Google & Apple
COVID-19 ~~contact tracing~~
exposure notification

Google & Apple COVID-19 contact tracing

- Apr 10, 2020: Apple and Google partner on COVID-19 ~~Contact Tracing (CT)~~ technology, renamed Exposure Notification (EN)
- Joint effort to enable the use of Bluetooth technology to help governments and health agencies reduce the spread of the virus
- Solution that includes application programming interfaces (APIs) and operating system-level technology to assist in enabling EN
- Available since May 2020

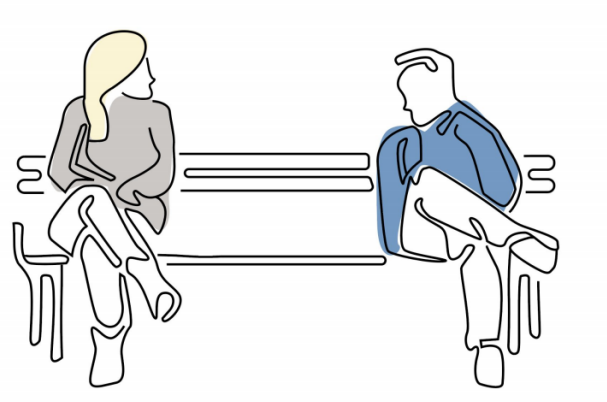
Privacy-safe contact tracing using Bluetooth Low Energy

- Explicit user consent required
- Doesn’t collect personally identifiable information or user location data
- List of people you’ve been in contact with never leaves your phone
- People who test positive are not identified to other users, Google or Apple
- Will only be used for contact tracing by public health authorities for COVID-19 pandemic management
- Doesn’t matter if you have an Android phone or an iPhone - works across both

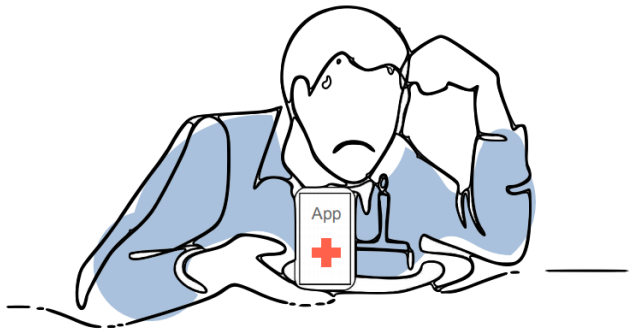
Google

Source: https://blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf

Alice and Bob meet each other for the first time and have a 10-minute conversation.

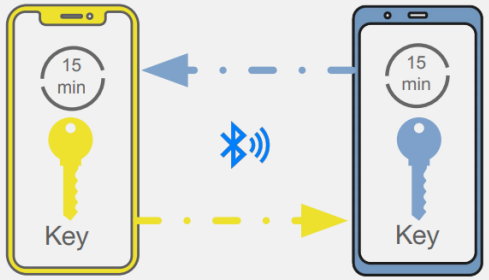


Bob is positively diagnosed for COVID-19 and enters the test result in an app from a public health authority.



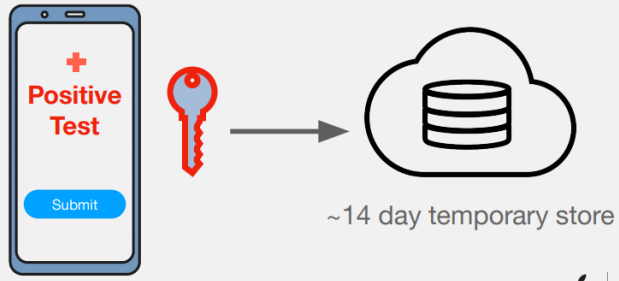
A few days later...

Their phones exchange anonymous identifier beacons (which change frequently).



With Bob's consent, his phone uploads the last 14 days of keys for his broadcast beacons to the cloud.

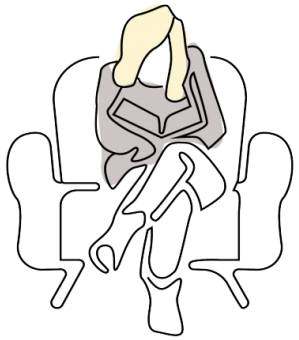
Apps can only get more information via user consent



Google

Source: https://blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf

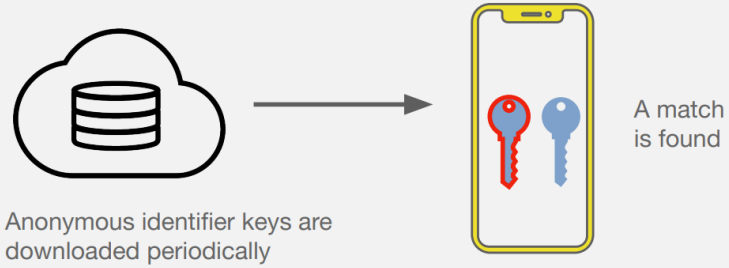
Alice continues her day unaware she had been near a potentially contagious person.



Alice sees a notification on her phone.

Sometime later...

Alice's phone periodically downloads the broadcast beacon keys of everyone who has tested positive for COVID-19 in her region. A match is found with the Bob's anonymous identifier beacons.



Alice's phone receives a notification with information about what to do next.

Additional information is provided by the health authority app or website

Google

Source: https://blog.google/documents/57/Overview_of_COVID-19_Contact_Tracing_Using_BLE.pdf

EN Bluetooth Specification v1.2

- Privacy-preserving Bluetooth protocol to support EN
- *Exposure Notification Service* is the vehicle for implementing contact tracing and uses the Bluetooth LE (Low Energy) for proximity detection of nearby smartphones
  - The BLE service for detecting device proximity

EN Bluetooth Specification v1.2

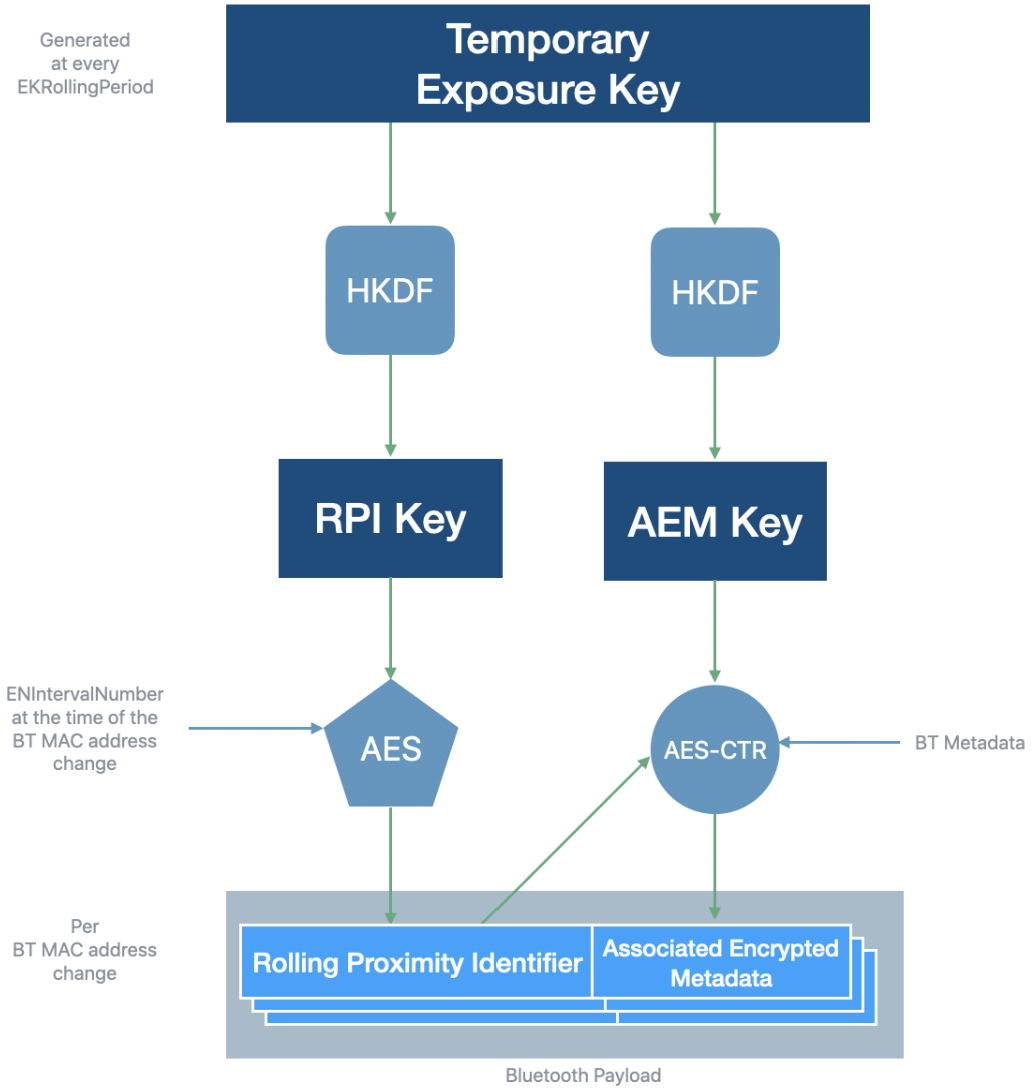
- Exposure Notification is a BLE service registered with the Bluetooth SIG with 16-bit UUID **0xFD6F**, it is designed to enable proximity sensing of **Rolling Proximity Identifier** between devices
- Devices broadcast and scan for the ENS by way of its 16-bit service UUID.
- The Service Data type with this service UUID shall contain a 128-bit Rolling Proximity Identifier and Associated Encryted Metadata (both change periodically)

EN Bluetooth Specification v1.2

- ***Temporary Exposure Key****:* a key generated every 24 hours for privacy consideration
- ***Diagnosis Keys****:* the subset of Temporary Exposure Keys which are uploaded when the device owner is diagnosed positive for COVID-19
- ***Rolling Proximity Identifier****:* a privacy preserving identifier derived from the Temporary Exposure Key and sent in the bluetooth advertisements
  - It changes every ~15 minutes to prevent wireless tracking of the device
- ***Associated Encrypted Metadata***: privacy preserving encrypted metadata that shall be used to carry protocol versioning and transmit (Tx) power for better distance approximation
  - it changes about every 15 minutes, at the same cadence as the Rolling Proximity Identifier

Key Schedule for Exposure Notification

- HKDF: Hashed Message Authentication Code (HMAC)-based key derivation function
- Each Rolling Proximity Identifier is derived from a Rolling Proximity Identifier Key, which is in turn derived from a Temporary Exposure Key and a discretized representation of time
- Rolling Proximity Identifier changes at the same frequency as the Bluetooth randomized address, to prevent linkability and wireless tracking
- Time is discretized in 10 minute intervals that are enumerated starting from Unix Epoch Time. **ENIntervalNumber** allows conversion of the current time to a number representing the interval it's in



EN Bluetooth Specification v1.2

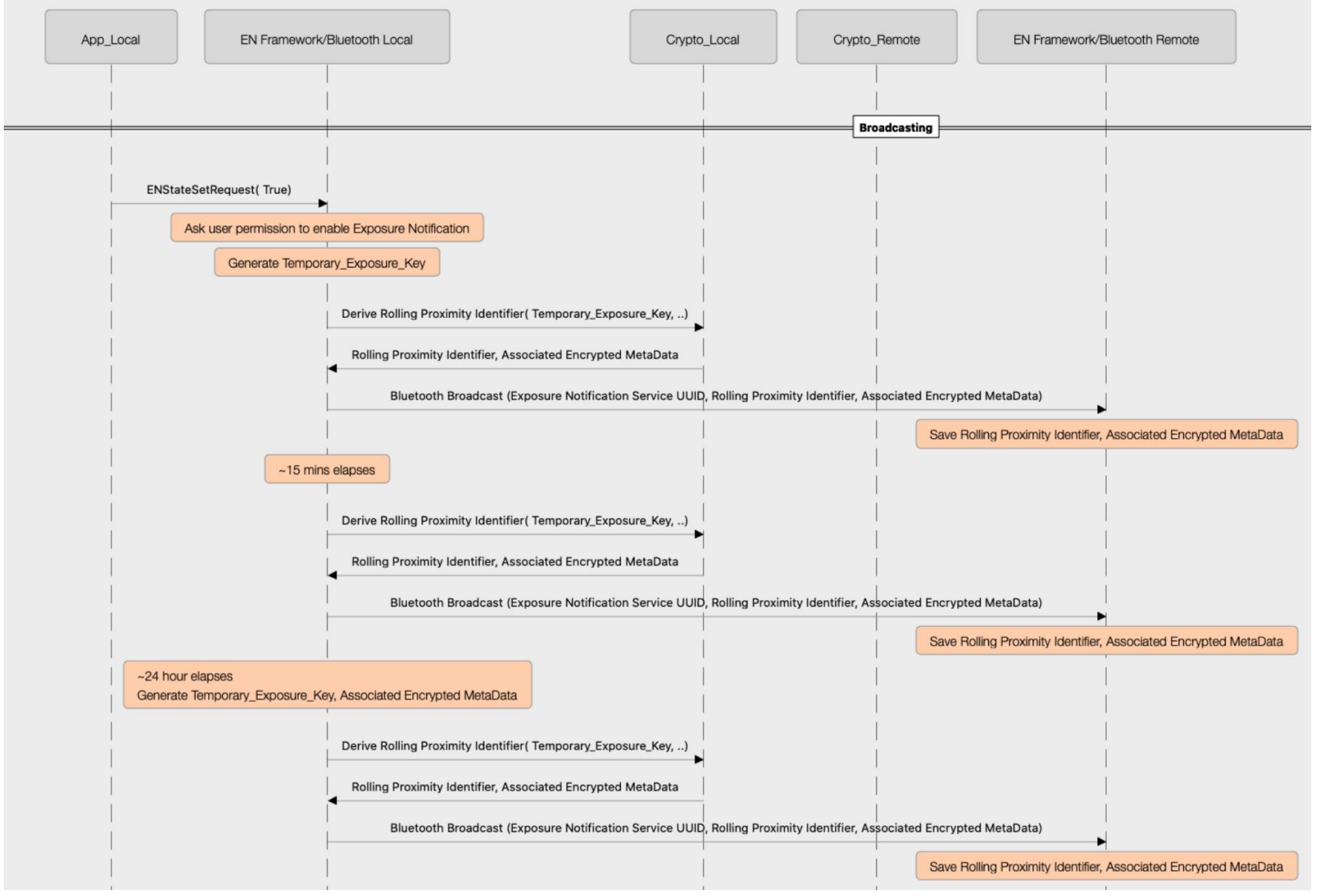
- Flags Section: BLE general discoverable mode (bit 1) shall be set to 1
- Complete 16-bit Service UUID Section: The UUID is 0xFD6F
- Service Data 16-bit UUID Section: This section shall have two different sections in its payload:
  - 16 byte Rolling Proximity Identifier
  - 4 byte Associated Encrypted Metadata that contains the following:
    - Byte 0: Versioning
    - Byte 1: Transmit power level, used to improve distance approximation
    - Byte 2&3: Reserved for future use

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**

Broadcasting

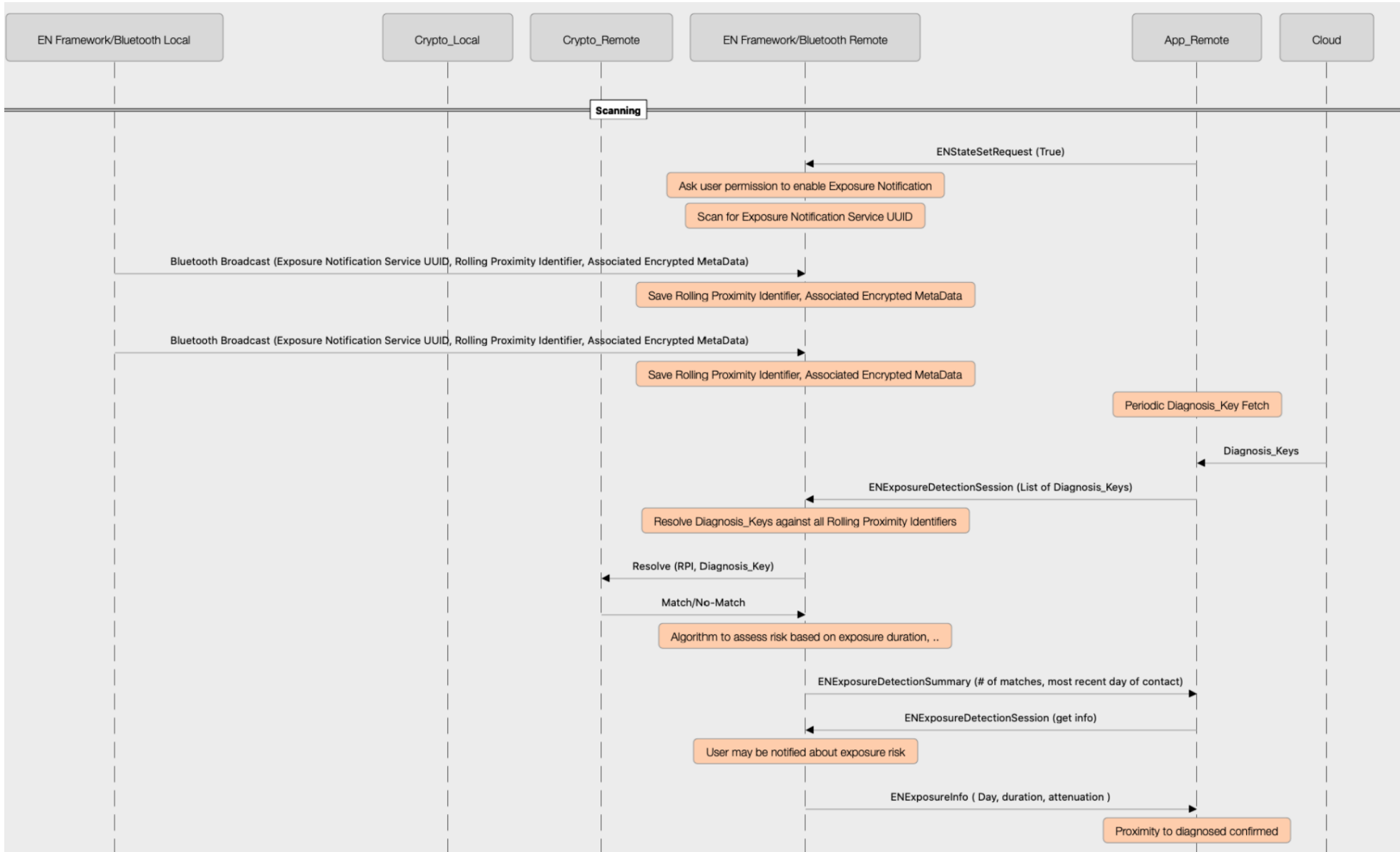
- The advertiser address type should be Random Non-resolvable
- On the platforms supporting Bluetooth Random Private Address with randomized rotation timeout interval, the advertiser address rotation period shall be a random value, greater than 10 minutes and less than 20 minutes
- Broadcasting interval: recommended to be 200-270 milliseconds

Broadcasting



Scanning

- Scan results shall be timestamped and RSSI-captured per advertisement



Positive diagnosis

- When a user tests positive, a limited set of Temporary Exposure Keys and their respective ENIntervalNumber (describing when their validity started) are uploaded to the Diagnosis Server
- This set of Temporary Exposure Keys is limited to the time window in which the user could have been exposing other users (for example, the most recent 14 days). This subset of keys is referred to as Diagnosis Keys.
- The Diagnosis Server aggregates the Diagnosis Keys from all users who have tested positive, and distributes them to all the user clients that are participating in exposure notification.

Value Matching of Positive Users

- Each client periodically fetches the list of new Diagnosis Keys from the Diagnosis Server
- Diagnosis Keys are sets of Temporary Exposure Keys with their associated ENIntervalNumber, each of the clients can again derive the sequence of Rolling Proximity Identifiers that were broadcast over Bluetooth from users who tested positive
- Derive the 144 Rolling Proximity Identifiers starting from ENIntervalNumber. The clients match each of the derived identifiers against the sequence they found through Bluetooth scanning

Android EN

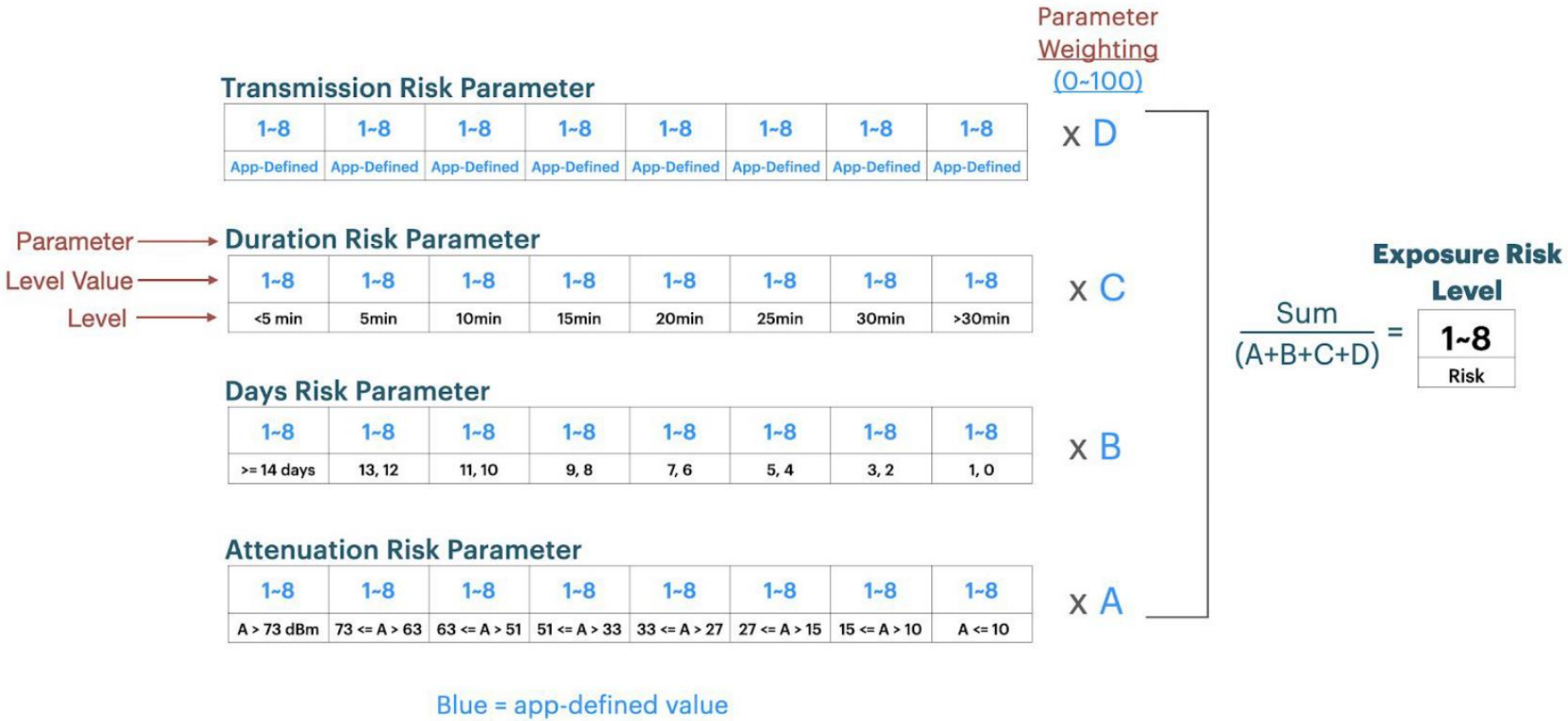
- Bluetooth functionality, including all broadcast and scanning for BLE beacons and local database storage, happens within Google Play services on-device
- App using it needs to have the BLUETOOTH permission in its manifest
- It automatically
  - Manages daily random keys
  - Manages Bluetooth broadcast and collection
  - Identifies whether the holder of the device was in close contact with a COVID-19 confirmed case
- No user interface other than the permission dialogs

COVID exposure notification app

- Mobile app implemented by authorities
- Uploads and downloads information to/from external servers
- Functionalities for confirming that the holder of the device has been tested to positive
- Defines the weigths used when computing risk

Computing risk

- These parameters are used to calculate risk for each exposure incident using the following formula



References

- https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology
- Exposure Notification Cryptography Specification Preliminary — Subject to Modification and Extension, April 2020 v1.2, Google & Apple
- Exposure Notification Bluetooth Specification Preliminary — Subject to Modification and Extension, April 2020 v1.2, Apple & Google
- Exposure Notification Android API Documentation Preliminary - Subject to Modification and Extension, April 2020 v1.2, Apple & Google