Bluetooth®

Bluetooth® Technology and the Response to the Covid-19 Pandemic

Martin Woolley

Bluetooth SIG

Twitter: @bluetooth_mdw

“How can we help?”

Proximity and Social Distancing

Exposure Notification (ENS)

Contact Tracing

Exposure Notification Systems (ENS)

Detect the presence of other people

Estimate distance between people and duration of encounters

Identify **significant** encounters with **affected people**

Notify **exposed people**

Smartphones and Bluetooth® Technology

Smartphones

because they’re in widespread use

Bluetooth® Technology

because no infrastructure is required

The Bluetooth SIG

No official involvement in any of the initial initiatives to respond to the pandemic

Bluetooth® Technology and ENS

Bluetooth technology has no specially designed capabilities or standard profiles for use in exposure notification systems at this stage

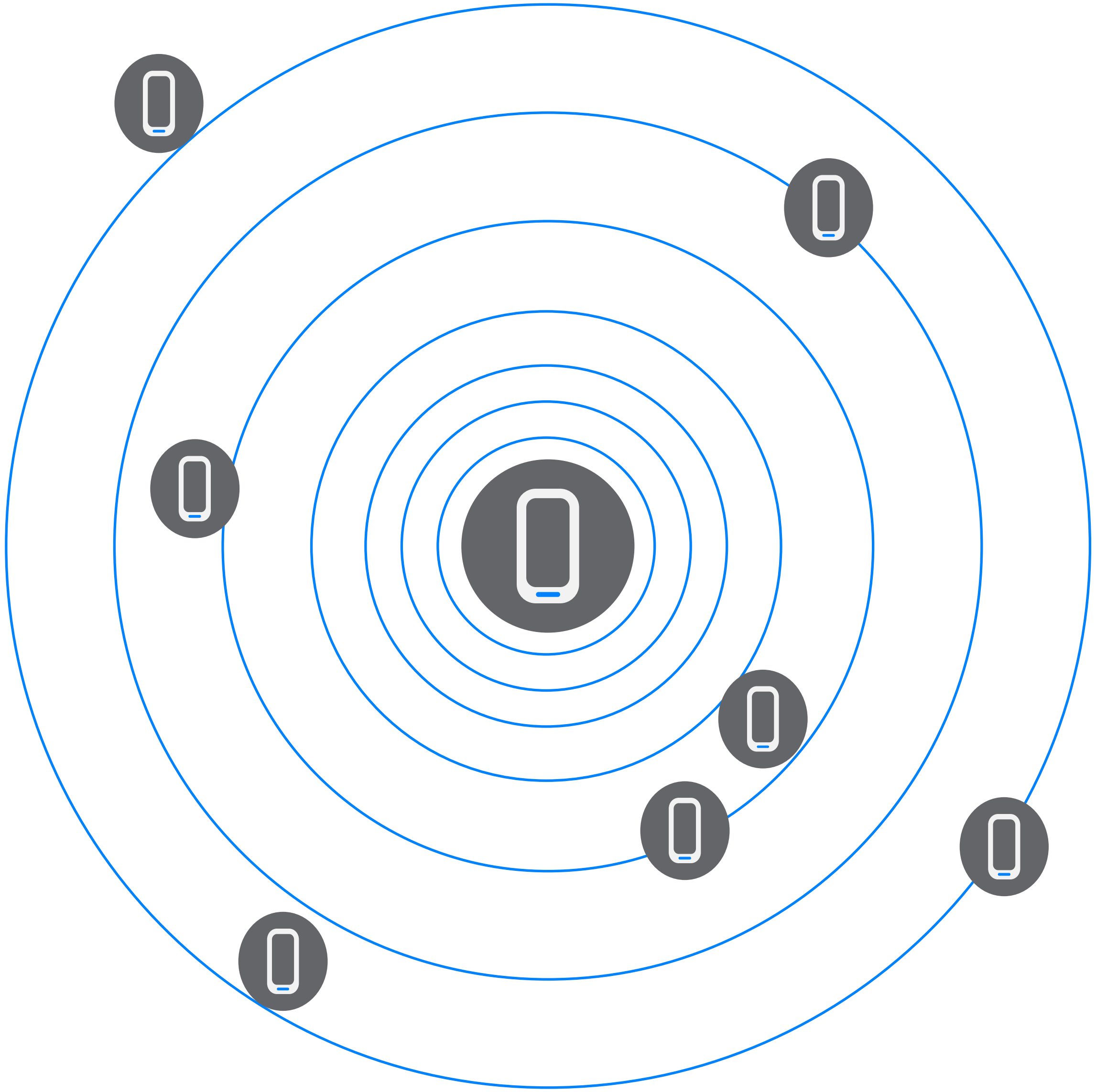
Work with What You’ve Got

The raw ingredients

Connection-Oriented Communication

- Point to point communication directly between two devices
- Reliable thanks to agreed timing parameters and acknowledgements in the protocol
- Encryption available if devices are paired
- Privacy mechanism available through random, rolling device addresses
- Limited scalability
- Smartphones can usually only accept 3 or 4 concurrent connections
  - *but note that this is an implementation limit, not a limit of Bluetooth technology itself*

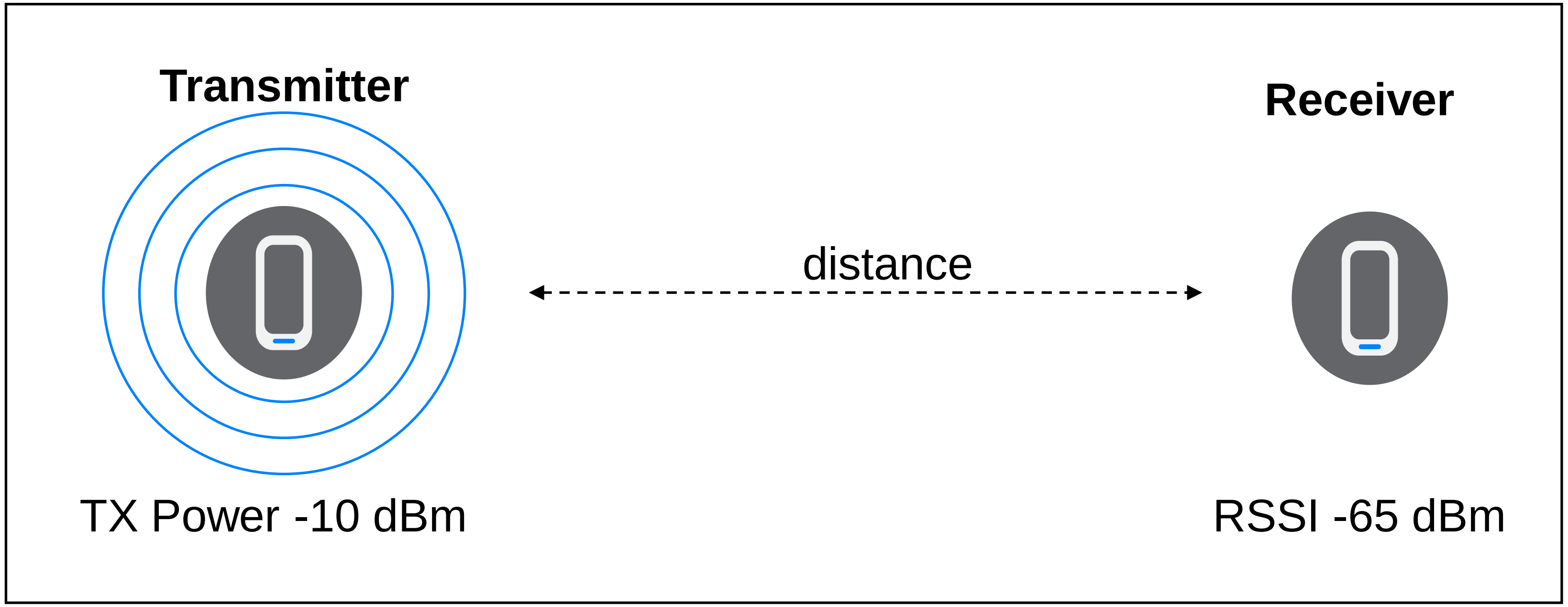
Connectionless Communication



- Broadcast communication from one device to many
- Very scalable - unlimited number of receivers
- Same privacy mechanism available

- No agreed timing between broadcasting device and receivers
- No acknowledgement of packets received
- Use of encryption is not defined for broadcast

Signal Strength

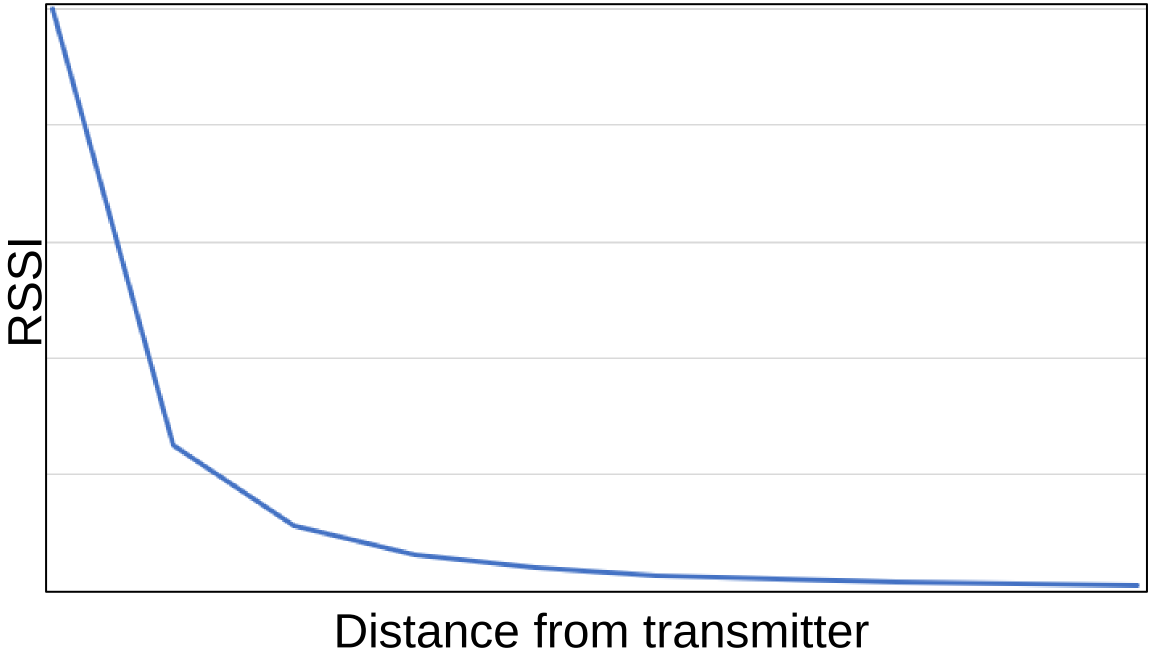


TX power is the transmit power

RSSI is the Received Signal Strength Indicator and is the signal strength as measured by the receiving device

RSSI reduces as the receiver is moved further from the transmitter

RSSI and Distance from the Transmitter



- Energy in radio waves decreases according to the **inverse square law**

- The RSSI is inversely proportional to the square of the distance from a transmitter

- *Path loss* or *attenuation* is the amount by which the signal strength is reduced when measured at a distance from the transmitter.

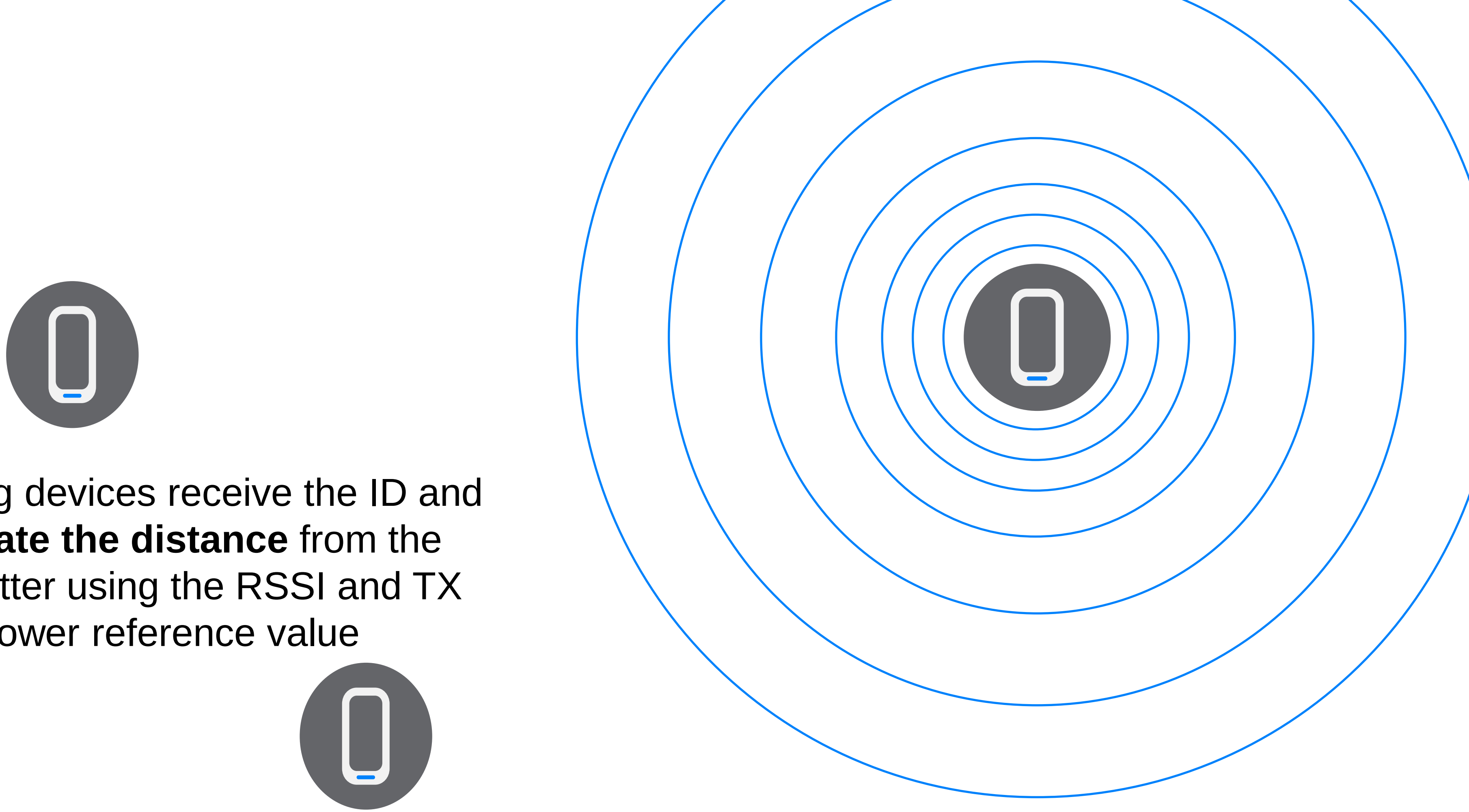
  - `TX Power – RSSI`

- **Attenuation can be used as a *noisy* proxy for distance**

Exposure Notification

The basic Idea

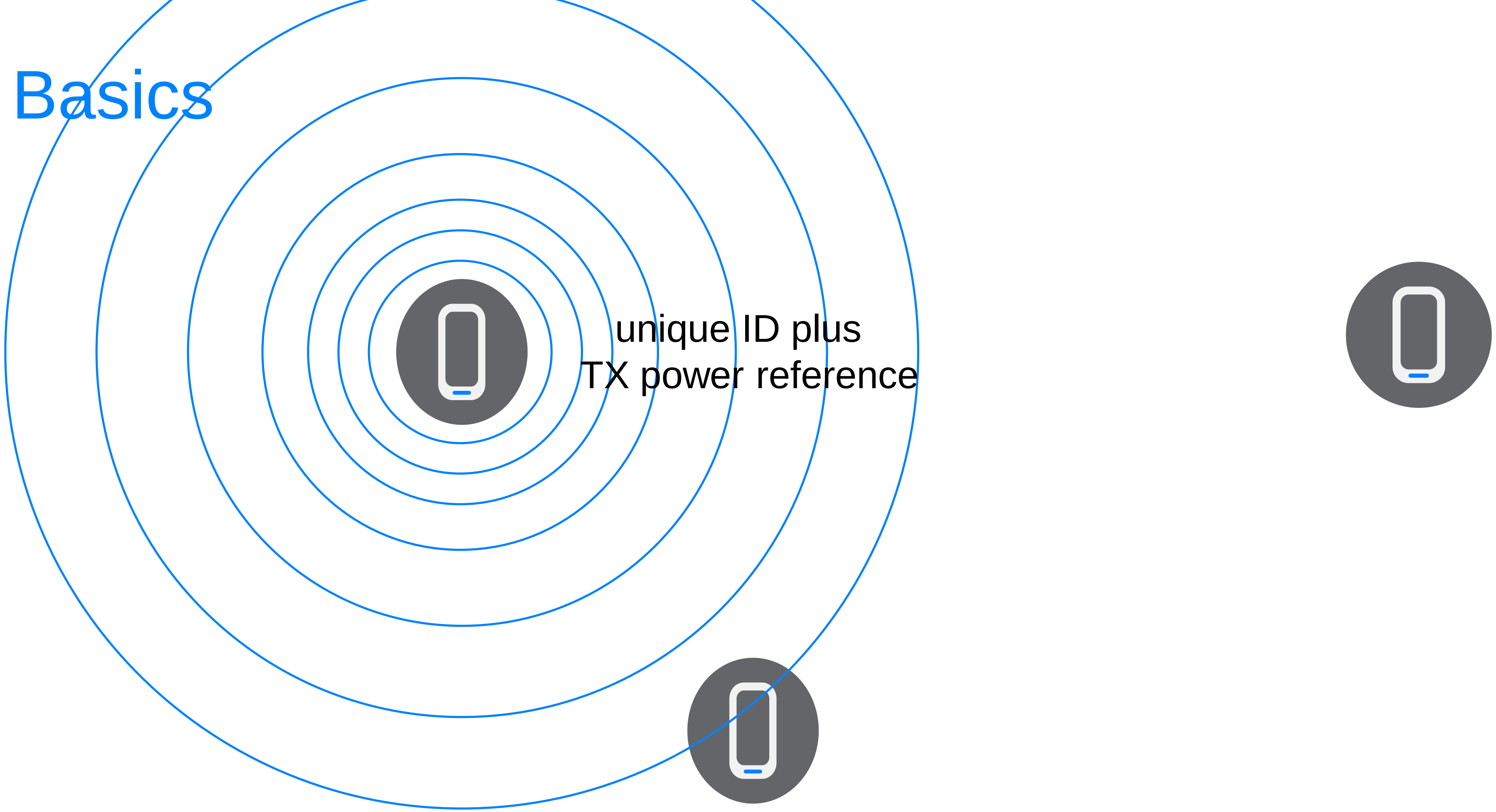
ENS Basics



Scanning devices receive the ID and **estimate the distance** from the transmitter using the RSSI and TX power reference value

Device broadcasts a unique ID plus a TX power reference value (*beaconing*)

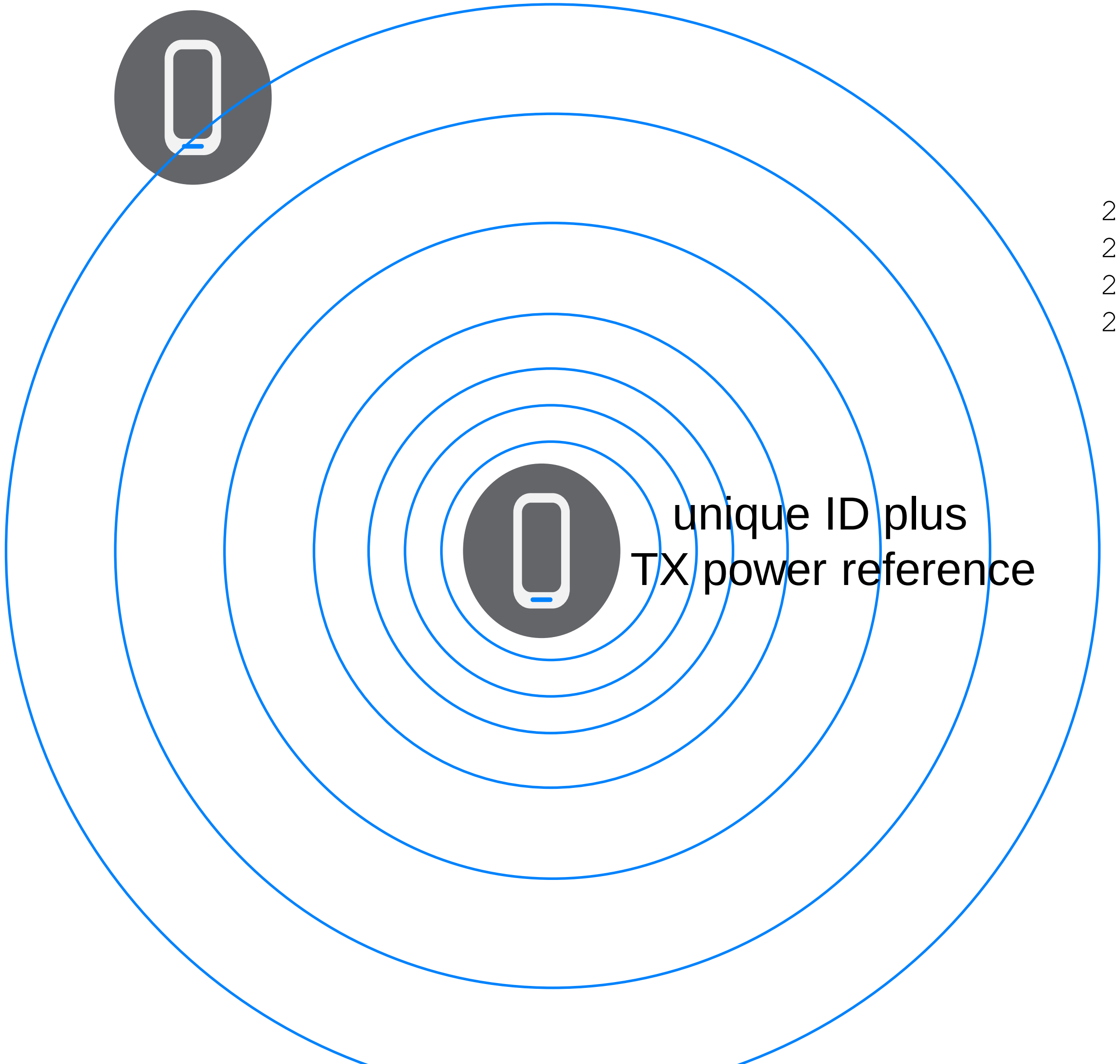
ENS Basics



unique ID plus
TX power reference

Devices interleave beaconing with scanning for beacons from other devices

ENS Basics

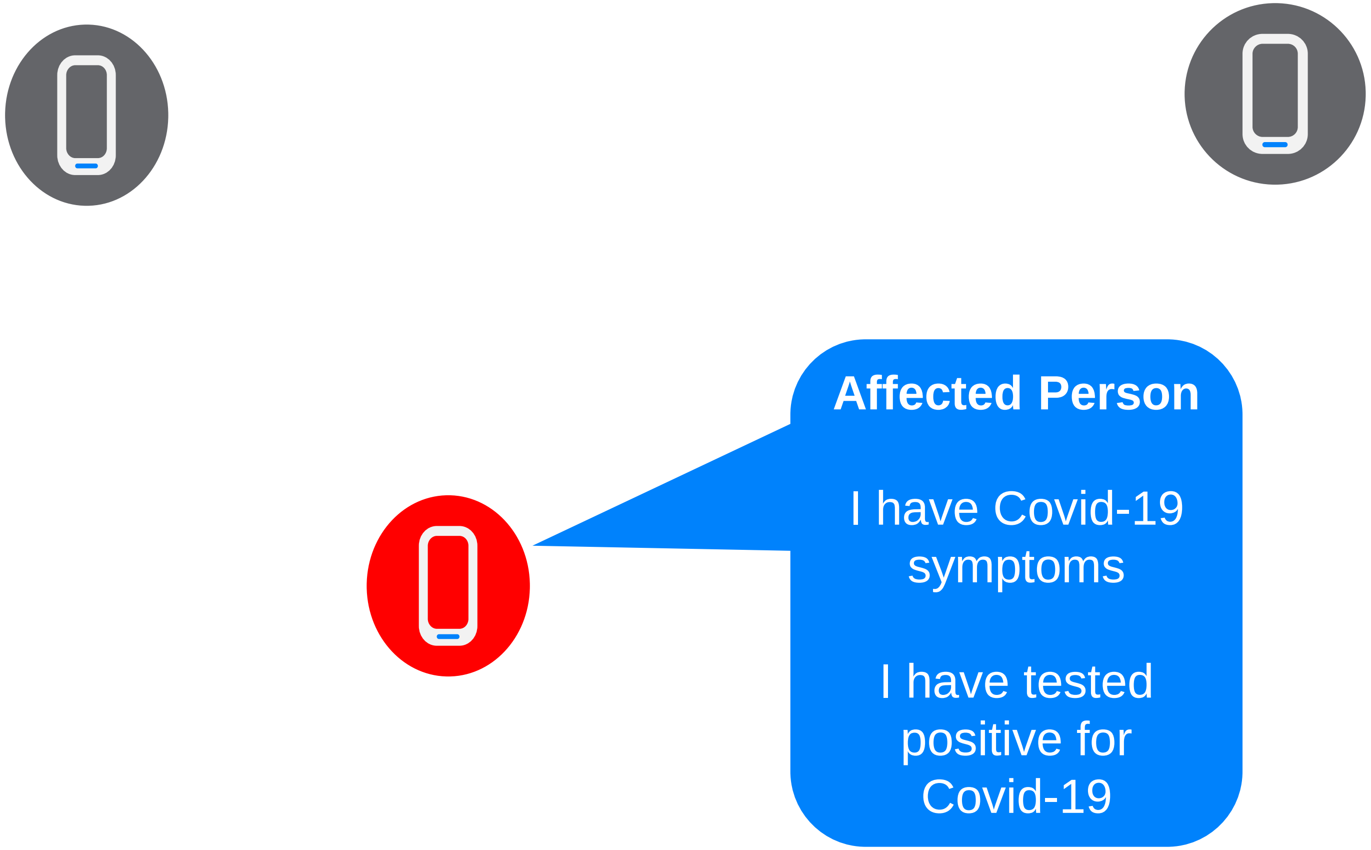


unique ID plus
TX power reference

And maintain a history of the
devices they have been near
over a period of time

```
25/03/2021 10:11 ID:12345678 RSSI -55
25/03/2021 15:33 ID:13456899 RSSI -87
25/03/2021 15:40 ID:98345678 RSSI -46
25/03/2021 15:45 ID:64867678 RSSI -60
```

ENS Basics

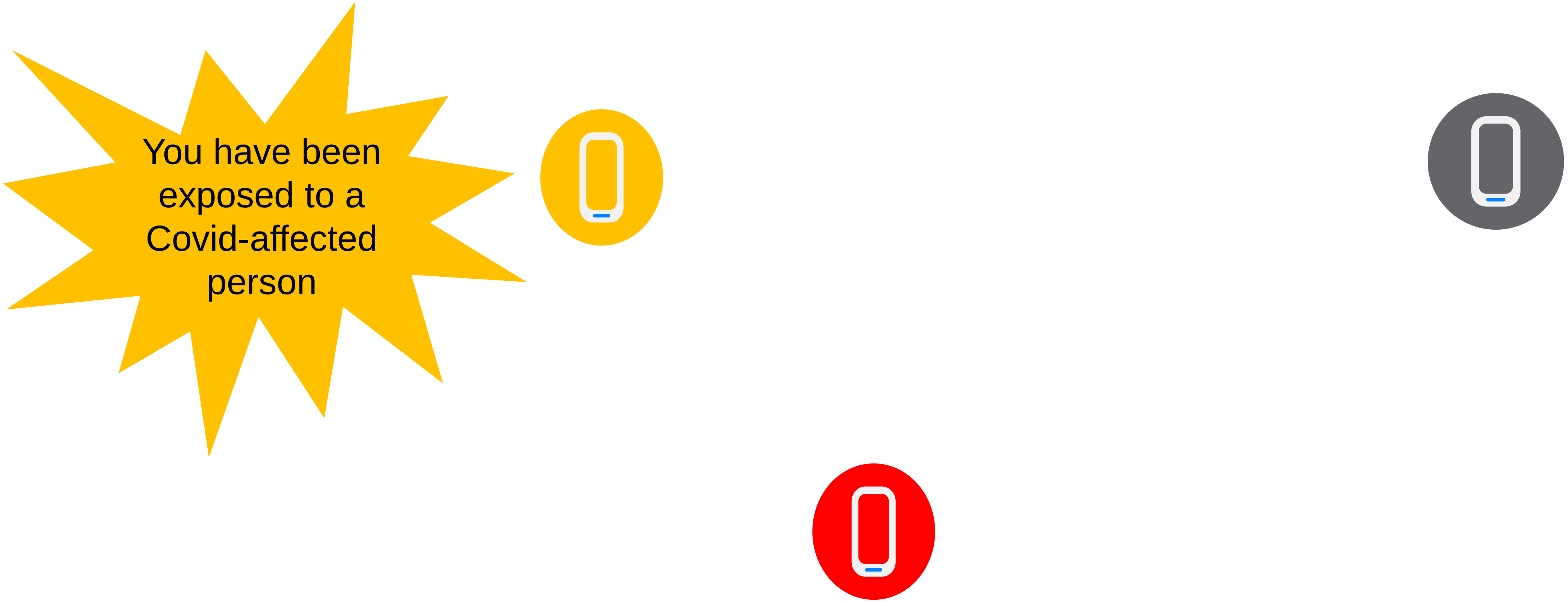


Affected Person

I have Covid-19 symptoms

I have tested positive for Covid-19

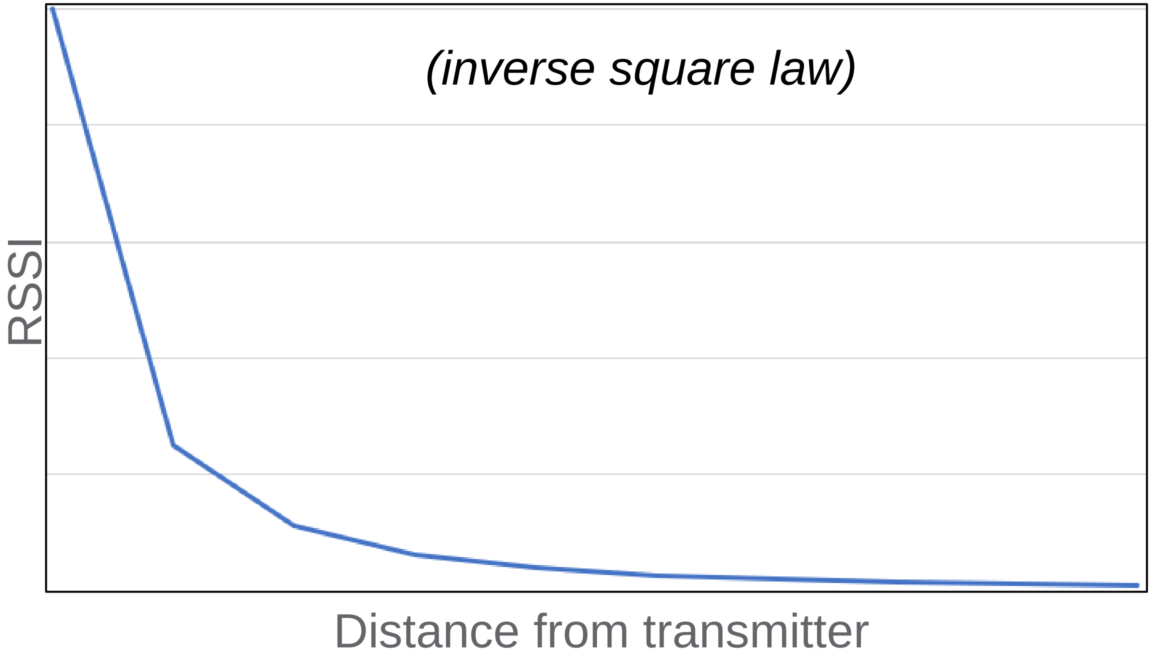
ENS Basics



You have been exposed to a Covid-affected person

The Issues

RSSI Distance Estimation and Accuracy



- Does it work?

- **Must** use a **TX reference power** value from the transmitter.

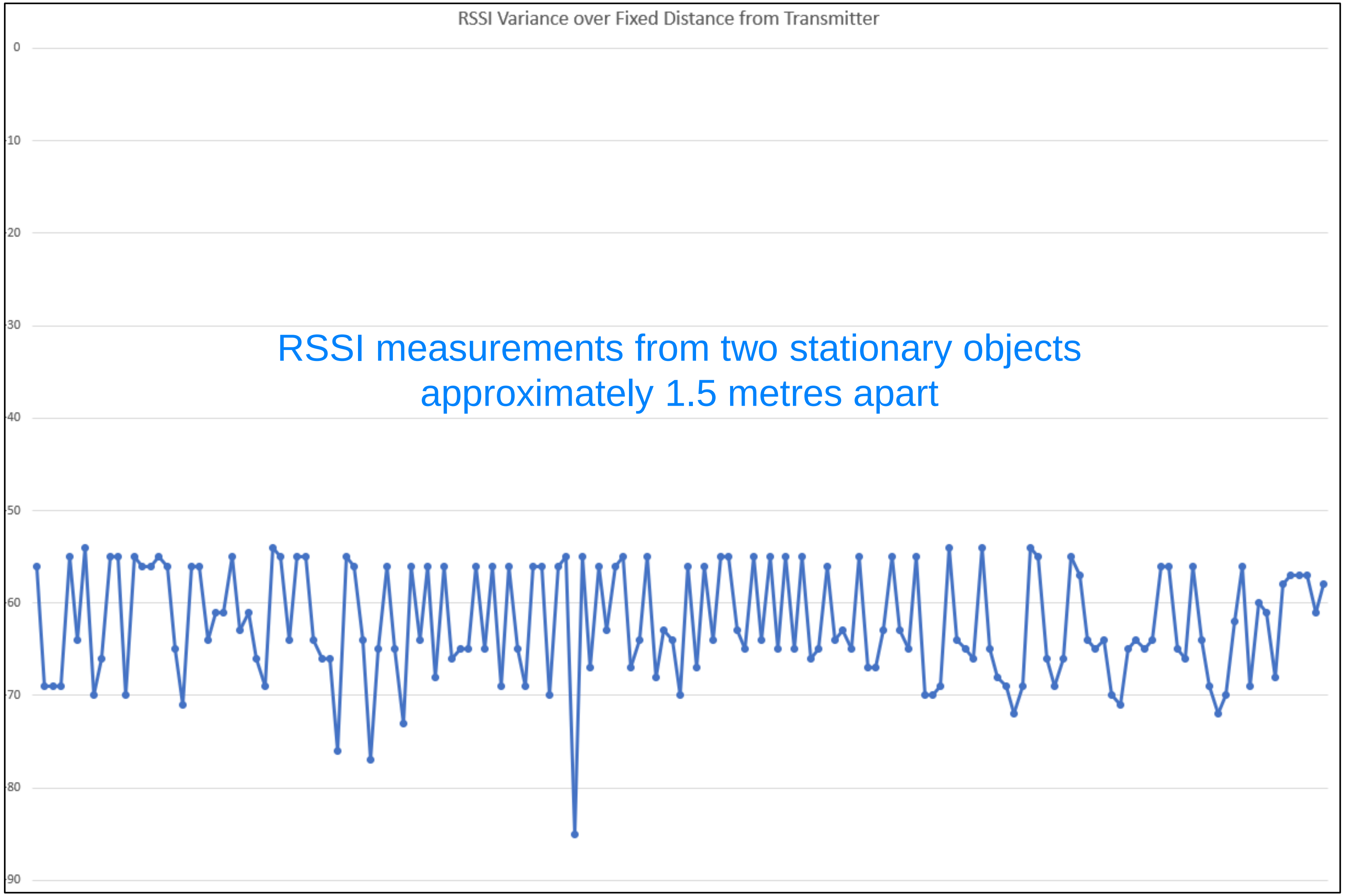
- Estimates made when closer to the transmitter can work well enough to be useful. Further away it becomes much less accurate.

- **Am I within 2 metres?** This question can be answered with sufficient reliability and accuracy.

- There are significant limitations - It’s not possible to get it right to within say the nearest 10cm.

- Precise accuracy is not the issue. **Usefulness** is.

RSSI Quality Issues



RSSI measurements from two stationary objects approximately 1.5 metres apart

- RSSI is very noisy.
- Different devices report different values.
- Antenna designs vary and signal strength varies depending on direction/orientation.
- RSSI sensors are not sophisticated. 8-bit A to D is common.
- ADV channel rotation - RSSI is tuned for one frequency
- Physical objects
- Reflections
- Humidity

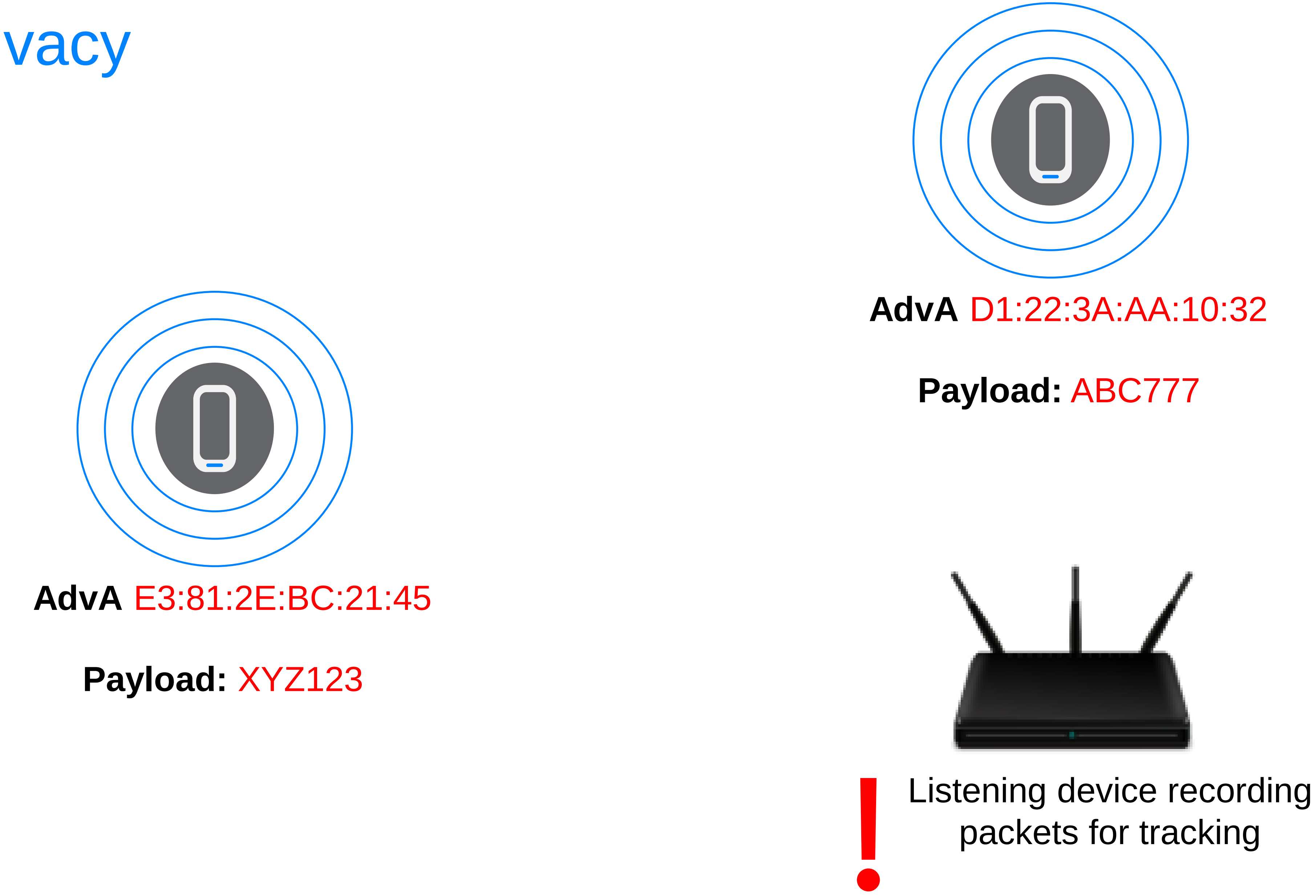
Smartphone Models and Receiver Variations

- Differences in radio circuitry, antenna design etc result in different phones reporting different RSSI values for the same signal and location

- There are **tens of thousands of Android smartphone models** alone

- Consistency requires calibration data for each make and model

Privacy



AdvA E3:81:2E:BC:21:45

Payload: XYZ123

AdvA D1:22:3A:AA:10:32

Payload: ABC777

! Listening device recording packets for tracking

Advertising and Scanning Parameters

Key parameters that need to be considered

- Advertising Interval - How often to advertise?
- Scan Interval - How often to scan?
- Scan Window - How long to scan for?

Impact

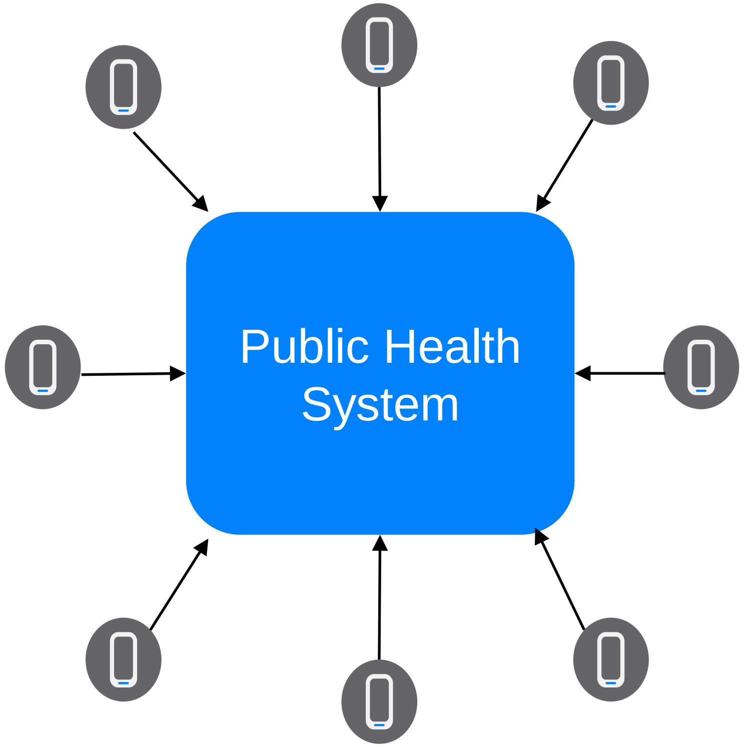
- Battery life
- Reliability
- Responsiveness

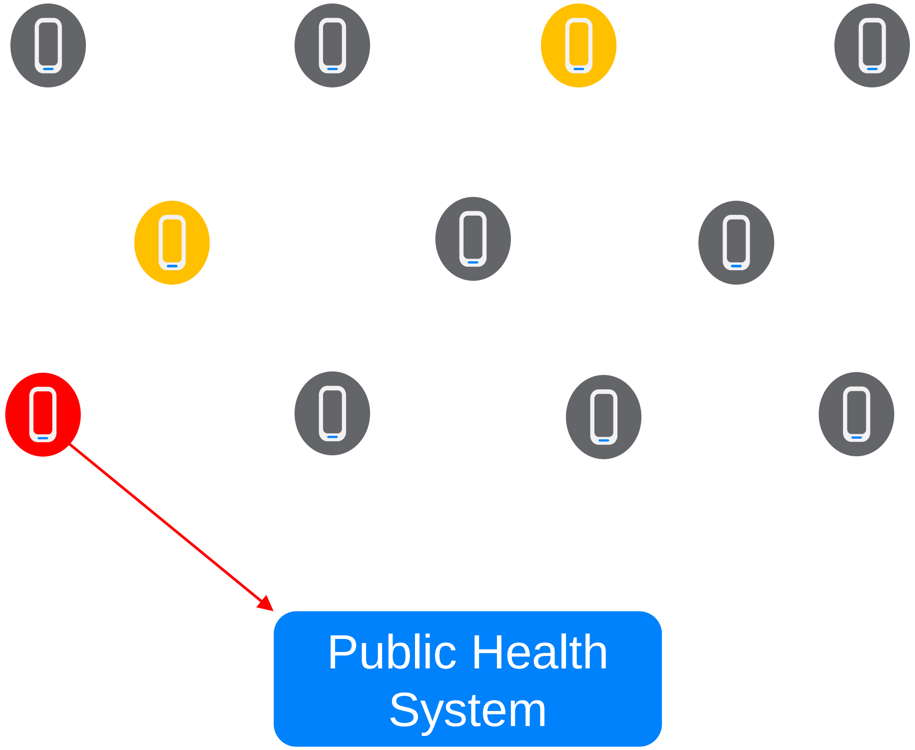
The Standard Android and iOS Bluetooth® APIs

- **APIs both enable and constrain** - for example:
- Can **non-connectable advertising** be performed?
    - iOS - NO
    - Android - YES
- What happens when the app is moved into the **background** or the phone is locked?
    - iOS - limitations regarding scanning and what data can be advertised in this state
    - Android - tricky but advertising and scanning can be done (ForegroundService) - varies by Android version

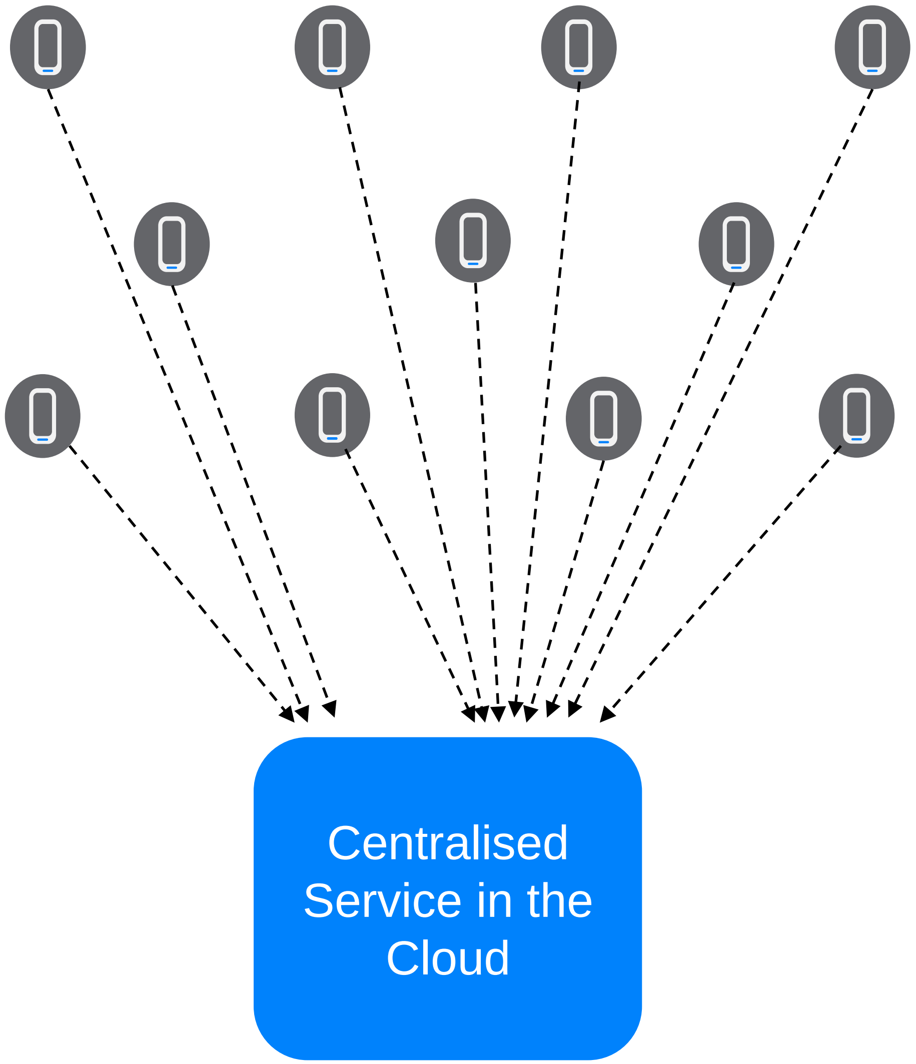
Architecture Choices

CENTRALISED	DECENTRALISED





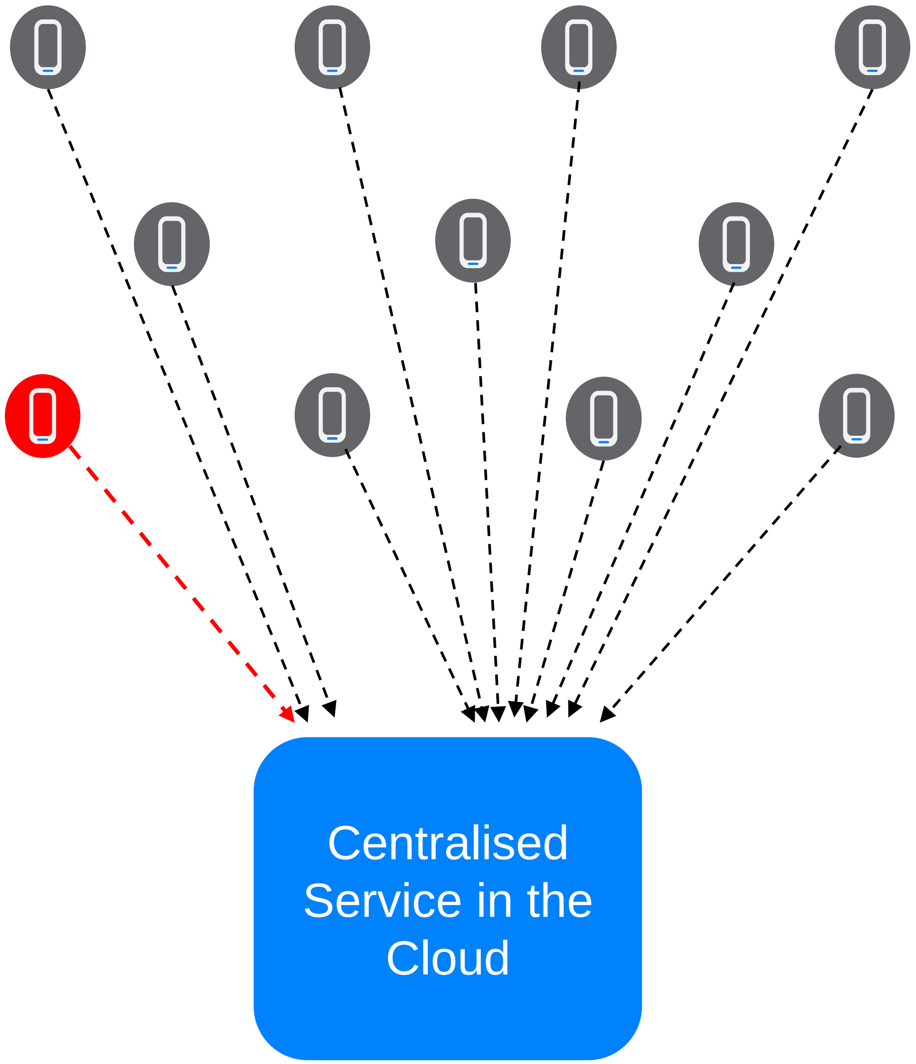
Centralised Architecture



Requires devices to share a list of observed devices with a centralized system.

The central system has a record of every sighting made by every device.

Centralised Architecture



- - - - - - - - ▸

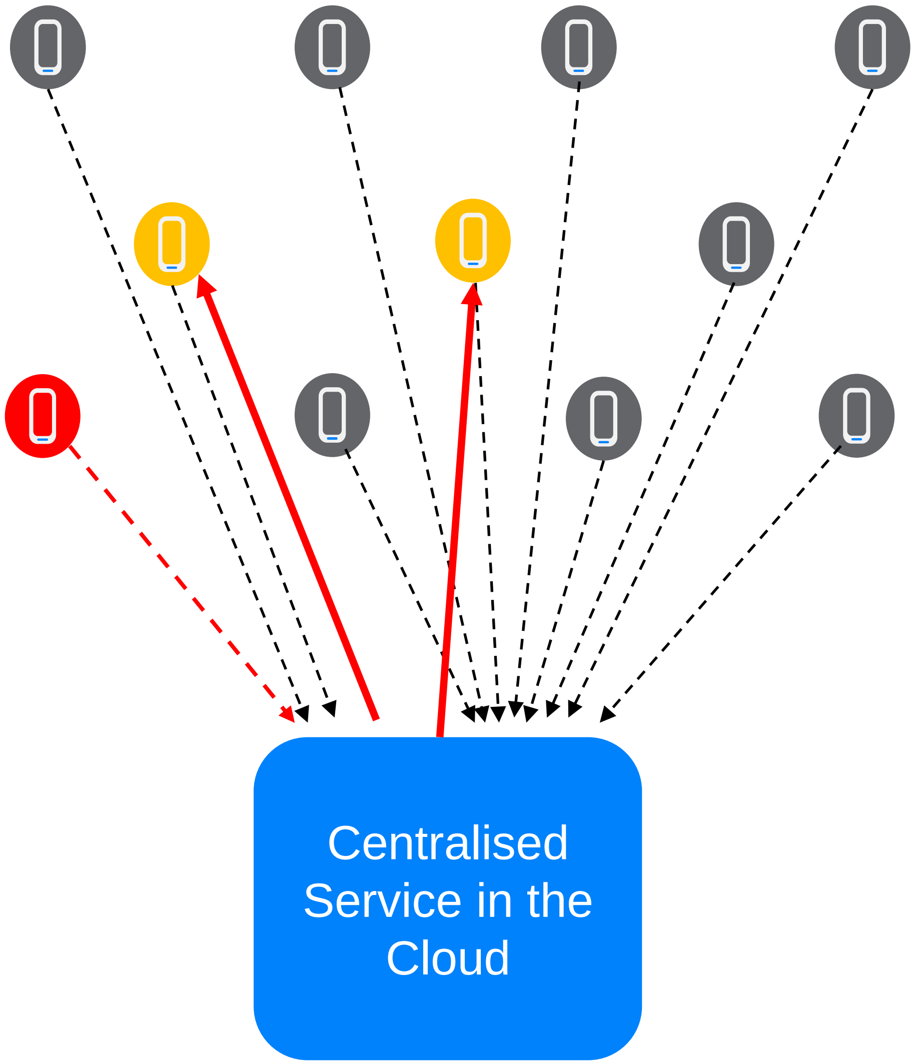
Requires devices to share a list of observed identifiers with a centralized system.

The central system has a record of every sighting made by every device.

− − − − − − ▸

Requires users to declare themselves affected to the central server

Centralised Architecture



←

A centralized server makes all decisions about whether to notify someone if they have been exposed

⇢

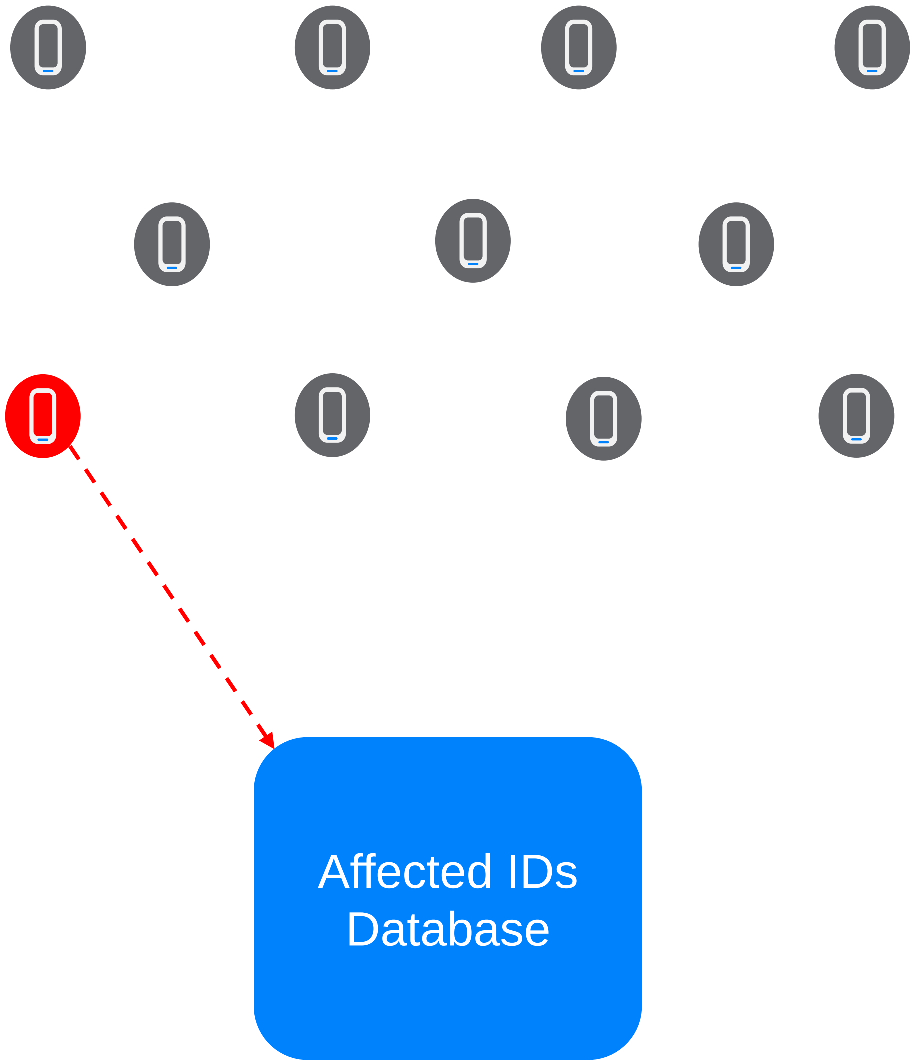
Requires devices to share a list of observed identifiers with a centralized system.

The central system has a record of every sighting made by every device.

⇢

Requires users to declare themselves affected to the central server

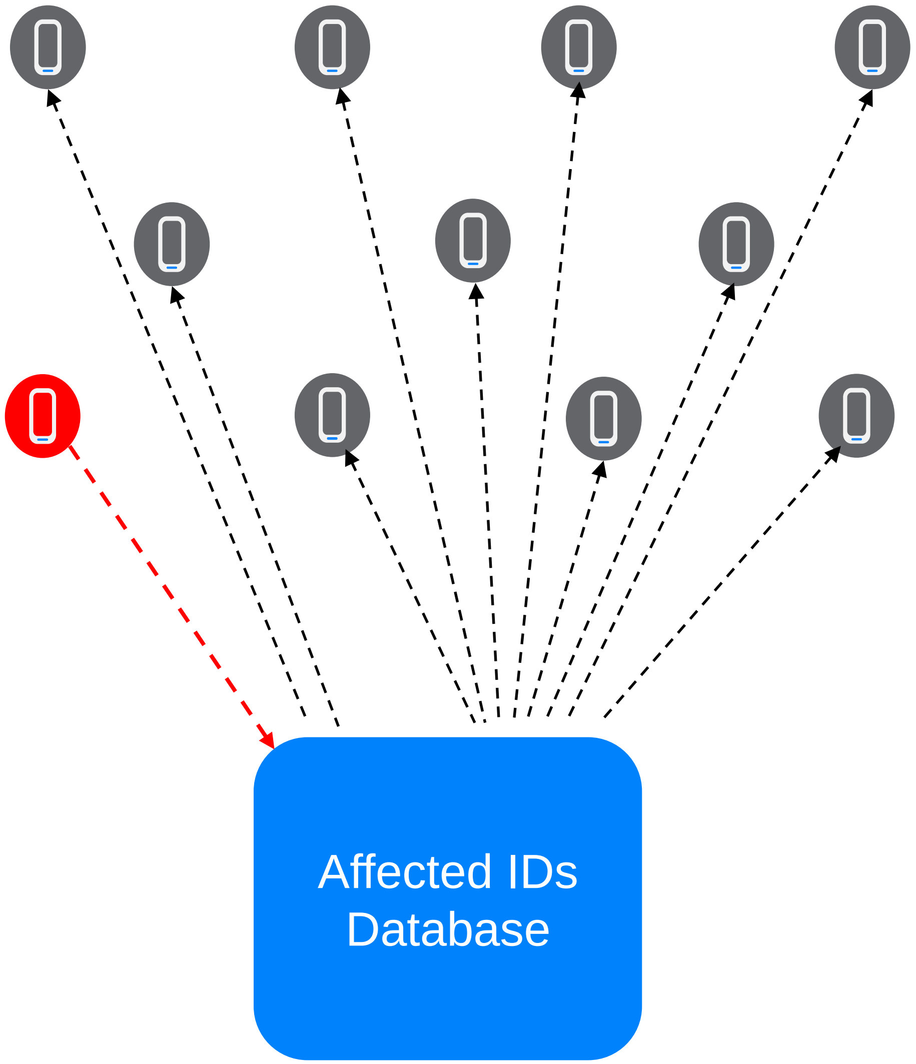
Decentralised Architecture



Requires users to declare themselves affected to the central server

Server does not know which other devices have been encountered by the affected user's device or any other devices

Decentralised Architecture

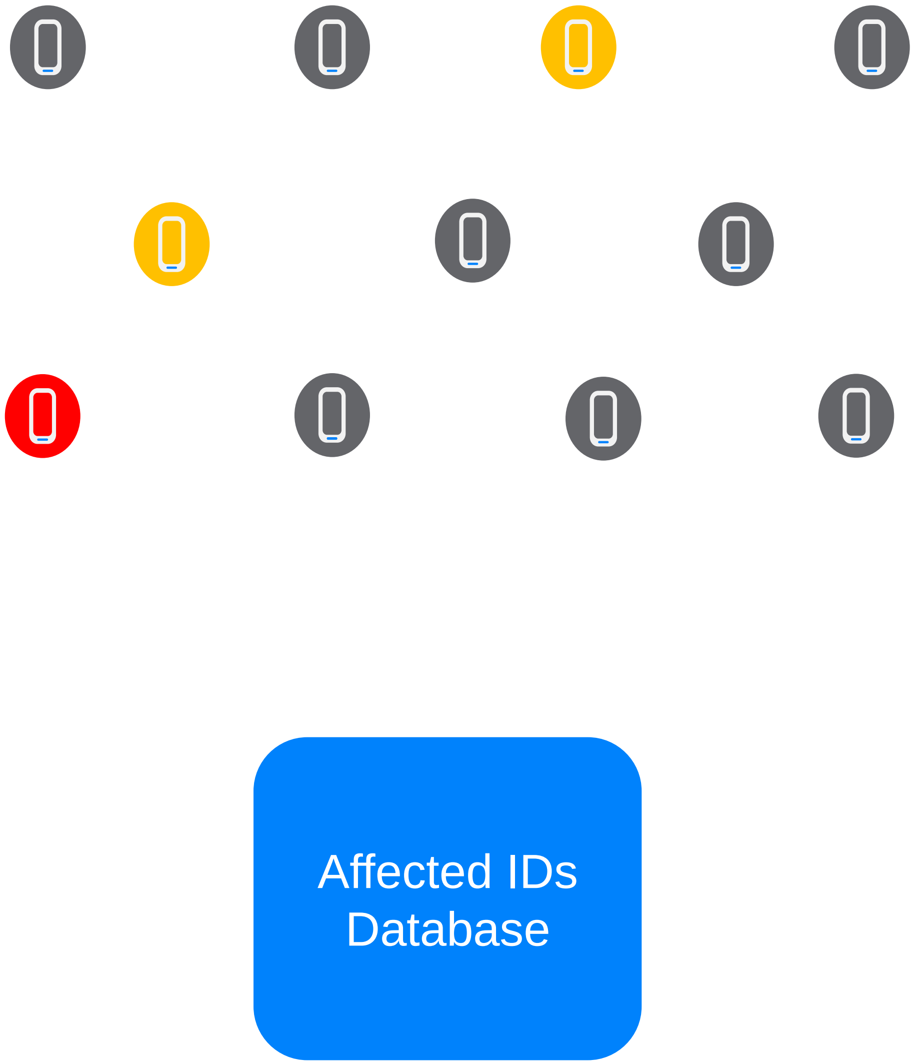


Devices periodically receive a list of all affected users' identifiers

Requires users to declare themselves affected to the central server

Server does not know which other devices have been encountered by the affected user’s device or any other devices

Decentralised Architecture



● ●

Devices decide locally whether to notify the user if they have been exposed by comparing their own list of sightings with the list of affected users from the central database

- - - - - - - - - - - - ▶

Devices periodically receive a list of all affected users' identifiers

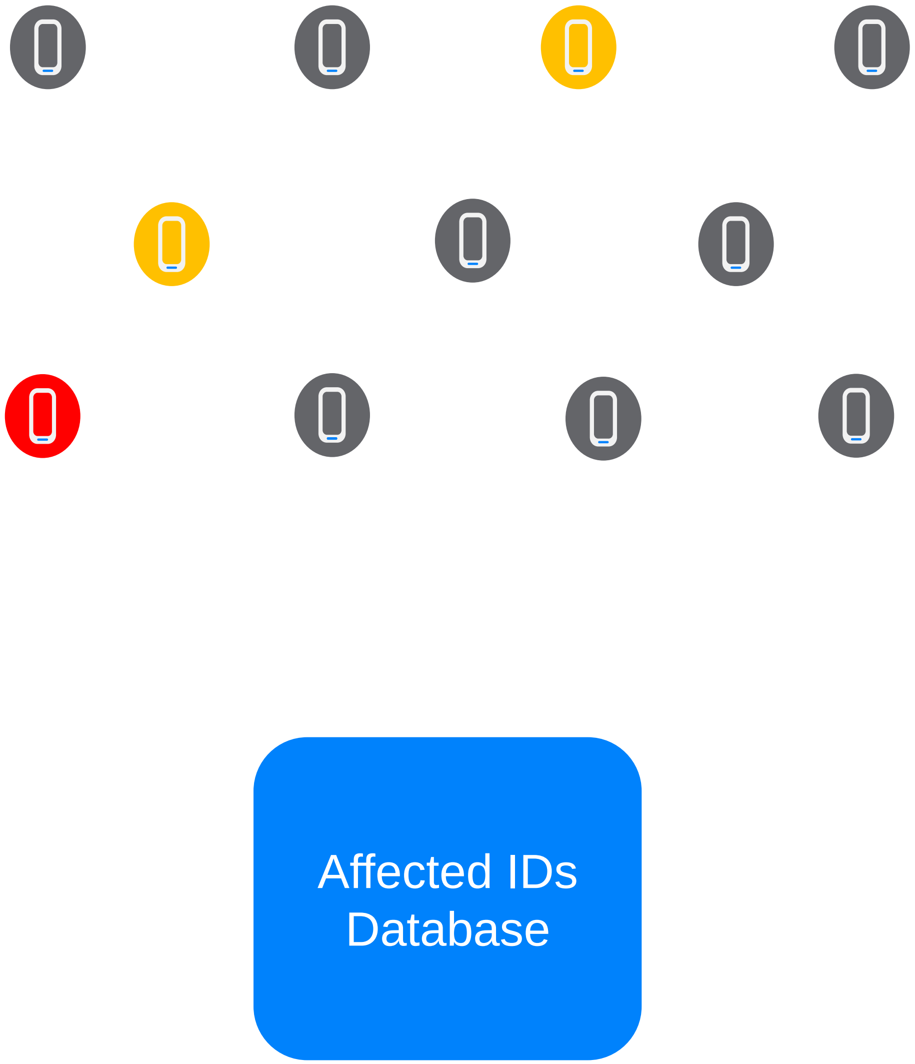
- - - - - - - ▶

Requires users to declare themselves affected to the central server

Server does not know which other devices have been encountered by the affected user’s device or any other devices

The Apple and Google ENS Framework

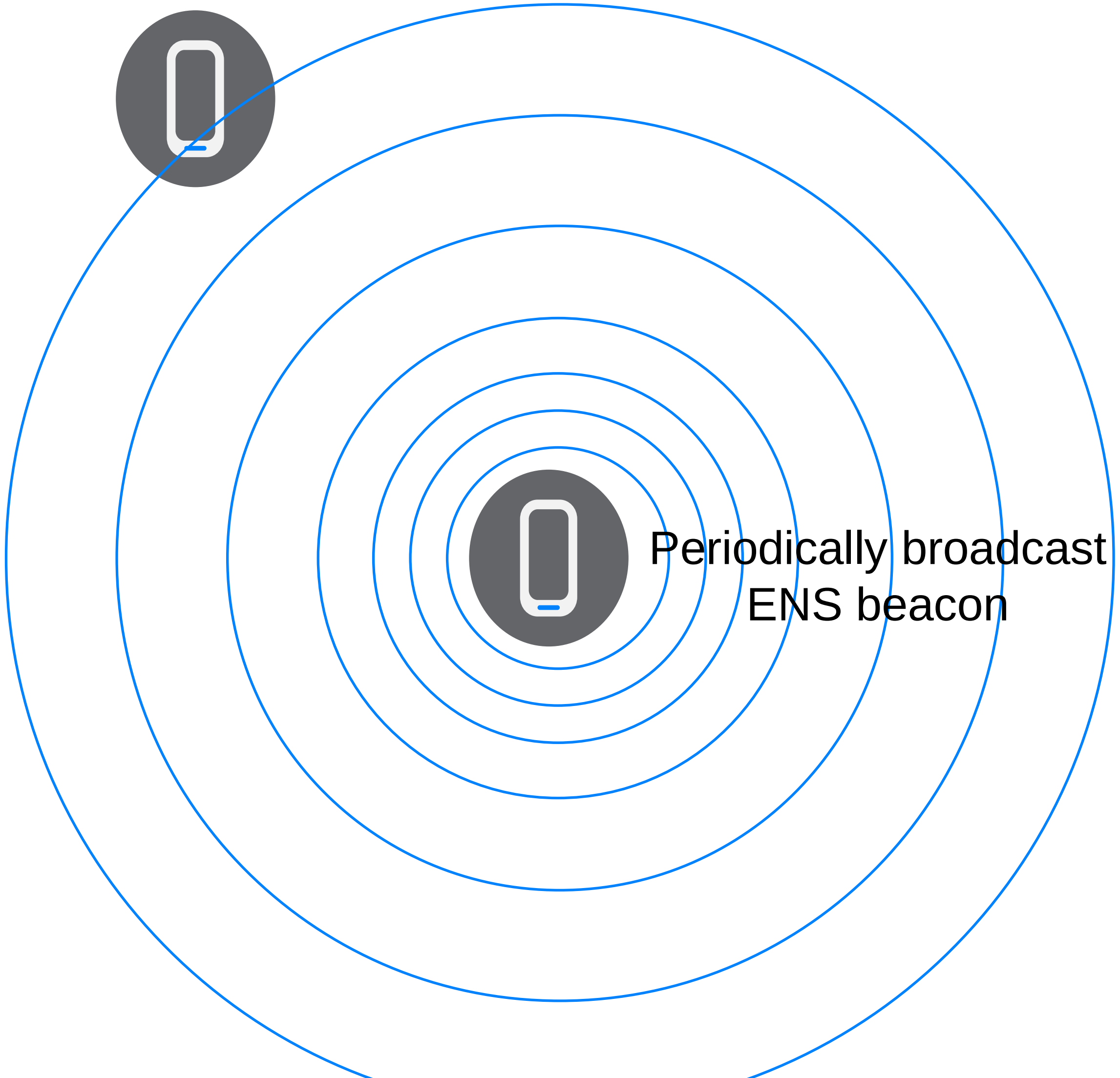
Apple Google ENS uses a Decentralised Architecture



Key points:

- No centralized database of encounters between users / devices - privacy benefit
- Requires users to voluntarily declare themselves affected to the central server
- Devices periodically receive a list of keys used by affected users from the central server
- Apple and Google **do not monetize** this data
    - Source: FAQ at https://www.google.com/covid19/exposurenotifications/

Connectionless Communication



Periodically broadcast ENS beacon

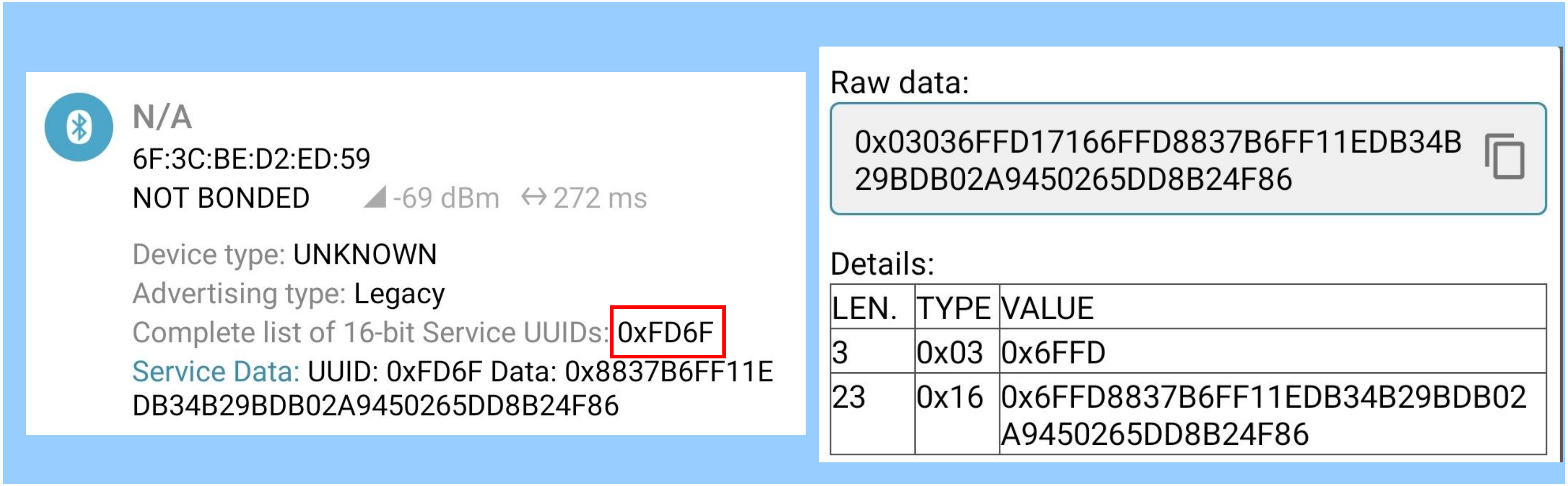
Devices record sightings of other devices from the last 14 days

```
25/03/2021 10:11 ID:12345678 RSSI -55
25/03/2021 15:33 ID:13456899 RSSI -87
25/03/2021 15:40 ID:98345678 RSSI -46
25/03/2021 15:45 ID:64867678 RSSI -60
```

ENS Beacons

- Uses Bluetooth **ADV_NONCONN_IND** packets

- ENS service identified by a registered 16-bit UUID value **0xFD6F**



N/A
6F:3C:BE:D2:ED:59
NOT BONDED -69 dBm ↔272 ms

Device type: UNKNOWN
Advertising type: Legacy
Complete list of 16-bit Service UUIDs: 0xFD6F
Service Data: UUID: 0xFD6F Data: 0x8837B6FF11EDB34B29BDB02A9450265DD8B24F86

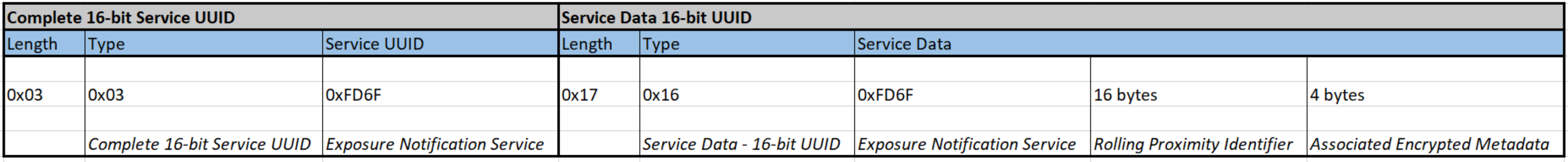
Raw data:

```
0x03036FFD17166FFD8837B6FF11EDB34B
29BDB02A9450265DD8B24F86
```

Details:

LEN.	TYPE	VALUE
3	0x03	0x6FFD
23	0x16	0x6FFD8837B6FF11EDB34B29BDB02A9450265DD8B24F86

ENS Beacons



Complete 16-bit Service UUID			Service Data 16-bit UUID				
Length	Type	Service UUID	Length	Type	Service Data		
0x03	0x03	0xFD6F	0x17	0x16	0xFD6F	16 bytes	4 bytes
	Complete 16-bit Service UUID	*Exposure Notification Service*		*Service Data - 16-bit UUID*	*Exposure Notification Service*	*Rolling Proximity Identifier*	*Associated Encrypted Metadata*

Rolling Proximity Identifier

Unique ID that changes every 15 minutes

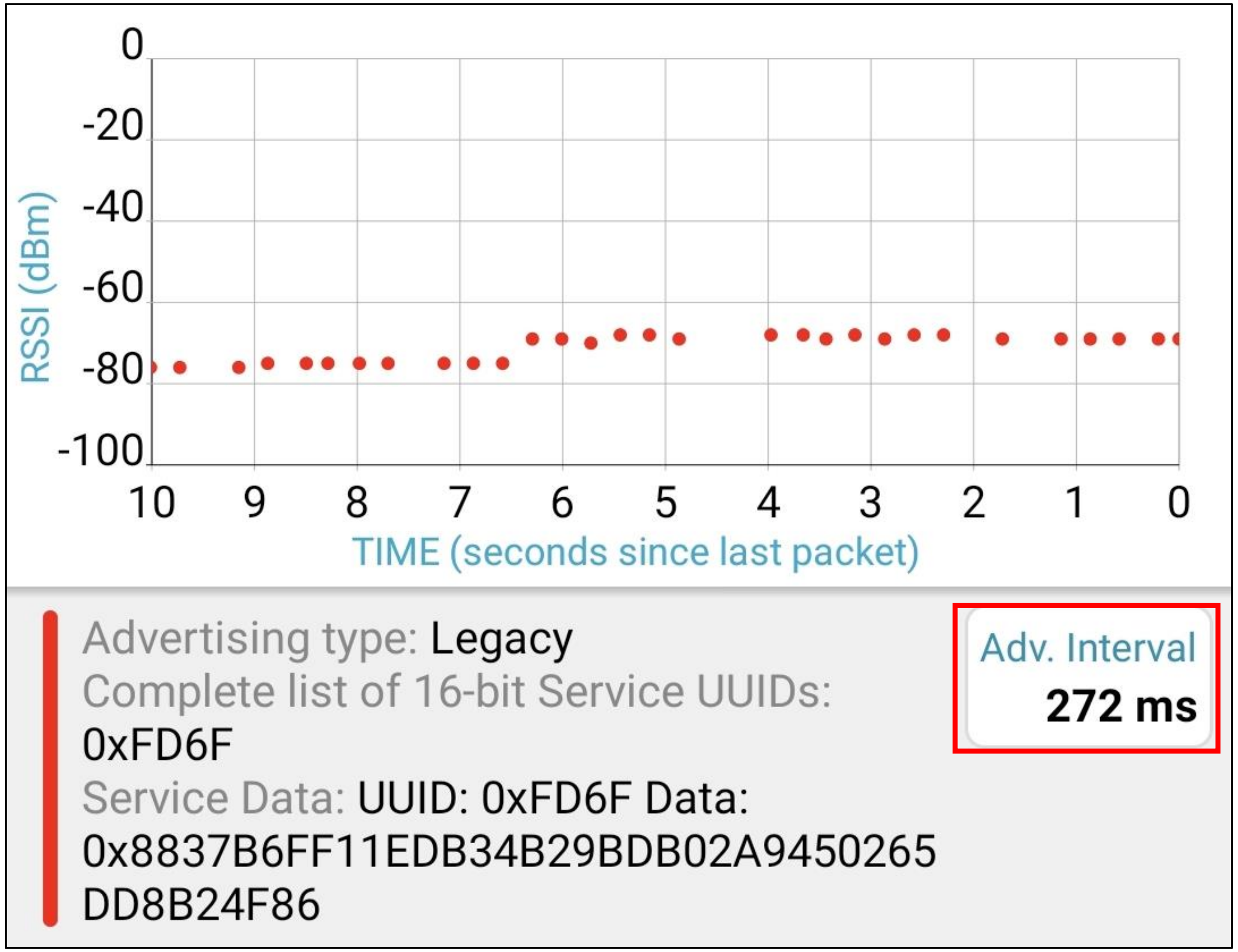
UUID 0xFD6F

identifies this as an ENS beacon

Associated Encrypted Metadata

Protocol versioning and transmit (Tx) reference power

ENS Beacons



Advertising type: Legacy
Complete list of 16-bit Service UUIDs:
0xFD6F
Service Data: UUID: 0xFD6F Data:
0x8837B6FF11EDB34B29BDB02A9450265
DD8B24F86

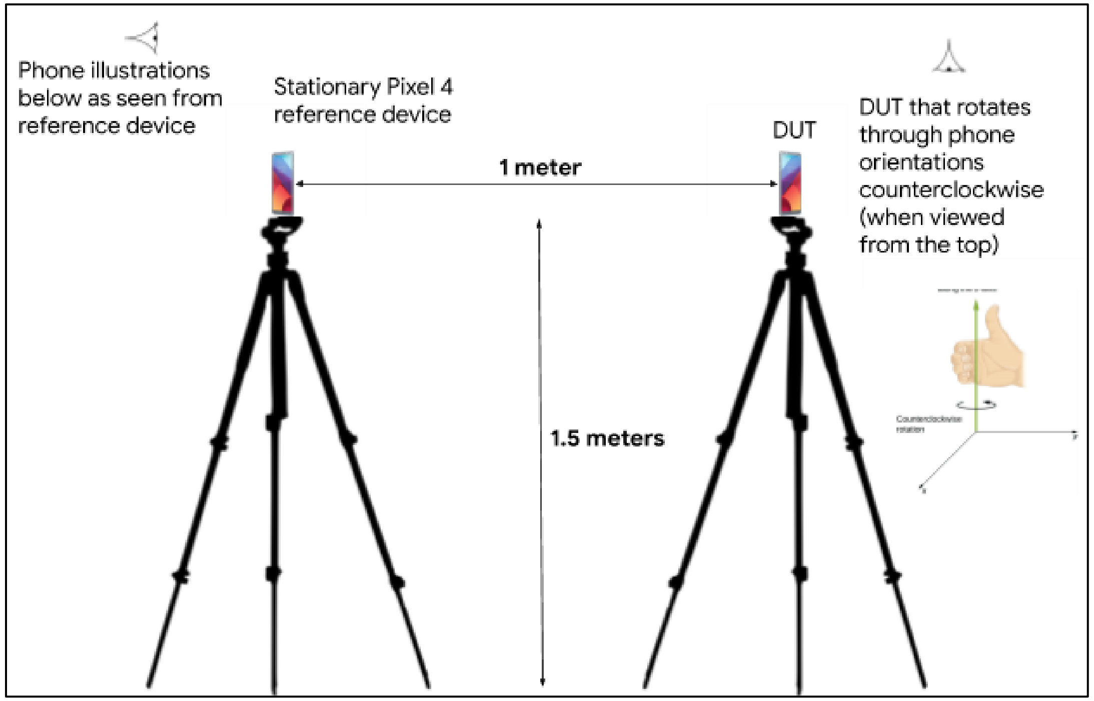
Adv. Interval
272 ms

- Beacons are emitted around 3 times a second
- Scan interval is opportunistic and designed to discover ENS beacons within 5 minutes
- Scan duration is for 4 seconds

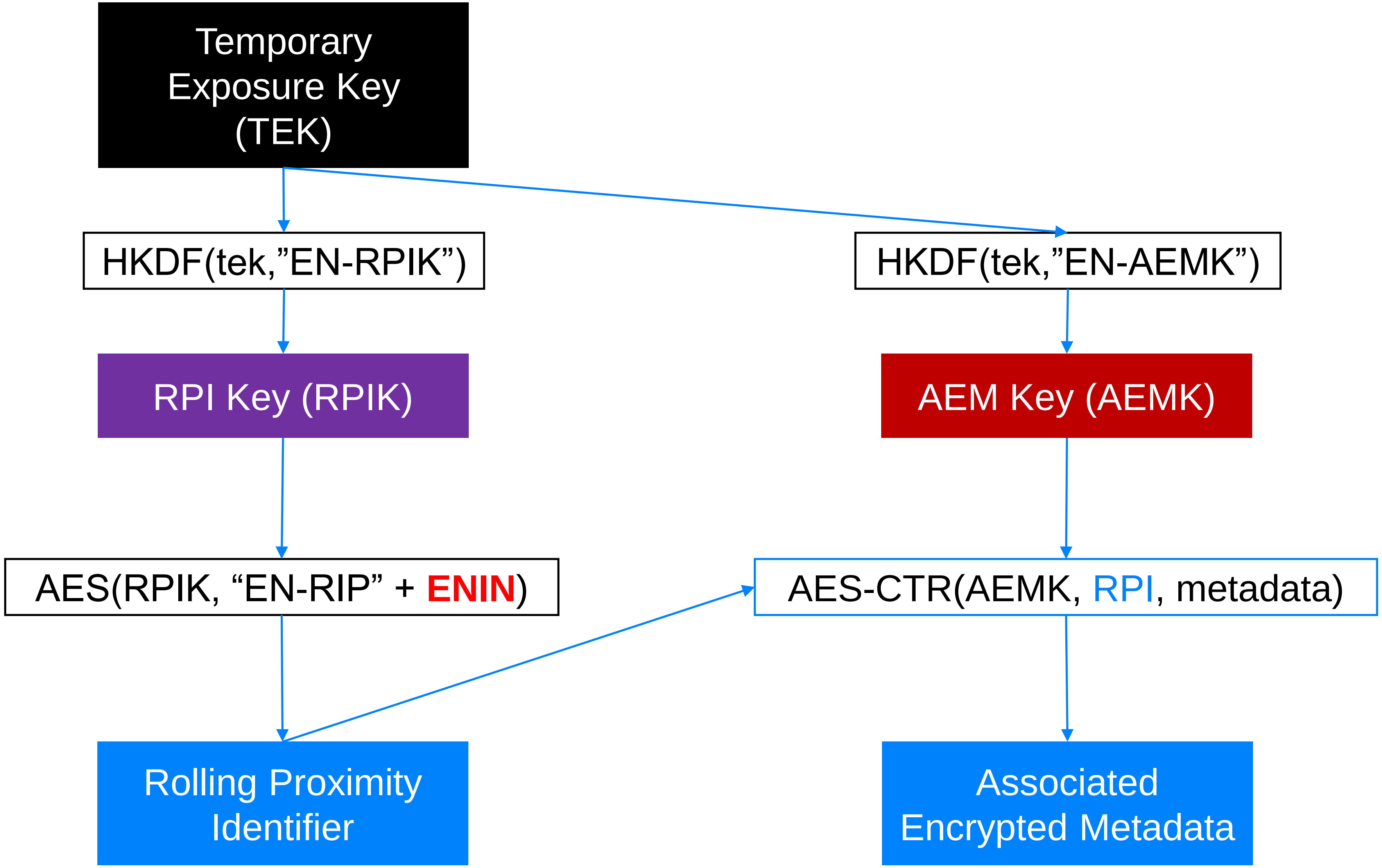
Improving Distance Estimation

- A calibration procedure is defined by Google
- Calibration test results are reported to Google by Android smartphone manufacturers
- The device calibration list is distributed to devices running the ENS framework (CSV file)
- Calibration data allows corrections to be applied to the measured signal strength before its use in distance estimate calculations.

- A confidence indicator included.
- Averaging and minimum reported distance provides data smoothing and allows better interpretation of risk.


Phone illustrations below as seen from reference device
Stationary Pixel 4 reference device
DUT
1 meter
DUT that rotates through phone orientations counterclockwise (when viewed from the top)
1.5 meters
Counterclockwise rotation

Cryptography Specification


Temporary Exposure Key (TEK)
HKDF(tek,"EN-RPIK")
HKDF(tek,"EN-AEMK")
RPI Key (RPIK)
AEM Key (AEMK)
AES(RPIK, "EN-RIP" + ENIN)
AES-CTR(AEMK, RPI, metadata)
Rolling Proximity Identifier
Associated Encrypted Metadata

TEK

128-bit random number

ENIntervalNumber

AKA **ENIN**
A specific **10-minute period in time** counted from the Unix Epoch of 00:00:00 UTC on 1 January 1970

e.g. 2021-03-29 09:46:33 has ENIntervalNumber : 2695012

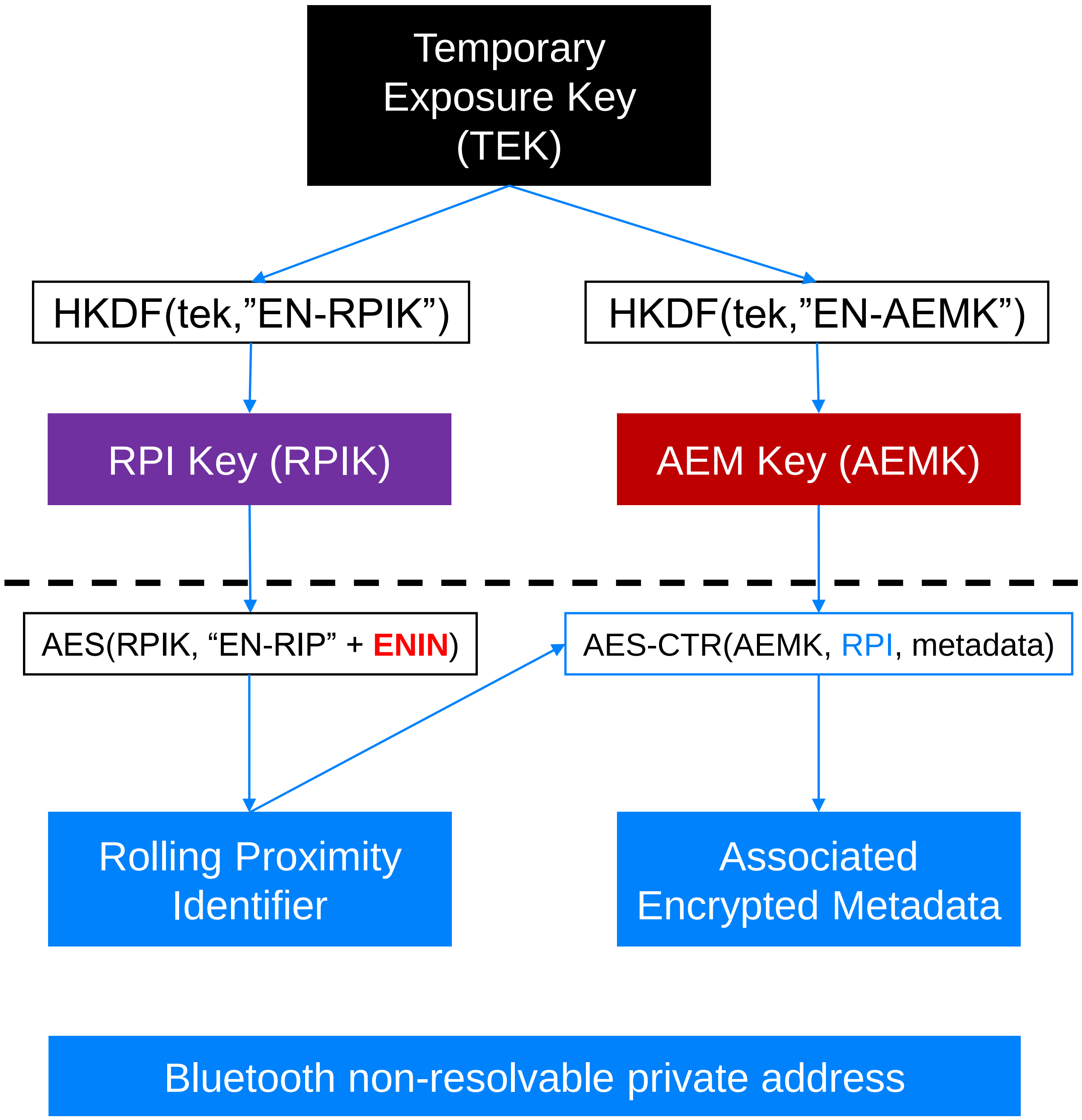
HKDF - RFC5869

Hash-based key derivation function

Privacy

AdvA E3:81:2E:BC:21:45

Payload:
Rolling Proximity Identifier
Associated Encrypted Metadata



Temporary Exposure Key (TEK)

HKDF(tek,"EN-RPIK")

HKDF(tek,"EN-AEMK")

RPI Key (RPIK)

AEM Key (AEMK)

AES(RPIK, "EN-RIP" + ENIN)

AES-CTR(AEMK, RPI, metadata)

Rolling Proximity Identifier

Associated Encrypted Metadata

Bluetooth non-resolvable private address

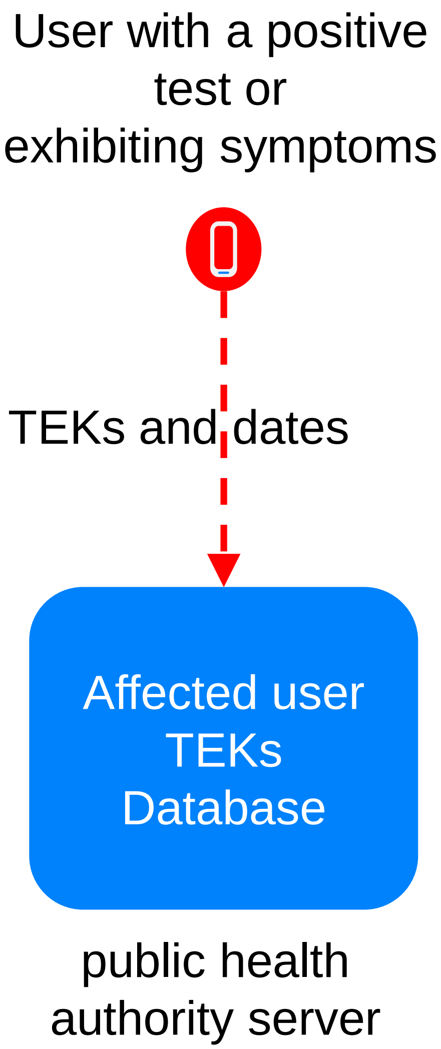
Every 24 Hours

14-days retained

Every 15 Minutes

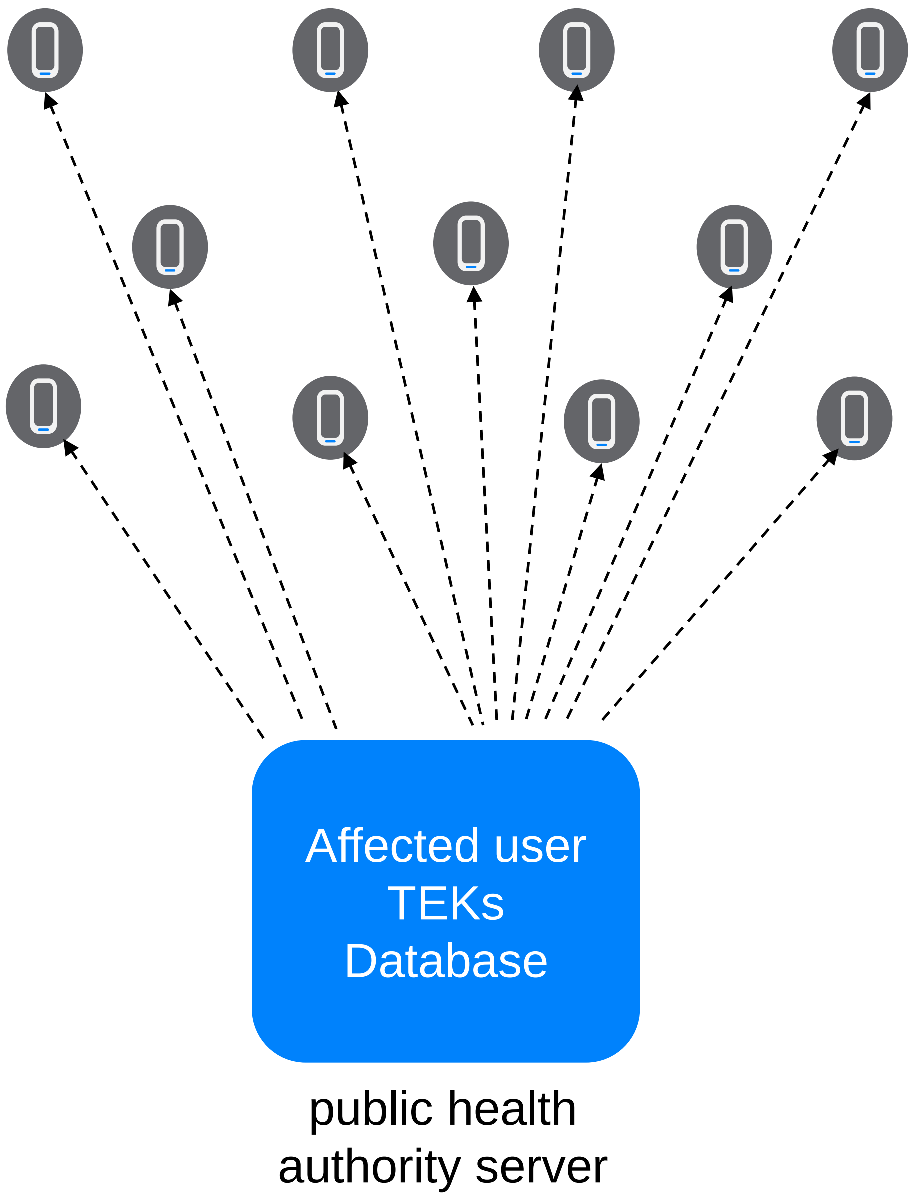
at the same time to prevent linkability

Affected User Declaration



- A user with a positive Covid-19 test or exhibiting symptoms is called an **affected user**
- Affected users voluntarily upload their Temporary Exposure Keys (TEKs) with their dates from the last 14 days to their local public health authority's server

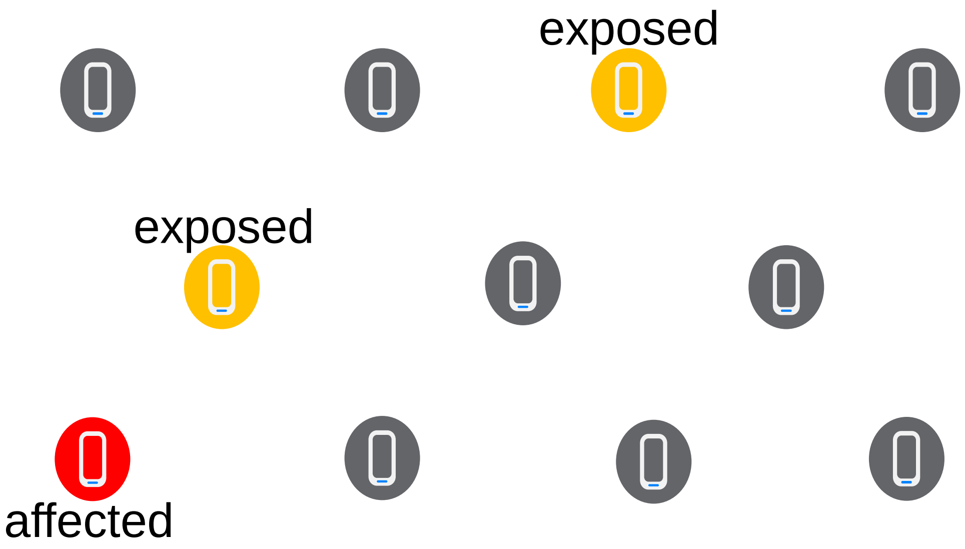
Diagnosis Key Distribution



- TEKs (with their dates) from affected users are distributed to devices periodically. Known as **diagnosis keys**.

- The public health application that is using the ENS framework has control over the schedule.

Exposure Notification



- Devices attempt to decrypt the data in their list of sightings using the distributed diagnosis keys of affected users.

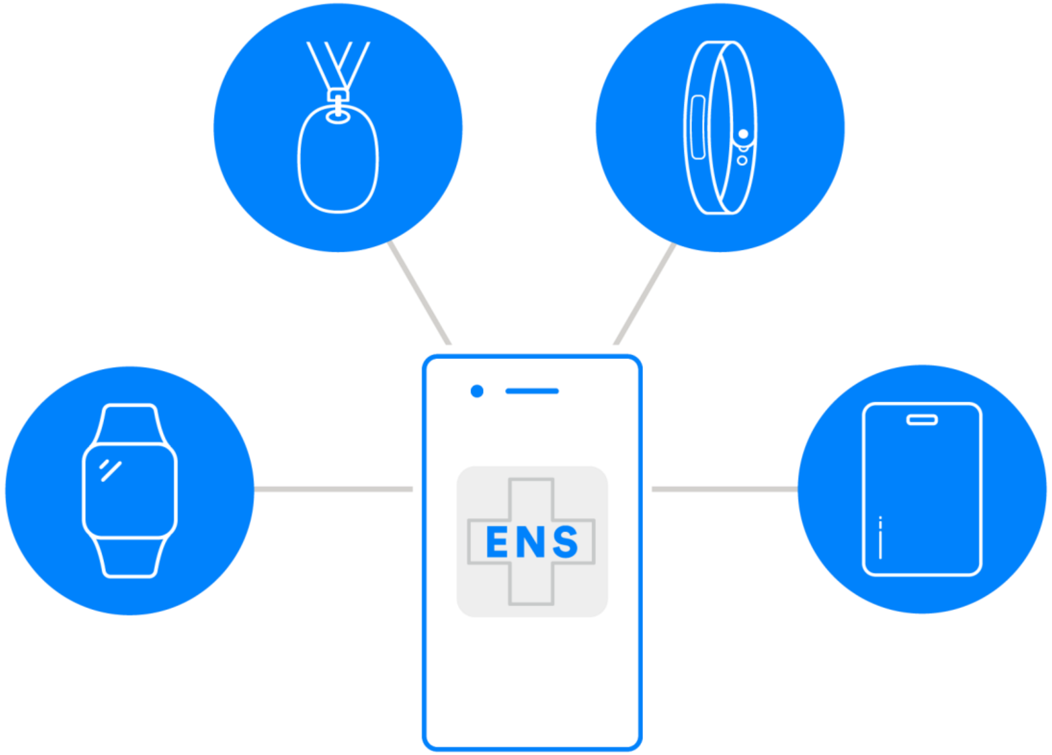
- Successful decryption indicates the sighting of a user who was or later became an **affected user**.

- The public health authority application applies its interpretation of the data to decide whether or not the sighting is epidemiologically significant using exposure time and distance thresholds and other risk factors.

- If the sighting is deemed epidemiologically significant then this user is designated an **exposed user** and notified.

The Future?

Wearables - Extending Access to ENS



- A large part of the global population does not own a smartphone

- Age and economics

- Cheap wearables like smart bracelets could make ENS available to a larger percentage of a population

- Singapore
  - TraceTogether Tokens
  - Battery life of 9 months

Resources

ENS Resources

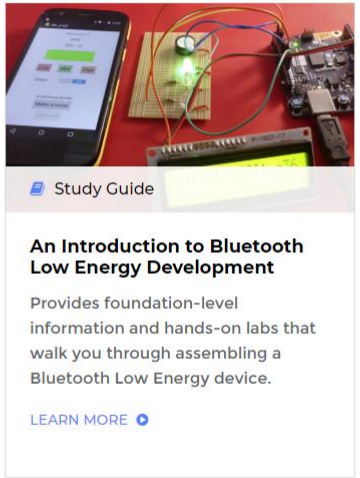
https://www.google.com/covid19/exposurenotifications/

https://covid19.apple.com/contacttracing

https://www.bluetooth.com/learn-about-bluetooth/use-cases/covid/

Bluetooth SIG Resources – Study Guides and Papers

Study Guides - Self-paced, self-study educational resources

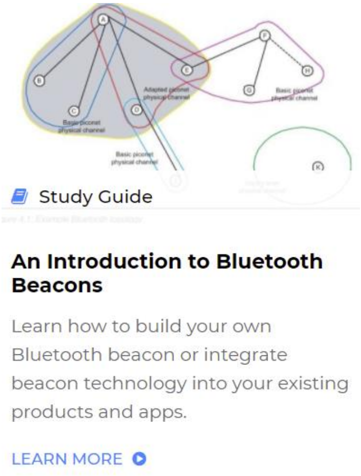


Study Guide

An Introduction to Bluetooth Low Energy Development

Provides foundation-level information and hands-on labs that walk you through assembling a Bluetooth Low Energy device.

LEARN MORE

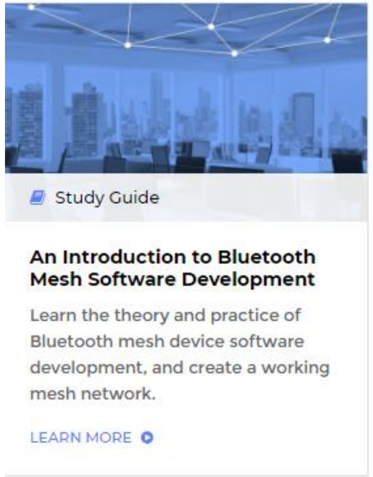


Study Guide

An Introduction to Bluetooth Beacons

Learn how to build your own Bluetooth beacon or integrate beacon technology into your existing products and apps.

LEARN MORE

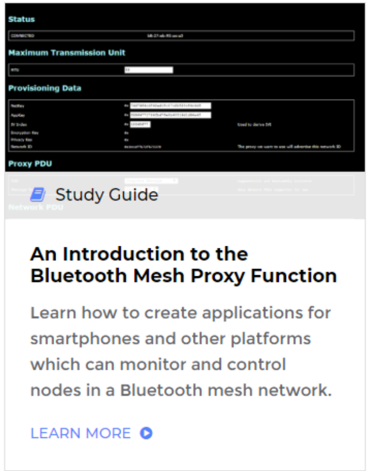


Study Guide

An Introduction to Bluetooth Mesh Software Development

Learn the theory and practice of Bluetooth mesh device software development, and create a working mesh network.

LEARN MORE

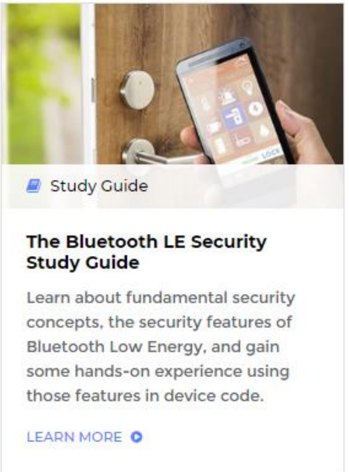


Study Guide

An Introduction to the Bluetooth Mesh Proxy Function

Learn how to create applications for smartphones and other platforms which can monitor and control nodes in a Bluetooth mesh network.

LEARN MORE

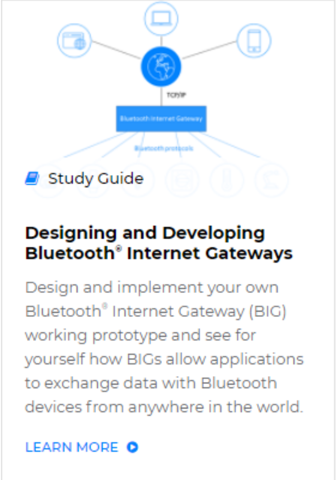


Study Guide

The Bluetooth LE Security Study Guide

Learn about fundamental security concepts, the security features of Bluetooth Low Energy, and gain some hands-on experience using those features in device code.

LEARN MORE



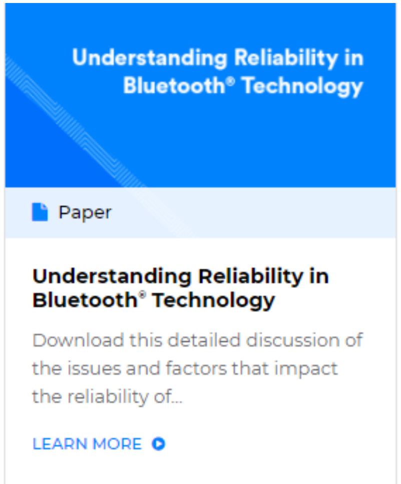
Study Guide

Designing and Developing Bluetooth® Internet Gateways

Design and implement your own Bluetooth® Internet Gateway (BIG) working prototype and see for yourself how BIGs allow applications to exchange data with Bluetooth devices from anywhere in the world.

LEARN MORE

Papers - short reads covering all sorts of Bluetooth® technology subjects

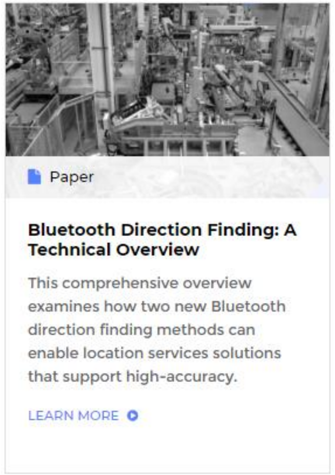


Paper

Understanding Reliability in Bluetooth® Technology

Download this detailed discussion of the issues and factors that impact the reliability of...

LEARN MORE

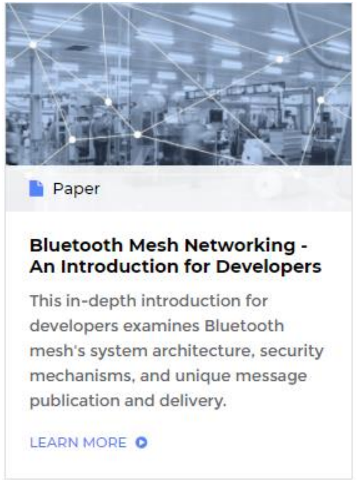


Paper

Bluetooth Direction Finding: A Technical Overview

This comprehensive overview examines how two new Bluetooth direction finding methods can enable location services solutions that support high-accuracy.

LEARN MORE

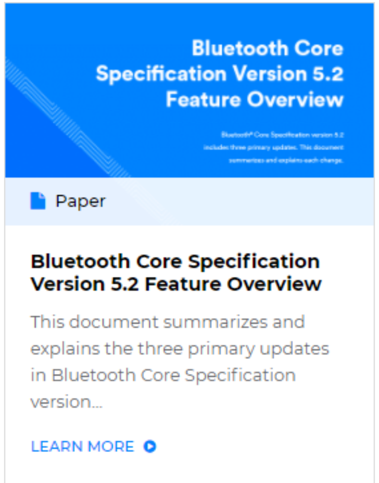


Paper

Bluetooth Mesh Networking - An Introduction for Developers

This in-depth introduction for developers examines Bluetooth mesh's system architecture, security mechanisms, and unique message publication and delivery.

LEARN MORE

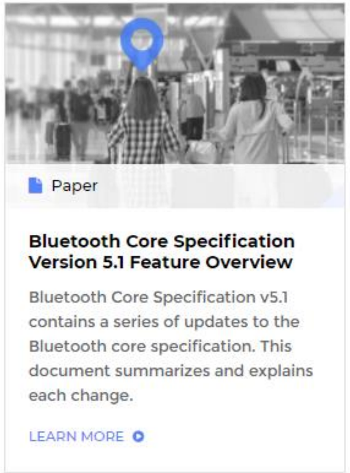


Paper

Bluetooth Core Specification Version 5.2 Feature Overview

This document summarizes and explains the three primary updates in Bluetooth Core Specification version...

LEARN MORE

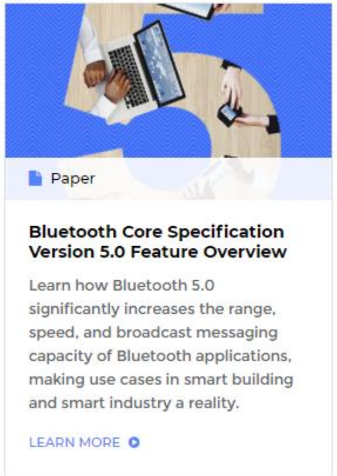


Paper

Bluetooth Core Specification Version 5.1 Feature Overview

Bluetooth Core Specification v5.1 contains a series of updates to the Bluetooth core specification. This document summarizes and explains each change.

LEARN MORE



Paper

Bluetooth Core Specification Version 5.0 Feature Overview

Learn how Bluetooth 5.0 significantly increases the range, speed, and broadcast messaging capacity of Bluetooth applications, making use cases in smart building and smart industry a reality.

LEARN MORE

bluetooth.com/developer

Thank You!

Martin Woolley
Bluetooth SIG

Twitter: @bluetooth_mdw

Background

30 January 2020

A Public Health Emergency of International Concern

11 March 2020

A Pandemic

Examples of the World’s Response

Slowing the Spread

Researching Vaccines

Bolstering Public Healthcare Facilities

Providing Economic Support

How Covid-19 Spreads

Through the air between people **in close enough proximity**

Via contaminated surfaces

Measures for Slowing the Spread

Social Distancing

Face Masks

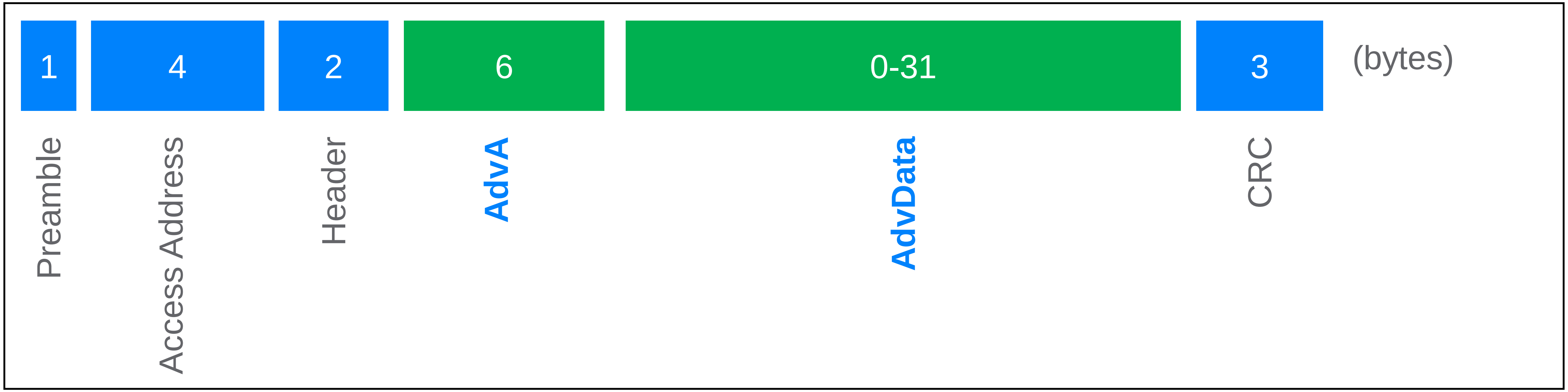
Contact Tracing

Testing

Isolation

Reducing the “R Number”

Advertising Packets - ADV_NONCONN_IND



1	4	2	6	0-31	3	(bytes)
Preamble	Access Address	Header	**AdvA**	**AdvData**	CRC	

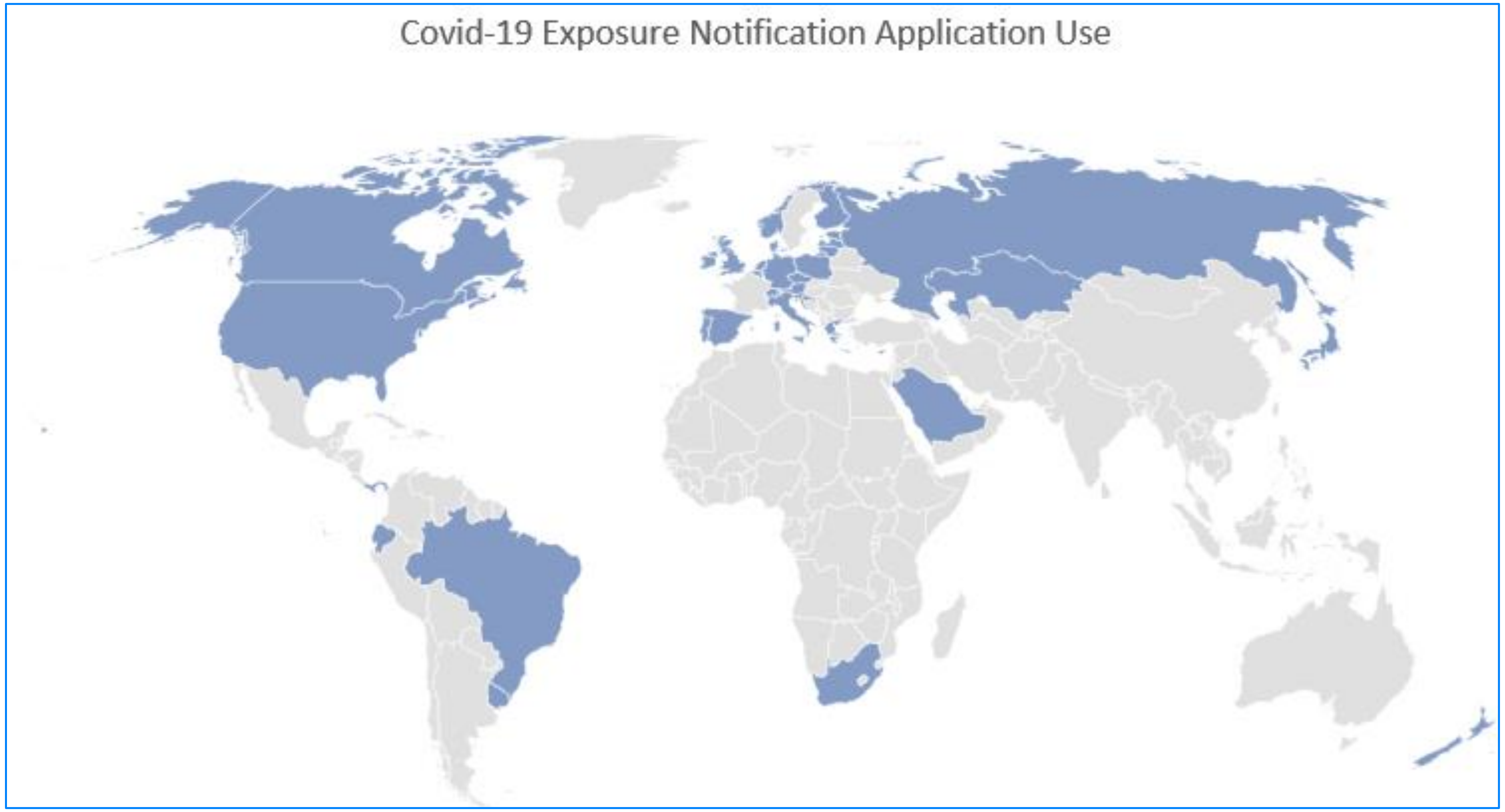
Maximum length 37 octets: 31 octets of data plus 6 octet advertising device address

AdvA is the transmitter’s device address - can be randomized and change regularly for **privacy protection**

AdvData contains **Tag/Length/Value** “AD types”

Timing of transmissions governed by the **advertising interval**

Extensive Adoption



Austria, Belgium, Brazil, Canada, Croatia, Cyprus, Czech Republic, Denmark, Ecuador, Estonia, Finland, Germany, Gibraltar, Greece, Ireland, Italy, Japan, Kazakhstan, Latvia, Lithuania, Malta, Netherlands, New Zealand, Northern Ireland, Norway, Panama, Poland, Portugal, Russia, Saudi Arabia, Scotland, Slovenia, South Africa, Spain, Switzerland, United Kingdom, United Kingdom, United Kingdom, Uruguay, United States

What about Asia? Singapore definitely has something - more research required

source: https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/ (Feb 2021)

Impact in the UK

Computer Weekly, February 9th 2021

NHS Covid-19 app alerts 1.7 million contacts

The developer of the UK’s Covid-19 contact-tracing app has revealed that approximately 600,000 cases have been prevented by the app since September 2020, possibly preventing 6,000 deaths. (OG)

Android Debug Logs

```
2021-03-26 10:01:28.708 3269-6717/? I/ExposureNotification: Starting scanning. scanMode=2 [CONTEXT
service_id=236 ]
2021-03-26 10:01:28.708 3269-6717/? I/ExposureNotification: Schedule stop the scan after 4 seconds [CONTEXT
service_id=236 ]

2021-03-26 10:01:28.757 3269-3269/? I/ExposureNotification: Scan device 23:21:C1:42:FC:B4, type=1,
id=C712253FC19C7058F470BAAE839F869B, raw_rssi=-86, calibrated_rssi=-80, meta=830DB900,
previous_scan=1616752809 [CONTEXT service_id=236 ]
2021-03-26 10:01:28.757 3269-3269/? I/ExposureNotification: BleDatabaseWriter.writeBleSighting,
id=C712253FC19C7058F470BAAE839F869B [CONTEXT service_id=236 ]

2021-03-26 10:01:29.895 3269-6717/? I/ExposureNotification: Start advertising with packet (AdvertiseData
[mServiceUuids=[0000fd6f-0000-1000-8000-00805f9b34fb], mManufacturerSpecificData={},
mServiceData={0000fd6f-0000-1000-8000-00805f9b34fb=[-20, 68, -112, -58, -113, -90, -105, -75, 22, 62, -53,
-3, -24, 6, 40, -2, 90, -18, 97, -40]}, mIncludeTxPowerLevel=false, mIncludeDeviceName=false,
mTransportDiscoveryData=null]) mode: ADVERTISE_MODE_BALANCED tx power level ADVERTISE_TX_POWER_LOW [CONTEXT
service_id=236 ]

2021-03-26 10:01:32.718 3269-6717/? I/ExposureNotification: Stopping scanning. [CONTEXT service_id=236 ]

2021-03-26 10:04:39.786 3269-6704/? I/ExposureNotification: Starting scanning. scanMode=2 [CONTEXT
service_id=236 ]
2021-03-26 10:04:39.786 3269-6704/? I/ExposureNotification: Schedule stop the scan after 4 seconds [CONTEXT
service_id=236 ]
```