# Epidose
# Contact tracing for all

**Greek Open Technologies Alliance**
**www.eellak.gr**

**Diomidis Spinellis (GFOSS, AUEB, TUDelft)**
**www.spinellis.gr**

EUROPEAN OPEN SCIENCE CLOUD



1

## Overview

- Non-profit organization established in 2008 with shareholders its members
- Members: 31 Universities and Research Centers
- Board of Directors (9 members)
- Scientific Committee (27 members)
- 8 working groups (>300 members)
  - policy
  - software
  - content


2

# Our objectives

***Develop and promote***

- Open source software
- Open standards
- Open content
- Open data
- Open governance
- Open educational resources
- Open hardware and design

3

# Our methods

- Workshops and hackathons
- Cooperate with established communities
- Prototyping
- Working groups
- Prepare and promote policy proposals
- Disseminate information regarding openness


4

# Partners and projects

GFOSS Open Technologies Alliance

creative commons Greece

Open Government Partnership

fablab Athens

enterprise europe network

NODE ATHENS

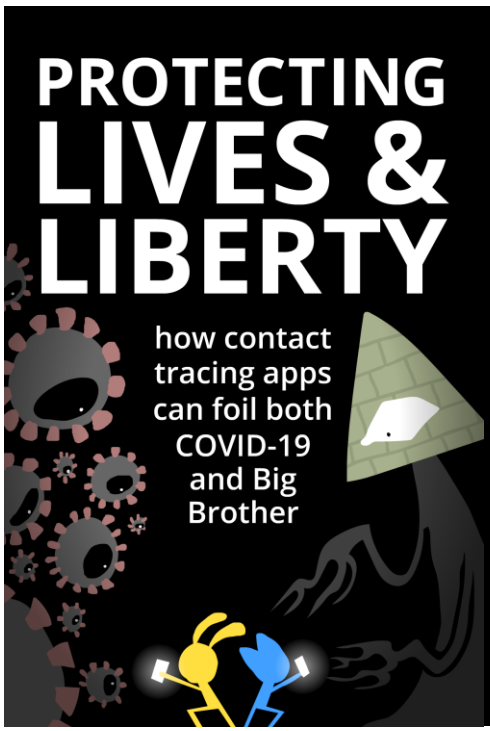
COMMUNIA
The European Thematic Network on the Digital Public Domain

YourDataStories

IBP INTERNATIONAL BUDGET PARTNERSHIP
Open Budgets. Transform Lives.

HOMER
Harmonising Open data in the Mediterranean through better access and Reuse of public sector information

5




- Contact tracing
- Issues with smartphones
- Epidose design
- Implementation

6

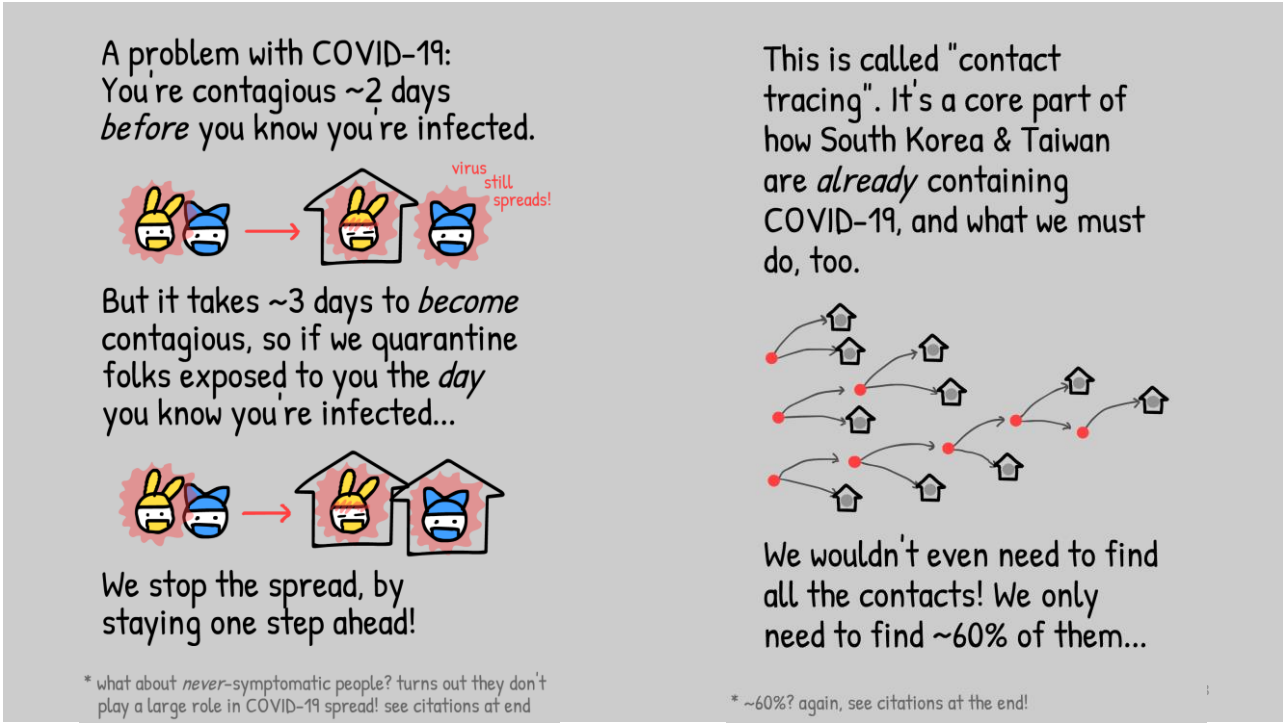
6

# DP3T — Decentralized Privacy-Preserving Proximity Tracing

- **EPFL**: Prof. Carmela Troncoso, Prof. Mathias Payer, Prof. Jean-Pierre Hubaux, Prof. Marcel Salathé, Prof. James Larus, Prof. Edouard Bugnion, Dr. Wouter Lueks, Theresa Stadler, Dr. Apostolos Pyrgelis, Dr. Daniele Antonioli, Ludovic Barman, Sylvain Chatel
- **ETHZ**: Prof. Kenneth Paterson, Prof. Srdjan Capkun, Prof. David Basin, Dr. Jan Beutel, Dennis Jackson
- **KU Leuven**: Prof. Bart Preneel, Prof. Nigel Smart, Dr. Dave Singelee, Dr. Aysajan Abidin
- **TU Delft**: Prof. Seda Gürses
- **University College London**: Dr. Michael Veale
- **CISPA Helmholtz Center for Information Security**: Prof. Cas Cremers, Prof. Michael Backes, Dr. Nils Ole Tippenhauer
- **University of Oxford**: Dr. Reuben Binns
- **University of Torino / ISI Foundation**: Prof. Ciro Cattuto
- **Aix Marseille Univ, Université de Toulon, CNRS, CPT**: Dr. Alain Barrat
- **University of Salerno**: Prof. Giuseppe Persiano
- **IMDEA Software**: Prof. Dario Fiore
- **University of Porto (FCUP) and INESC TEC**: Prof. Manuel Barbosa
- **Stanford University**: Prof. Dan Boneh

7

7




8

...but we *do* need to find them quickly. Traditional contact tracing, with interviews, is too slow.

Hence, why we need contact tracing *apps.*

But do we have to sacrifice privacy for health?


9

9

It's entirely possible to protect peoples' lives AND liberties, with a really simple process!

Let's see how it works, with the help of Alice & Bob...

10

10

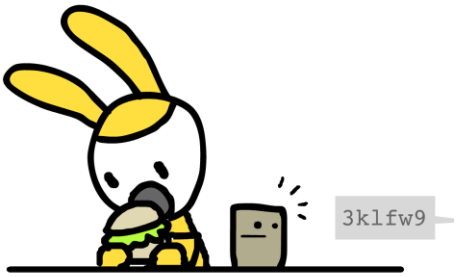
Alice gets a tracing app! (& its code is open to the public, so folks can verify it in fact does the following...)


Every 5 minutes, her phone says uniquely random gibberish to all nearby devices, using Bluetooth.

* 5 minutes is just an example! and technically it's "pseudo-random," since it's not quantum... does NOT matter.

11

Because the messages are random & don't use GPS, they contain NO INFO about Alice's identity, location or anything.




Now - while her phone sends out random messages, it also *listens* for messages from nearby phones.

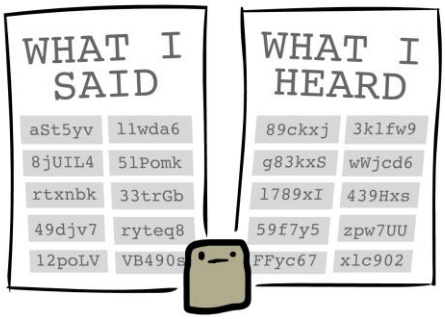
For example, Bob's.

Bob also has a privacy-first tracing app, that's compatible with (or the same as) Alice's.


If Alice & Bob stay close to each other for 5+ minutes, their phones will exchange unique gibberish.

12

Both their phones remember all the messages they said & heard over the last 14 days.




Again: because the random messages contain NO INFO, Alice's privacy is protected from Bob, and vice versa!

* 14 days is also just an example! epidemiologists may learn that the "infectious period" is actually shorter or longer.

The next day, Alice develops a dry cough and fever.

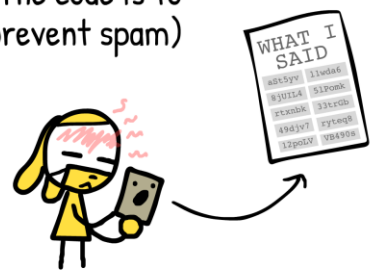
Alice gets tested.

Alice has COVID-19.

It is not a good day for Alice.

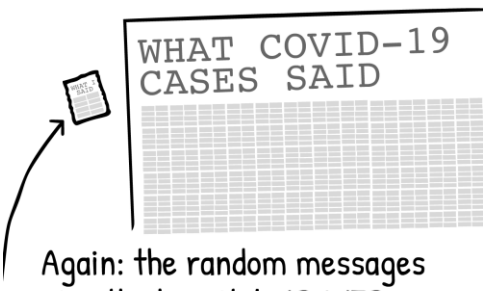
13

But she shan't suffer in vain! Alice uploads her "What I Said" messages to a hospital database, using a one-time passcode given by her doctor. (The code is to prevent spam)




Alice can also *hide* messages from times she wants to keep private, like evenings at home!

The database stores Alice's gibberish:

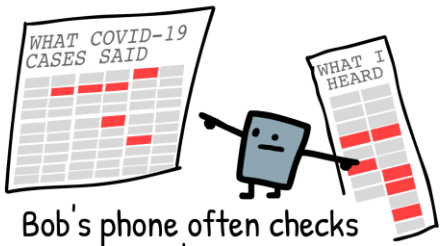



Again: the random messages give the hospital NO INFO on where Alice was, who she was with, what they were doing, or even *how many* people Alice met! It's meaningless to the hospital...

* different countries' hospitals could exchange messages, but because they contain no info, no privacy is lost.

14

...but not to Bob!




Bob's phone often checks the hospital's list of random messages from COVID-19 cases, and see if it "heard" any of them from nearby phones in the last 14 days.

(The gibberish gives Bob NO OTHER PERSONAL INFO.)

* the real DP-3T protocol is even MORE secure! it uses a "cuckoo filter" so phones know ONLY the covid-19 messages they heard, without revealing ALL covid-19 messages.

If it heard, say, 6 or more COVID-19 cases' messages (6 x 5 min = 30 min total exposure), the phone warns Bob to self-quarantine.

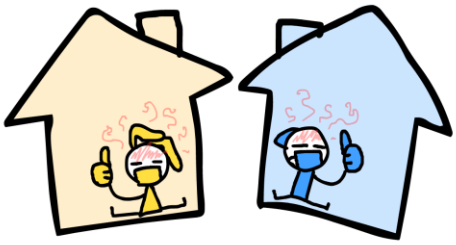
And thus, Bob cuts the chain of transmission - one step ahead of the virus!

* again, these numbers are just examples!

15

And that's it!

That's how digital contact tracing can proactively prevent the spread of COVID-19 *while also* protecting our rights.



Thanks, Alice & Bob!
Stay safe.

16

Google

**Exposure Notification**

**Bluetooth Specification**

Preliminary — Subject to Modification and Extension

April 2020

v1.2



Contents



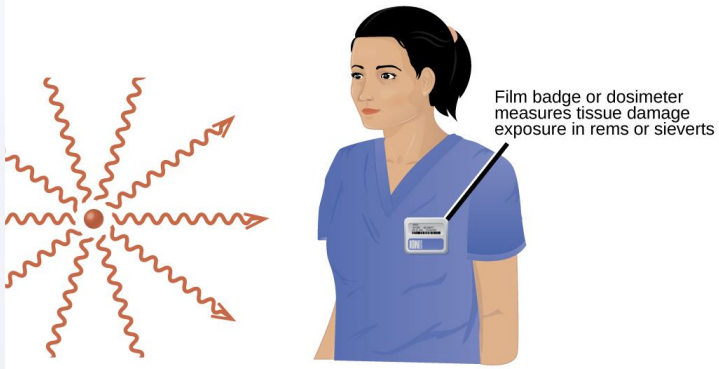


16


WAZNI MOBILE SHO

17


RADEX
0.17
MENU
OFF
QUARTA

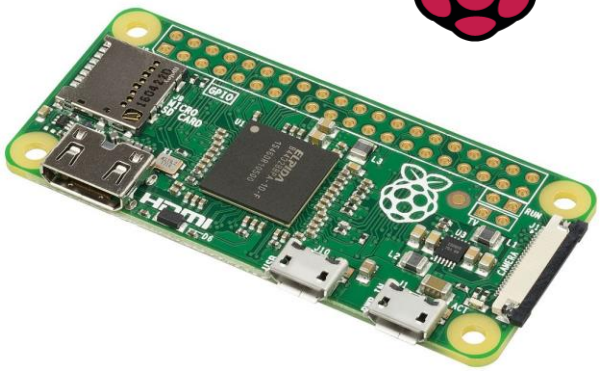

Film badge or dosimeter measures tissue damage exposure in rems or sieverts
Rate of radioactive decay measured in bequerels or curies
Absorbed dose measured in grays or rads

18

18

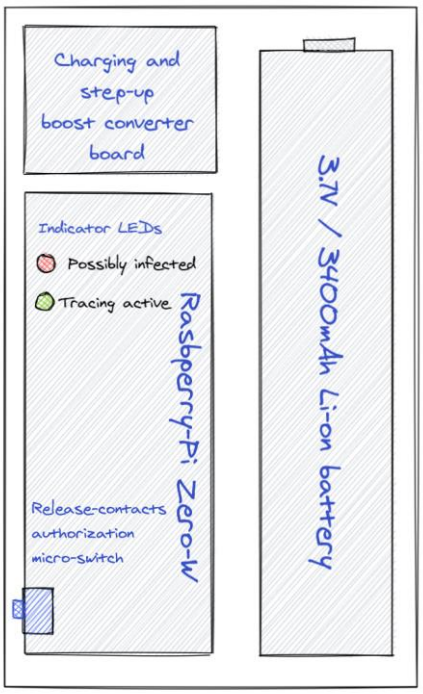
# Raspberry Pi Zero W

- 1GHz, single-core CPU
- 512MB RAM
- HAT-compatible 40-pin header
- 802.11 b/g/n wireless LAN
- Bluetooth 4.1
- Bluetooth Low Energy (BLE)
- Runs Linux
- Cost: $10



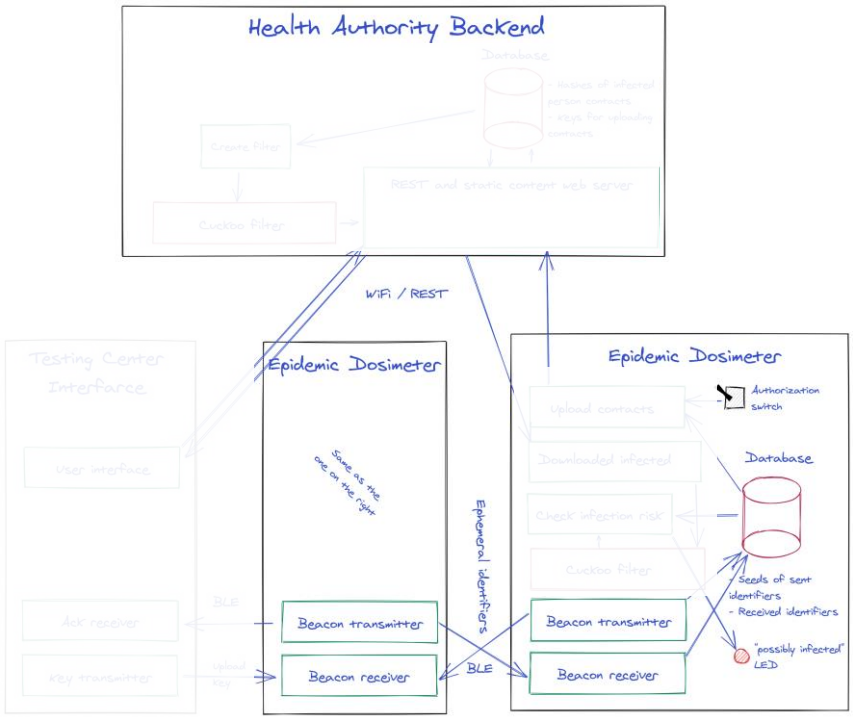
19

19




20

20




21



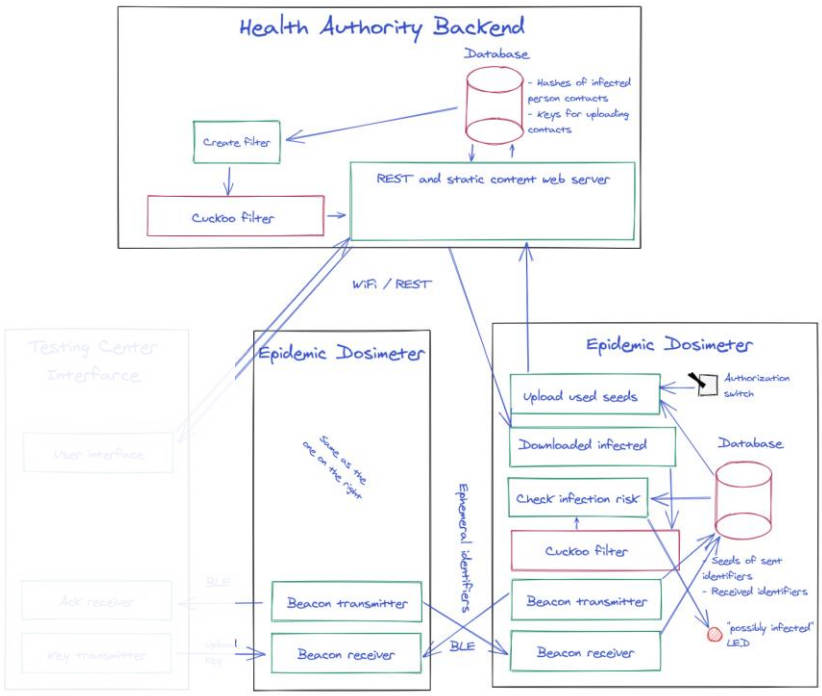
zero-wdds

```
2020-05-29 10:44:48,299: Got ephid 42ed52cf531ce647b4b35aa5622ad716 RSSI -34
2020-05-29 10:44:49,583: Got ephid 42ed52cf531ce647b4b35aa5622ad716 RSSI -51
2020-05-29 10:44:50,866: Got ephid 42ed52cf531ce647b4b35aa5622ad716 RSSI -48
2020-05-29 10:44:52,145: Got ephid 42ed52cf531ce647b4b35aa5622ad716 RSSI -50
2020-05-29 10:44:53,427: Got ephid 42ed52cf531ce647b4b35aa5622ad716 RSSI -51
2020-05-29 10:44:54,708: Got ephid 42ed52cf531ce647b4b35aa5622ad716 RSSI -49
2020-05-29 10:44:55,990: Got ephid 42ed52cf531ce647b4b35aa5622ad716 RSSI -50
2020-05-29 10:44:57,275: Got ephid 42ed52cf531ce647b4b35aa5622ad716 RSSI -48
2020-05-29 10:44:58,557: Got ephid 42ed52cf531ce647b4b35aa5622ad716 RSSI -52
2020-05-29 10:44:59,837: Got ephid 42ed52cf531ce647b4b35aa5622ad716 RSSI -48
2020-05-29 10:45:00,097: hcitool -i hci0 cmd 0x08 0x0008 1c 02 01 1a 03 03 6f fd
 13 16 6f fd 53 c0 13 80 01 e0 6a 9f d8 b1 9e 9e dd 12 88 6a c0 01
2020-05-29 10:45:00,124: Change ephid to 53c0138001e06a9fd8b19e9edd12886a
2020-05-29 10:45:01,117: Got ephid 389e88eed9c5581f95dd1d832114fdee RSSI -49
2020-05-29 10:45:02,398: Got ephid 389e88eed9c5581f95dd1d832114fdee RSSI -51
2020-05-29 10:45:04,957: Got ephid 389e88eed9c5581f95dd1d832114fdee RSSI -49
2020-05-29 10:45:06,238: Got ephid 389e88eed9c5581f95dd1d832114fdee RSSI -51
2020-05-29 10:45:07,519: Got ephid 389e88eed9c5581f95dd1d832114fdee RSSI -48
2020-05-29 10:45:08,798: Got ephid 389e88eed9c5581f95dd1d832114fdee RSSI -50
2020-05-29 10:45:10,079: Got ephid 389e88eed9c5581f95dd1d832114fdee RSSI -51
2020-05-29 10:45:11,363: Got ephid 389e88eed9c5581f95dd1d832114fdee RSSI -34
2020-05-29 10:45:12,643: Got ephid 389e88eed9c5581f95dd1d832114fdee RSSI -48
2020-05-29 10:45:13,923: Got ephid 389e88eed9c5581f95dd1d832114fdee RSSI -46
2020-05-29 10:45:15,205: Got ephid 389e88eed9c5581f95dd1d832114fdee RSSI -51
```

generic:e

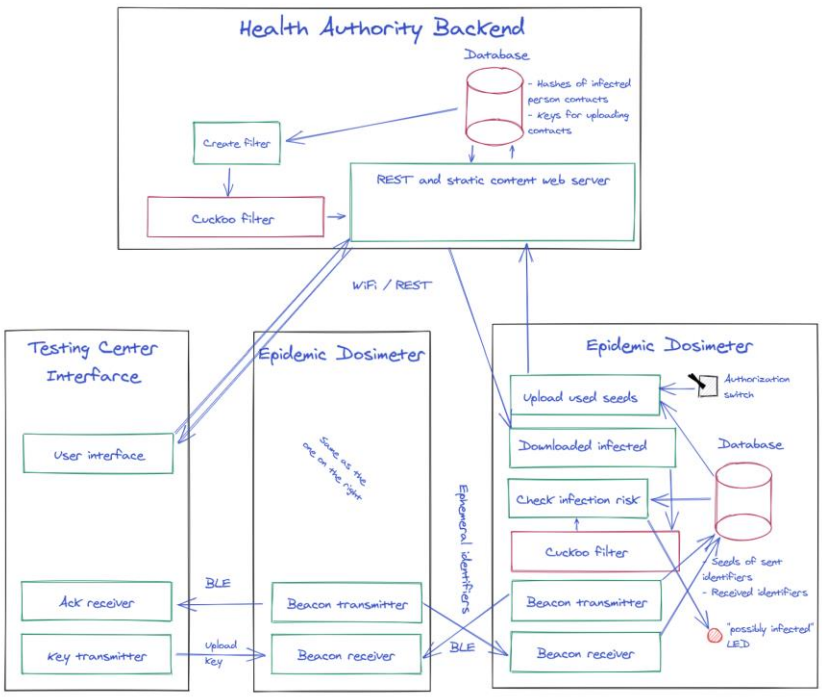
```
2020-05-29 10:44:45,354: Got ephid d06994cc4d55a3aff0bb1fa2dc6148b4 RSSI -35
2020-05-29 10:44:46,639: Got ephid d06994cc4d55a3aff0bb1fa2dc6148b4 RSSI -38
2020-05-29 10:44:47,921: Got ephid d06994cc4d55a3aff0bb1fa2dc6148b4 RSSI -40
2020-05-29 10:44:49,202: Got ephid d06994cc4d55a3aff0bb1fa2dc6148b4 RSSI -39
2020-05-29 10:44:50,485: Got ephid d06994cc4d55a3aff0bb1fa2dc6148b4 RSSI -38
2020-05-29 10:44:54,328: Got ephid d06994cc4d55a3aff0bb1fa2dc6148b4 RSSI -39
2020-05-29 10:44:55,609: Got ephid d06994cc4d55a3aff0bb1fa2dc6148b4 RSSI -38
2020-05-29 10:44:56,894: Got ephid d06994cc4d55a3aff0bb1fa2dc6148b4 RSSI -39
2020-05-29 10:44:58,175: Got ephid d06994cc4d55a3aff0bb1fa2dc6148b4 RSSI -39
2020-05-29 10:44:59,458: Got ephid d06994cc4d55a3aff0bb1fa2dc6148b4 RSSI -39
2020-05-29 10:45:00,248: hcitool -i hci0 cmd 0x08 0x0008 1c 02 01 1a 03 03 6f fd
 13 16 6f fd 38 9e 88 ee d9 c5 58 1f 95 dd 1d 83 21 14 fd ee c0 01
2020-05-29 10:45:00,262: Change ephid to 389e88eed9c5581f95dd1d832114fdee
2020-05-29 10:45:02,022: Got ephid 53c0138001e06a9fd8b19e9edd12886a RSSI -34
2020-05-29 10:45:03,303: Got ephid 53c0138001e06a9fd8b19e9edd12886a RSSI -39
2020-05-29 10:45:04,584: Got ephid 53c0138001e06a9fd8b19e9edd12886a RSSI -37
2020-05-29 10:45:05,865: Got ephid 53c0138001e06a9fd8b19e9edd12886a RSSI -34
2020-05-29 10:45:07,150: Got ephid 53c0138001e06a9fd8b19e9edd12886a RSSI -34
2020-05-29 10:45:08,433: Got ephid 53c0138001e06a9fd8b19e9edd12886a RSSI -39
2020-05-29 10:45:09,713: Got ephid 53c0138001e06a9fd8b19e9edd12886a RSSI -38
2020-05-29 10:45:10,992: Got ephid 53c0138001e06a9fd8b19e9edd12886a RSSI -34
2020-05-29 10:45:14,840: Got ephid 53c0138001e06a9fd8b19e9edd12886a RSSI -38
2020-05-29 10:45:16,125: Got ephid 53c0138001e06a9fd8b19e9edd12886a RSSI -39
2020-05-29 10:45:17,406: Got ephid 53c0138001e06a9fd8b19e9edd12886a RSSI -39
```

22


Health Authority Backend
Database
- Hashes of infected person contacts
- keys for uploading contacts
Create filter
Cuckoo filter
REST and static content web server
WiFi / REST
Testing Center Interface
User interface
Ack receiver
Key transmitter
Epidemic Dosimeter
Same as the one on the right
Beacon transmitter
Beacon receiver
BLE
Upload Key
Ephemeral identifiers
Epidemic Dosimeter
Upload used seeds
Authorization switch
Downloaded infected
Database
Check infection risk
Cuckoo filter
Seeds of sent identifiers
- Received identifiers
Beacon transmitter
Beacon receiver
BLE
"possibly infected" LED

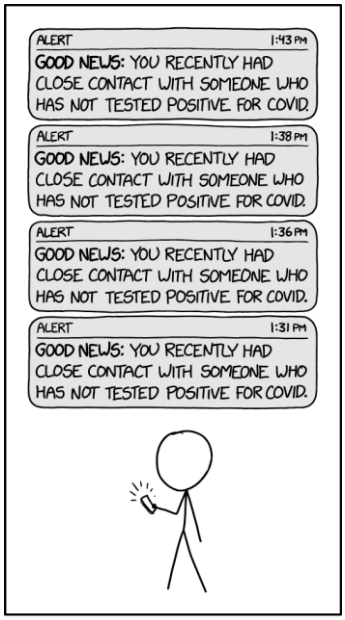
23

23


Health Authority Backend
Database
- Hashes of infected person contacts
- keys for uploading contacts
Create filter
Cuckoo filter
REST and static content web server
WiFi / REST
Testing Center Interface
User interface
Ack receiver
Key transmitter
BLE
Upload Key
Epidemic Dosimeter
Same as the one on the right
Beacon transmitter
Beacon receiver
Ephemeral identifiers
Epidemic Dosimeter
Upload used seeds
Authorization switch
Downloaded infected
Database
Check infection risk
Cuckoo filter
Seeds of sent identifiers
- Received identifiers
Beacon transmitter
Beacon receiver
BLE
"possibly infected" LED

24

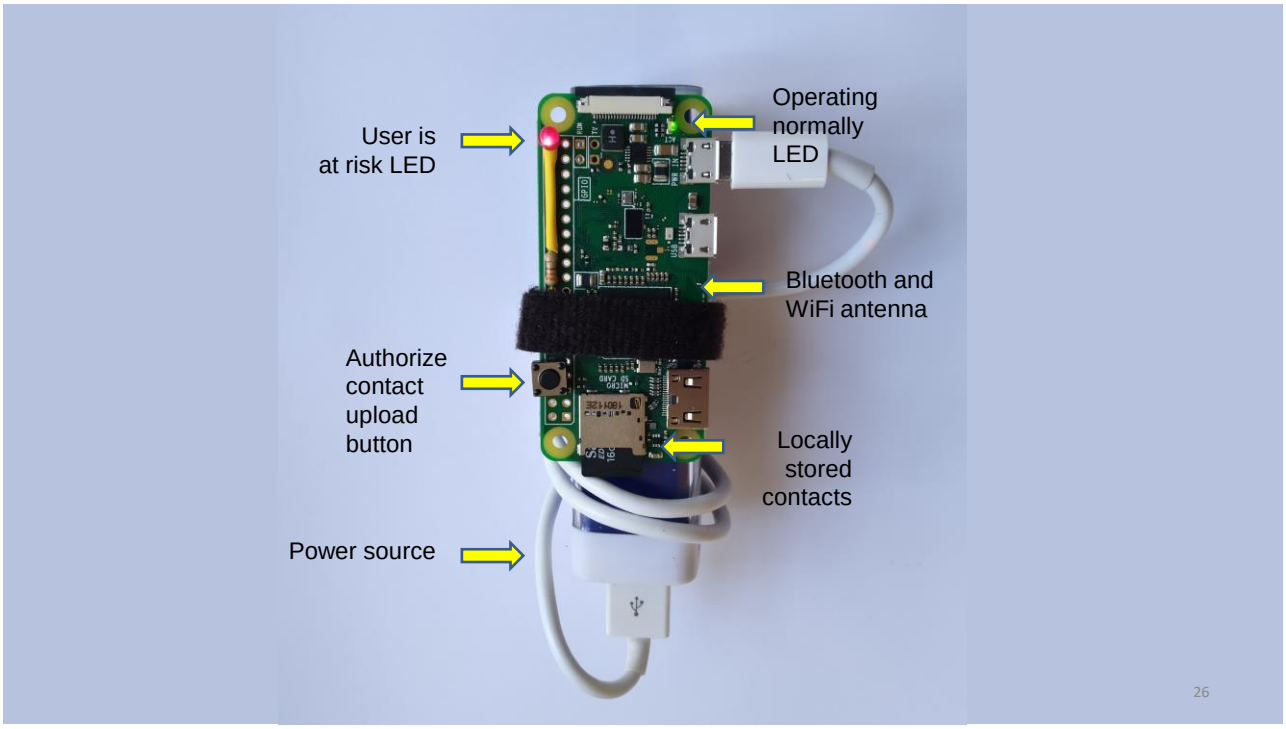
24



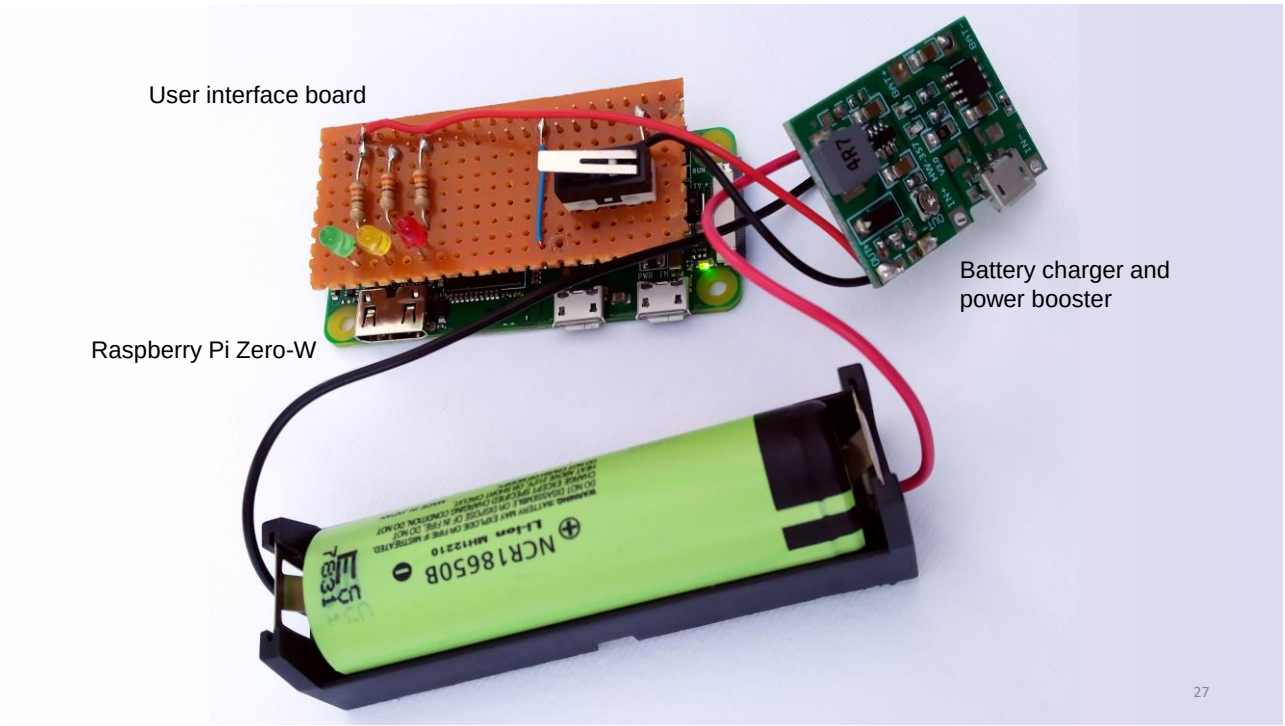

NO ONE LIKES MY NEW COVID EXPOSURE NOTIFICATION APP

25

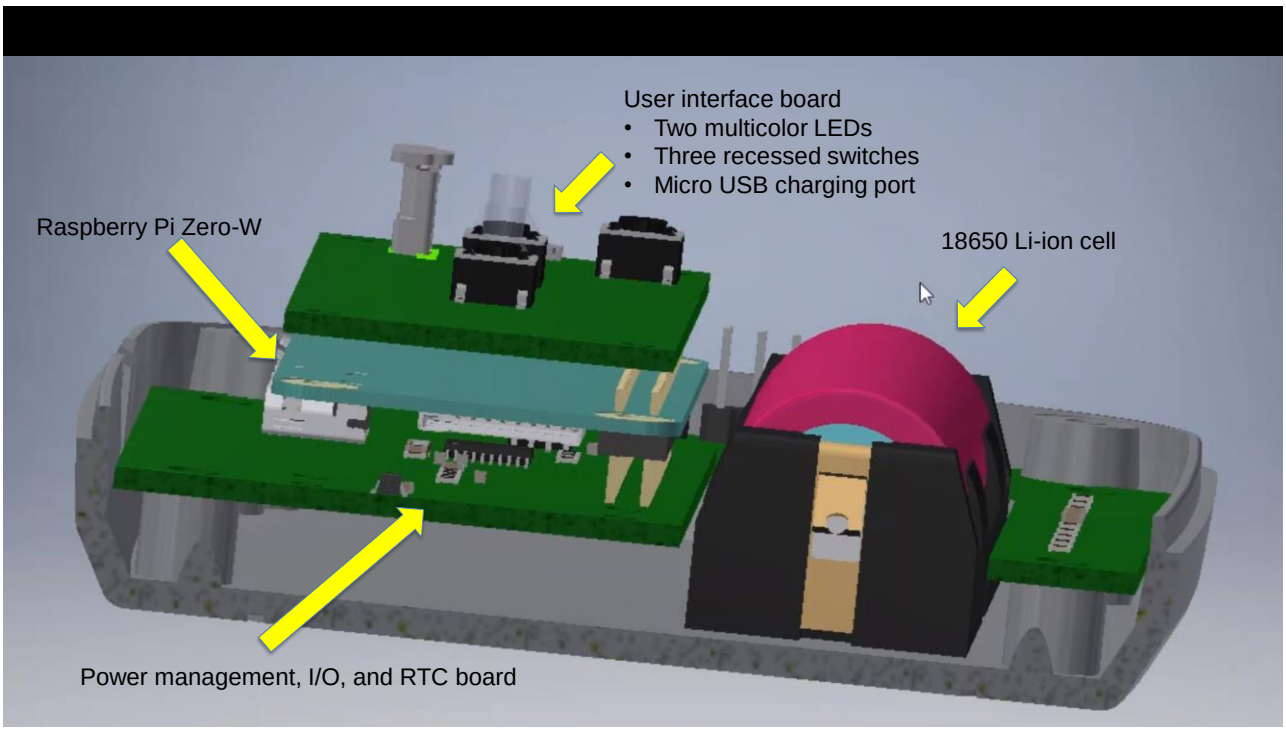
25



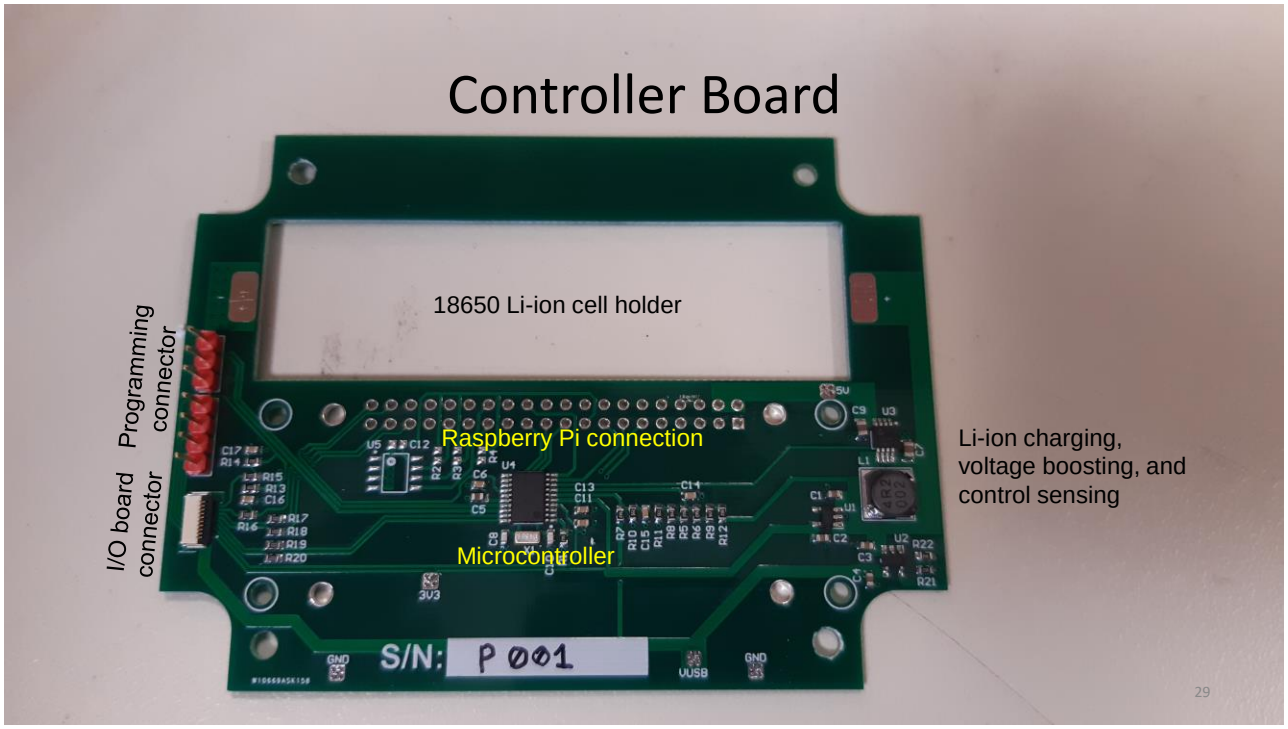

26


User interface board
Battery charger and
power booster
Raspberry Pi Zero-W
27

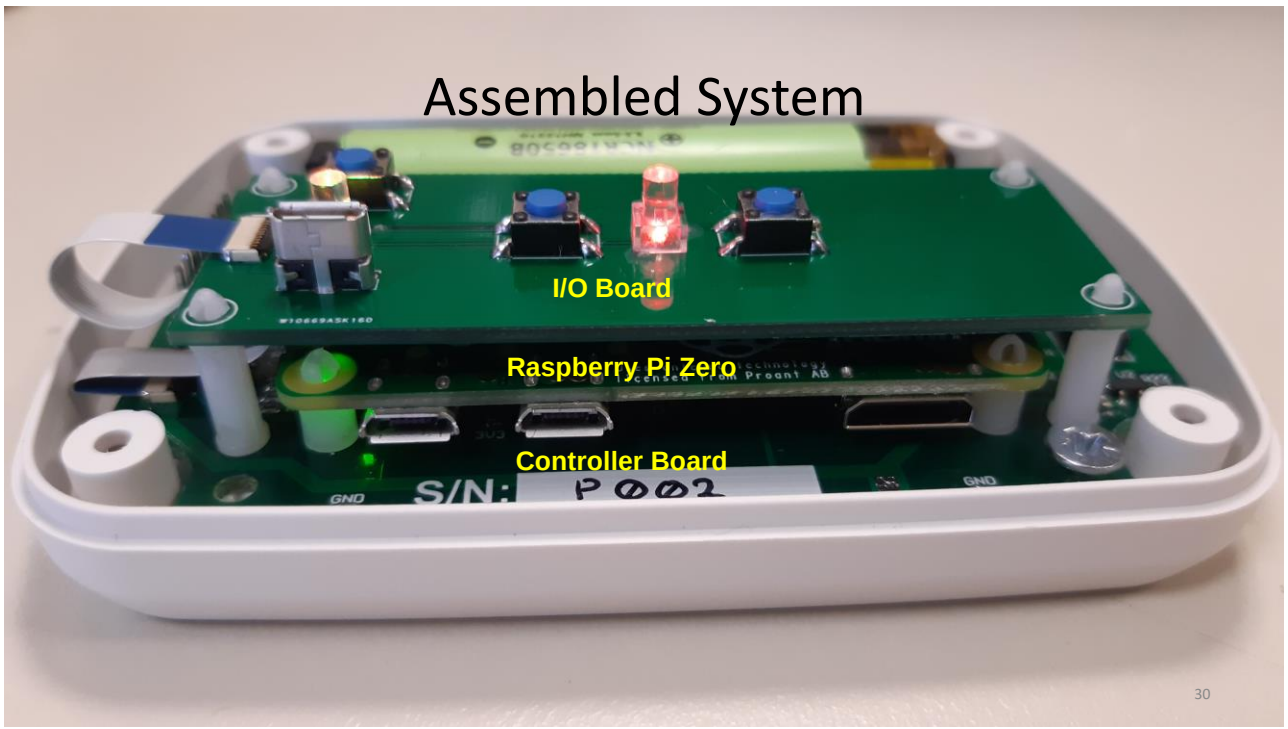
27


User interface board
• Two multicolor LEDs
• Three recessed switches
• Micro USB charging port
Raspberry Pi Zero-W
18650 Li-ion cell
Power management, I/O, and RTC board

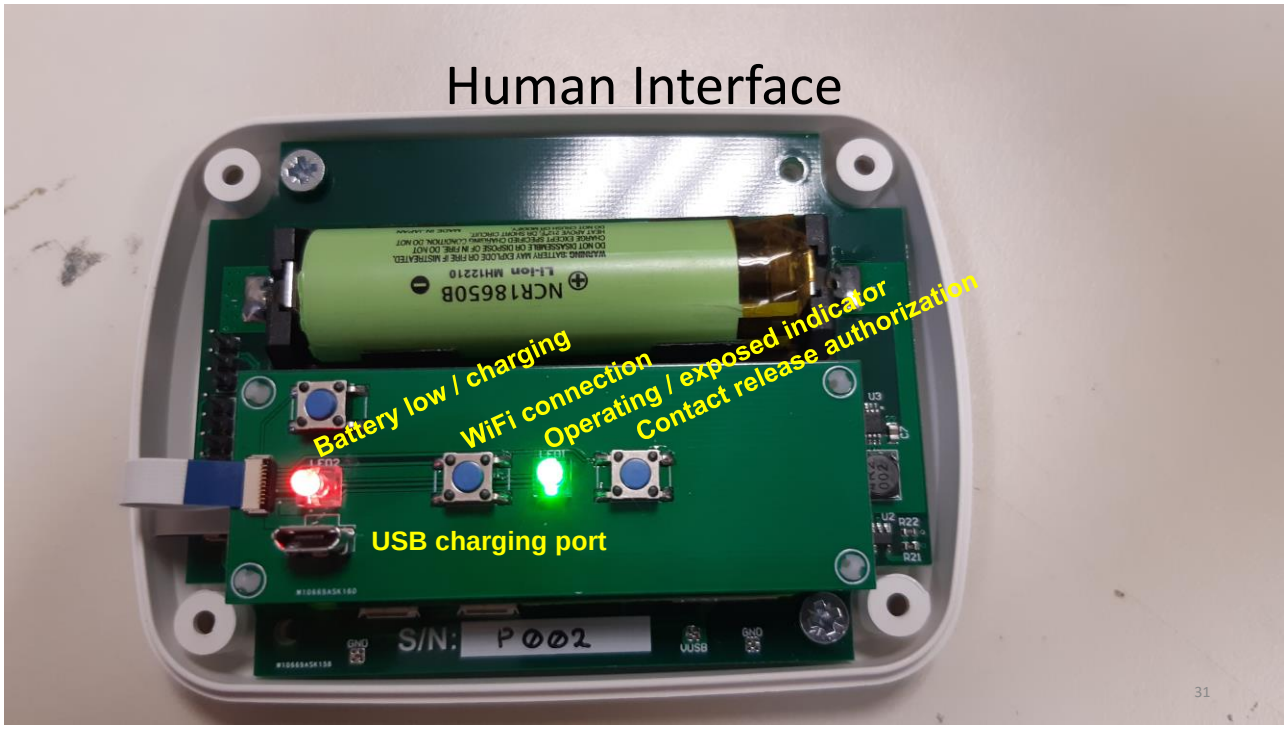
28


Controller Board
18650 Li-ion cell holder
Programming connector
I/O board connector
Raspberry Pi connection
Microcontroller
Li-ion charging, voltage boosting, and control sensing
S/N: P001
29

29


Assembled System
I/O Board
Raspberry Pi Zero
Controller Board
S/N: P002
30

30




31

# Nest steps: **verification**

- Verify functionality prototype boards
- Interface with new boards
  - User interface
  - Power management
  - Real time clock
- Implement mesh networking for cuckoo filter distribution
- Optimize power consumption
- Fine-tune software for production

32

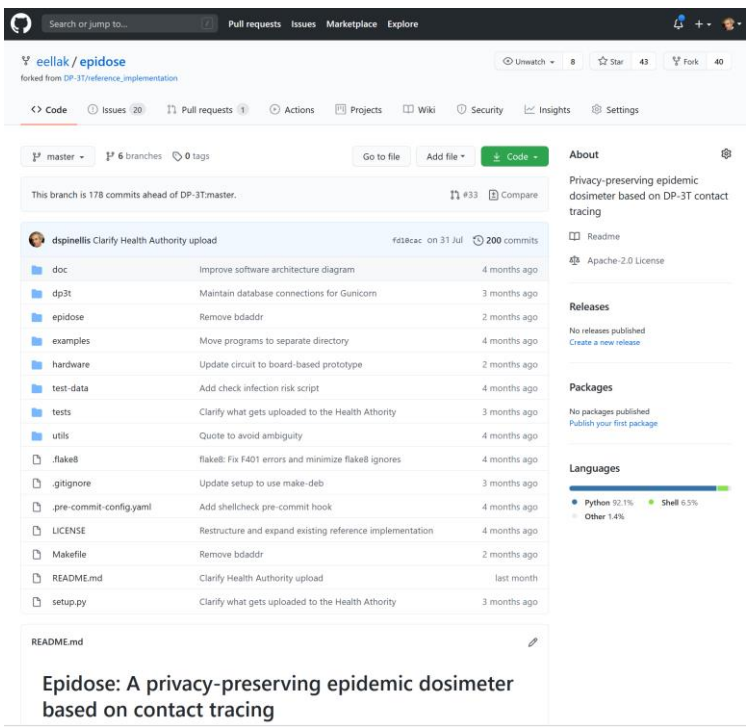
32

# Nest steps: **validation**

- Run Health Authority server on EOSC Compute Cloud, e.g.:
  - Jelastic Platform-as-a-Service
  - SWITCHengines
  - de.NBI Cloud: Cloud Computing for Life Sciences
  - CSC ePouta
- Mass-produce 100 prototypes
- Design adoption study
- Distribute devices to the general population
- Monitor device adoption and usage in the field

33

33




34

34

# Thank you!

**Greek Open Technologies Alliance**
**www.eellak.gr**

**Epidose repository**
**https://github.com/eellak/epidose**

EUROPEAN OPEN SCIENCE CLOUD

**Diomidis Spinellis**
**www.spinellis.gr**



35