

Epidose

Ιχνηλάτηση επαφών για όλους

Οργανισμός Ανοιχτών Τεχνολογιών
www.eellak.gr

Διομήδης Σπινέλλης (ΕΕΛΛΑΚ, ΟΠΑ, TUDelft)
www.spinellis.gr



Οργανισμός

- Μη κερδοσκοπικός οργανισμός που ιδρύθηκε το 2008
- Μέλη: 31 Ακαδημαϊκά Ιδρύματα, Ερευνητικά Κέντρα και Κοινωφελής Οργανισμοί
- Διοικητικό Συμβούλιο (9 μέλη)
- Επιστημονική επιτροπή (27 μέλη)
- 8 ομάδες εργασίας(>300 μέλη)
 - πολιτική
 - λογισμικό
 - περιεχόμενο





Ανάπτυξη και Προώθηση

- ✓ Ανοιχτών Προτύπων
- ✓ Ανοιχτού Λογισμικού
- ✓ Ανοιχτού Περιεχομένου
- ✓ Ανοιχτών Δεδομένων
- ✓ Ανοιχτής Διακυβέρνησης
- ✓ Ανοιχτών Εκπαιδευτικών Πηγών
- ✓ Αδειών Creative Commons
- ✓ Τεχνολογιών Ανοιχτού Υλικού & Σχεδίων
(open hardware & design)



Πώς?

- ✓ Διοργάνωση Ημερίδων / Hackathons
- ✓ Συνεργασίες με Κοινότητες
- ✓ Ομάδες Εργασίας
- ✓ Προτάσεις Πολιτικής
- ✓ Ενημέρωση σε θέματα που αφορούν την ανοιχτότητα



Έργα/Συνεργασίες



Project co-financed by the European
Regional Development Fund



Project co-financed by the European
Regional Development Fund



ΠΡΟΣΤΑΤΕΥΟΝΤΑΣ ΖΩΕΣ & ΕΛΕΥΘΕΡΙΕΣ

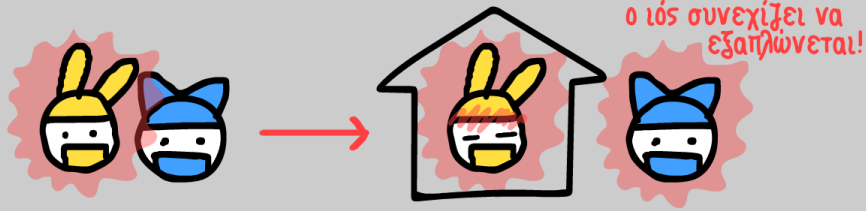
πώς τα app
ιχνηλάτησης
επαφών
μπορούν να
εμποδίσουν και
την COVID-19
και τον Μεγάλο
Αδελφό

- Ιχνηλάτηση Επαφών
- Προβλήματα με smartphones
- Σχεδιασμός Epidose
- Υλοποίηση

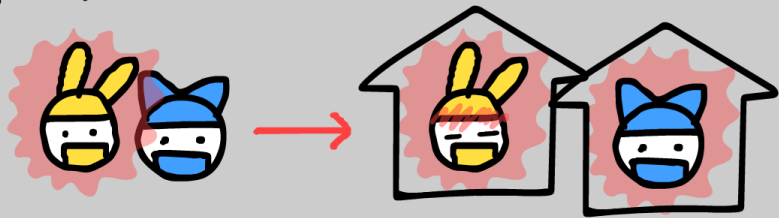
DP3T — Αποκεντρωμένη Προστασία της Ιδιωτικότητας – Ανίχνευση Εγγύτητας

- **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

Το πρόβλημα με την COVID-19:
Είσαι μεταδοτικός/η ~2 μέρες
πριν μάθεις ότι έχεις προσβληθεί.

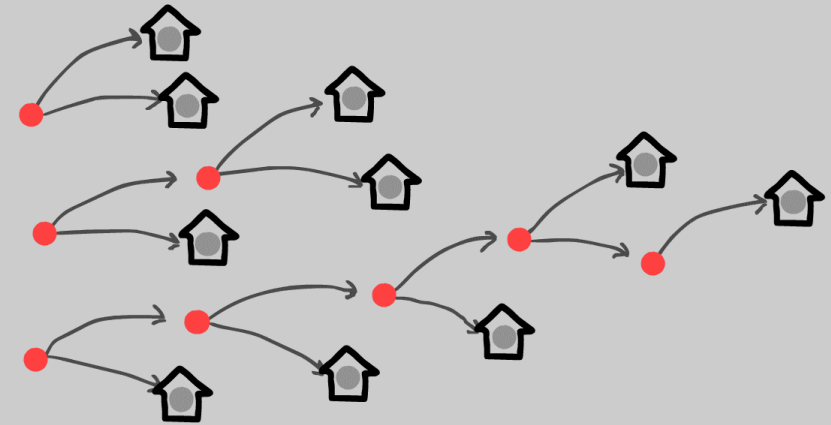


Θέλει όμως ~3 μέρες για να γίνεις
μεταδοτικός/η, άρα αν μπουν σε
καραντίνα όσοι εκτεθούν σε σένα την
ίδια μέρα που μάθεις ότι έχεις
προσβληθεί...



Σταματάμε την εξάπλωση, καθώς
είμαστε ένα βήμα μπροστά!

Αυτό ονομάζεται "ιχνηλάτηση
επαφών". Αποτελεί βασικό
μέρος του πώς η Νότια Κορέα
και η Ταϊβάν ήδη περιορίζουν
την COVID-19, και του τι
πρέπει να κάνουμε κι εμείς.



Δεν χρειάζεται καν να βρούμε
όλες τις επαφές! Αρκεί να
βρούμε το ~60%...

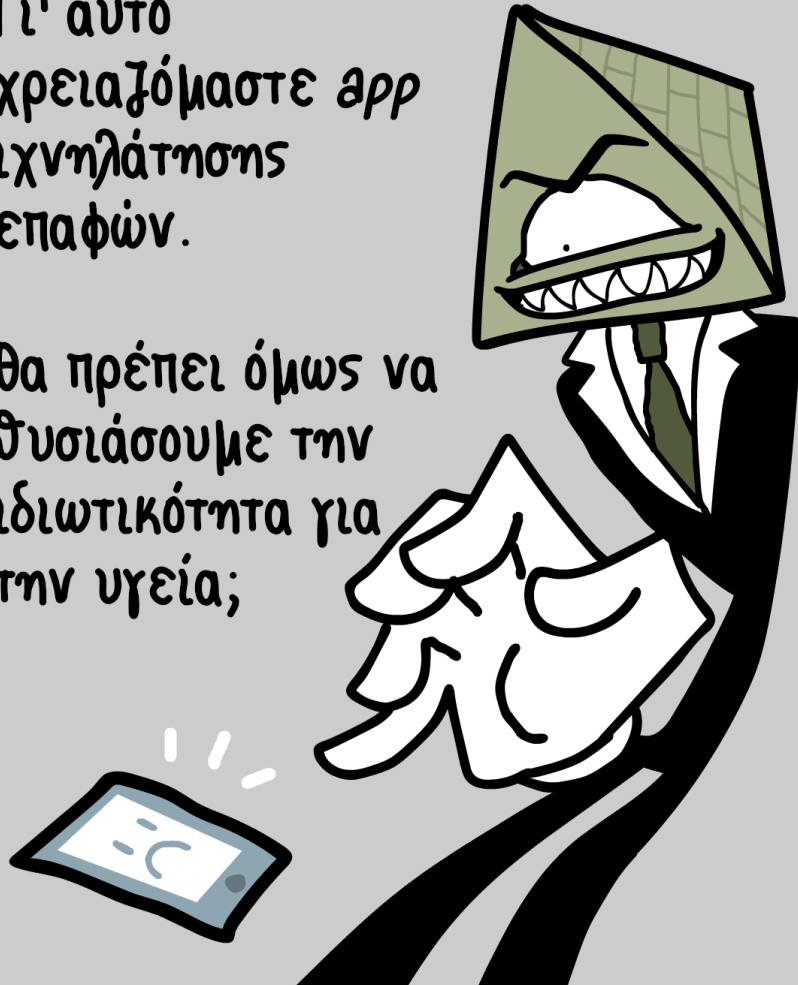
* και τι γίνεται με τα ασυμπτωματικά άτομα; απ' ό,τι φαίνεται δεν παίζουν μεγάλο ρόλο στην εξάπλωση της COVID-19! δες τις πηγές στο τέλος

* 60%; πάλι, δες τις πηγές στο τέλος!

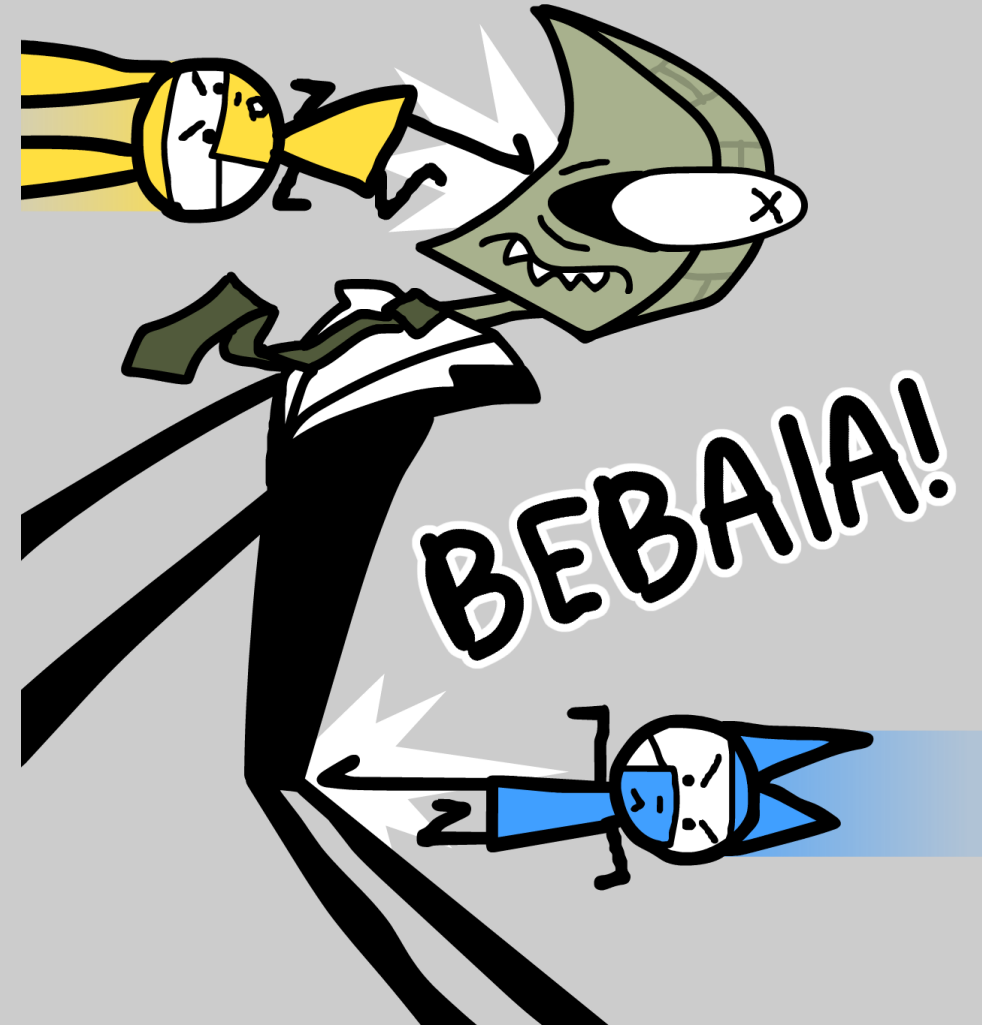
...χρειάζεται όμως να τις
βρούμε γρήγορα. Η κλασική
ιχνηλάτηση επαφών με
συνεντεύξεις είναι πολύ αργή.

Γι' αυτό
χρειαζόμαστε app
ιχνηλάτησης
επαφών.

Θα πρέπει όμως να
θυσιάσουμε την
ιδιωτικότητα για
την υγεία;



OXI



Είναι απολύτως εφικτό να
προστατεύσουμε τις ζωές ΚΑΙ
τις ελευθερίες των
ανθρώπων, με μία πολύ
απλή διαδικασία!

Ας δούμε πώς λειτουργεί,
με τη βοήθεια της
Αλίκης και του Βασίλη...



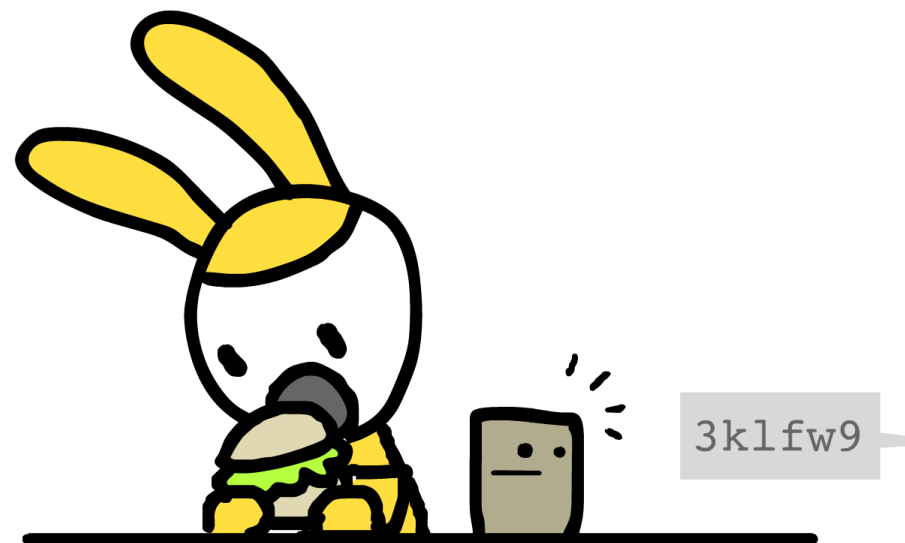
Η Αλίκη κατεβάζει το app!
(& ο κώδικάς του είναι δημόσιος
ώστε όλοι να μπορούν να
επιβεβαιώσουν ότι κάνει
πράγματι τα εξής...)



Κάθε 5 λεπτά, το κινητό της
στέλνει μοναδικές τυχαίες
ασυναρτησίες σε όλες τις
κοντινές συσκευές, μέσω
Bluetooth.

* τα 5 λεπτά είναι απλά ενδεικτικά! και τεχνικά είναι
"ψευδο-τυχαία", αφού δεν είναι κβαντικά... ΔΕΝ έχει σημασία.

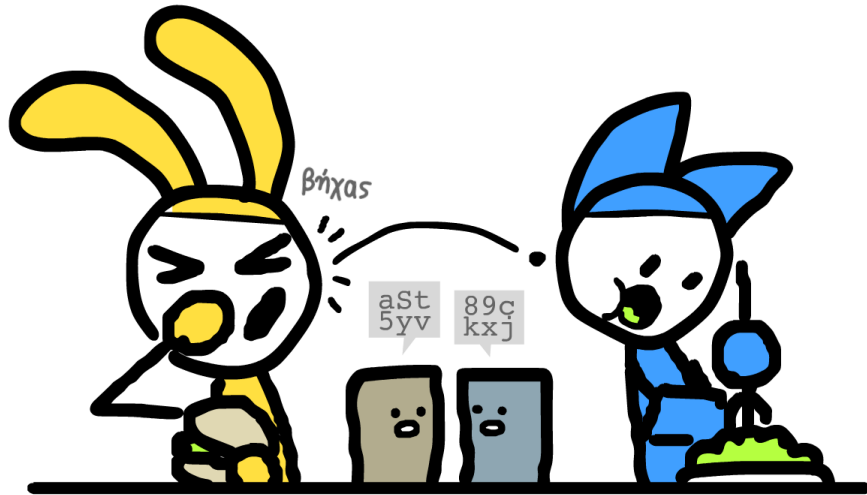
Επειδή τα μηνύματα είναι τυχαία
& δεν χρησιμοποιούν το GPS, δεν
έχουν ΚΑΜΙΑ ΠΛΗΡΟΦΟΡΙΑ για την
ταυτότητα της Αλίκης, την
τοποθεσία της ή οτιδήποτε άλλο.



Τώρα, καθώς το κινητό της
στέλνει τυχαία μηνύματα, ακούει
ταυτόχρονα για μηνύματα από
κοντινά κινητά.

Για παράδειγμα, του Βασίλη.

Ο Βασίλης έχει ένα app
ιχνηλάτησης με ιδιωτικότητα, που
είναι συμβατό (ή το ίδιο) με αυτό
της Αλίκης.



Αν η Αλίκη και ο Βασίλης
μείνουν κοντά για 5+ λεπτά, τα
κινητά τους θα ανταλλάξουν τις
ασυναρτησίες.

Και τα δύο κινητά θυμούνται όλα
τα μηνύματα που έστειλαν ή
έλαβαν τις τελευταίες 14 μέρες.



Ξανά: Επειδή τα τυχαία
μηνύματα δεν περιέχουν ΚΑΜΙΑ
ΠΛΗΡΟΦΟΡΙΑ, η ιδιωτικότητα της
Αλίκης από τον Βασίλη είναι
προστατευμένη, και αντίστροφα!

* οι 14 μέρες είναι πάλι ενδεικτικές! οι επιδημιολόγοι μπορεί να
βρουν ότι η "περίοδος επώασης" είναι μικρότερη ή μεγαλύτερη.

Την επόμενη μέρα, η Αλίκη
έχει ξηρό βήχα και πυρετό.

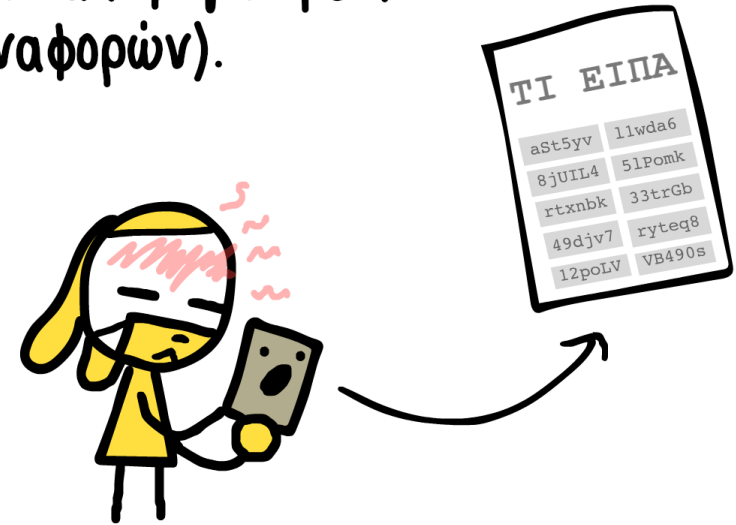
Υποβάλλεται σε τεστ.



Η Αλίκη έχει COVID-19.

Δεν είναι καλή μέρα για την Αλίκη.

Γιατί όμως να υποφέρει μάταια;
Η Αλίκη ανεβάζει τα μηνύματα που
είχε στείλει, στη βάση δεδομένων
ενός νοσοκομείου, μέσω ενός
κωδικού μιας χρήσης από τον
γιατρό της (ο κωδικός είναι για
την αποφυγή spam
αναφορών).



Η Αλίκη μπορεί επίσης να κρύψει
τα μηνύματα που στάλθηκαν σε
κάποια ιδιωτική στιγμή, όπως ένα
δείπνο στο σπίτι!

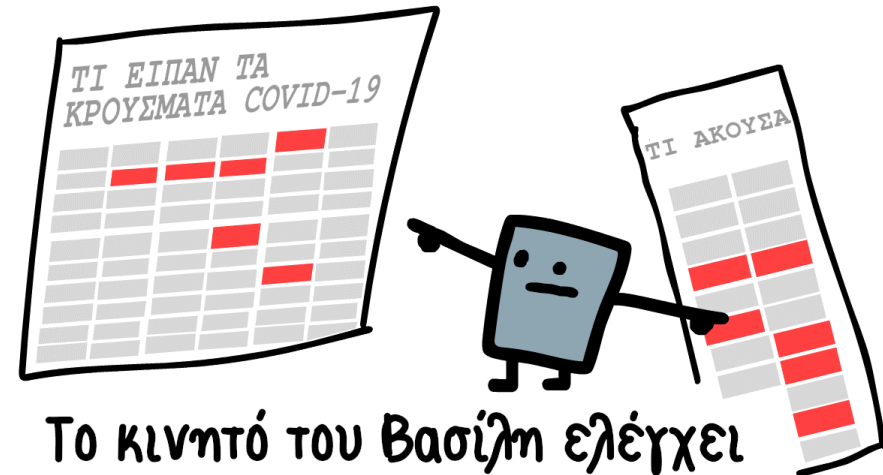
Οι ασυναρτησίες της Αλίκης
αποθηκεύονται στη βάση δεδομένων:



Ξανά: τα τυχαία μηνύματα δεν
αποκαλύπτουν ΚΑΜΙΑ ΠΛΗΡΟΦΟΡΙΑ για
το πού ήταν η Αλίκη, με ποιον, τι
έκαναν, ή ακόμη και το πόσα άτομα
συνάντησε η Αλίκη! Είναι
ακατανόητα για το νοσοκομείο...

* τα νοσοκομεία διαφορετικών χωρών μπορούν να ανταλλάζουν
τα μηνύματα, αλλά επειδή αυτά δεν έχουν καμία
πληροφορία, δεν χάνεται η ιδιωτικότητα.

...όχι όμως και για τον Βασίλη!



Το κινητό του Βασίλη ελέγχει
συχνά τη λίστα του νοσοκομείου
με τα τυχαία μηνύματα
κρουσμάτων COVID-19, και βλέπει
αν "άκουσε" κάποιο από αυτά τις
τελευταίες 14 μέρες.

(Οι ασυναρτησίες δεν
αποκαλύπτουν ΚΑΝΕΝΑ ΑΛΛΟ
ΠΡΟΣΩΠΙΚΟ ΔΕΔΟΜΕΝΟ στον Βασίλη).

* το πραγματικό πρωτόκολλο DP-3T είναι ΑΚΟΜΗ πιο ασφαλές! χρησιμοποιεί
ένα "cuckoo filter" ώστε τα κινητά να μαθαίνουν ΜΟΝΟ τα μηνύματα
COVID-19 που άκουσαν, χωρίς να αποκαλύπτονται ΟΛΑ τα μηνύματα.

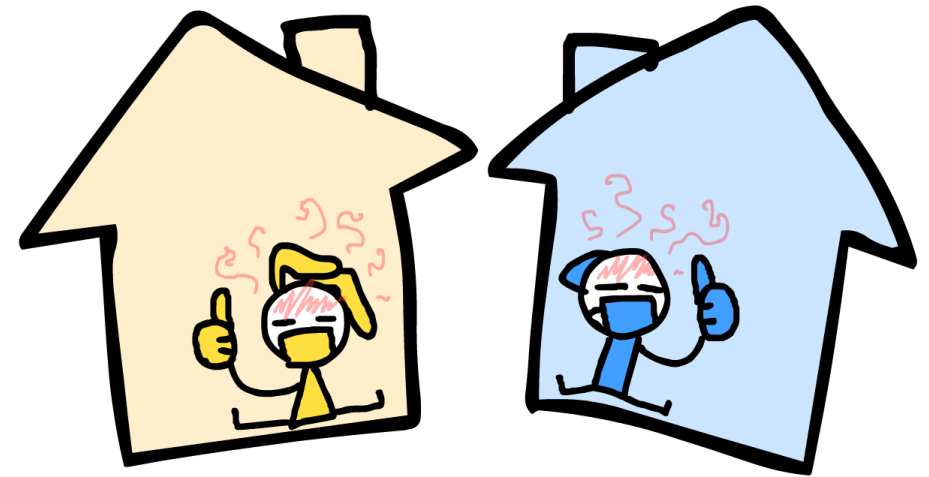
Αν άκουσε, για παράδειγμα, 6 ή παραπάνω μηνύματα κρουσμάτων COVID-19 (6 x 5 λεπτά = 30 λεπτά συνολικής έκθεσης), τότε το κινητό ειδοποιεί τον Βασίλη ώστε να μπει σε αυτοπεριορισμό.



Και έτσι, ο Βασίλης σπάει την αλυσίδα μετάδοσης - είναι ένα βήμα πιο μπροστά από τον ιό!

Αυτό ήταν!

Έτσι, η ψηφιακή ιχνηλάτηση επαφών μπορεί να εμποδίσει προληπτικά τη μετάδοση της COVID-19 προστατεύοντας ταυτόχρονα τα δικαιώματά μας.



Αλίκη & Βασίλη, σας ευχαριστούμε!
Μείνετε ασφαλείς.



Exposure Notification

Bluetooth Specification

Preliminary — Subject to Modification and Extension

April 2020

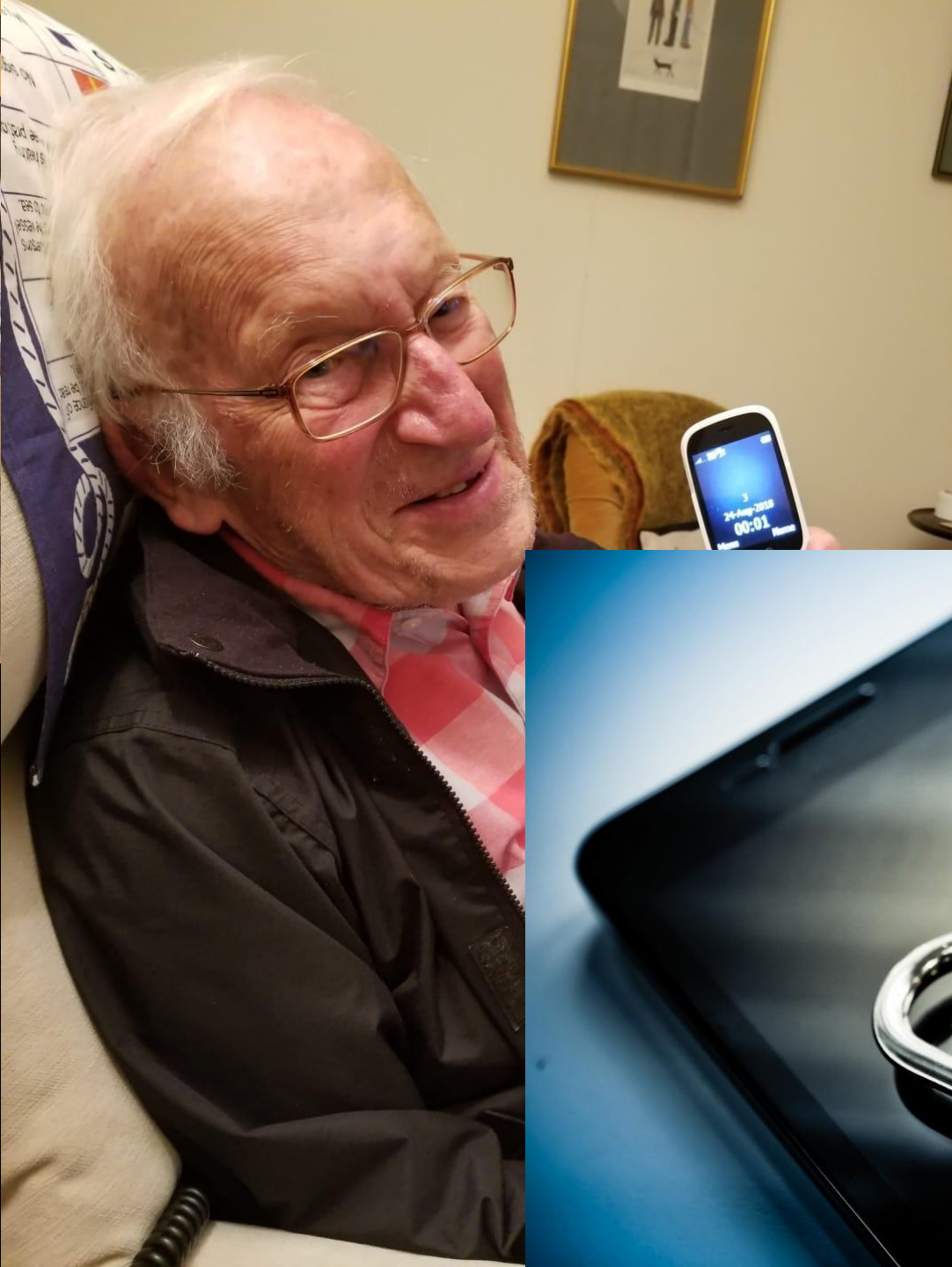
v1.2

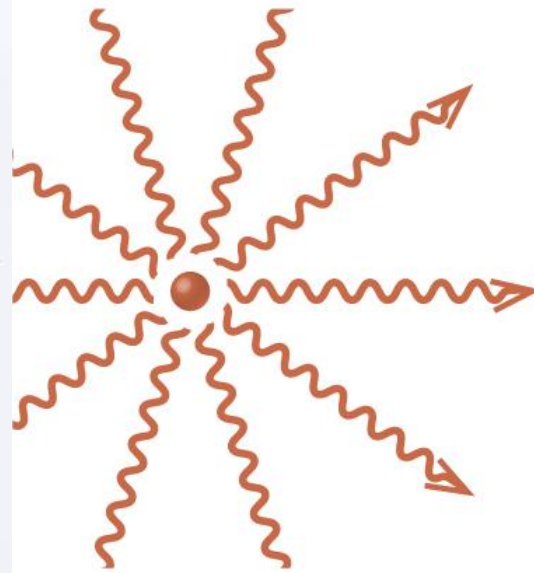
Information subject to copyright. All rights reserved.

Contents

Overview	3
Exposure Notification Service	4
Advertising Payload	4
Broadcasting Behavior	5
Broadcasting Flow	5
Scanning Behavior	6
Scan Power Considerations	6
Scanning Flow	6
Privacy	7
Revision History	8

Exposure Notification - Bluetooth Specification
Information subject to copyright. All rights reserved.





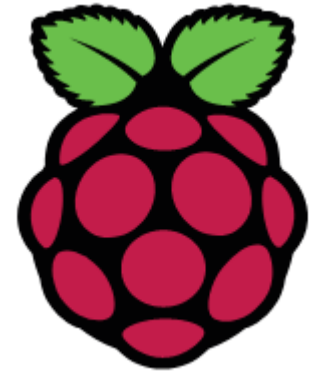
Rate of radioactive decay
measured in bequerels or curies



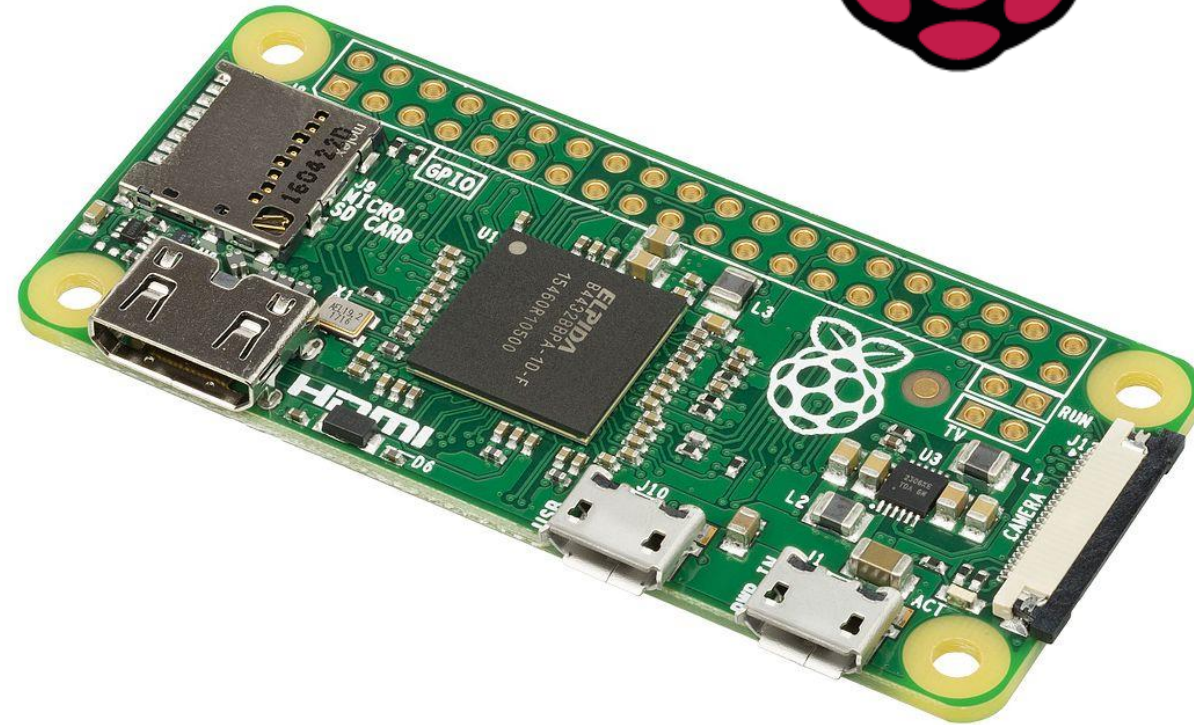
Film badge or dosimeter
measures tissue damage
exposure in rems or sieverts

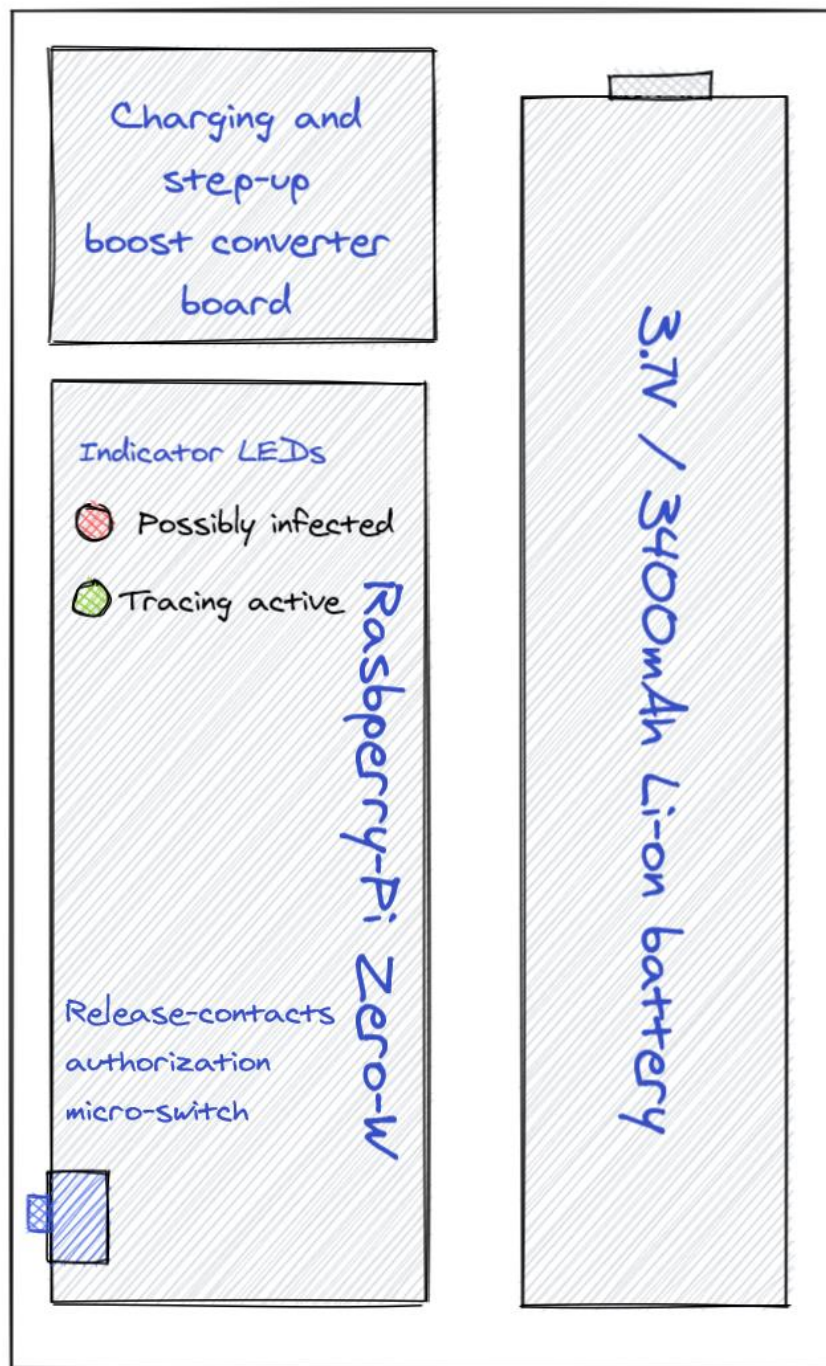
Absorbed dose measured in grays or rads

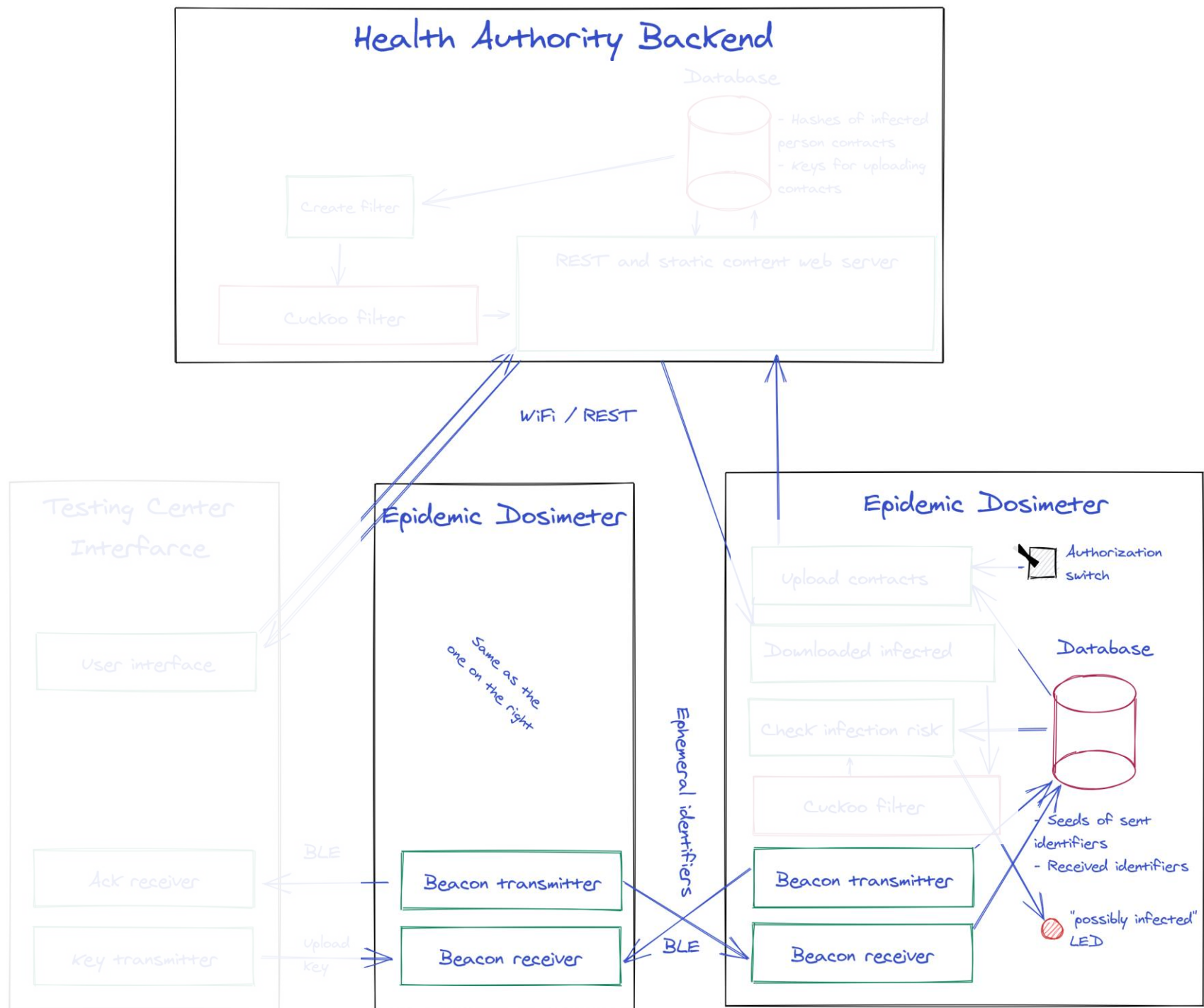
Raspberry Pi Zero W



- Επεξεργαστής 1GHz
- 512MB RAM
- Σύνδεση Ε/Ε 40 επαφών
- Δίκτυο 802.11 b/g/n
- Bluetooth 4.1
- Bluetooth Low Energy (BLE)
- Λειτουργεί με Linux
- Κόστος: 8€







```

zero-w:dds
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

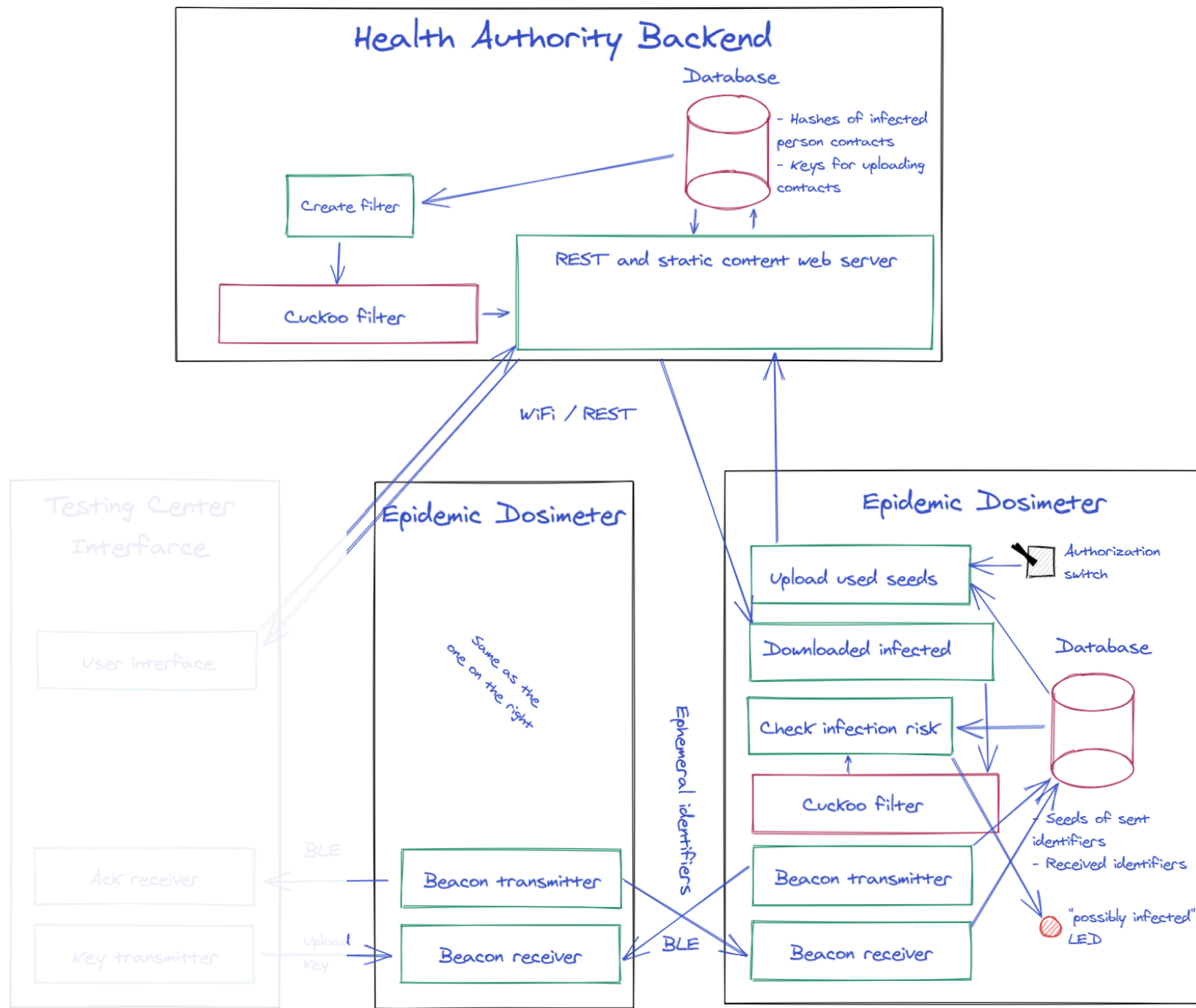
```

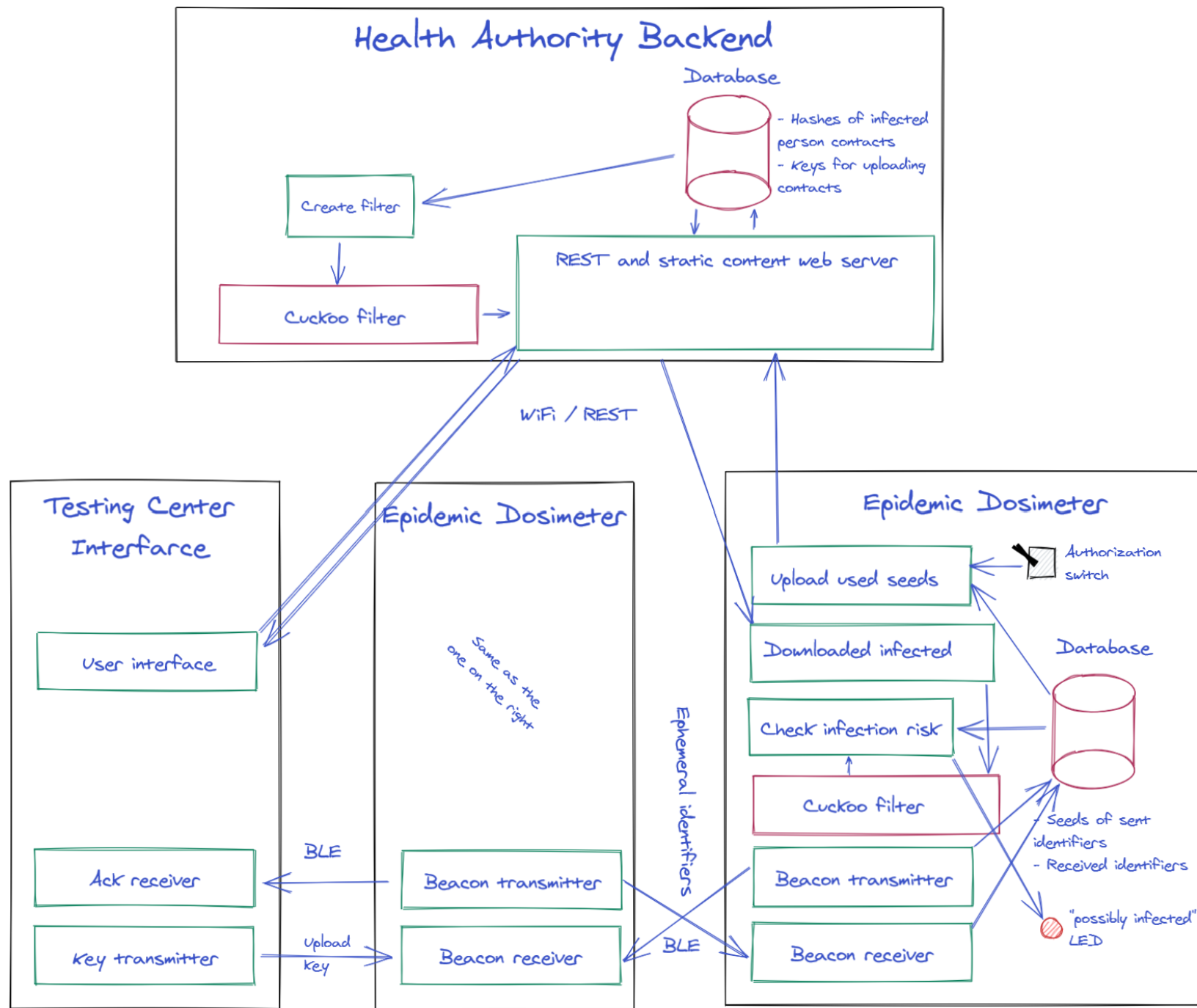


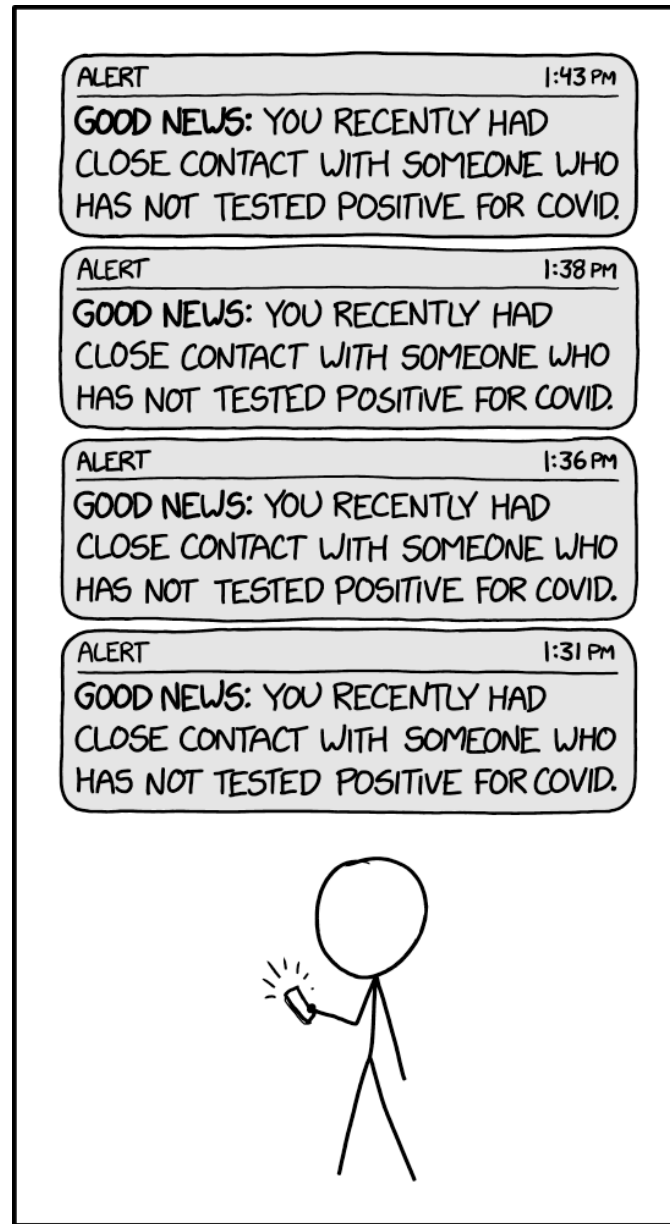
```

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

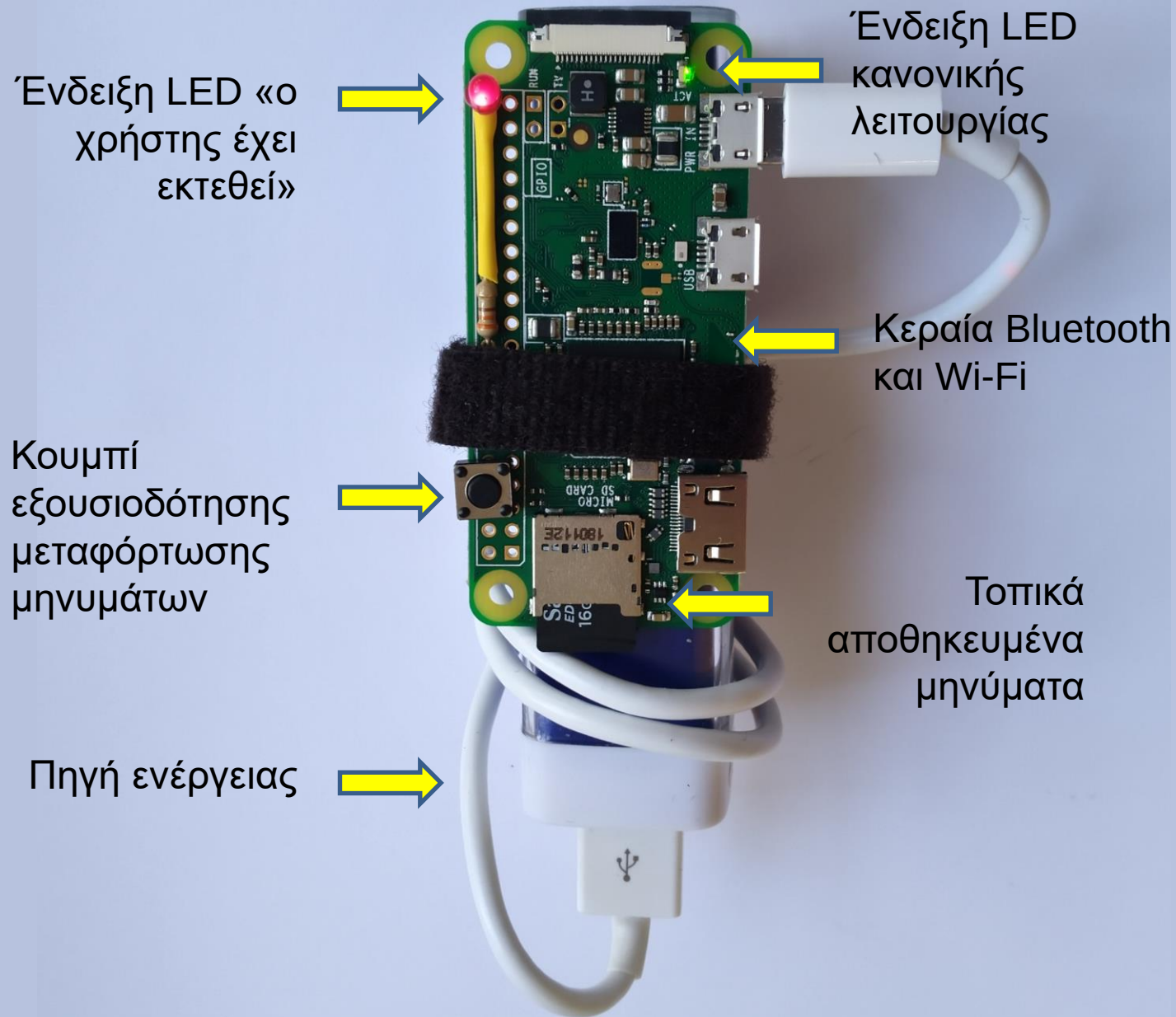
```







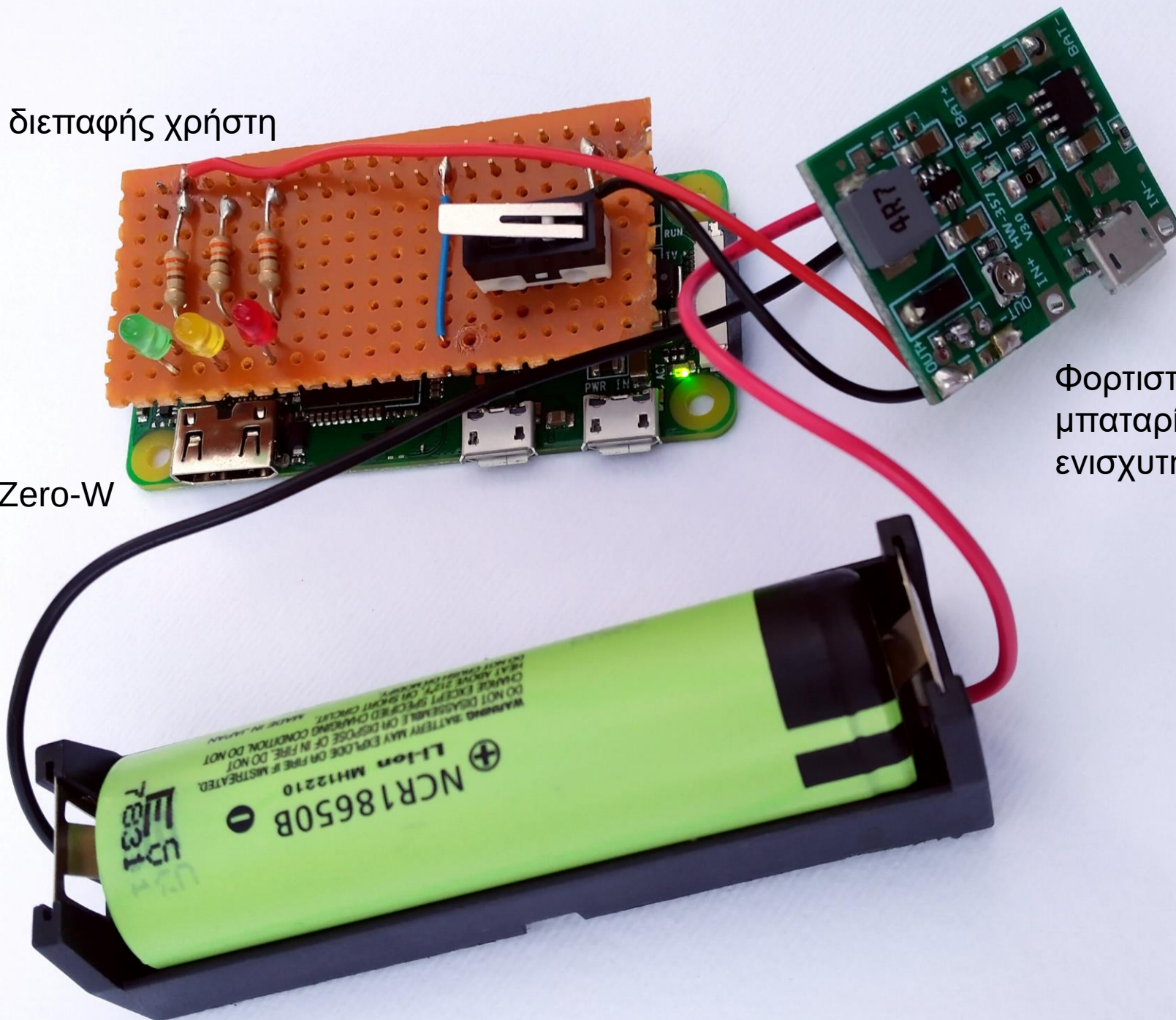
NO ONE LIKES MY NEW COVID
EXPOSURE NOTIFICATION APP

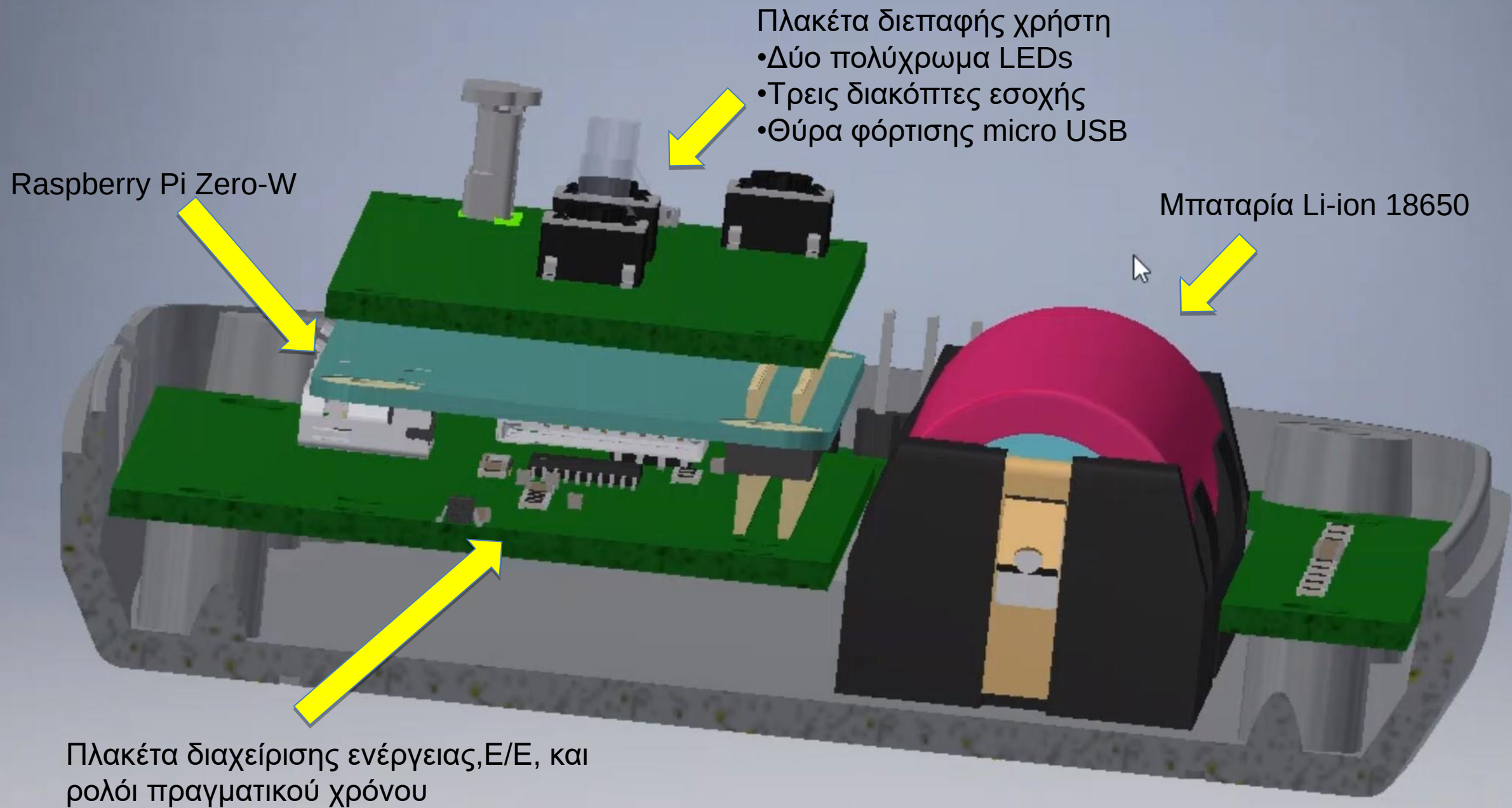


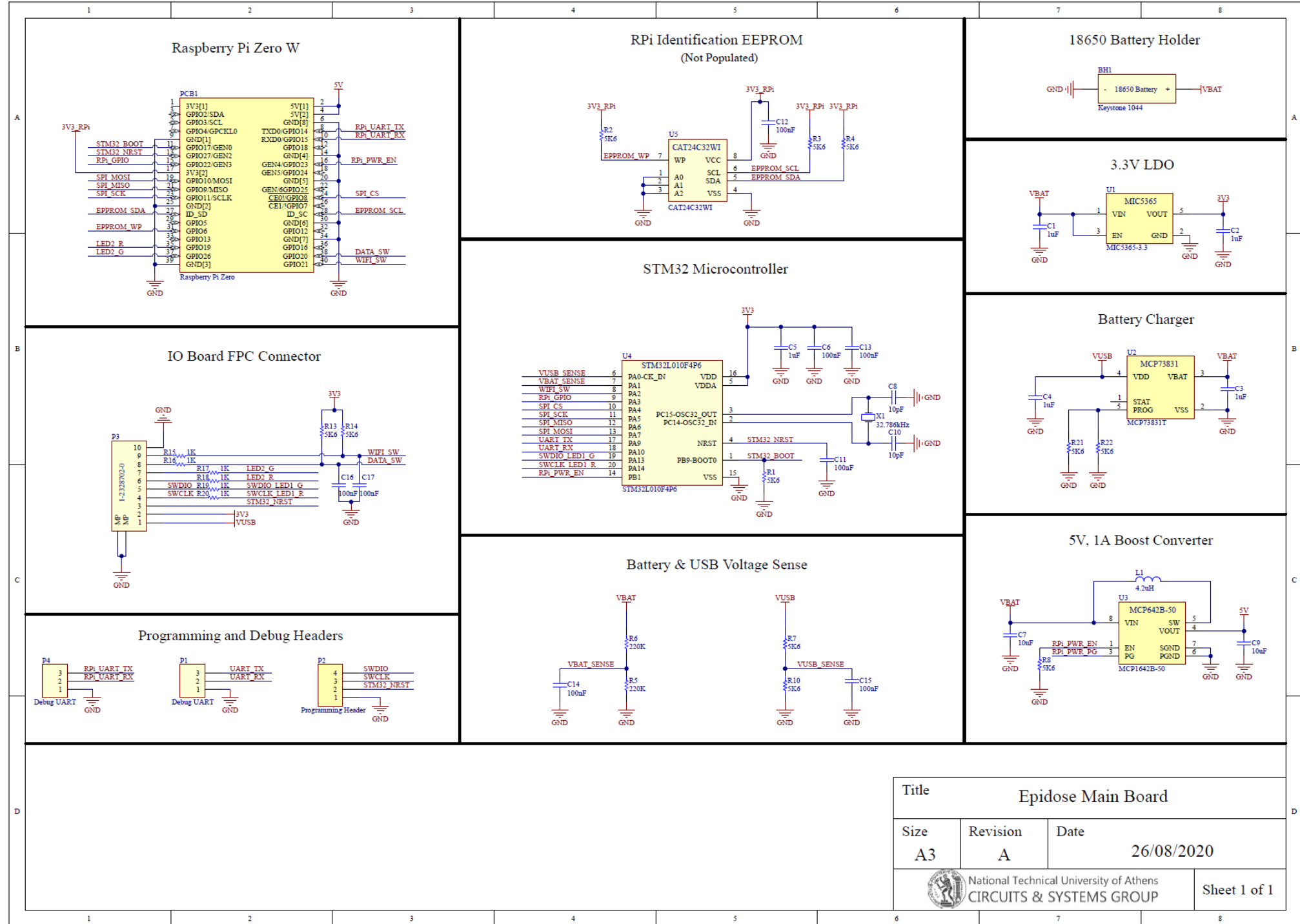
Πλακέτα διεπαφής χρήστη

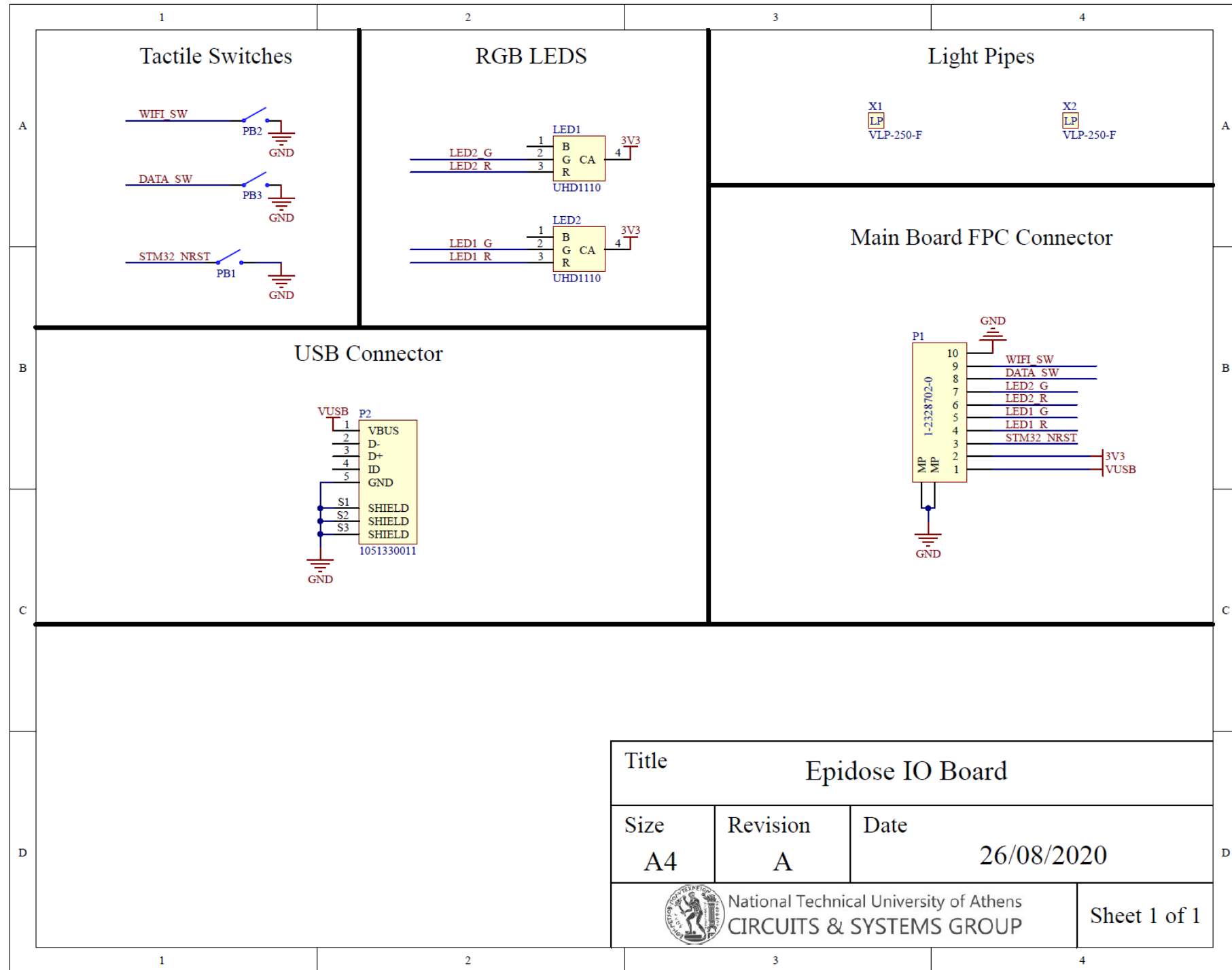
Raspberry Pi Zero-W

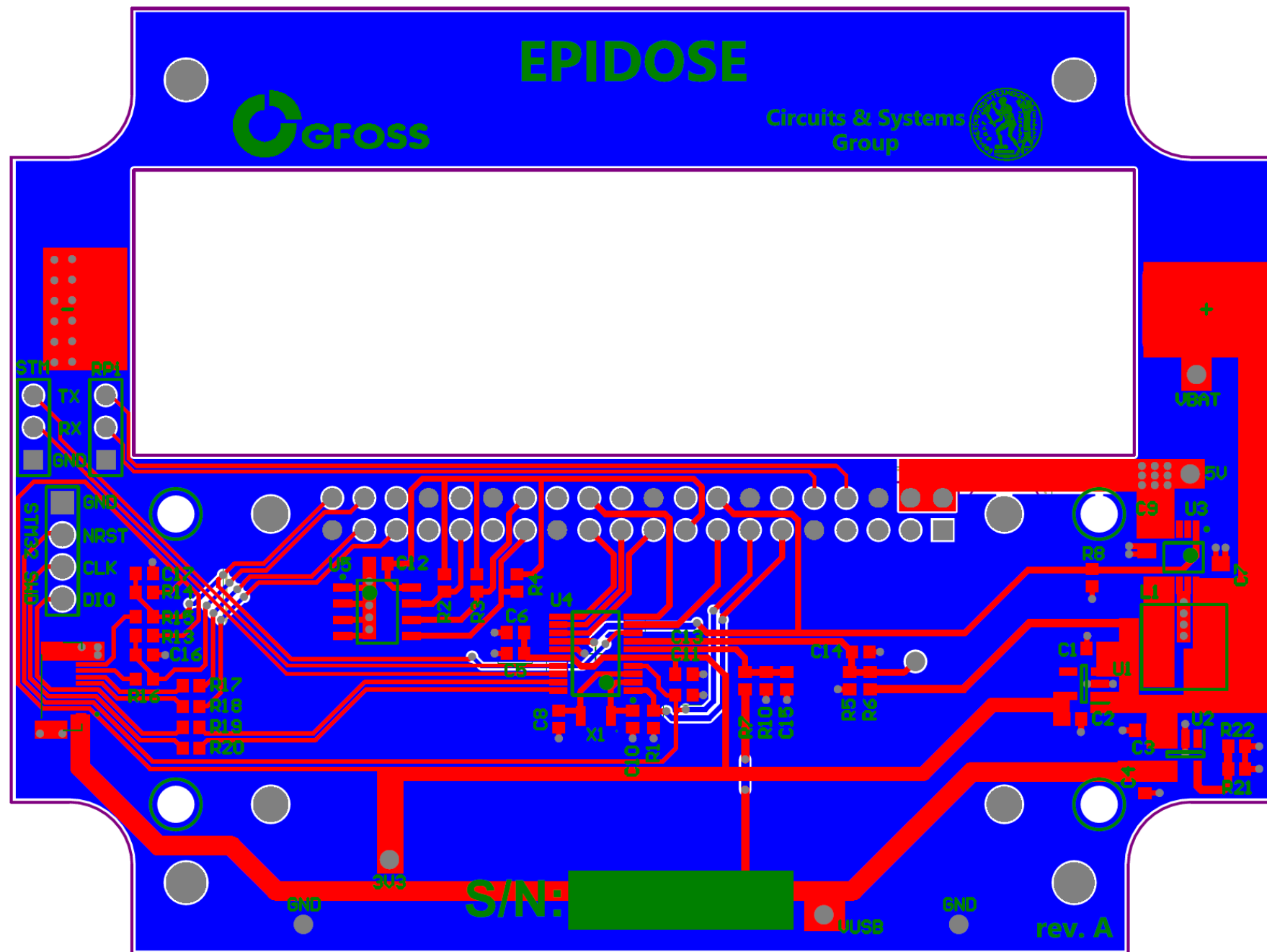
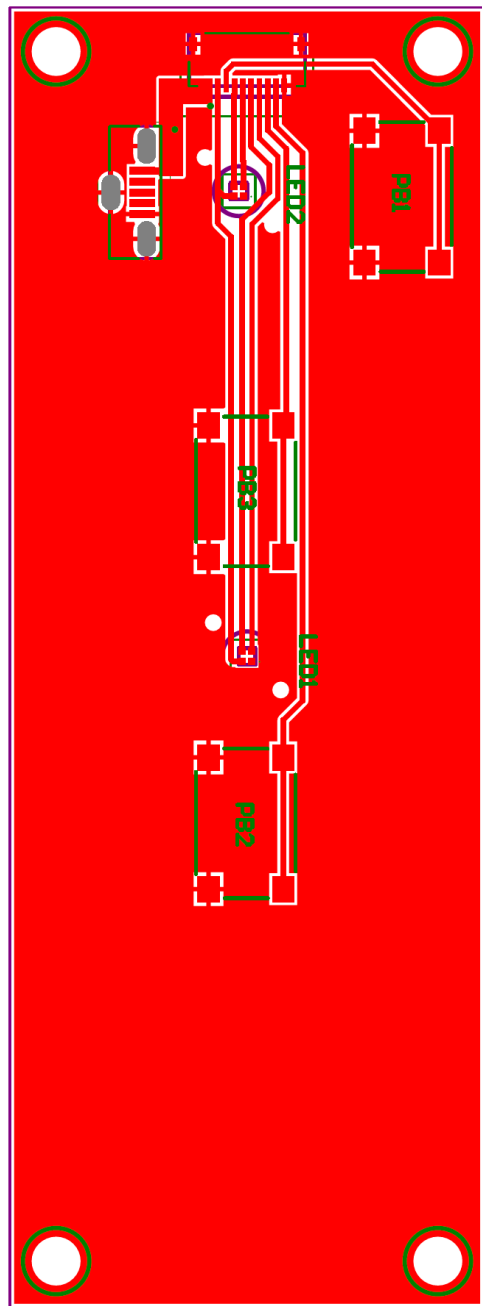
Φορτιστής
μπαταρίας και
ενισχυτής τάσης









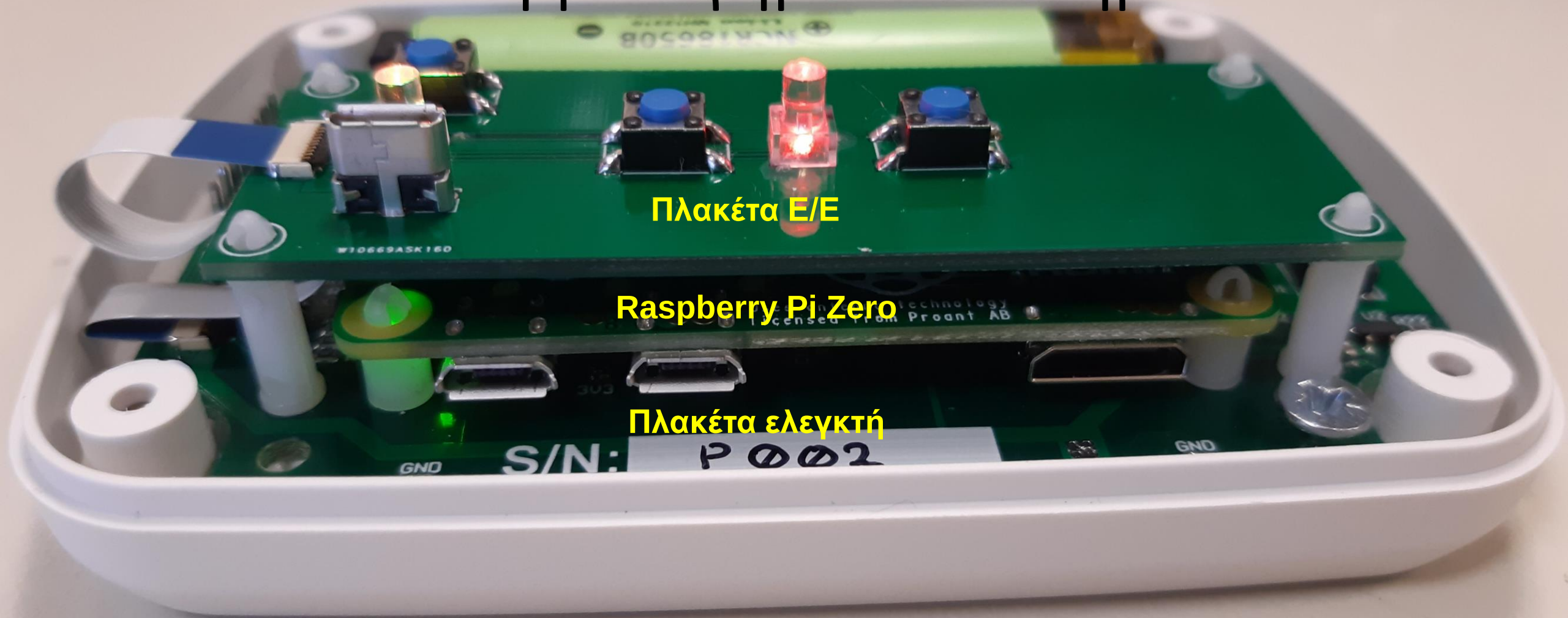


Πλακέτα ελεγκτή



Φόρτιση Li-ion,
ενισχυτής τάσης, και
ελεγκτής εκφόρτωσης

Συναρμολογημένο σύστημα



Ανθρώπινη διεπαφή



Επόμενα Βήματα: επαλήθευση

- Επαλήθευση λειτουργικότητας πρωτότυπων πλακετών
- Διεπαφή με νέες πλακέτες
 - Διεπαφή χρήστη
 - Διαχείριση ισχύος
 - Real Time Clock
- Δικτύωση πλέγματος για διανομή κουκοφίλτρου
- Βελτιστοποίηση ενεργειακής κατανάλωσης
- Ρύθμιση λογισμικού για λειτουργία σε περιβάλλον παραγωγής

Επόμενα βήματα: επικύρωση

- Εκτέλεση υποδομής φορέα υγείας στο EOSC Compute Cloud:
 - Jelastic Platform-as-a-Service
 - SWITCH engines
 - de.NBI Cloud: Cloud Computing for Life Sciences
 - CSC ePouta
- Μαζική παραγωγή 100 πρωτοτύπων
- Σχεδίαση μελέτης υιοθέτησης
- Διανομή συσκευών στον ευρύ πληθυσμό
- Παρακολούθηση υιοθέτησης και χρήσης των συσκευών

Search or jump to...

/

Pull requests

Issues

Marketplace

Explore

eellak / epidose

forked from DP-3T/reference_implementation

Unwatch

8

Star

43

Fork

40

<> Code

! Issues20

🔗 Pull requests1

▶ Actions

📁 Projects

📖 Wiki

🛡 Security

📈 Insights

⚙ Settings

🔗 master

🔗 6 branches

🏷 0 tags

Go to file

Add file

📄 Code

This branch is 178 commits ahead of DP-3T:master.

🔗 #33

🔗 Compare

dspinellis

Clarify Health Authority upload

fd10cac on 31 Jul 200 commits

📁 doc	Improve software architecture diagram	4 months ago
📁 dp3t	Maintain database connections for Gunicorn	3 months ago
📁 epidose	Remove bdaddr	2 months ago
📁 examples	Move programs to separate directory	4 months ago
📁 hardware	Update circuit to board-based prototype	2 months ago
📁 test-data	Add check infection risk script	4 months ago
📁 tests	Clarify what gets uploaded to the Health Athority	3 months ago
📁 utils	Quote to avoid ambiguity	4 months ago
📄 .flake8	flake8: Fix F401 errors and minimize flake8 ignores	4 months ago
📄 .gitignore	Update setup to use make-deb	3 months ago
📄 .pre-commit-config.yaml	Add shellcheck pre-commit hook	4 months ago
📄 LICENSE	Restructure and expand existing reference implementation	4 months ago
📄 Makefile	Remove bdaddr	2 months ago
📄 README.md	Clarify Health Authority upload	last month
📄 setup.py	Clarify what gets uploaded to the Health Athority	3 months ago

README.md

Epidose: A privacy-preserving epidemic dosimeter based on contact tracing

About

Privacy-preserving epidemic dosimeter based on DP-3T contact tracing

📖 Readme

📄 Apache-2.0 License

Releases

No releases published

[Create a new release](#)

Packages

No packages published

[Publish your first package](#)

Languages

Python92.1%

Shell6.5%

Other1.4%

37

Ευχαριστώ!

Οργανισμός Ανοιχτών Τεχνολογιών
www.eellak.gr

Αποθετήριο ΕΛ/ΛΑΚ
github.com/eellak/epidose

Διομήδης Σπινέλλης
www.spinellis.gr

