BluePass Design and Protocol

D'Crypt Pte Ltd

14 July 2020

1 Introduction

The disruption and economic impact of COVID-19 is unparalleled and nations around the world are facing an unenviable dilemma – impose lockdowns that curtail contagion but cripple economies, or resume business-as-usual, with the prospect of waves of repeat infection.

A vaccine would represent a comprehensive solution, and if one were available, a small nation like Singapore has the wherewithal and determination to vaccinate everyone. But this does not scale globally with ease. Herd immunity is still dubious, and even if proven, is costly in terms of lives.

In the absence of a solution, epidemiologists worldwide concur that contact tracing is one of the best ways to manage the situation. Indeed, comprehensive contact tracing with rapid reaction is what is believed to be a key enabler to re-opening the economy.

Singapore has been a pioneer in the use of smartphones for contact-tracing. Our government's TraceTogether app employs peer-to-peer Bluetooth communications to develop a contact tracing history with cryptographically protected privacy which (with user permission) can be disclosed when tracing infections.

Unfortunately, TraceTogether adoption is still below the threshold that is considered necessary for effective contact tracing. We believe this arises because our smartphones have become a very personal device, and "inviting" TraceTogether into our smartphones raises many privacy concerns. These concerns have more to do with how the public use smart-phones and is not because of some shortcoming of the underlying contact tracing technology or system concept.

2 BluePass

BluePass is D'Crypt's response to the COVID-19 pandemic. It is a small, battery-powered, wearable device that is issued to the public. Use instructions are simple and non-threatening – ***Bring It With You***. BluePass devices exchange contact-tracing records automatically and without any user intervention. If a user is diagnosed to be infected, records extracted from his/her BluePass and decrypted at a secure backend facilitate contact-tracing.

3 Interoperability

BluePass is designed from the ground up to interoperate with other systems.

- BluePass is built around Bluetooth Low Energy (BLE), a technology that is considered suitable for contact-tracing. BLE is the basis for a number of other contact tracing solutions, including Trace-Together.
- BluePass employs the standard Connectionless Advertise/Scan model of BLE systems to exchange contact tracing

records. This aligns with industry as the method of choice for Bluetooth-based contact-tracing solutions.

- D'Crypt publishes full details of the protocol in this document to facilitate and encourage other systems to interoperate with BluePass. We are also prepared to adapt BluePass to interoperate with other systems.
- BluePass uses the BlueNRG-2 Bluetooth Low Energy System-On-Chip from ST Microelectronics. This chip is firmware-programmable and we are prepared to integrate other protocols into BluePass, subject to chip limitations.

4 Open Disclosure

While the world recognizes that contact-tracing is an effective means to manage COVID-19, there are still privacy concerns around contact-tracing solutions.

D'Crypt believes that the best way to address privacy concerns is to be open about the product and what it does. Accordingly, we adopt the following:

- We publish full details of the protocol (in this document) to allow independent scrutiny. Through this scrutiny, it should be possible to discern that the BluePass preserves privacy (certainly to an extent that is better than some of the contact-tracing solutions in use today). It should also be possible to ascertain that BluePass is not susceptible to being deployed for purposes other than contact-tracing.
- It is an established tenet in the cryptography and security business that a truly secure system will remain secure as long as the cryptographic keys are kept secret, even if all other details of its design are known to the adversary. We believe BluePass meets this gold standard and are prepared to allow it to be subject to scrutiny.
- We are prepared to facilitate testing and validation. A suitably-qualified Tester can provide a set of cryptographic keys to be injected into a small sample of BluePasses. These specially-injected BluePasses can then be provided to the Tester, who can then scrutinize the protocol by monitoring the radio transmission and thus be able to verify the correctness of the implementation and its compliance to the protocol description.
- With open-disclosure, we believe that we will also benefit from good feedback. This will help the overall effort against COVID-19.

5 BluePass Design and Protocol

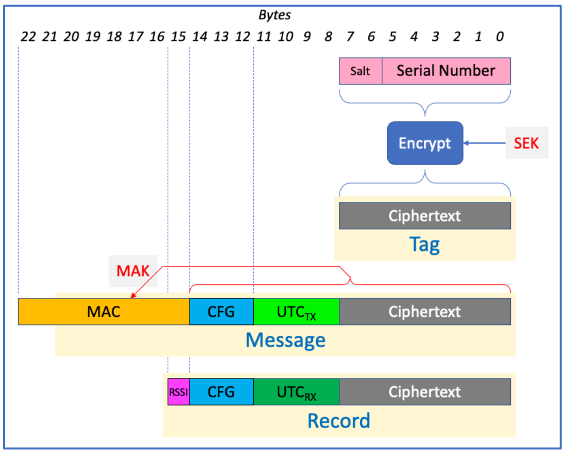

Figure 1: BluePass Formats

Figure 1 shows the format of the data that BluePass exchanges.

5.1 Tag Generation and Storage

Each BluePass is assigned a unique 48-bit serial number. During manufacturing, this serial number is concatenated with a 16-bit integer salt and then encrypted using Triple-DES with a 168-bit System Encryption Key (SEK). The result is an 64-bit Ciphertext block referred to as the Tag. Each BluePass is pre-configured with a list of 2^{16} Tags using the same serial number and all possible values for the salt.

We remark that SEK is a system-wide key that is maintained only at the backend; BluePass is not loaded with SEK.

We choose Triple-DES because of its smaller encryption block-size, which yields 64-bit Tags. Using the more conventional AES would have resulted in Tags that are double the size.

BluePass allocates 512KB of non-volatile Flash memory to store this array of Tags. As this Flash memory is external to the BlueNRG-2 chip, BluePass re-encrypts Tags using AES with a 128-bit Tag Encryption Key (TEK) for storage into this Flash memory. The Tag Encryption Key is self-generated by BluePass during factory-configuration using the on-chip Hardware Random Bit Generator and is therefore different across different BluePasses.

5.2 Tag Advertisement

Tags are advertised on all three Bluetooth advertisement channels at an advertisement interval of 0.5s. The current Tag is employed for 10 minutes, and then retired and replaced by the next Tag in the list. In this fashion, the 2^{16} Tags will last about 1.25 years, which exceeds the anticipated life of the battery.

BluePasses exchange Tags using Bluetooth Low Energy's connectionless Advertise-Scan profile. Each BluePass constructs a message that comprises the current 64-bitTag, the current UTC time represented as a 32-bit unsigned integer, and a 24-bit configuration field which is fixed for each group of BluePasses. This entire 120-bit vector is then subjected to HMAC-SHA-256 using a 256-bit Message Authentication Key (MAK). The first 64-bits of the resulting MAC are appended to the message. The message is then inserted as the payload for advertisement. The MAC authenticates the message and embedding the UTC time guards against replay attacks. Note that even though Tags are refreshed only once every 10 minutes, the Message must be recomputed every second since the UTC time embedded in the message changes.

We remark that the MAK is a system-wide key; every BluePass device must be loaded with this key. Its compromise would result in BluePass being vulnerable to spoofing. So while contact-tracing records can still be exchanged, malicious adversaries can inject spurious records into the BluePass system without being detected.

5.3 Message Reception and Validation

BluePass scans for 3 seconds every 10 minutes, during which time it receives advertisements. Each advertisement payload that it receives is subject to simple filtering checks (message length, configuration field format etc). If these checks pass, the MAC is validated using the MAK. Once validated, the UTC embedded in the message is checked to detect replay attacks. If all these checks succeed, the message is compared to other recently-received messages to detect and drop duplicates. If the message passes all these checks, the MAC is dropped, the UTC of the receiver replaces the UTC of the advertiser, and the Received Signal Strength (RSSI) is appended to form a 128-bit Record that is then written to non-volatile memory.

We have validated that BluePass can receive, filter, authenticate, and store up to 80 Records per second when it is scanning.

5.4 Record Storage

BluePass can store up to 384K records. While the duration that records are retained is configurable, D'Crypt currently assumes that records need to be maintained across 3 disease cycles, which translates to 63 days. There is adequate memory to record in excess of 6240 records per day. Records are maintained in a circular buffer and the newest record overwrites the oldest record.

6 Reporting

The BluePass Reporting Station is a Bluetooth device that scans to establish connections using the Generic Attribute protocol GATT.

When a BluePass user is diagnosed to be infected, he/she uploads the Records captured and stored in BluePass by pressing a pushbutton on the BluePass while in the vicinity of the Reporting Station.

BluePass responds by advertising the connect and thus establishes a GATT connection with the Reporting Station.

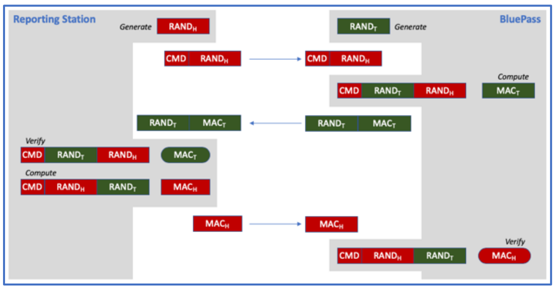

Figure 2: BluePass Command Mutual Authentication

Once the connection is established, BluePass responds to commands from the Reporting Station. Each command is subject to 3-pass mutual authentication using a bidirectional 64-bit random challenge, where the responses are the 64-bit prefix of the Message

Authentication Code generated by applying HMAC-SHA-256 to the challenges, all this secured by a 256-bit Command Authentication Key (CAK). The Mutual Authentication protocol is shown in Figure 2. BluePass only executes commands after it has authenticated the Reporting Station, and the Reporting Station should trust returned results only if it has authenticated BluePass.

It is important to note that BluePass treats the GATT connection as a communication channel and does not rely on any of Bluetooth's cryptographic features for privacy or other security assurance.

Some of the commands supported include:

6.1 Reporting Records

When BluePass is instructed to report, it transfers its stored records in reverse chronological order. Each 128-bit record is protected against errors during transmission with a 16-bit CRC and a further 16-bit sequence number ensures in-order reception and also allows multiple records to be in flight to improve transmission rates in the presence of channel latency.

6.2 Reporting Statistics

As part of housekeeping, BluePass maintains statistics of the number of Tags used, the number of Records received, filtered, validated, and stored. These and other statistics can be reported and analysed to deeper insight into how BluePass is used and how it behaves in the deployment.

6.3 Reporting Errors

BluePass tracks many possible error conditions, and the error statistics can also be reported.

6.4 Reporting Logs

BluePass logs all important events and the log can be retrieved.

7 Tracing

Records carry encrypted Tags and so are of little use to communication intermediaries such as the Reporting Station. The identity behind the Tag is only revealed when the Tag returns to the Backend where the System Encryption Key (SEK) is employed to decrypt the Tag to reveal the serial number. This decryption is performed with a Tag Decryption Device.

Recognizing the criticality of the SEK in preserving user privacy, the Tag Decryption Device is built using D'Crypt's *d'Cryptor* SC FIPS140-2 Level 4 certified cryptographic token.

8 Privacy and Usability

While the protocol is designed to prevent tracking or to preserve privacy, it is still necessary to retain some user-specific information in order for BluePass to be usable as a contact-tracing solution.

BluePasses are uniquely identified by their serial numbers, and our design of BluePass does not stipulate or restrict how a BluePass is associated with a user.

- We believe that at a national level, the best way to associate BluePass with the user is to identify the user through a contactable phone number, further disambiguated by the last 4 characters of the user's identity document such as the NRIC, FIN, or Passport. Not insisting that the phone number be a mobile phone number allows families to use the home line-phone. Seniors who live communally can also quote their communal phone. Children who may not yet own a cell-phone can be reached through their parents phones. In situations where multiple users share the same contact number, the precise user is disambiguated through the last 4 characters of the identity document.
- At a company level, it perhaps makes more sense to be associating the BluePass with a Staff ID number. The company then takes on the responsibility to contact the staff in the event that a Tag from the staff's BluePass was received by an infected person.
- The association of the BluePass to its user does not have to be permanent. All that is required is to know the time interval over which a particular user was associated with the BluePass. This will allow us to filter and discern which Records collected by the BluePass are associated with the specific user. Such a feature allows BluePass to be issued temporarily to company visitors, as

well as to itinerant workers such as those commuting into Singapore from neighbouring countries.

- There is also nothing stopping a user from owning more than 1 BluePass. In this case, all the user has to do is to remember to bring at least 1 BluePass along. If the user is diagnosed as infected, he/she would have to upload the Records collected by all of his/her BluePasses.

9 Deployment

BluePass is designed for mass deployment:

- BluePass is Small and light. In its current form, BluePass is 3×5cm and weighs about 15g, approximately the weight of two Singapore $1 coins.
- BluePass is Easy to Use. BluePass does not require any user configuration or management. The user only has to remember to ***Bring It With You***. Designed with no user-serviceable parts, It is built to withstand robust usage, being able to survive drops onto a hard surface and being submerged in liquid.
- BluePass Registration is Easy. All that is required is for the user to be associated with the BluePass serial number. There is no need to enable or configure the BluePass. This allows deployment even in scenario where there is no computer.

10 Distributed Deployment and Interoperation

Our aim is to deploy BluePass at company or organization level for contact-tracing as well as for rapid isolation and containment for business continuity purposes. We envision companies and organizations issuing BluePasses to their staff to achieve this aim. In order for companies to be effective in isolation and containment, it is our view that they must be able to see the data that the BluePass system collects and this means that they must be able to decrypt Tags locally. So we envision each company owning its own backend and generating its own System Encryption Key with which to encrypt the Tags in its BluePasses.

At the same time, when staff of a company are not at work, they may encounter other BluePasses issued by other companies or organizations. Messages will still be advertised and received.

Considering both the "at work" and "not at work" scenarios, when someone is diagnosed as infected and uploads his/her records, the Configuration Field identifies the organization that the Tag originated from.

So the BluePass system employs a central registry to relay Tags to the relevant organization for decryption. We envision two ways in which this registry can take shape:

1. If the model for BluePass is for companies to form a loose and cooperative confederation, then each company undertakes to decrypt those Tags that it issued, even if they are received by BluePasses belonging to other companies or organizations. In this case, the central registry is a relaying service.
2. If national policy so dictates, an organization may only be allowed to decrypt its own Tags since this is all that is necessary for any workplace isolation or containment action. Tags originating from BluePasses belonging to other organizations can only be decrypted at a national level. In this case, the registry can be owned by the government. The government generates and retains a Master SEK and issues unique configuration fields to all companies. Each company employs an SEK that is diversified (using this Configuration Field) from this Master SEK.

11 BlueGate

BlueGate is a derivative product; it employs the same BluePass electronics, but is tethered to an unlimited power source and is set to scanning mode all the time – it does not advertise Tags. Given the frequency of BluePass advertisement (every 0.5s) a BlueGate deployed at a location will be able to pick up the advertisements of every BluePass in its immediate vicinity.

We believe that BlueGate can replace SafeEntry. This will relieve the public of needing to manipulate a smart-phone app or scan a QR code. All that is now required is for us to walk past the BlueGate, which will pick up our advertisement.

As an augmentation, we imagine a pair of BlueGates separated by some distances (a few metres) and time-synchronized accurately will be able to compare advertisement time-of-reception to discern whether a particular BluePass was entering or exiting a location. We do point out that at the time of writing, this concept has not yet been field-tested.

BlueGates can also be deployed at critical locations where the possibility of virus transmission is higher. Some examples of such locations could be public toilets, common dining facilities, taxis and lifts.

BlueGates can also be deployed in Meeting Rooms or other facilities to monitor and limit the number of simultaneous participants and enforce social distancing.

BlueGates can also be emplaced to exclusion zones. This may be particularly useful in offices or worksites that are segregated into Team A/Team B, since BlueGate can be used to monitor if Team members have transgressed into the other team's areas.

For many of these monitoring purposes, BlueGate can be interfaced to a loud buzzer to sound alarms.

11.1 BlueGate and Privacy

We acknowledge that a BlueGate picking up advertisements of neighbouring BluePasses does intrude on individual privacy, but we contend that this approach is no worse than what we are doing currently by furnishing our full NRIC number or using our SingPass phone-app. We also note that BlueGate receives only encrypted Tags which it cannot make sense of. Tags can only be decrypted to reveal the serial number after they have been put through the Tag Decryption Device at the backend.

12 Conclusion

We share BluePass design and protocol details with the dual aim of receiving feedback to improve the design, and of achieving an open platform for interoperation. We stress that we are not insisting that everybody conform to our protocol. Rather, we disclose with the aim of promoting an open standard for interoperability among contact tracing devices, and we are both willing and able to do our part to adapt BluePass protocol to something else if this is what it takes to achieve interoperability and adoption.

This document is filed at https://www.d-crypt.com/BluePass/Protocol.pdf and can be retrieved using the link.

We are happy to receive feedback on BluePass, at bluepass@d-crypt.com.