Exposure Notification

Bluetooth Specification

Preliminary — Subject to Modification and Extension

April 2020

v1.2

Contents

Overview

This document provides the detailed technical specification for a new privacy-preserving Bluetooth protocol to support Exposure Notification. Exposure Notification makes it possible to combat the spread of the coronavirus — the pathogen that causes COVID-19 — by alerting participants about possible exposure to someone they have recently been in contact with, who has subsequently been positively diagnosed as having the virus. The Exposure Notification Service is the vehicle for implementing exposure notification and uses the Bluetooth Low Energy wireless technology for proximity detection of nearby smartphones, and for the data exchange mechanism.

Definitions

- Exposure Notification Service — The Bluetooth Low Energy service for detecting device proximity.
- Temporary Exposure Key — A key that's generated every 24 hours for privacy consideration.
- Diagnosis Key — The subset of Temporary Exposure Keys uploaded when the device owner is diagnosed as positive for the coronavirus.
- Rolling Proximity Identifier — A privacy preserving identifier derived from the Temporary Exposure Key and sent in the broadcast of the Bluetooth payload. The identifier changes about every 15 minutes to prevent wireless tracking of the device.
- Associated Encrypted Metadata (AEM) — A privacy preserving encrypted metadata that shall be used to carry protocol versioning and transmit (Tx) power for better distance approximation. The Associated Encrypted Metadata changes about every 15 minutes, at the same cadence as the Rolling Proximity Identifier, to prevent wireless tracking of the device.

Exposure Notification Service

Exposure Notification is a Bluetooth Low Energy service registered with the Bluetooth Special Interest Group with 16-bit UUID 0xFD6F. It is designed to enable proximity sensing of the Rolling Proximity Identifier between devices for the purpose of computing an exposure event.

Devices broadcast and scan for the Exposure Notification Service by way of its 16-bit service UUID. The Service Data type with this service UUID shall contain a Rolling Proximity Identifier and Associated Encrypted Metadata that will both change periodically.

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**

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.

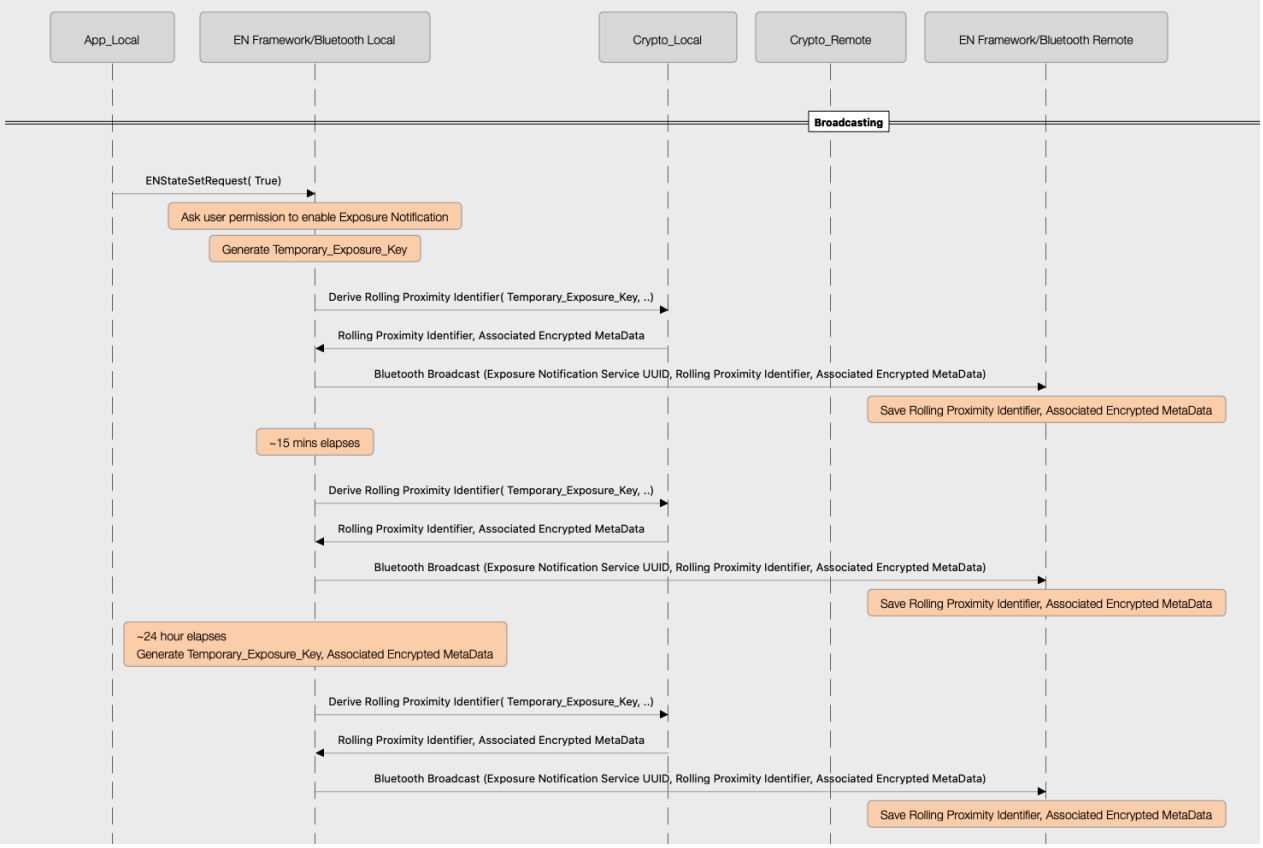
[1] The terms “Advertisement,” “Advertiser,” and “Advertising” are used in this document as defined in the Bluetooth Standard.

Broadcasting Behavior

- During the Bluetooth broadcast, advertisements are to be non-connectable undirected of type `ADV_NONCONN_IND` (Section 2.3.1.3 of 5.2 Core Spec).
- The advertiser address type shall be Random Non-resolvable.
- On platforms supporting the Bluetooth Random Private Address with a randomized rotation timeout interval, the advertiser address rotation period shall be a random value that is greater than 10 minutes and less than 20 minutes.
- The advertiser address, Rolling Proximity Identifier, and Associated Encrypted Metadata shall be changed synchronously so that they cannot be linked.
- If the hardware allows, a separate Bluetooth broadcasting instance shall be used to provide reliability and flexibility in choosing optimal interval.
- The broadcasting interval is subject to change, but is currently recommended to be 200-270 milliseconds.

Broadcasting Flow

The following diagram illustrates the flow of broadcasting between devices.



Scanning Behavior

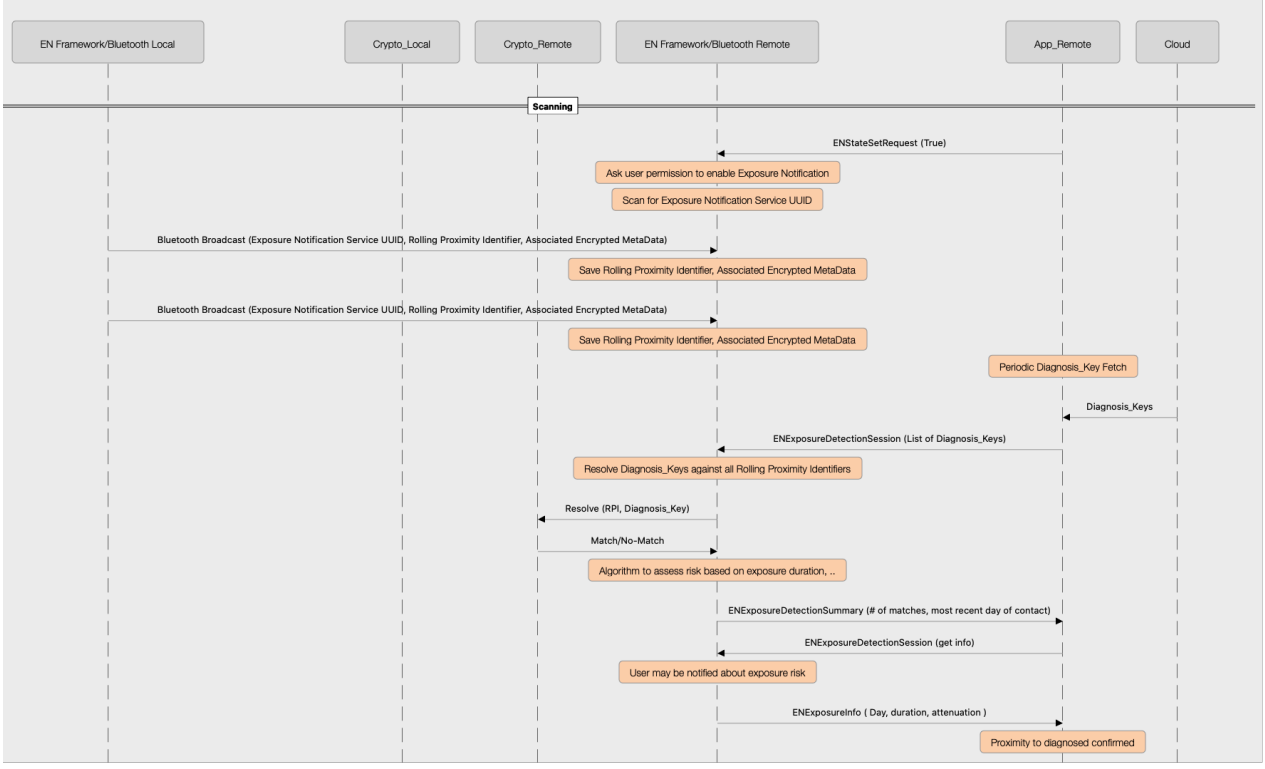
- Discovered Exposure Notification Service advertisements shall be kept on the device.
- Scan results shall be timestamped and RSSI-captured per broadcast.
- The scanning interval and window shall have sufficient coverage to discover nearby Exposure Notification Service advertisements within 5 minutes.
- The scanning strategy that works best is opportunistic (leveraging existing wakes and scan windows) and with minimum periodic sampling every 5 minutes.

Scan Power Considerations

- Platforms running the Exposure Notification Service shall be designed to account for a large volume of broadcasters in public spaces and shall frequently rotate their Random Non-resolvable address and Rolling Proximity Identifier.
- Wherever supported by the hardware and the operating system, Bluetooth controller duplicate filters and other hardware filters shall be used to prevent excessive power drain.

Scanning Flow

The following diagram illustrates the flow and behavior of device scanning.



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.

Revision History

v1.2 - April 30, 2020

- Made grammatical corrections.

v1.1 - April 23, 2020

- Renamed the specification from “Contact Tracing” to “Exposure Notification,” along with all related terminology.
- Added information to the Privacy section.
- Added Associated Encrypted Metadata to terminology, Exposure Notification Service, payload structure, and flow diagrams.
- Added the Bluetooth transmit power level definition.
- Added user notification information when the app asks for details on an exposure event.
- Changed the length of the service data to be 0x17.
- Reformatted the title page and table of contents for consistency across documents.
- Replaced the term “advertise” with the term “broadcast” when used generically.
- Replaced the term “Contact Detection Service” with “Exposure Notification Service.”