Contact Tracing

Christian Menschel CocoaHeads Aachen April 30 2020 -
last edit April 30 2020 - things change daily - check the sources for updates

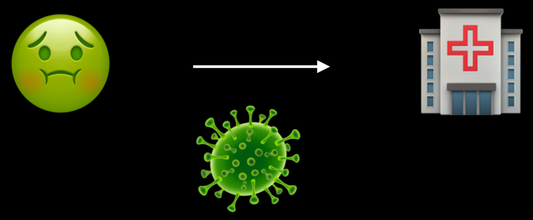
Exposure Notification

Combat Covid-19

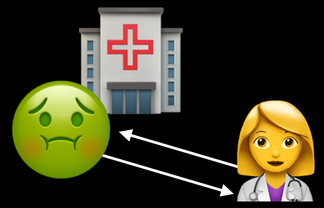
Contact tracing

Contact tracing

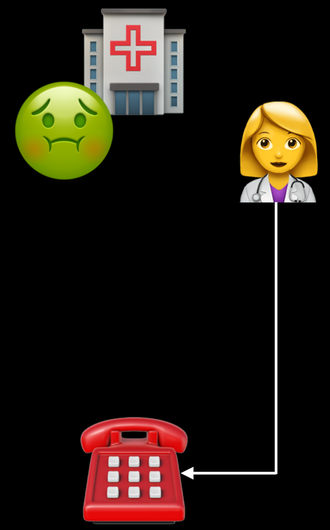
Contact tracing



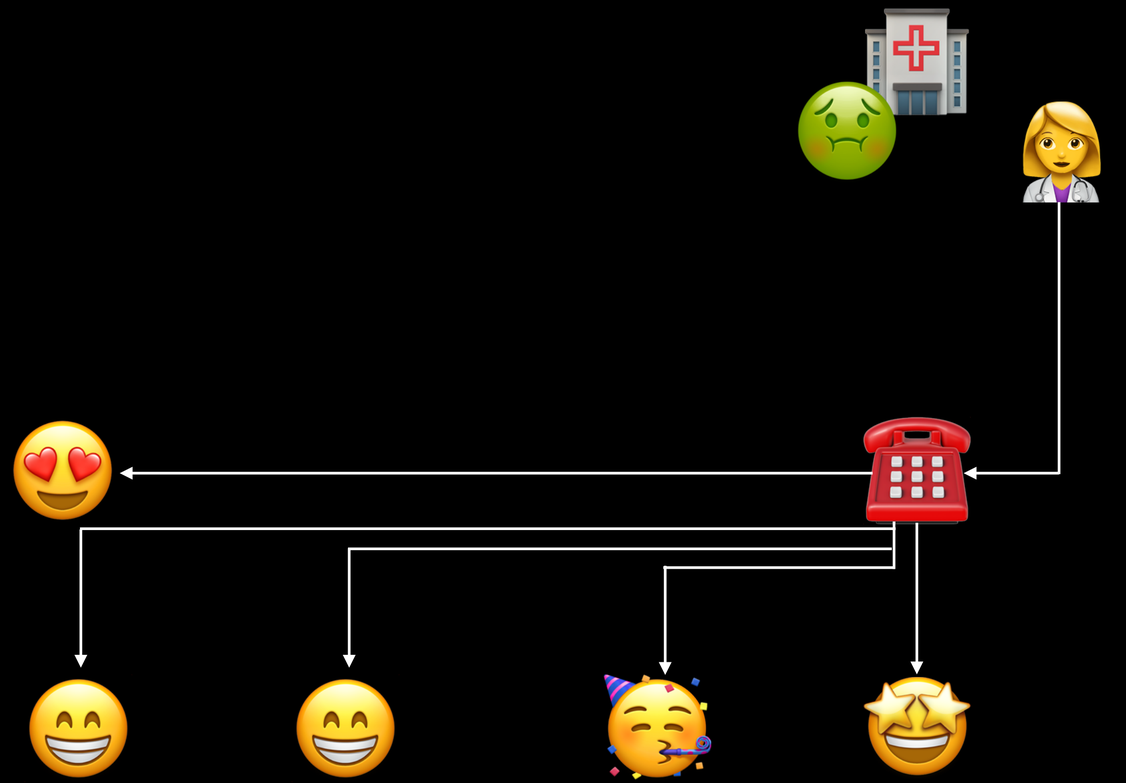
Contact tracing



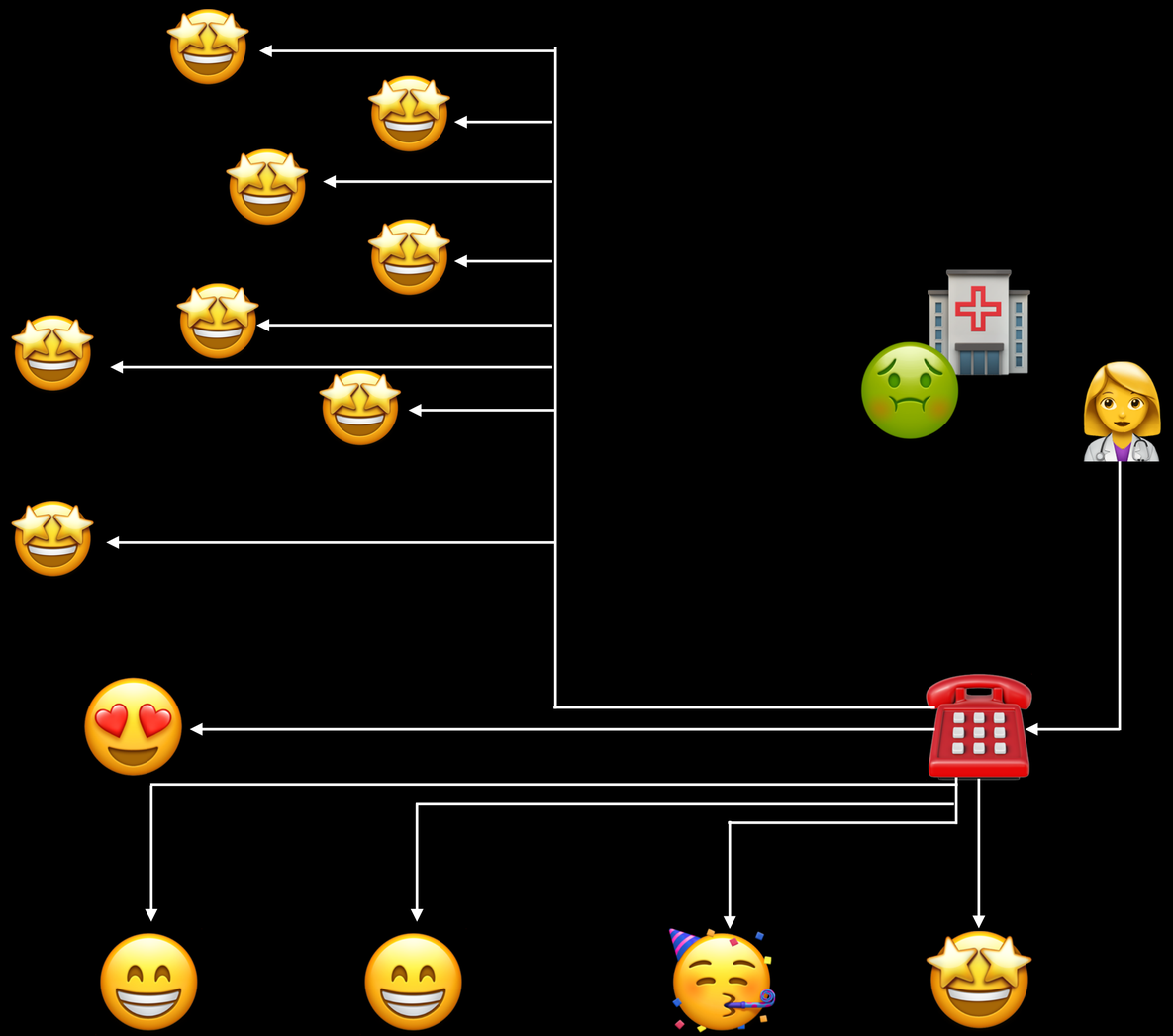
Contact tracing



Contact tracing

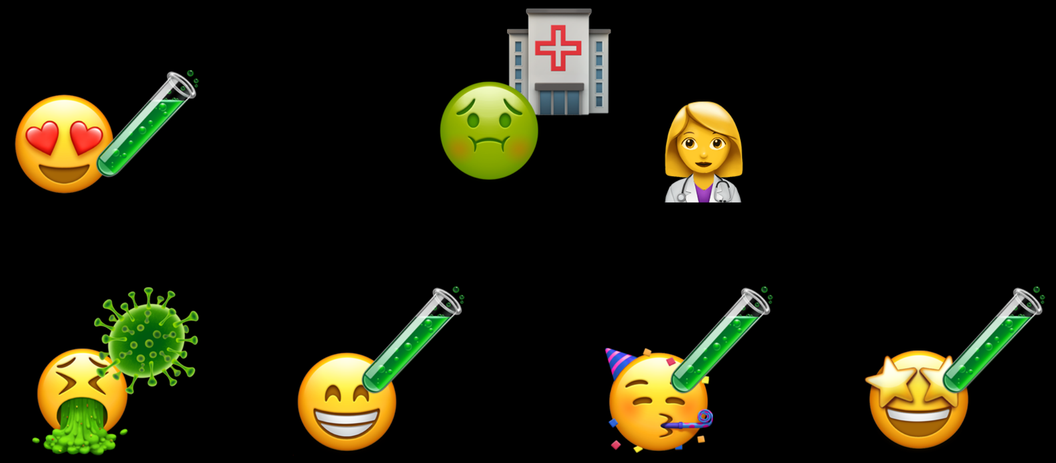


Contact tracing



Contact tracing

This takes too long!

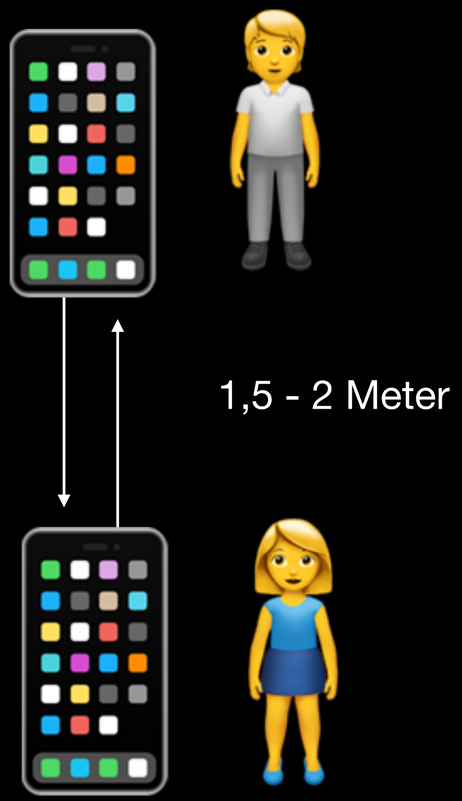


But contact tracing is essential for isolating infected to leave the lockdown and get back to containment mode

Instant tracing with Bluetooth

Advertisement mode (Send)

Exchange proximity identifier (rotating)



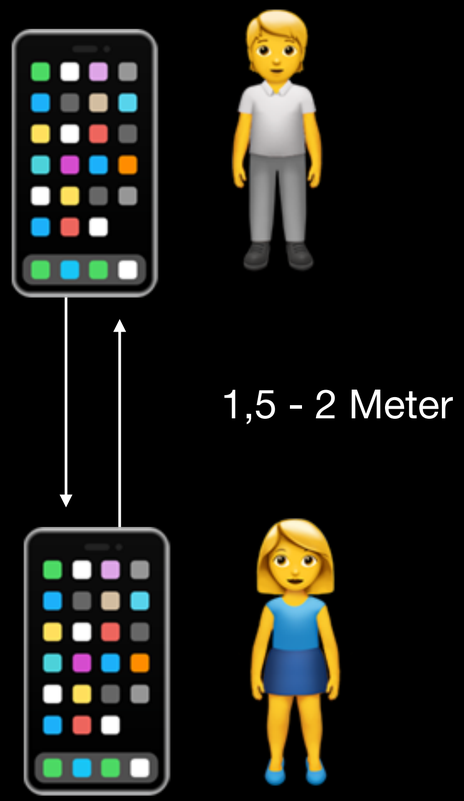
Instant tracing with Bluetooth

Advertisement mode (Send)

Exchange proximity identifier (rotating)

Scanning mode (Receiving)

Receive proximity and store data with date and duration



Instant tracing with Bluetooth

Advertisement mode (Send)

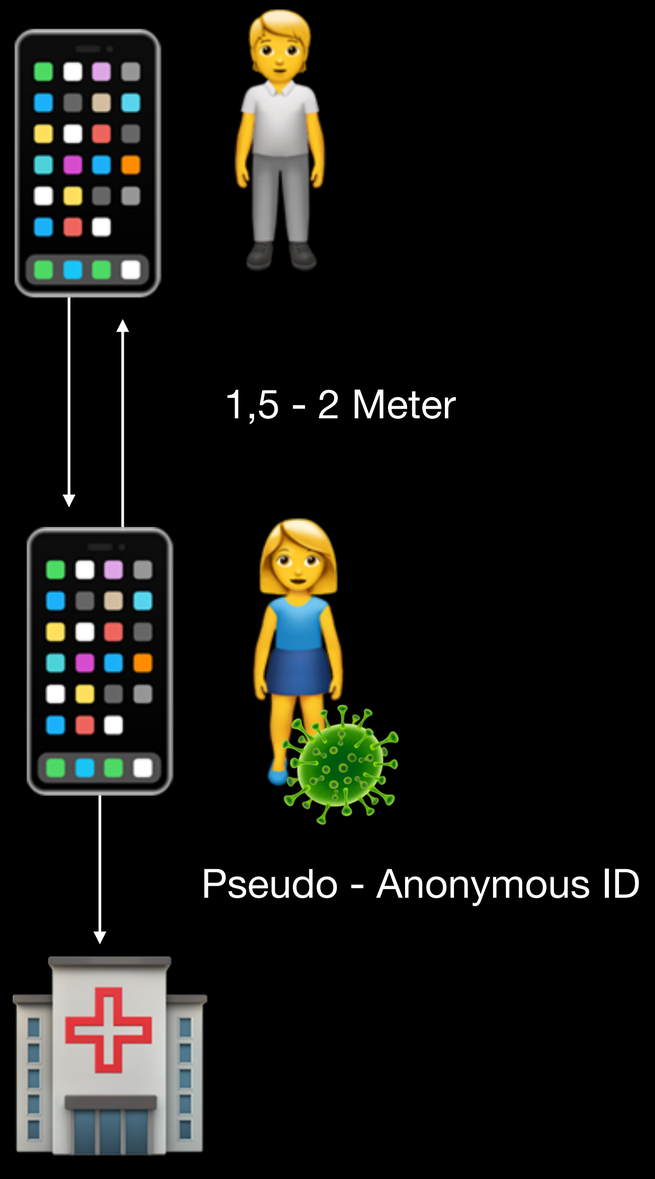
Exchange proximity identifier (rotating)

Scanning mode (Receiving)

Receive proximity and store data with date and duration

Infection

Send data to health authorities with consent



Decentralized vs. Centralized

Decentralized

Reports infection with random keys (generated in the last ~14 days) to health authority

Decentralized

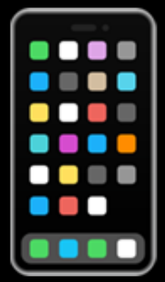
Reports infection with random keys (generated in the last ~14 days) to health authority

Apps download (daily) a list of keys that belong to infected persons

Decentralized

Reports infection with random keys (generated in the last ~14 days) to health authority

Apps download (daily) a list of keys that belong to infected persons



Match infected persons with local contact history on device

Health authority never has access to history

Centralized

Infected person sends keys and
history of proximity data
to health authority

Centralized

Health authority matches gathered
proximity data with infected persons
and makes data research

Infected person sends keys and
history of proximity data
to health authority

Centralized

Health authority matches gathered
proximity data with infected persons
and makes data research

Health authority
notifies people who
were in contact with infected

Infected person
sends history of proximity data
to health authority

Health authority has access to history of all infected persons

Projects in April 2020

- Bluetooth LE based & no GPS (except China, Norway, South Korea)
- Pseudo anonymous data
- Some kind of encryption
- Use rolling keys to prevent tracking users
- Users opt-in (can withdraw the consent later)

Projects in April 2020

- Bluetooth LE based & no GPS (except China, Norway, South Korea)
- Pseudo anonymous data
- Some kind of encryption
- Use rolling keys to prevent tracking users
- Users opt-in (can withdraw the consent later)

BlueTrace Protocol

Google

dp3t

COVIDSAFE

DP-3T

- Swiss research group
- Decentralized
- Good transparency - Already contributed a lot
- Open Source
- Endorsed by Apple & Google
- NO proximity data on server
- Server publishes a list of infected persons (keys)
- Will be used by Austria, Estonia, Finland & Germany (now)

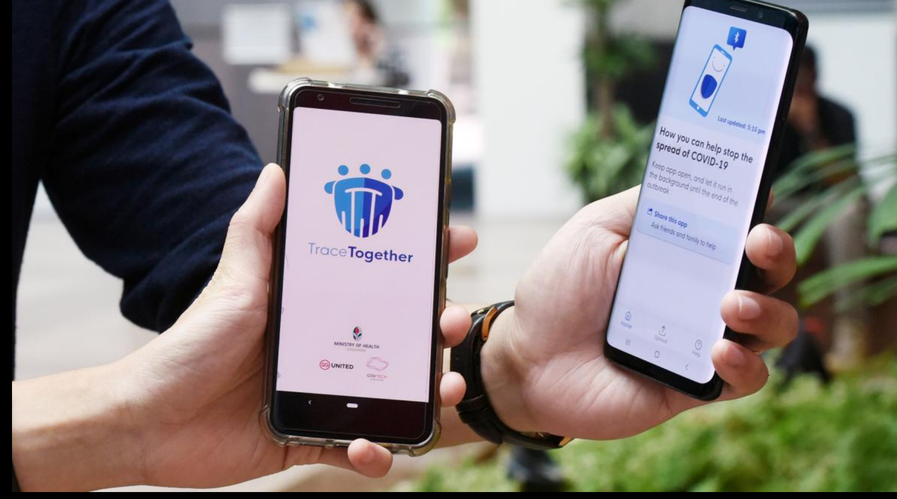
https://github.com/DP-3T

PEPP-PT

- Started by German company (Chris Boos - a German tech gov. consultant)
- Centralized reporting
- Operates transnational (Pan-European)
- Collects proximity history of infected on server
- Matching with infected persons on server
- Not yet open sourced - minor transparency - no code yet
- NOT endorsed by Apple & Google
- Bluetooth won’t operate in background

https://www.pepp-pt.org

BlueTrace



- Singapore government
- Centralized reporting
- Over two million downloads (COVIDSafe & TraceTogether)
  - TraceTogether (Singapore, started March 20)
  - COVIDSafe (Australia, started April 25)
- Open Source ? (OpenTrace Fork)
- Runs Firebase or AWS (COVIDSafe)
- App must be in foreground to advertise proximity data

https://www.health.gov.au/resources/apps-and-tools/covidsafe-app

https://bluetrace.io https://www.tracetogether.gov.sg

How Apple & Google came together

Mid-March

- Apple's Myoung Cha, some developers and crypto experts (CryptoKit devs: Yannick Sierra and Frederic Jacobs) started brainstorming about contact tracing with iPhones under the codename "***Bubble***".
- They got support from Craig Federighi and Jeff Williams
- Were inspired by the Swiss DP-3T and Singapore app
- It should be decentralized and background operable.

March 21st

- Swiss engineering professor Edouard Bugnion (DP-3T) reached out Apple to address the concerns

Beginning April

- Google engineers started with a project called with codename "***Apollo***"
- Google's Android VP Dave Burke reached Apple's Myoung Cha

April 6th

- Apple's Myoung Cha made a call with Swiss researcher Bugnion

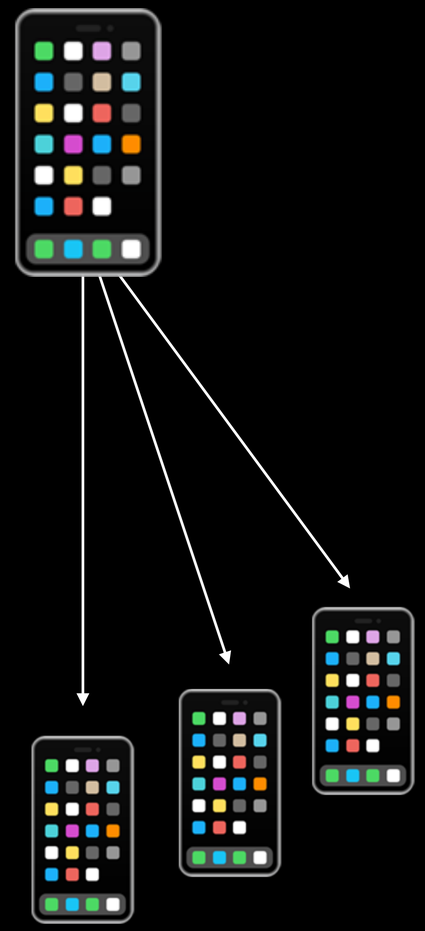
April 10th

- Tim Cook and Sundar Pichai officially announced the Apple & Google partnership

https://www.cnbc.com/2020/04/28/apple-iphone-contact-tracing-how-it-came-together.html

Apple & Google proposal

Advertising (Sending) mode

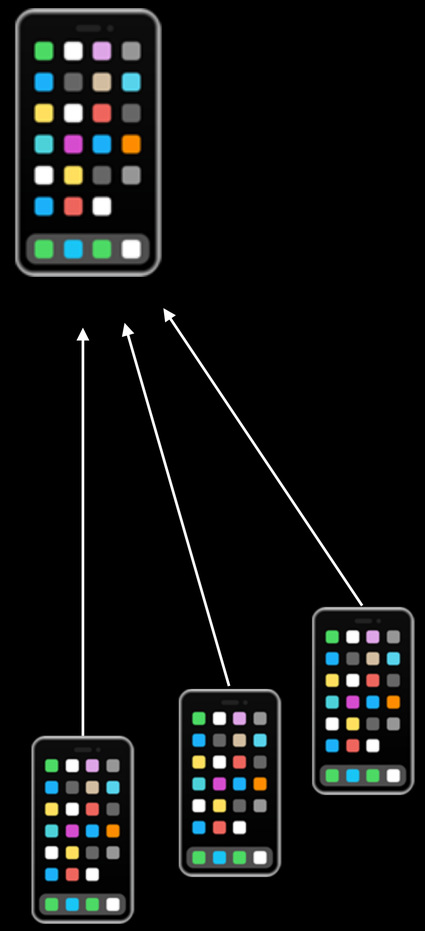


1. Device creates a “Temporary Exposure Key” every day (will be sent only for infections)
2. Device sends via bluetooth “Rolling Proximity Identifier” (=> derived from the Temporary Exposure Key) + meta values
   Changed every ~15 minutes to prevent wireless tracking

https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.1.pdf

Apple & Google proposal

Scanning mode



1. Receive and store the “Rolling Proximity Identifier” & encrypted meta data (protocol versioning and transmit power for better distance approximation) with timestamp and RSSI information (every ~5 minutes)

2. Periodically downloading the “Diagnosis Keys” — The subset of “Temporary Exposure Keys” of infected persons

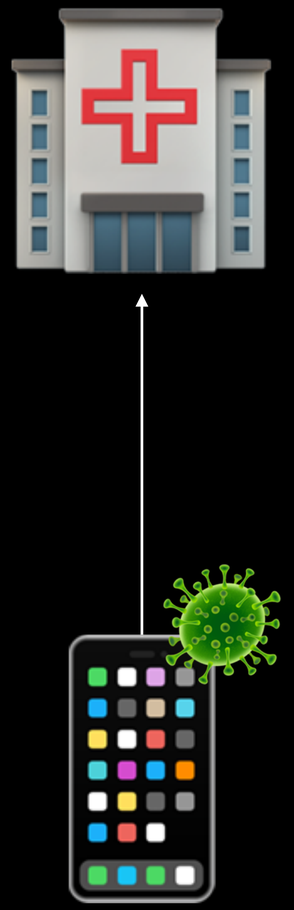
3. Match “Diagnosis Keys” against stored “Rolling Proximity Identifier”

4. If match found an algorithm assess risk based on duration, informs the Health Authority app and sends an alert to the user

https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.1.pdf

Apple & Google proposal

Infected mode



1. User is infected and consents to share the “Diagnosis Keys” (all keys in the last ~14 days) with the server of the health authorities

2. Diagnosis Keys for the infected person will be stored at the health authorities and provided to other persons

https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.1.pdf

Apple & Google proposal

Infected mode

1. User is infected and consents to share the “Diagnosis Keys” (all keys in the last ~14 days) with the server of the health authorities

2. Diagnosis Keys for the infected person will be stored at the health authorities and provided to other persons

Affected User: A user who has a confirmed or suspected diagnosis of COVID-19

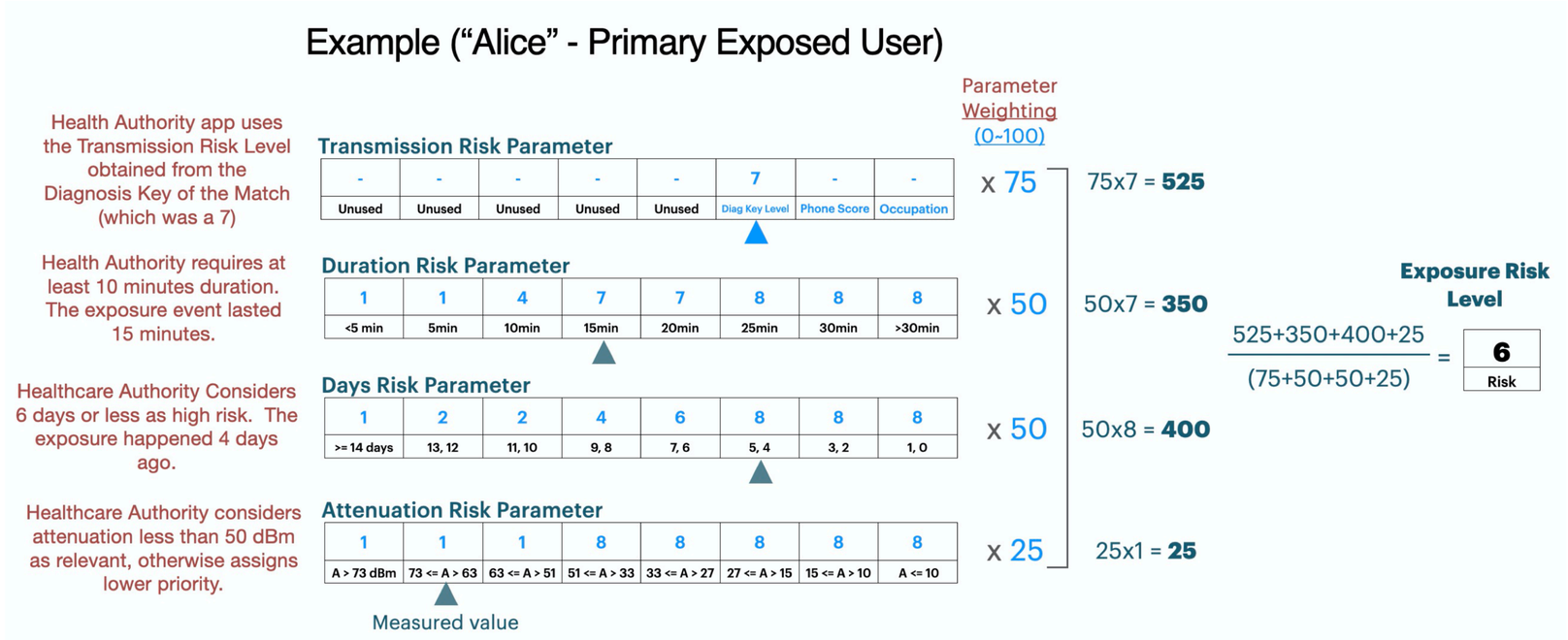
Exposed User: User who have a potential exposure

https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.1.pdf

Apple & Google proposal

Exposure Risk Level

The following diagram illustrates an example of an Exposure Risk Level calculated for a person named Alice who was exposed to person (Bob) who was diagnosed positive. So, Alice is considered a primary exposed user.

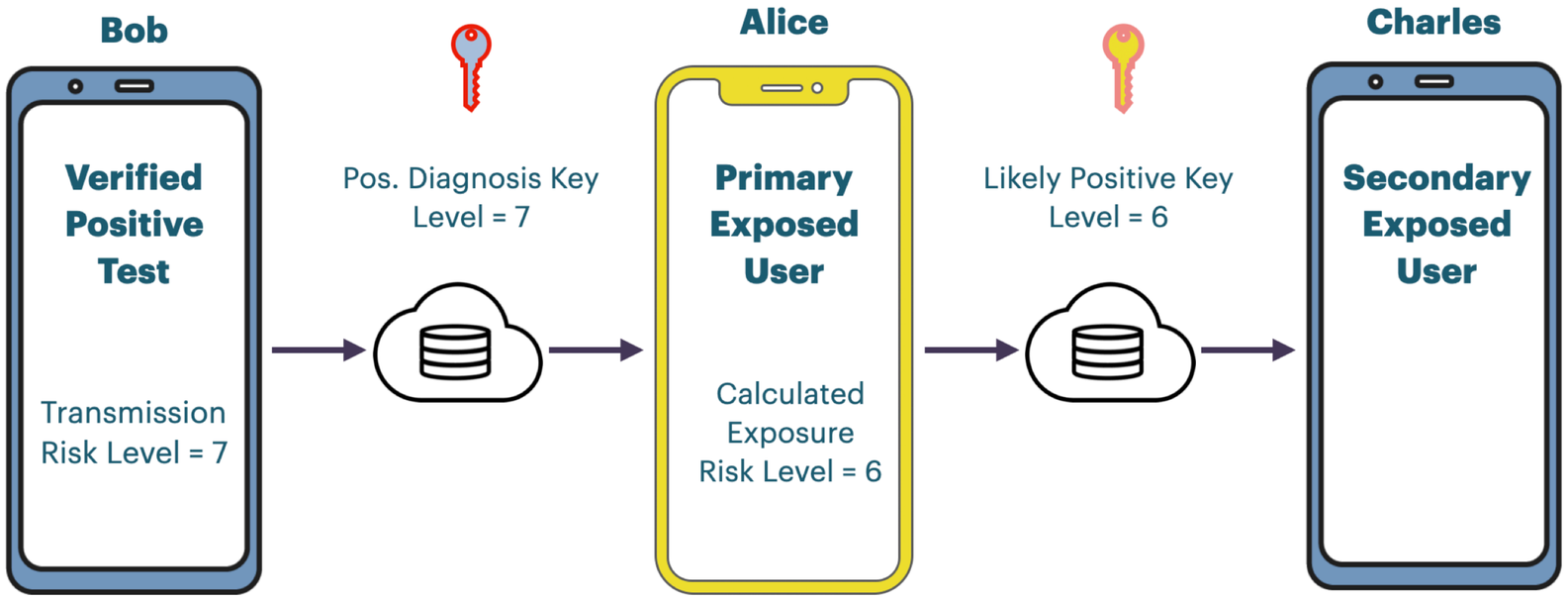


https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.1.pdf

Apple & Google proposal

Exposure Risk Level

The following diagram shows how Exposure Risk Levels can be transferred along with the Diagnosis Keys via the key-sharing schema. In this way, a secondary exposed user (Charles) who was recently near Alice, may optionally be notified by the app (should it determine that Alice's exposure risk level is high enough that she is likely COVID-19 positive).



https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.1.pdf

Apple & Google proposal

Privacy first

1. No location data - Only Bluetooth LE
2. Rolling Proximity Identifier changes every ~15 minutes
3. Proximity identifiers stays on device
4. Users must opt-in and grant consents
5. If diagnosed with COVID-19 users must again give the consent to the “Diagnosis Keys” with the Health Authorities
6. Only health authorities will be capable to build an app with exposure notification

https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.1.pdf

Apple & Google proposal

Open Questions?

1. How long will the “Rolling Proximity Identifier” be stored on device?

2. How often will the system download “Diagnosis Keys” ? Daily?

3. What’s the traffic size for the “Diagnosis Keys” ?

4. How does the system decide which “Diagnosis Keys” should be loaded?
   What happens if I cross borders?

5. How to handle False Positives? Walls and windows?

6. How are DDoS attacks prevented ?

7. What if battery is low? Low power mode?

Apple & Google proposal

Apple is not releasing the exposure notification API to all developers, but rather only to public health authorities.

On Friday, May 1, Apple and Google representatives say both companies will release additional information to developers. This will include sample code to help developers further understand how the exposure notification system will work.

Note: The “COVID-19 Exposure Notifications” toggle is enabled by default in this beta of iOS 13.5. This does not actually collect any data, and app authorization will be required once the feature ships. Apple and Google’s exposure notification system will be completely opt-in.

https://9to5mac.com/2020/04/29/ios-13-5-beta-covid-19-contact-tracing/

The chaos in Germany

- March: First plan: Use PEPP-PT (Centralized)
- 300 researchers & CCC warn to use a centralized app (Surveillance risks)
- Many researchers left PEPP-PT and follow DP-3T
- German government talked to Apple & Google
- They said: NO to centralized apps!
- April 26: Jens Spahn changed plans to decentralized app
- Deutsche Telekom and SAP will follow DP-3T’s approach (SDK)

Issues & risks

- Low adoption and mistrust by population
- 60% of the population should install the app
- Singapore: 16% only installed since March 20
- Privacy risks with centralized solutions
- False Positives & too many wrong notifications

Tech obstacles

- Bluetooth rssi not consistent among all iOS & Android devices
- Centralized solution is more complex (=> error prone and security risks)
- False Positives (i.e. standing close between windows)
- DDoS attack vectors (Sending a large number of False Positives) to health auth.
- Interfere the bluetooth signal
- Bluetooth app must operate always (also when closed) - Sep. process?

Countries

Germany: DP3T based by Deutsche Telekom & SAP (Decentral)

Austria: DP-3T

Australia: BlueTrace

Estonia: DP-3T

Finland: DP-3T

France: some Central

UK: some Central + evtl GPS

Singapore: BlueTrace (Central)

Switzerland: DP-3T

New Zealand: BlueTrace (Central)

Norway: Centralized + GPS

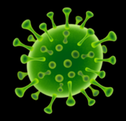
China: GPS

South Korea: GPS

…more smaller solutions (VAE,..)

Conclusion



- The app is one solution of many to trace infections
- Privacy matters
- Many solutions (decentralized vs. centralized)
- GPS based would too inaccurate
- Trust & big coverage (60%) are crucial
- Decentralized seems the way to go
- There is no way around Apple or Google
- Apple & Google remind governments to protect users’ privacy