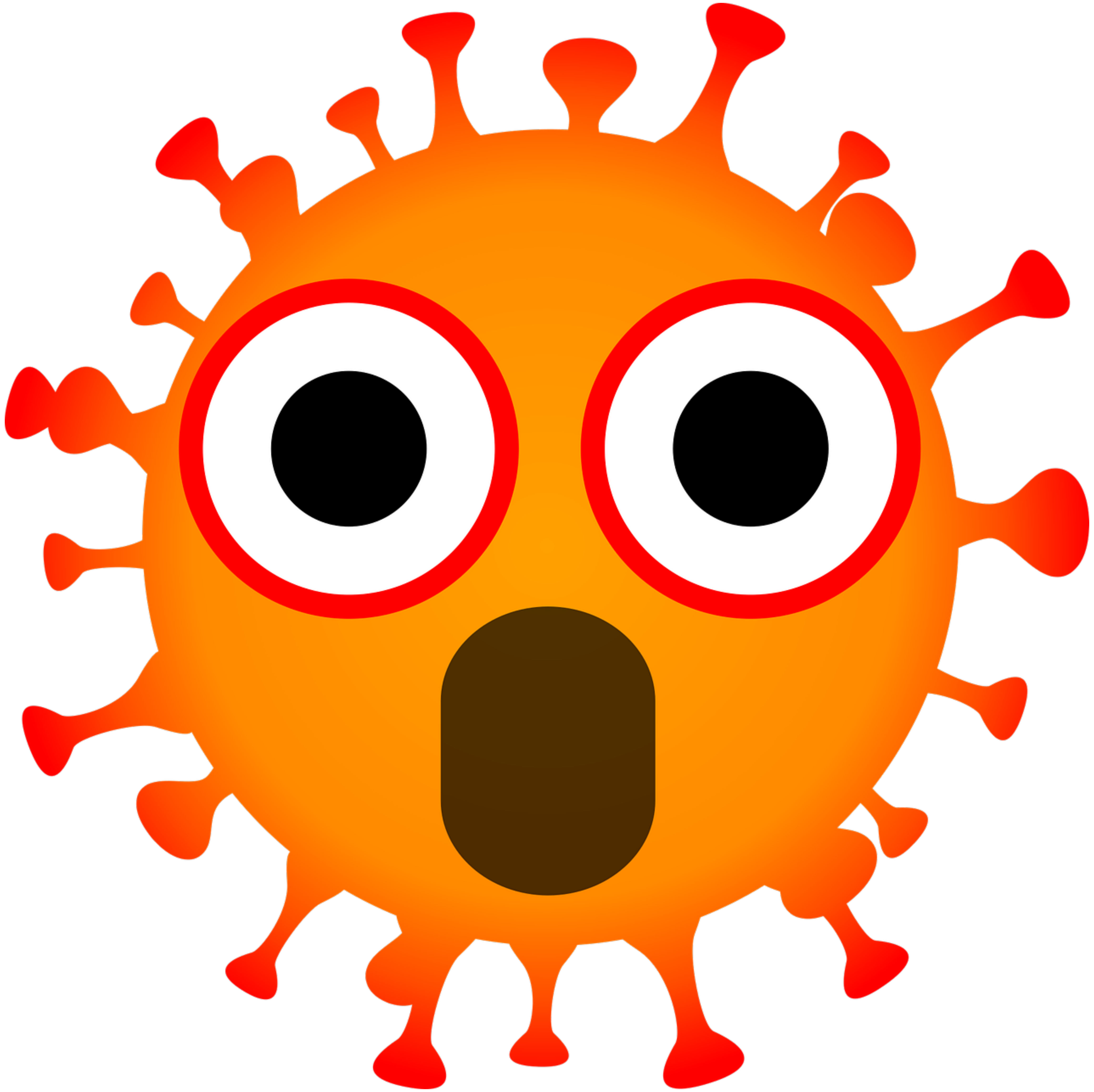
Proximity Tracing

Jean-Pierre Höhmann June 17, 2020

The Problem

Contact Tracing

- Ways to constrain a pandemic:
  - Lockdown → ☹
  - Contact Tracing → ☺
- Manual contact tracing is…
  - …labour intensive
  - …slow
- Automate it!

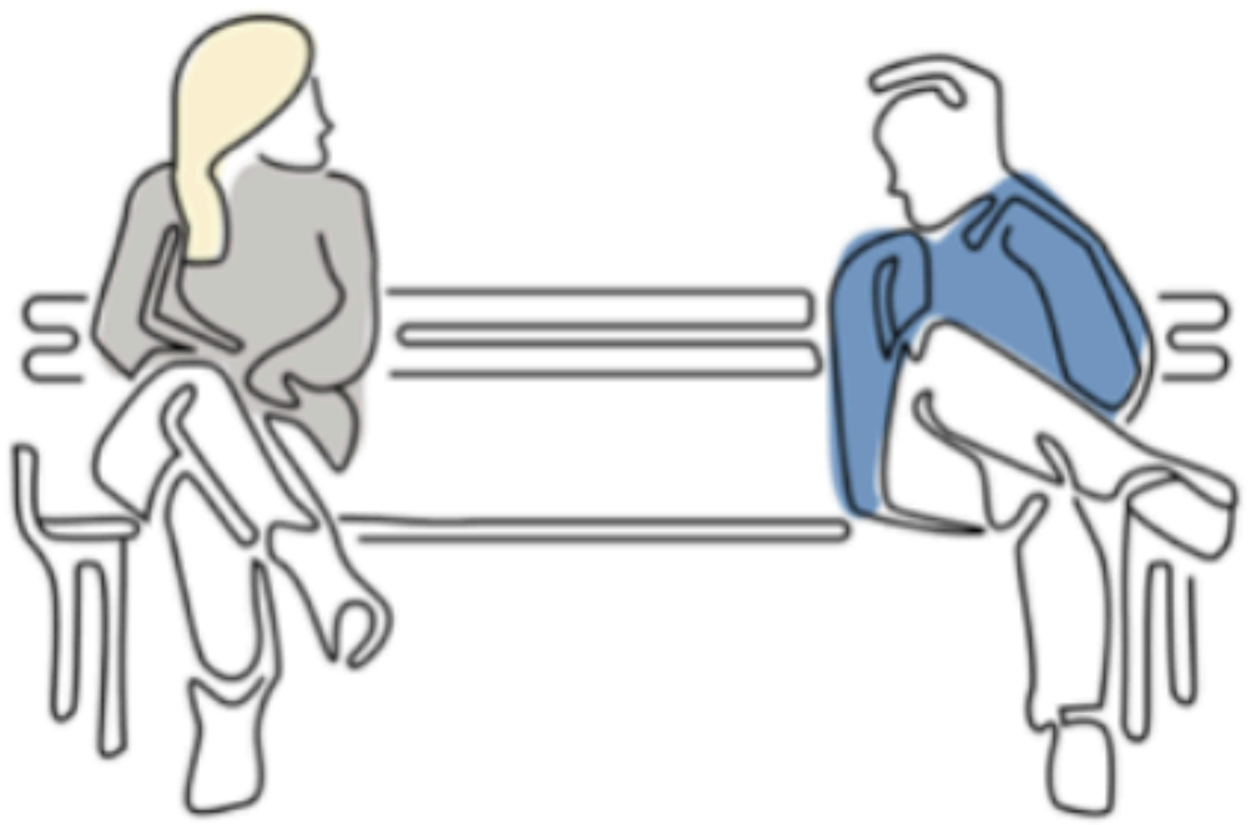


The Solution

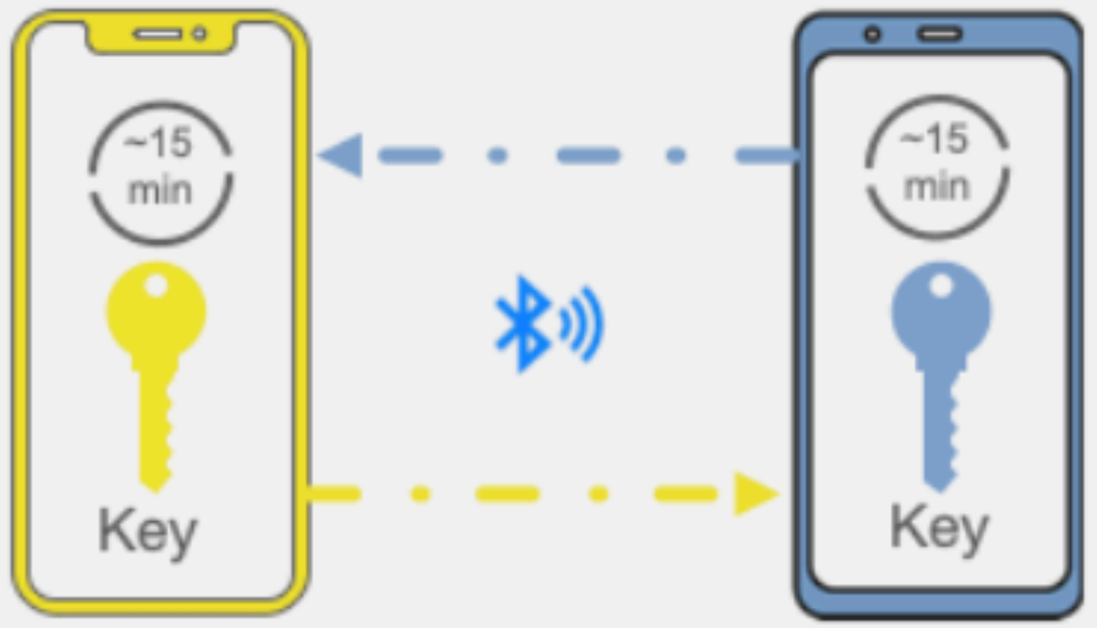
Bluetooth Beacons

- Widely available
- More accurate than cell tower location
- Less invasive than ultrasonic
- More privacy-preserving than GPS

Alice and Bob don’t know each other, but have a lengthy conversation sitting a few feet apart



Their phones exchange beacons with random Bluetooth identifiers (which change frequently)

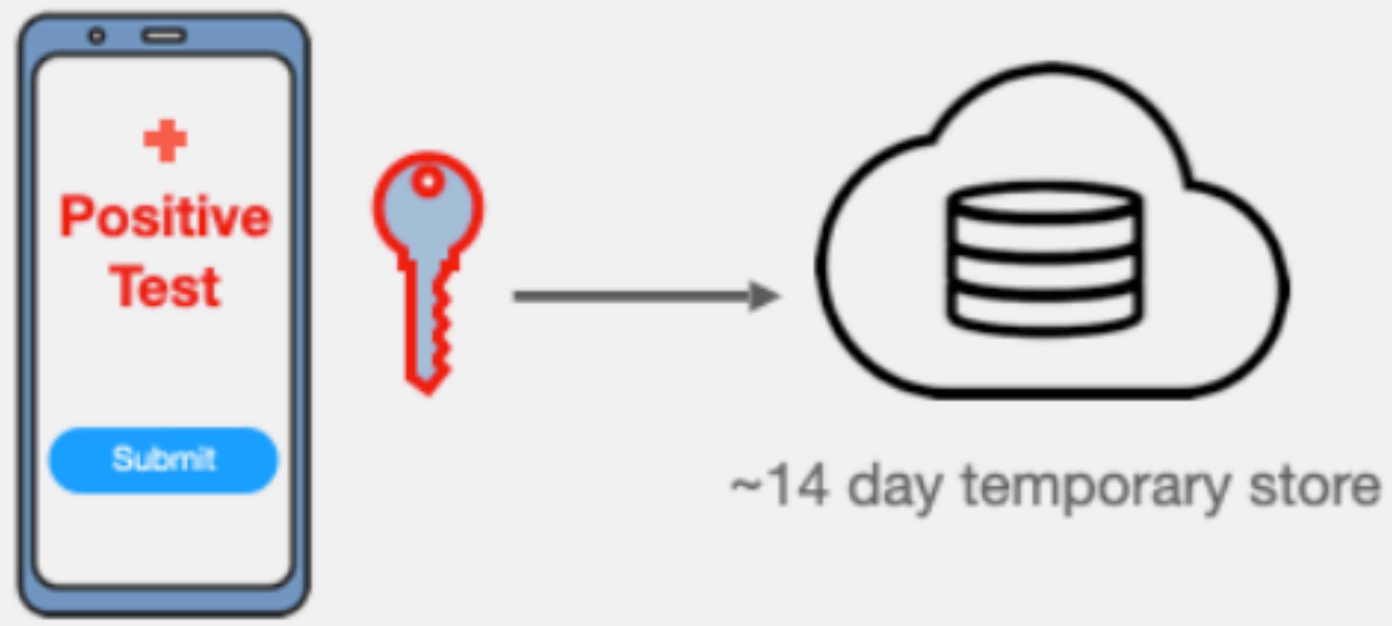


A few days later…

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

With Bob’s consent, his phone uploads the last 14 days of keys for his Bluetooth beacons to the server

Apps can only get more information via user consent



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

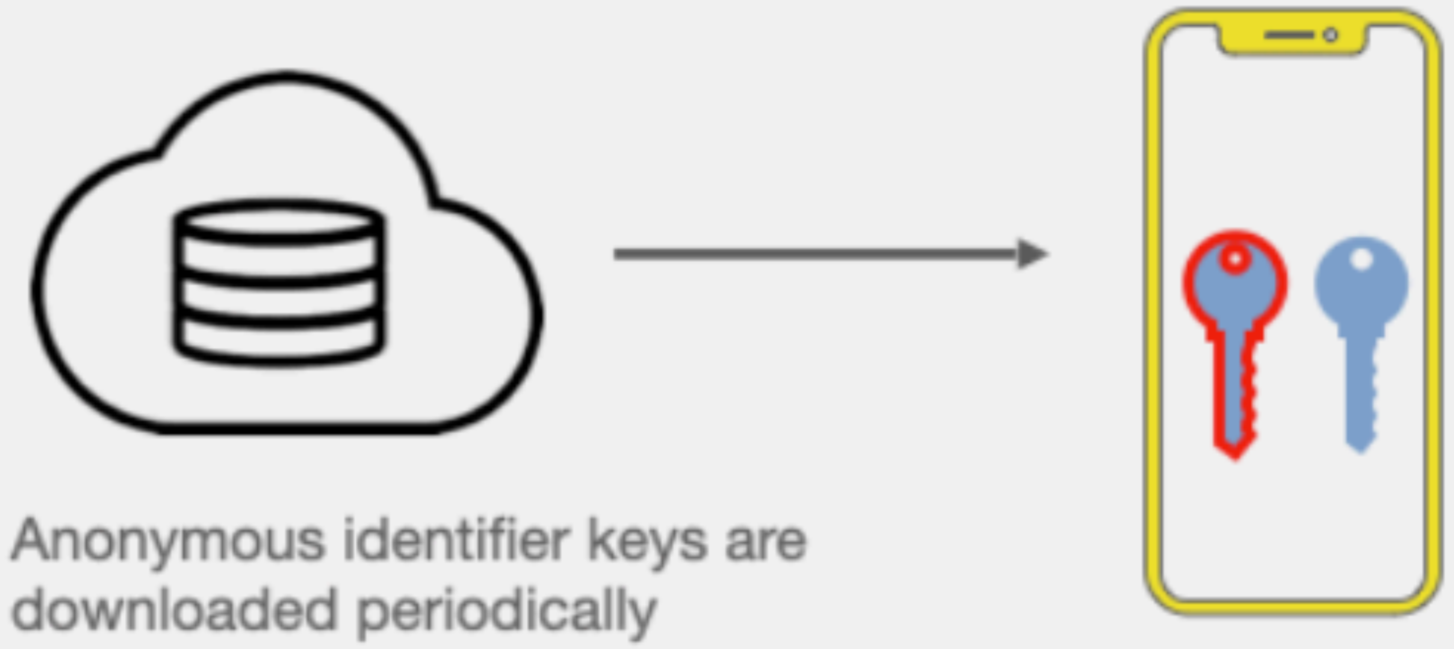
Alice sees a notification on her phone

ALERT: you have recently come in contact with someone who has tested positive for Covid-19

Tap for more information -->

Sometime later...

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



Anonymous identifier keys are downloaded periodically

A match is found

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

Additional information is provided by the health authority app

The European academic effort

PEPP-PT & DP-3T

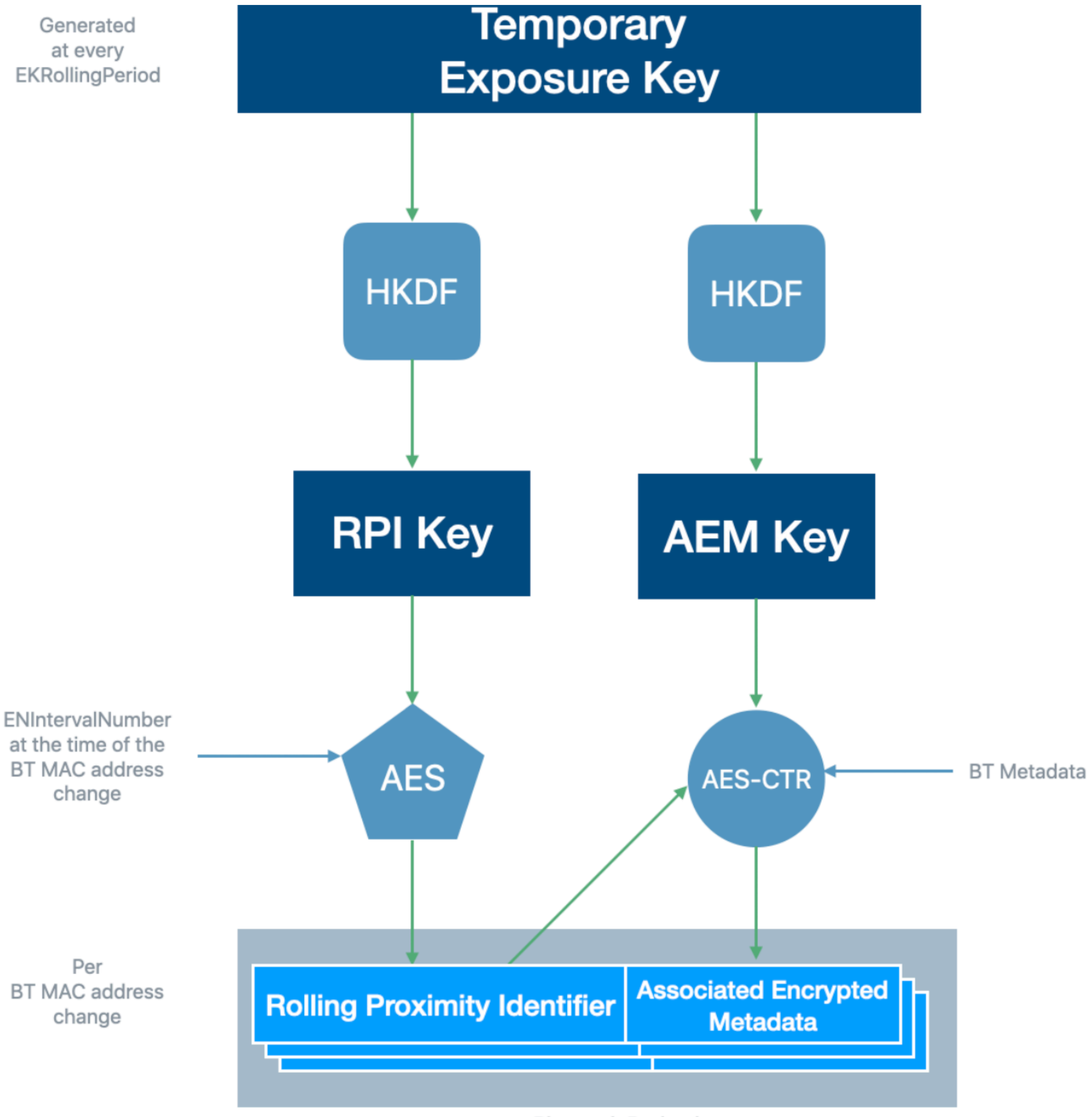
- PEPP-PT: Pan-European Privacy-Preserving Proximity Tracing
    - Centralized protocol
    - Initially supported by Germany
    - Still favored by France
- DP-3T: Decentralized Privacy-Preserving Proximity Tracing
    - Decentralized version of PEPP-PT
    - Originally developed by EPFL and ETHZ

Google

~~Privacy-Preserving Proximity Tracing~~

Exposure Notification API

- The current de-facto standard
- Similar to DP-3T
- Very low privacy footprint
- Until an exposure actually occurs, no PII leaves the device



Generated at every EKRollingPeriod

Temporary Exposure Key

HKDF

HKDF

RPI Key

AEM Key

ENIntervalNumber at the time of the BT MAC address change

AES

AES-CTR

BT Metadata

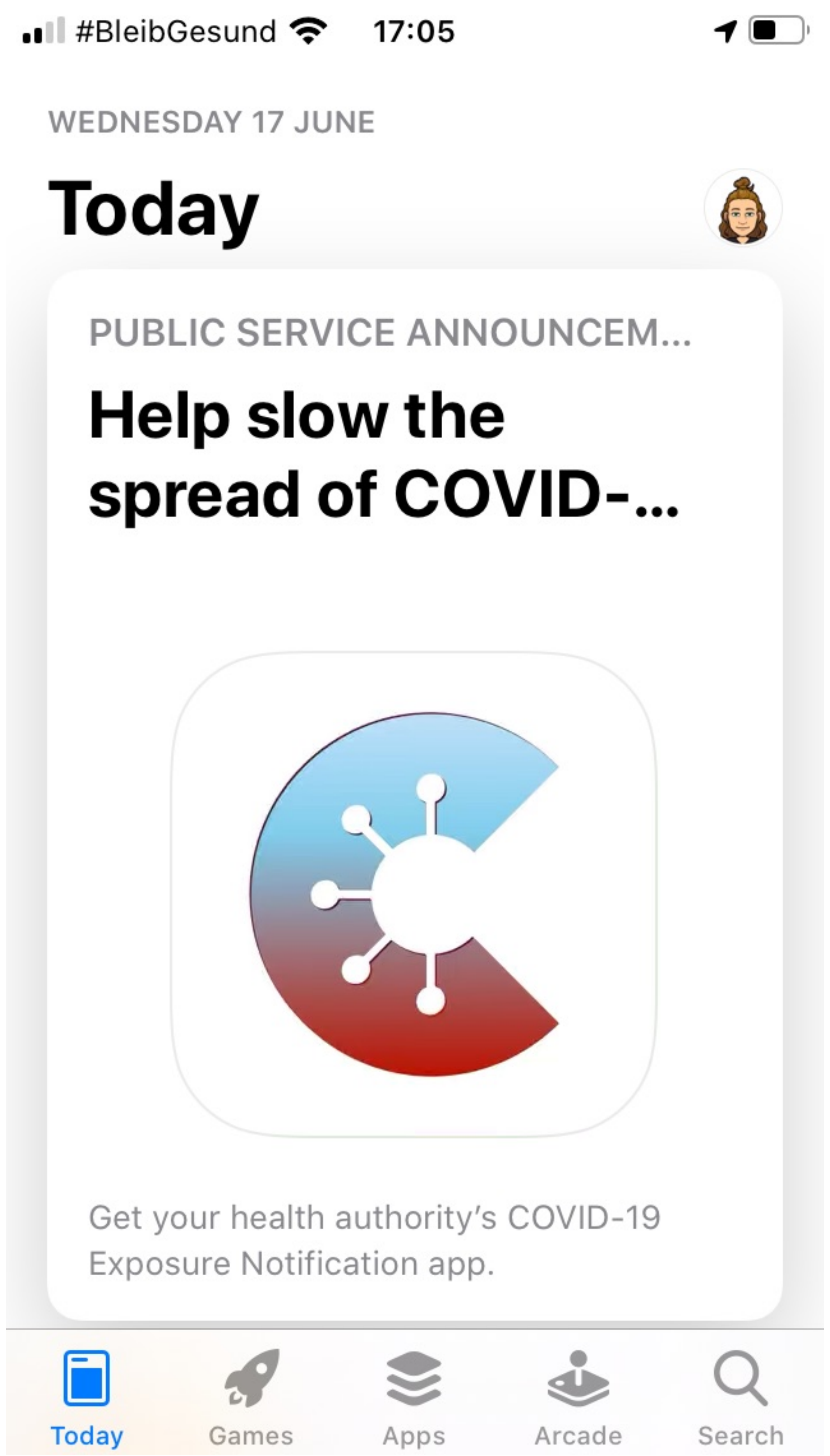
Per BT MAC address change

Rolling Proximity Identifier

Associated Encrypted Metadata

Situation in Germany

Corona-Warn-App



#BleibGesund 17:05

WEDNESDAY 17 JUNE

Today

PUBLIC SERVICE ANNOUNCEM...

Help slow the spread of COVID-...

Get your health authority's COVID-19 Exposure Notification app.

Corona-Warn-App

- Jointly developed by SAP (App) and Telekom (Infrastructure)
- Available since the 15th of June 2020
- Pretty simple interface
- Not much to see for the user

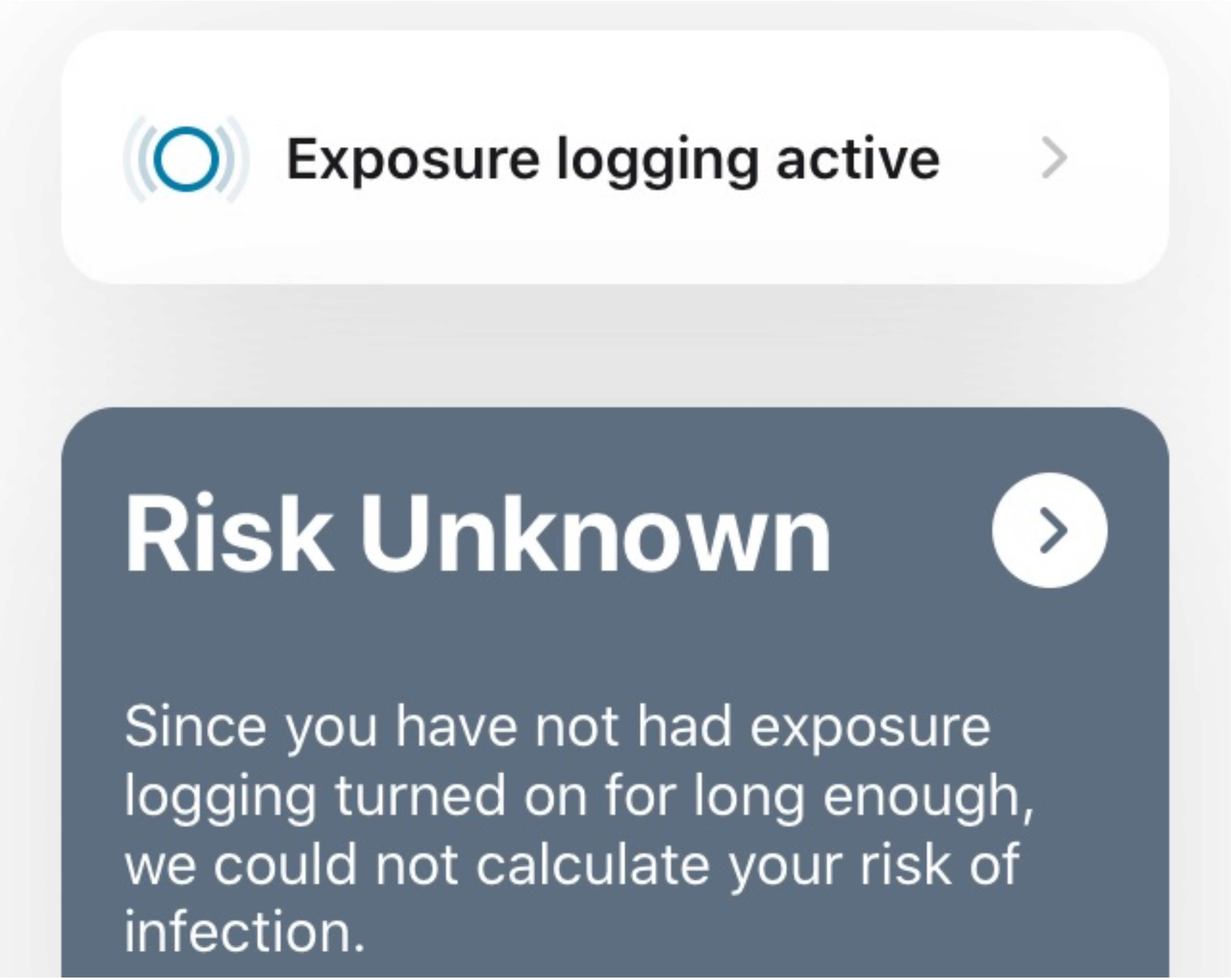
Corona-Warn-App

Let's fight Corona together

4.8 ★★★★★
26K Ratings

No1
Health & Fitness

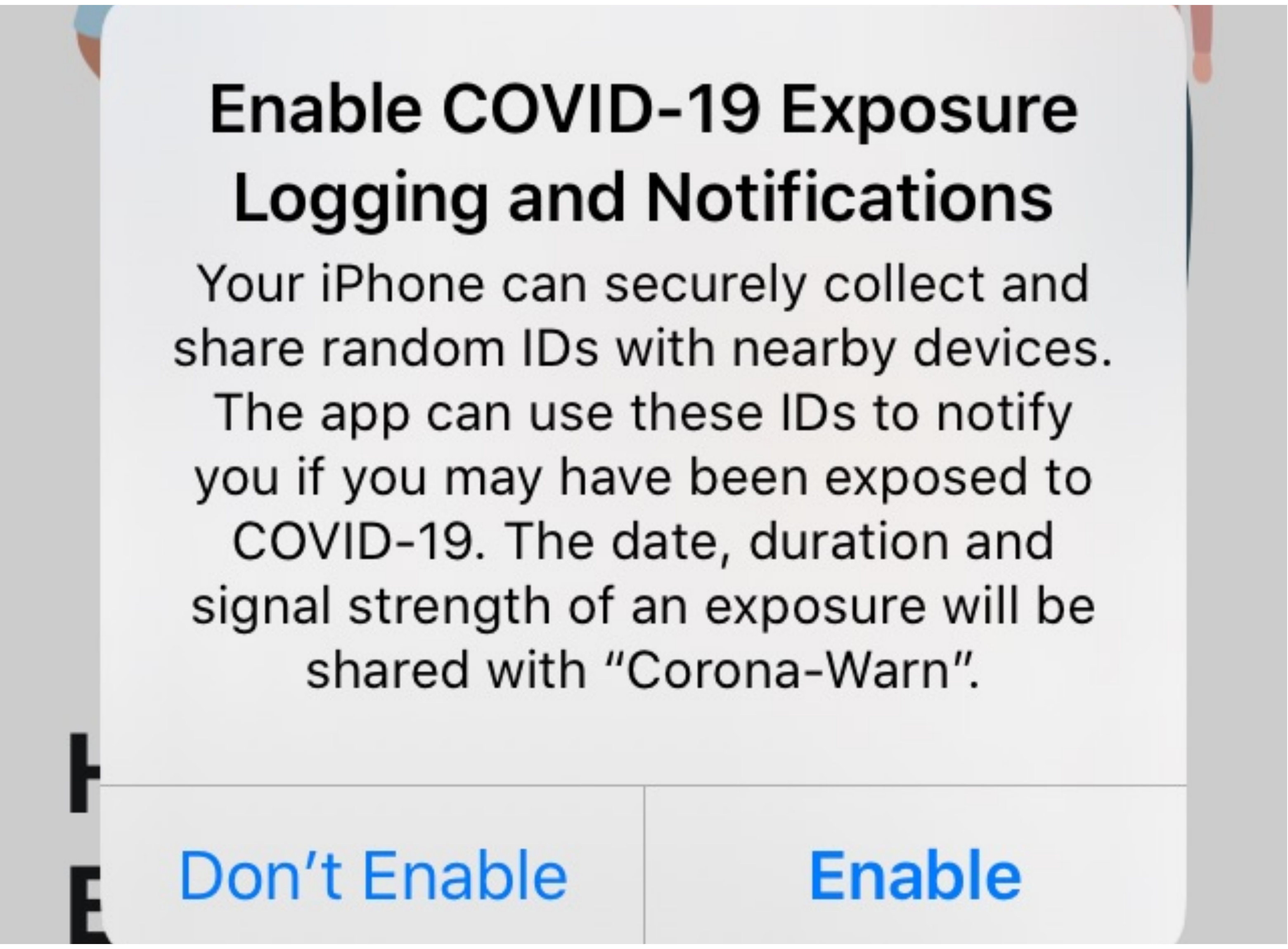
17+
Age



Exposure logging active

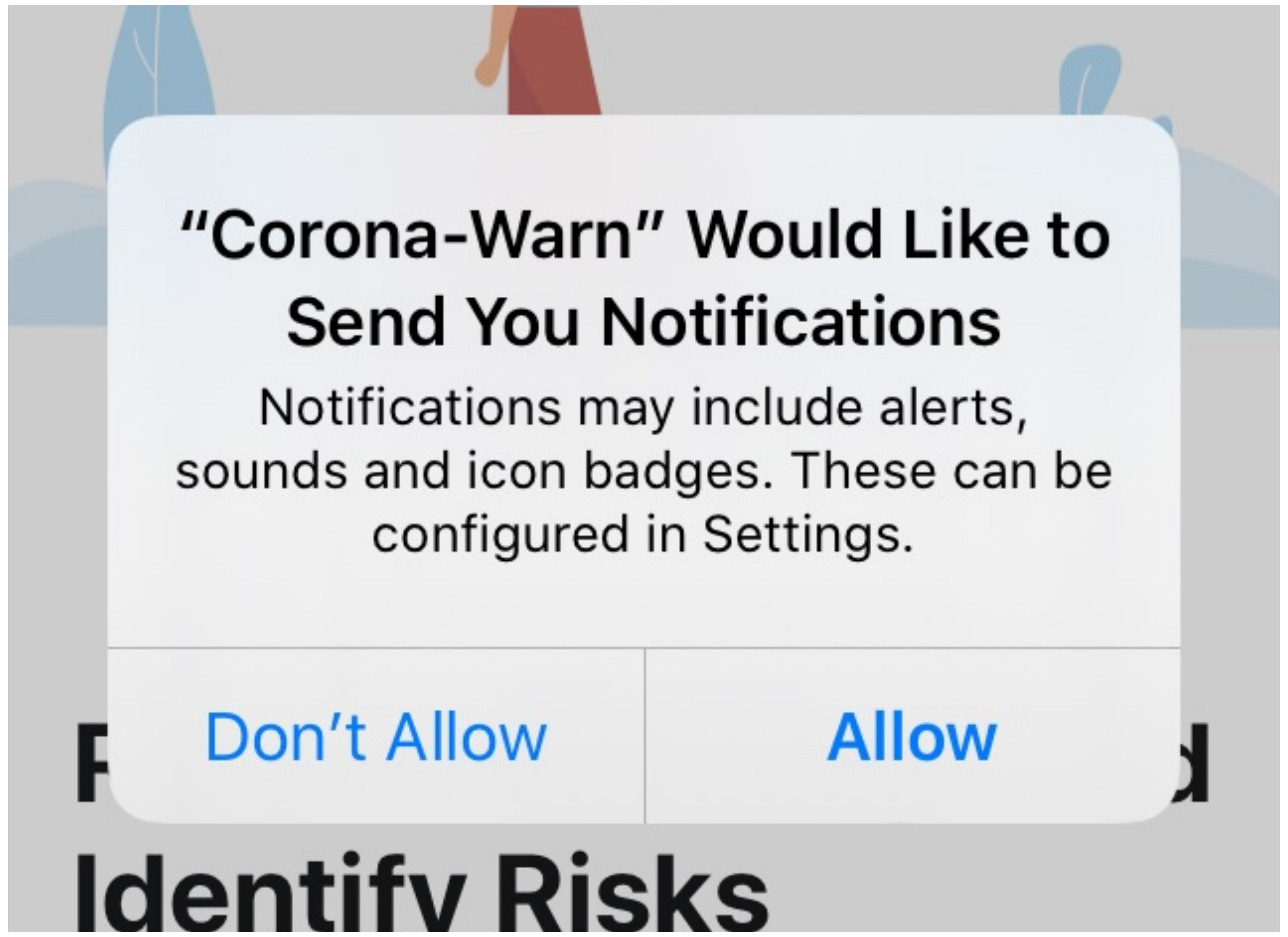
Risk Unknown

Since you have not had exposure logging turned on for long enough, we could not calculate your risk of infection.



Enable COVID-19 Exposure Logging and Notifications

Your iPhone can securely collect and share random IDs with nearby devices. The app can use these IDs to notify you if you may have been exposed to COVID-19. The date, duration and signal strength of an exposure will be shared with “Corona-Warn”.



“Corona-Warn” Would Like to Send You Notifications

Notifications may include alerts, sounds and icon badges. These can be configured in Settings.

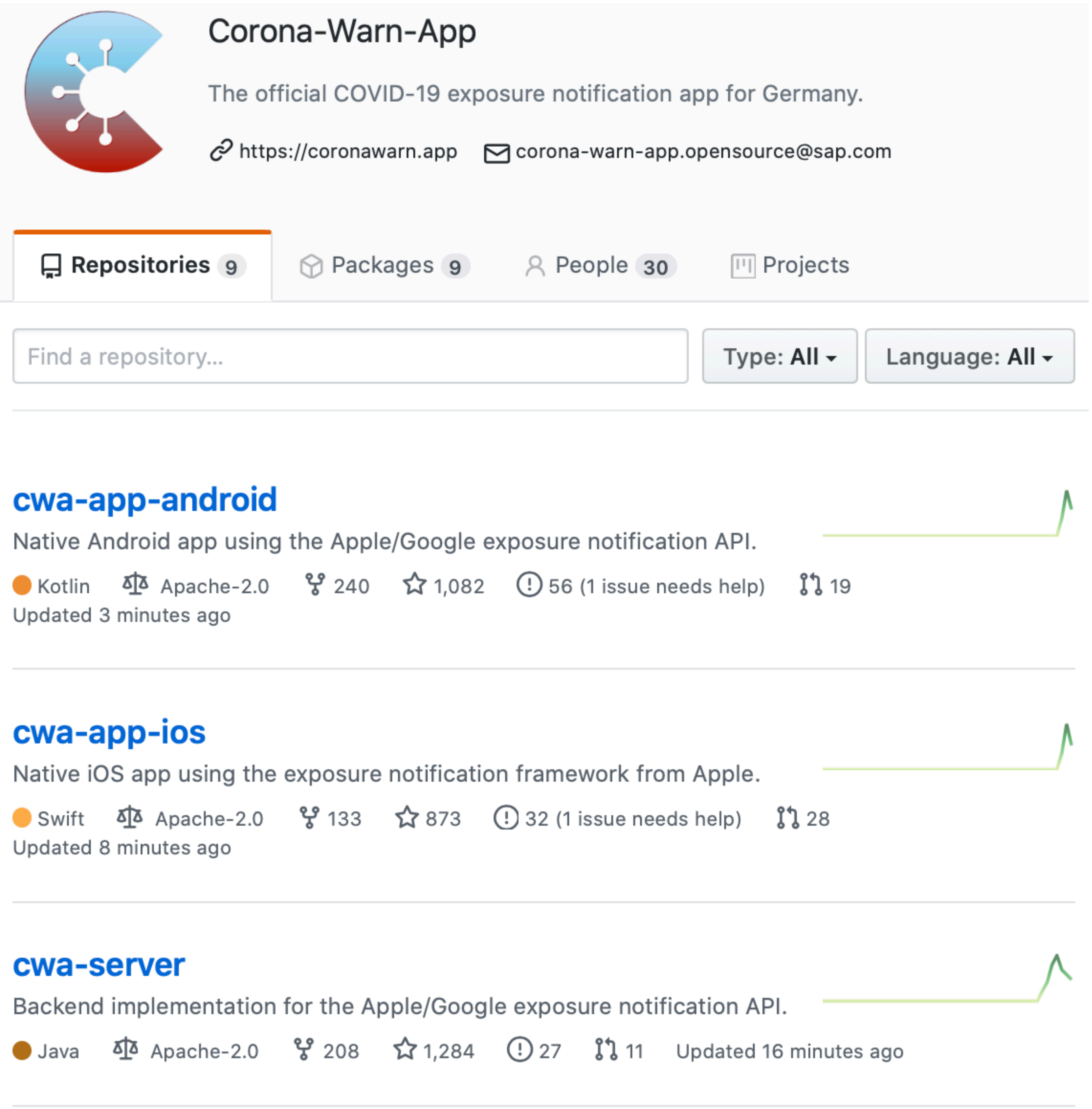
SAP®

T

Transparency:

Surprisingly Good

- Almost everything is open-source
- There is documentation
- It’s written in markdown
- Most issues are public
- Pull-requests are accepted



Corona-Warn-App

The official COVID-19 exposure notification app for Germany.

https://coronawarn.app corona-warn-app.opensource@sap.com

cwa-app-android

Native Android app using the Apple/Google exposure notification API.

● Kotlin Apache-2.0 240 ☆ 1,082 56 (1 issue needs help) 19
Updated 3 minutes ago

cwa-app-ios

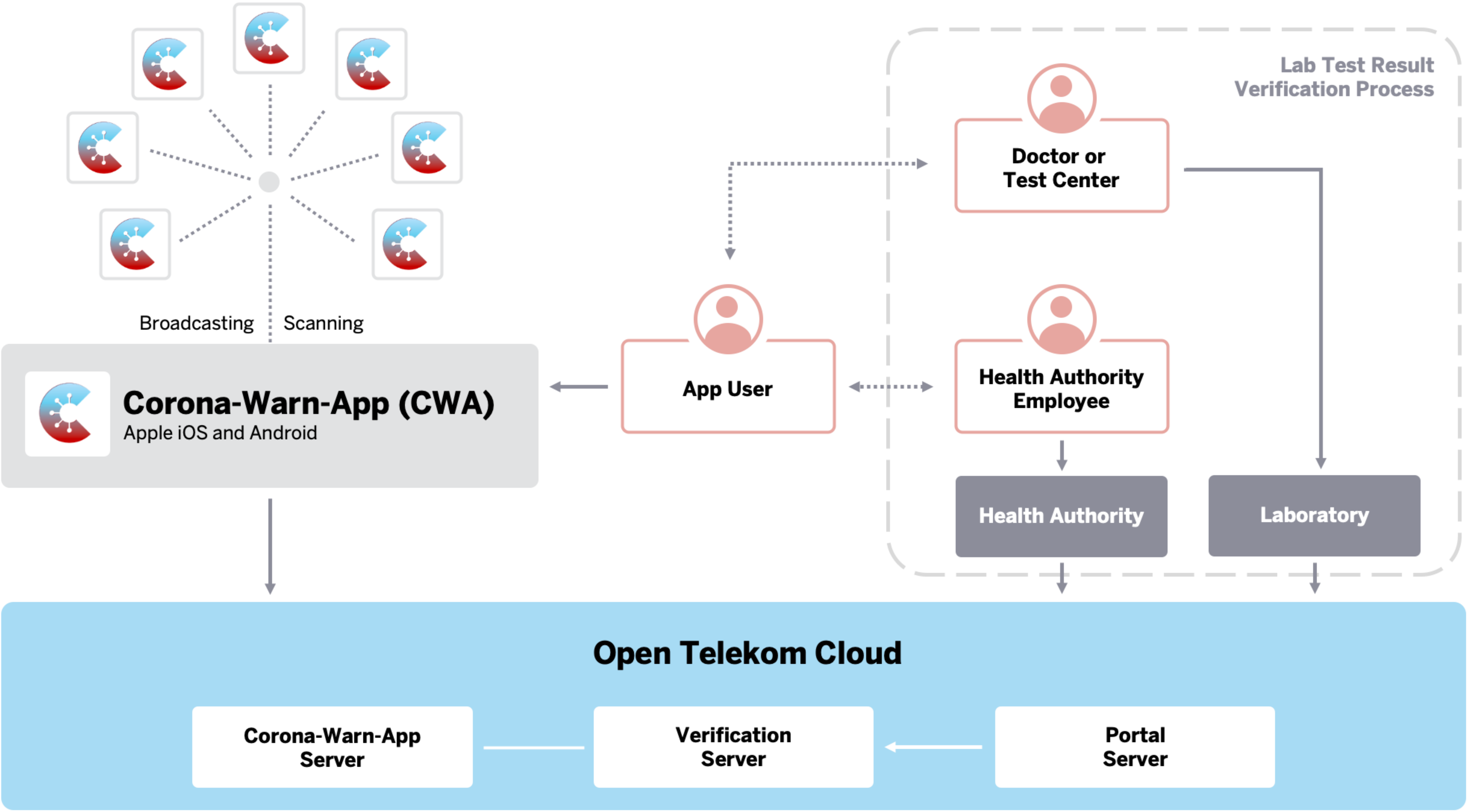
Native iOS app using the exposure notification framework from Apple.

● Swift Apache-2.0 133 ☆ 873 32 (1 issue needs help) 28
Updated 8 minutes ago

cwa-server

Backend implementation for the Apple/Google exposure notification API.

● Java Apache-2.0 208 ☆ 1,284 27 11 Updated 16 minutes ago


Broadcasting
Scanning
Corona-Warn-App (CWA)
Apple iOS and Android
App User
Lab Test Result Verification Process
Doctor or Test Center
Health Authority Employee
Health Authority
Laboratory
Open Telekom Cloud
Corona-Warn-App Server
Verification Server
Portal Server

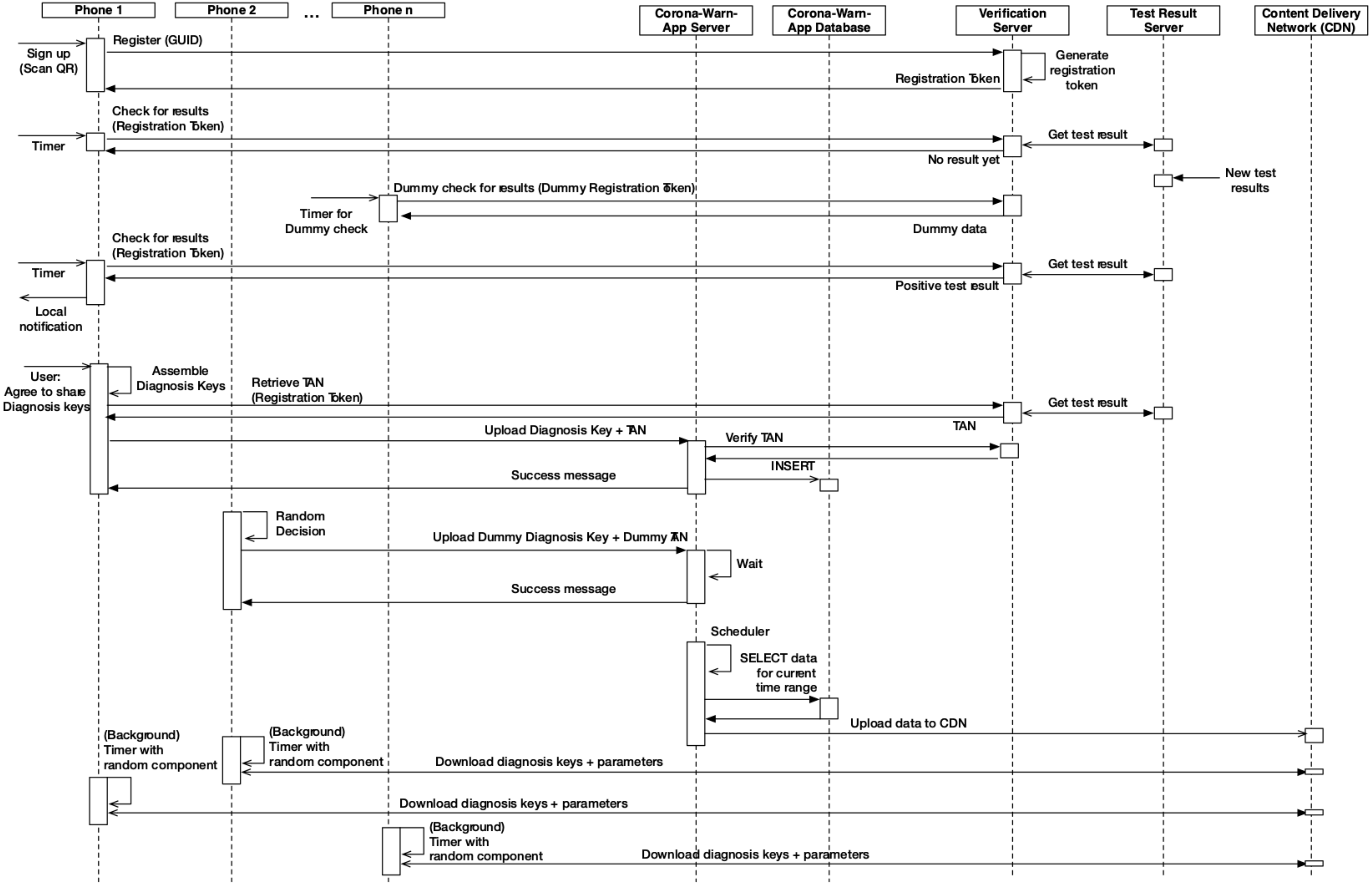
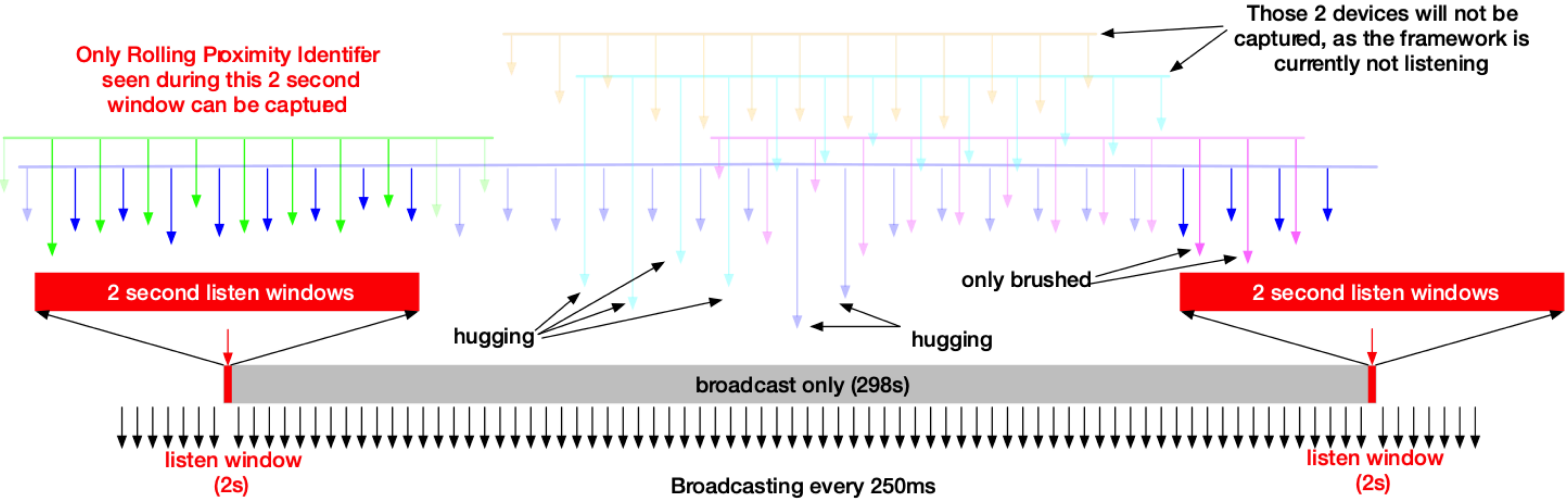

Phone 1
Phone 2
...
Phone n
Corona-Warn-App Server
Corona-Warn-App Database
Verification Server
Test Result Server
Content Delivery Network (CDN)
Sign up (Scan QR)
Register (GUID)
Generate registration token
Registration Token
Timer
Check for results (Registration Token)
Get test result
No result yet
New test results
Timer for Dummy check
Dummy check for results (Dummy Registration Token)
Dummy data
Timer
Check for results (Registration Token)
Get test result
Positive test result
Local notification
User: Agree to share Diagnosis keys
Assemble Diagnosis Keys
Retrieve TAN (Registration Token)
Get test result
TAN
Upload Diagnosis Key + TAN
Verify TAN
INSERT
Success message
Random Decision
Upload Dummy Diagnosis Key + Dummy TAN
Wait
Success message
Scheduler
SELECT data for current time range
Upload data to CDN
(Background) Timer with random component
(Background) Timer with random component
Download diagnosis keys + parameters
Download diagnosis keys + parameters
(Background) Timer with random component
Download diagnosis keys + parameters

Figure 7: Interaction of the mobile application(s) with the backend servers and CDN


Only Rolling Proximity Identifier seen during this 2 second window can be captured
Those 2 devices will not be captured, as the framework is currently not listening
2 second listen windows
hugging
hugging
only brushed
2 second listen windows
broadcast only (298s)
listen window (2s)
Broadcasting every 250ms
listen window (2s)

	Device 1	Device 2	Device 3	Device 4	Device 5
Reality	Met on the street 3 minutes, distance	Met occasionally 7 minutes, distance, but hugged in between	Stood on train platform 2 minutes, distance	Met occasionally 3 minutes, distance, hugged for prolonged time	Brushed each other at supermarket 2 seconds
Detected by phone	seen once <5 min >50dB (far)	seen twice 5 min >50dB (far)	never seen	never seen	seen once <5 min <50dB (close)

Figure 14: Limitations of the Bluetooth Low Energy approach

In summary

It's pretty good – you should install it

✓ No Central Entity to Trust

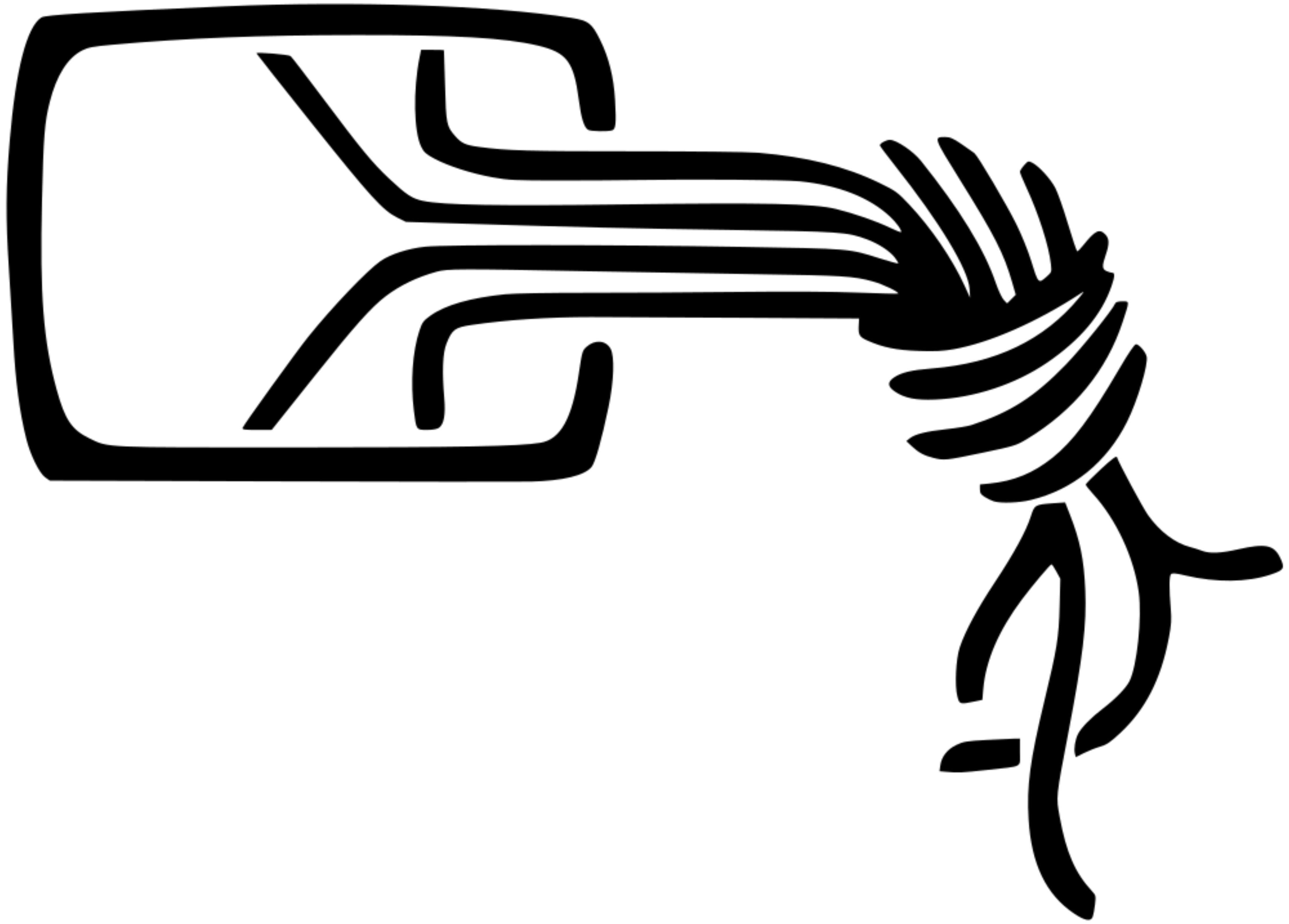
✓ Data Minimization

✓ Anonymity (Pseudonymity)

✓ No Central Movement Profiles

✓ Unlinkability

✓ Unobservability of Communication



More infos and sources

- https://ukw.fm/ukw030-die-corona-warn-app/
- https://github.com/corona-warn-app/cwa-documentation
- https://www.apple.com/covid19/contacttracing
- https://www.google.com/covid19/exposurenotifications/