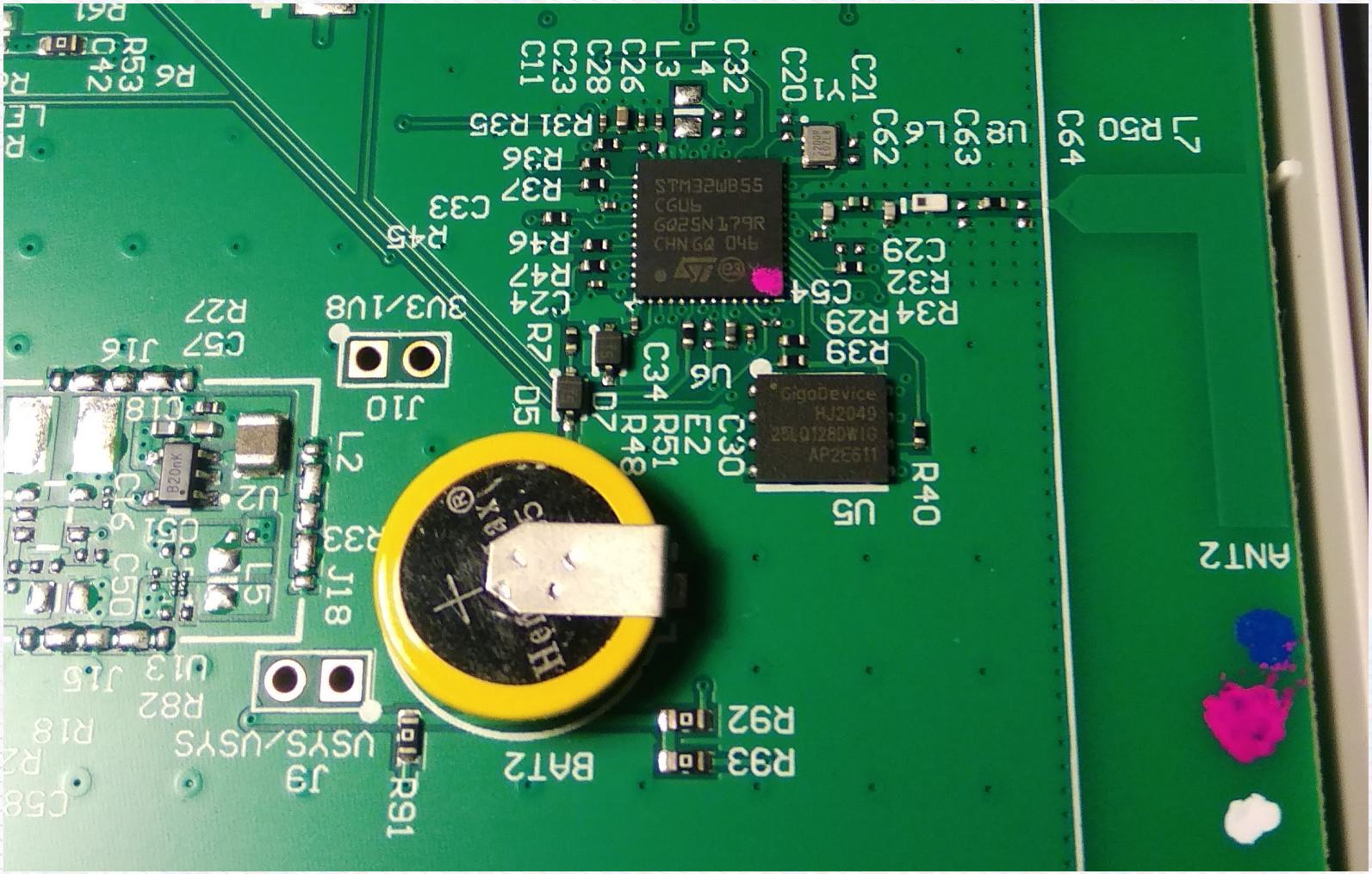
SafeEntry Gateway – Teardown

SafeEntry Gateway – Teardown

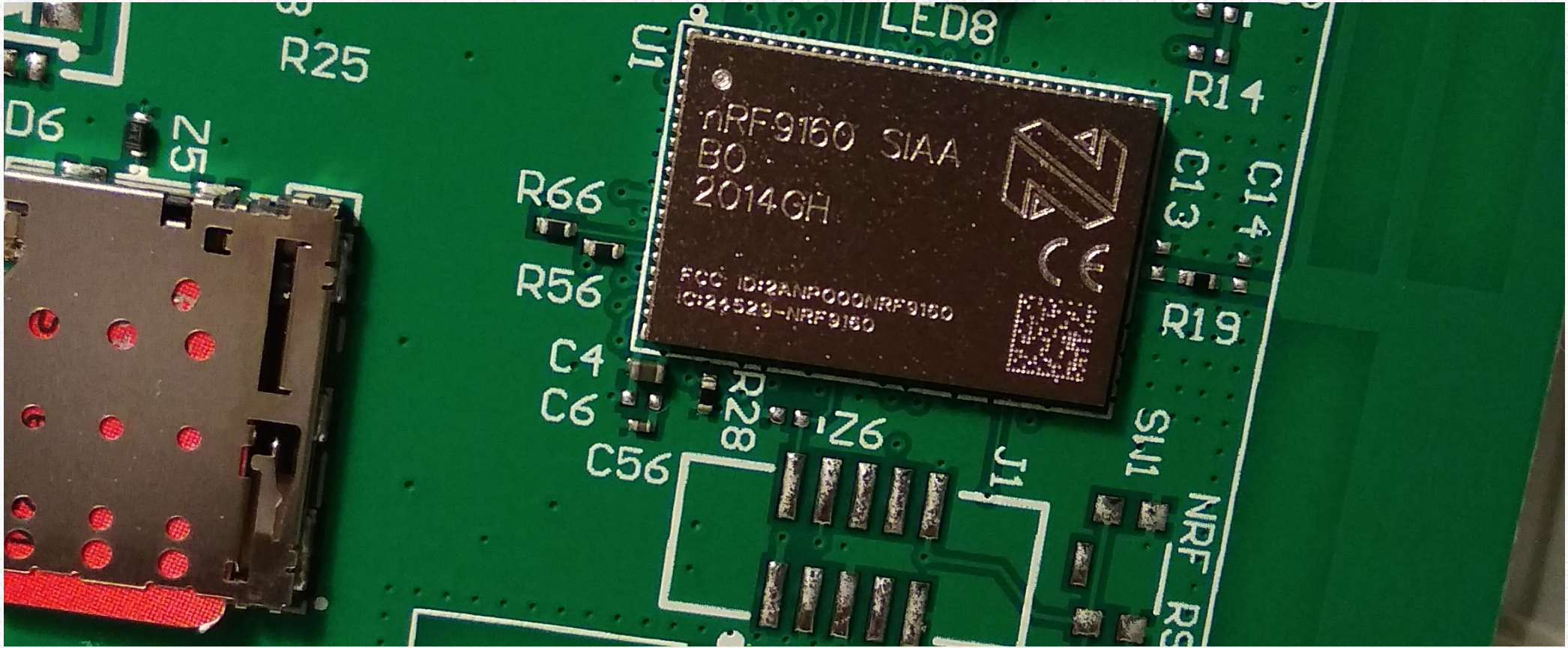




SafeEntry Gateway – Teardown



SafeEntry Gateway – Teardown



Nordic Semiconductor nRF9160 LTE modem

SafeEntry Gateway – Teardown

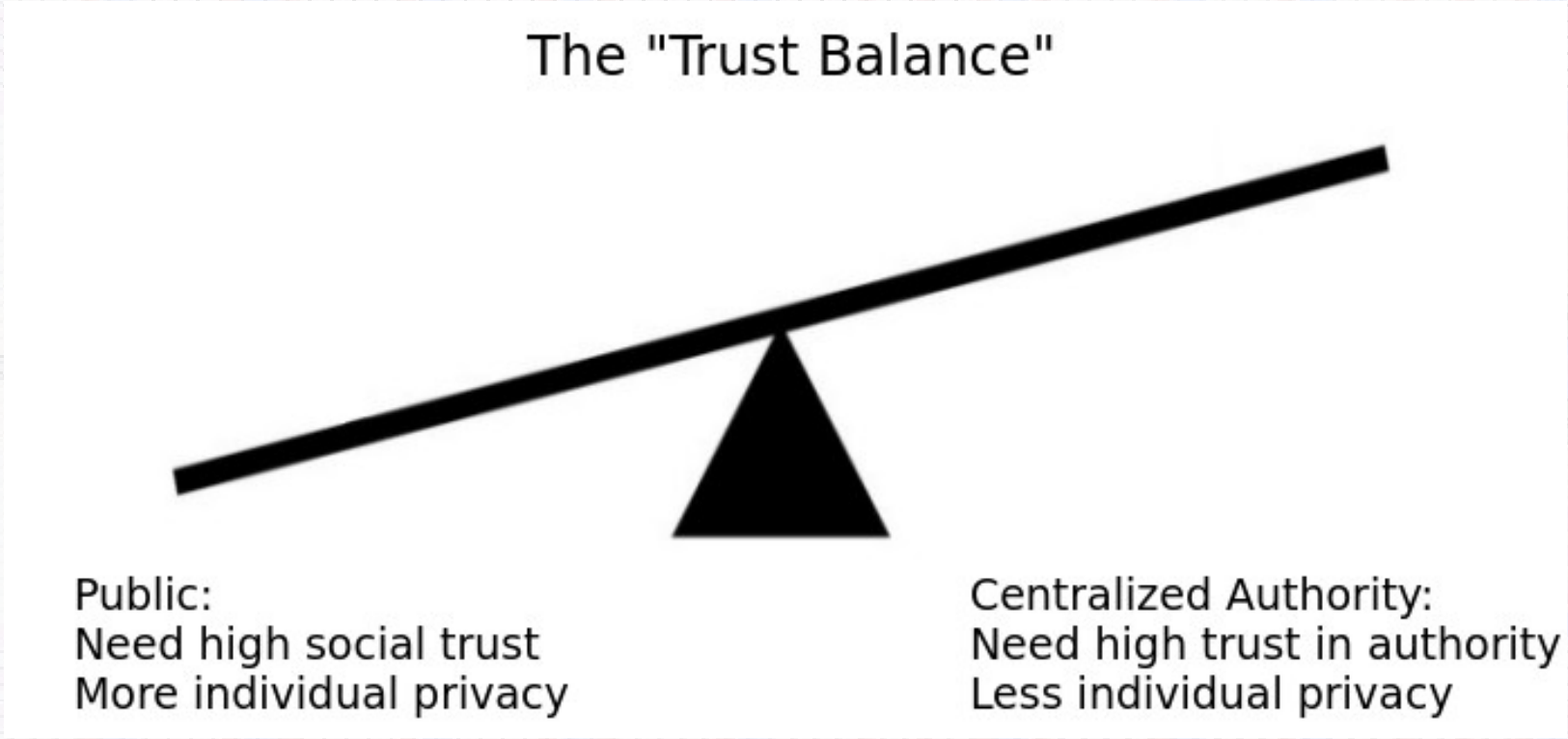
Basically a TraceTogether Pod V1.2 Rev F + nRF9160 4G IoT cellular modem!

Main hardware components:
U1: nRF9160 4G IoT cellular SiP
U5: GD25WQ64E 64Mbits Serial NOR Flash memory
U6: ST Microelectronics STM32WB55CG MCU with BLE 5.4

TraceTogether – Policy Analysis

With the introduction of the Gateway, has the privacy assumptions changed?

TraceTogether – Policy Analysis



Where is TraceTogether on the “Trust Balance?”

TraceTogether – Policy Analysis

Centralised vs decentralised contact tracing

BlueTrace envisages a blend of **decentralised proximity data collection** and logging, with a **centralised contact tracing capability**.

Encounter messages and encounter histories are exchanged and stored in a decentralised, peer-to-peer manner, without the participation of a central server.

We defer the centralised collection and processing of data to the last possible moment—when a diagnosis of COVID-19 is made—and then provide this data to the trusted public health authority in the OpenTrace reference implementation. Depending on the prevailing trust environment within which public health institutions operate, other jurisdictions may have different considerations that may favour a similar hybrid model or one that is completely decentralised.

We see various challenges with a purely decentralised contact tracing system. Individuals falsely declaring themselves infected would cause unnecessary anxiety and panic in other users, and erode trust in the system. Some form of authorisation for users to either flag themselves as positive COVID-19 cases, or to upload encounter history, is therefore necessary to protect against abuse.

Ultimately, this will have to be provided by a credentialed health institution or healthcare worker, who may or may not be part of a public health authority's infectious disease surveillance system, but would likely have to obtain the upload authorisation code through a chain of trust rooted in a centralised public health authority. This also has the benefit of ensuring that relevant information about the epidemic and the effect and effectiveness of such contact tracing systems is provided to the public health authority, to aid in planning public health interventions.

Finally, another advantage of a centralised approach is keeping humans in the loop in making the assessment of the appropriate follow-up actions.

Does possibility of abuse necessitate centralized contact tracing?

TraceTogether – Policy Analysis

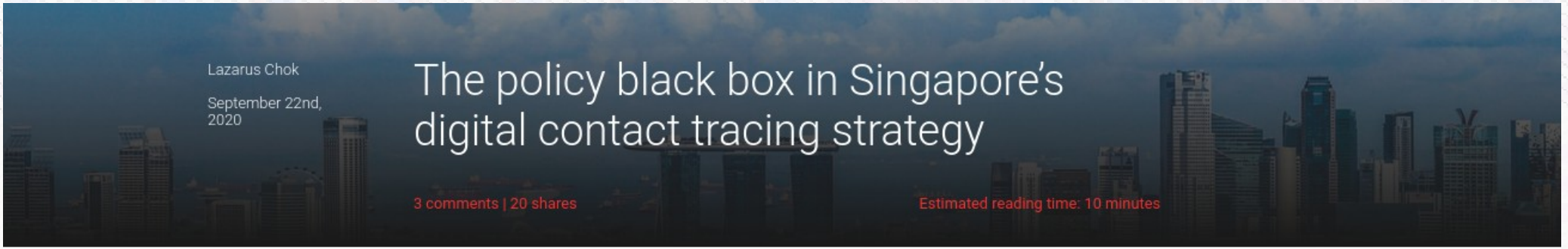
Human-in-the-loop vs Human-out-of-the-loop

It is possible to implement the BlueTrace protocol and have automated notification of probable close contacts of persons who have been diagnosed with COVID-19. In theory, we appreciate the privacy and scalability benefits of doing so. *In practice, our ongoing conversations with public health authority officials performing epidemic surveillance and conducting contact tracing operations compel us to recommend otherwise.*

An automated algorithm will necessarily generate both false negatives and false positives. A human contact tracer will similarly make mistakes. However, because a human contact tracer would seek to incorporate information beyond just physical proximity, he/she can correct for systematic biases introduced by a purely automated notification system.

Does human intervention necessarily remove biases?

TraceTogether – Policy Analysis



Lazarus Chok

September 22nd, 2020

The policy black box in Singapore's digital contact tracing strategy

3 comments | 20 shares

Estimated reading time: 10 minutes

20
Shares

"The emerging consensus is that government agencies must strike the right balance between public health interests and increased surveillance", writes ***Lazarus Chok****, a recent graduate from the LSE Department of Geography & Environment and Master's candidate at the New York University Center for Urban Science + Progress*

The COVID-19 pandemic has left cities struggling to reopen their economies while preventing hospital systems from being overwhelmed by recurring viral infections. Due to the novel coronavirus' ability to transmit pre-symptomatically or even asymptomatically, public health experts have deemed it essential for cities to rapidly identify and isolate close contacts of infected persons (Kretschmar et al., 2020). Cities around the world are rolling out contact tracing

TraceTogether – Policy Analysis

SafeEntry is the location tracking complement to TraceTogether (Figure 2). By scanning a Quick Response (QR) code at the premise, users log their time of entry/exit into SafeEntry. All data collected is encrypted and stored on government servers for 25 days. According to SafeEntry FAQs, data will only be accessed for the purposes of "preventing or controlling the transmission of COVID-19", a rather wide mandate compared to TraceTogether's purpose-limited design. Beyond the intuitive use case of identifying where infected persons visited, SafeEntry data may also be "de-identified and aggregated for analytics purposes". Ironically, while GovTech incessantly assures citizens that TraceTogether will not store location data, SafeEntry does *exactly* that – providing a comprehensive log of residents' movements. Beginning September 14, more venues would progressively trial "TT-only SafeEntry" systems where digital check-ins can only be done using the TraceTogether app or token, drafting into question whether the proximity and location databases are interoperable. If interoperability is possible, then the assurances that TraceTogether does not store location data could be moot.

TraceTogether – Policy Analysis

New normals in surveillance

One of the more interesting long-term consequences of habituating citizens to increased surveillance is the ratcheting effect of public policies. Expansions in state surveillance during the COVID-19 pandemic may be difficult to retract as habits stick and ideologies shift to the right. TraceTogether and SafeEntry are novel acts of self-administered surveillance (Rowe, 2020). The high degree of compliance suggests that Singaporean society is growing accustomed to surrendering private data to the government. Will this ratchet up a ‘new normal’ in everyday surveillance administered by the self?

TraceTogether – Policy Analysis

Singapore's partial success at containing COVID-19 has not been tempered by a critical analysis of its tradeoffs. Avoiding discussions of TraceTogether and SafeEntry's efficacy might lead Singaporeans to believe that 'innovative' solutions are merely performing a 'theatre of prevention' (e.g. Datta, 2020), or worse, suspect that they are a facade for something far more disingenuous. Like many other East Asian countries with a strong tradition of state intervention, the dichotomy of public health versus personal privacy has been falsely constructed to justify exceptionally intrusive measures (e.g. South Korea's disclosure of patient information). But beyond the intrusiveness of surveillance, this analysis suggests that the dichotomy elides over important questions of efficacy and the acceptability of using private data for large-scale experiments that could unlock, hitherto inaccessible, public good.

TraceTogether – Policy Analysis

THE STRAITS TIMES SINGAPORE

TraceTogether data was accessed in May 2020 for Punggol Fields murder investigation

TraceTogether – Policy Analysis

Some cited past remarks by Education Minister Lawrence Wong and Foreign Minister Vivian Balakrishnan on the use of TraceTogether data.

Last June, Mr Wong had said "there is no intention to use a TraceTogether app or TraceTogether Token as a means of picking up breaches of existing rules".

He said at a Multi-Ministry Task Force press conference that "the app and the device, plus SafeEntry, combined are meant to provide us with information in a timely manner so that we can do speedy, and fast and effective contact tracing.

"It's not meant as a way to detect offences and breaches of rules".

TraceTogether – Policy Analysis

Singapore

Bill restricting use of TraceTogether data for serious crimes passed by Parliament

A user displays a TraceTogether token in Singapore on Jan 5, 2021. (Photo: AFP/Roslan Rahman)

Tang See Kit
@SeeKitCNA

02 Feb 2021 10:58PM
(Updated: 03 Feb 2021 10:42AM)

TraceTogether – Policy Questions

Some Policy Questions:

- Why is the possibility of abuse of the system a factor in determining using a centralized system over a decentralized one? Don’t systems using Exposure Notification or DP-3T protocols require a key from health authorities to even upload contact tracing information? Why a top-down governance approach?
- Bluetrace whitepaper admits “it is possible to implement the BlueTrace protocol and have automated notification of probable close contacts”, but dismisses the idea due to bias; who writes the algorithms to begin with, and don’t the systemic biases of a centralized organization affect how humans work?
- SafeEntry Gateways are linked to specific locations (such as mall entrances). Doesn’t this then create location datapoints that could be used to track a person’s movements, invalidating bunnie et al’s assessments?

TraceTogether – Policy Questions

Some Policy Questions:

- The public was promised that TraceTogether data would be used only for contact tracing – it was revealed that the Criminal Procedure Code allows police officers to use TraceTogether data for criminal investigations and overrides TraceTogether's privacy policies.

  Why pass a bill making it legal for TraceTogether data to be used in specific criminal investigations instead of passing a bill to ensure that TraceTogether data would only be used for contact tracing?

- Are there proper counters to prevent departments from intentionally or accidentally sharing our data and information with other agencies, or employers, or even governments? How might these drive or reshape our consumer habits cyclically?

Finally...

TraceTogether – Policy Analysis

THE STRAITS TIMES SINGAPORE

Users who modify TraceTogether tokens could be breaking the law

TraceTogether – Policy Analysis

Under the Computer Misuse Act, unauthorised access to computer material carries a jail term of up to two years, a fine of up to $5,000, or both.

Those who make unauthorised modifications of computer material can be jailed for up to three years, fined up to $10,000, or both.

Infectious disease specialist Leong Hoe Nam said those who tamper with the token are irresponsible and put others at risk.

He said: "Manipulating the token is akin to sabotaging your country. Why are they so thick-headed?"

Why is taking a look at the token a crime? :P

Contact:

Email: bitowlsec@protonmail.com
Twitter/Mastodon: @quantumcatgirl/@sleepyowl

Teardown files will be uploaded to:
https://github.com/bitowlonline/TraceTogether-Teardown

Further writeups/reverse engineering will be posted at:
https://bitowl.online/

References:

The policy black box in Singapore’s digital contact tracing strategy – Lazarus Chok, London School of Economics and Political Science

Little Electronics Art Projects #571 – TraceTogether Token

Exposure Notification – Bluetooth Specification (Google)

BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders (now only found on Internet Archive)