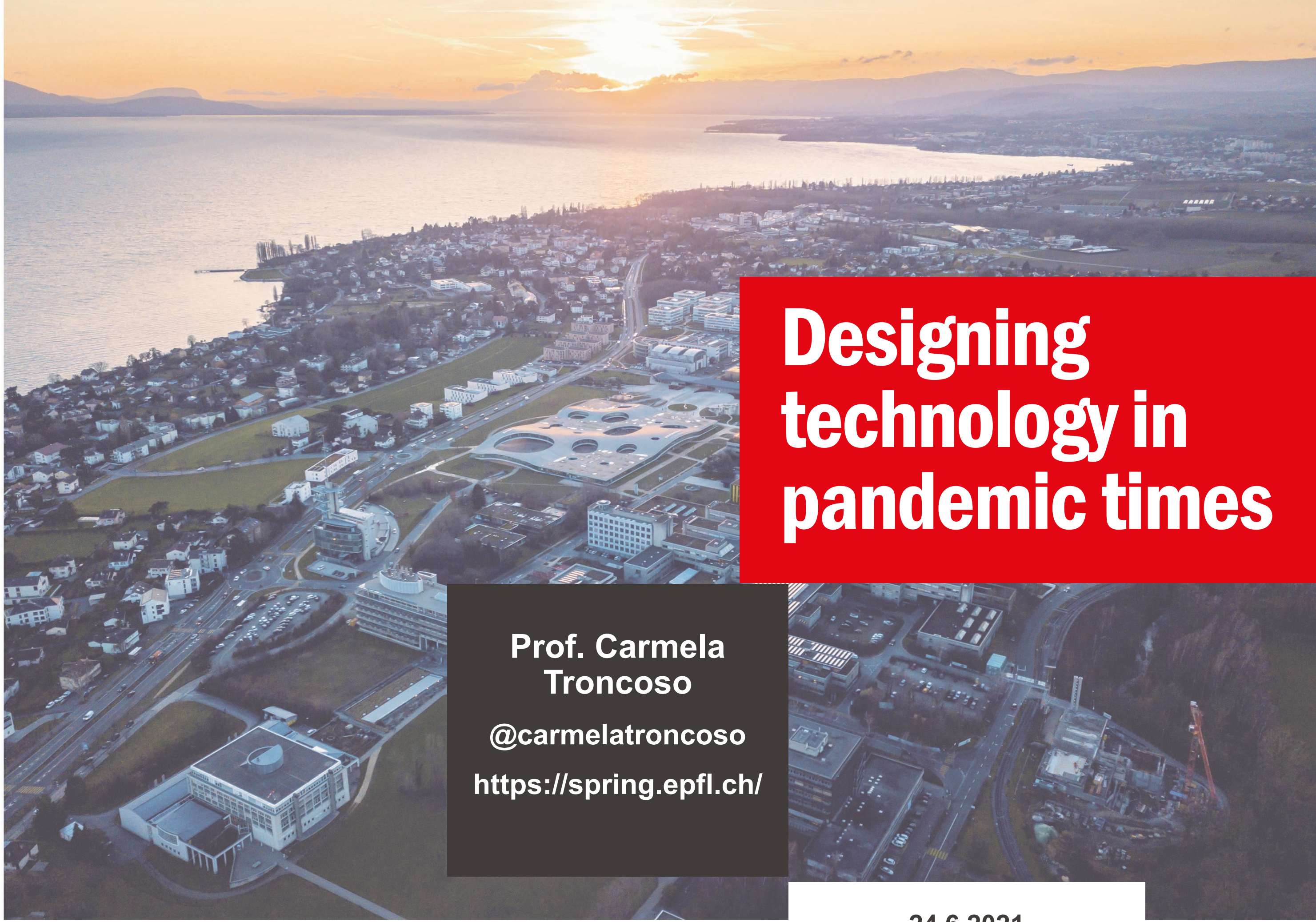
EPFL



Designing technology in pandemic times

Prof. Carmela Troncoso

@carmelatroncoso

https://spring.epfl.ch/

24.6.2021

École polytechnique fédérale de Lausanne

A collaborative ~~sprint~~ ~~Marathon~~ Ironman

March 2020 - **Start**

April 2020 – **GAEN is announced**

May 2020 – **Final version DP3T**

June 2020 – **Pilot SwissCovid (& EU apps)**

July 2020 – **SwissCovid launch**

EPFL ETH zürich

UCL CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY UNIVERSITY OF OXFORD UNIVERSITÀ DEGLI STUDI DI TORINO

TU Delft KU LEUVEN institute imdea software INESCTEC

Maintenance and support

September 2020 – **Design Presence tracing**

Jan/Feb 2021 – **Presence tracing pilot@EPFL**

March/April 2021 – **Presence tracing expansions & metrics**

May/July 2021 – **Towards deployment presence tracing in SwissCovid**

EPFL ETH zürich TU Delft UCL

Technology to help with pandemic contention

- **Manual tracing overwhelmed**

- **The need**
  - **A complement** to **notify** users that have been exposed to COVID19 and they are at risk of infection
  - In a **timely, efficient, and scalable** manner

- **The proposal**: **an app**

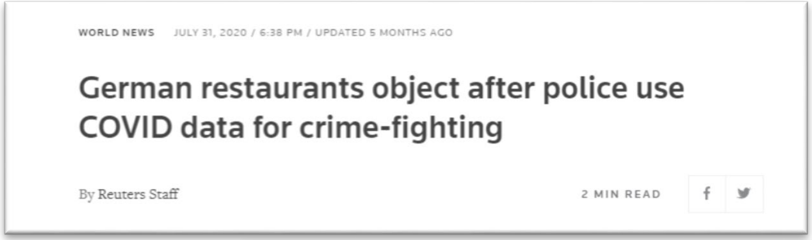
Carmela Troncoso

Technology to help with pandemic contention

- **Manual tracing overwhelmed**
- **The need**
  - **A complement** to **notify** users that have been exposed to COVID19 and they are at risk of infection
  - In a **timely, efficient, and scalable** manner
- **The proposal**: ~~an app~~ **an infrastructure** to leverage phone sensors
  - network, backends, UI towards health workers
  - **dependencies**: mobile OS, cloud infrastructure
    - mostly privatized… Health system has little infrastructure

Why infrastructure matters hard to remove

Why infrastructure matters hard to control

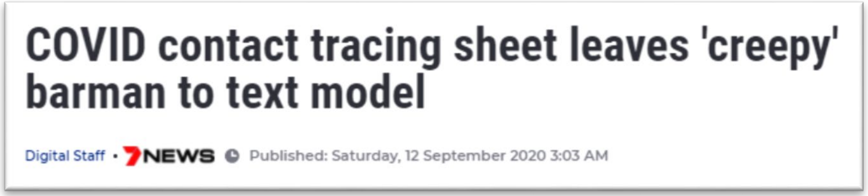


WORLD NEWS JULY 31, 2020 / 6:38 PM / UPDATED 5 MONTHS AGO

German restaurants object after police use COVID data for crime-fighting

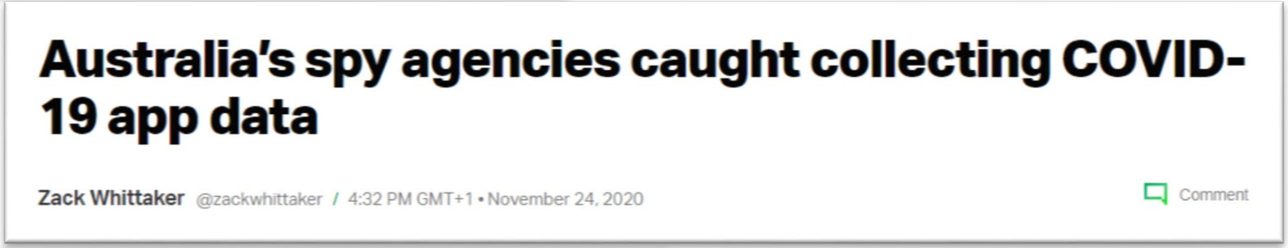
By Reuters Staff

2 MIN READ



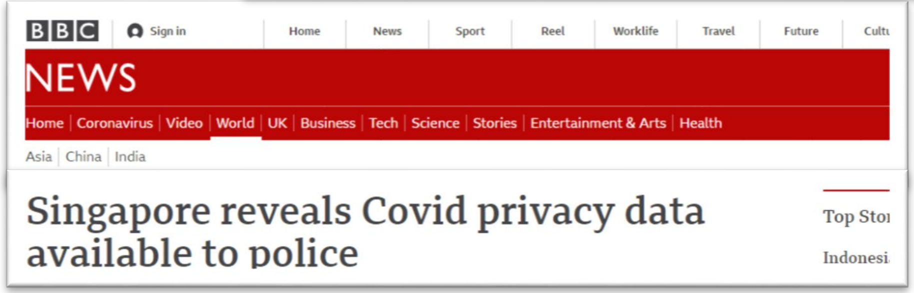
COVID contact tracing sheet leaves 'creepy' barman to text model

Digital Staff • 7NEWS Published: Saturday, 12 September 2020 3:03 AM

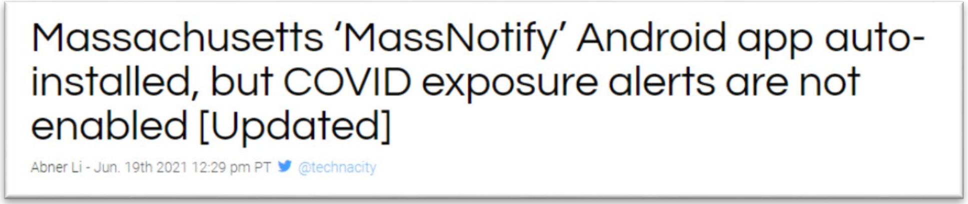


Australia's spy agencies caught collecting COVID-19 app data

Zack Whittaker @zackwhittaker / 4:32 PM GMT+1 • November 24, 2020



Singapore reveals Covid privacy data available to police



Massachusetts 'MassNotify' Android app auto-installed, but COVID exposure alerts are not enabled [Updated]

Abner Li - Jun. 19th 2021 12:29 pm PT @technacity

The constraints: Security and Privacy

- Protect health-related data
- Protect from misuse (surveillance, manipulation, etc)
  - **Purpose limitation by default**

Seda Gurses, Carmela Troncoso, Claudia Diaz. Engineering Privacy by Design.Computers, Privacy & Data Protection. 2011

The constraints: Security and Privacy

- Protect health-related data
- Protect from misuse (surveillance, manipulation, etc)
  - **Purpose limitation by default**
  - hide users identity, location, and behavior (social graph)

Seda Gurses, Carmela Troncoso, Claudia Diaz. Engineering Privacy by Design.Computers, Privacy & Data Protection. 2011

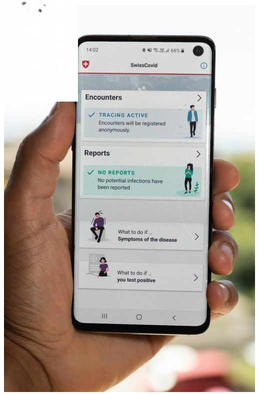
The constraints: Security and Privacy

- Protect health-related data
- Protect from misuse (surveillance, manipulation, etc)
  - **Purpose limitation by default**
  - hide users identity, location, and behavior (social graph)
- Preserve system integrity
  - Prevent false alarms & Denial of Service

Seda Gurses, Carmela Troncoso, Claudia Diaz. Engineering Privacy by Design.Computers, Privacy & Data Protection. 2011

The “hidden” constraint
Reality

- High scalability and reliability
- Design under time pressure!
  - Need fast, robust verification
    - KISS principle: Keep It Simple Stupid
    - Avoid new technologies or non-mainstream
  - Use existing infrastructure
    - BLE beacons
- Dependencies, dependencies, dependencies



Encounters

✓ TRACING ACTIVE
Encounters will be registered anonymously.

Reports

✓ NO REPORTS
No potential infections have been reported

What to do if ...
Symptoms of the disease

What to do if ...
you test positive

Blagovesta Kostova, Seda Gürses, Carmela Troncoso. Privacy Engineering Meets Software Engineering. On the Challenges of Engineering Privacy By Design

Reality
Use existing infrastructure

- Battery and CPU usage
  - Limited round trips
  - Google and Apple **must** be involved

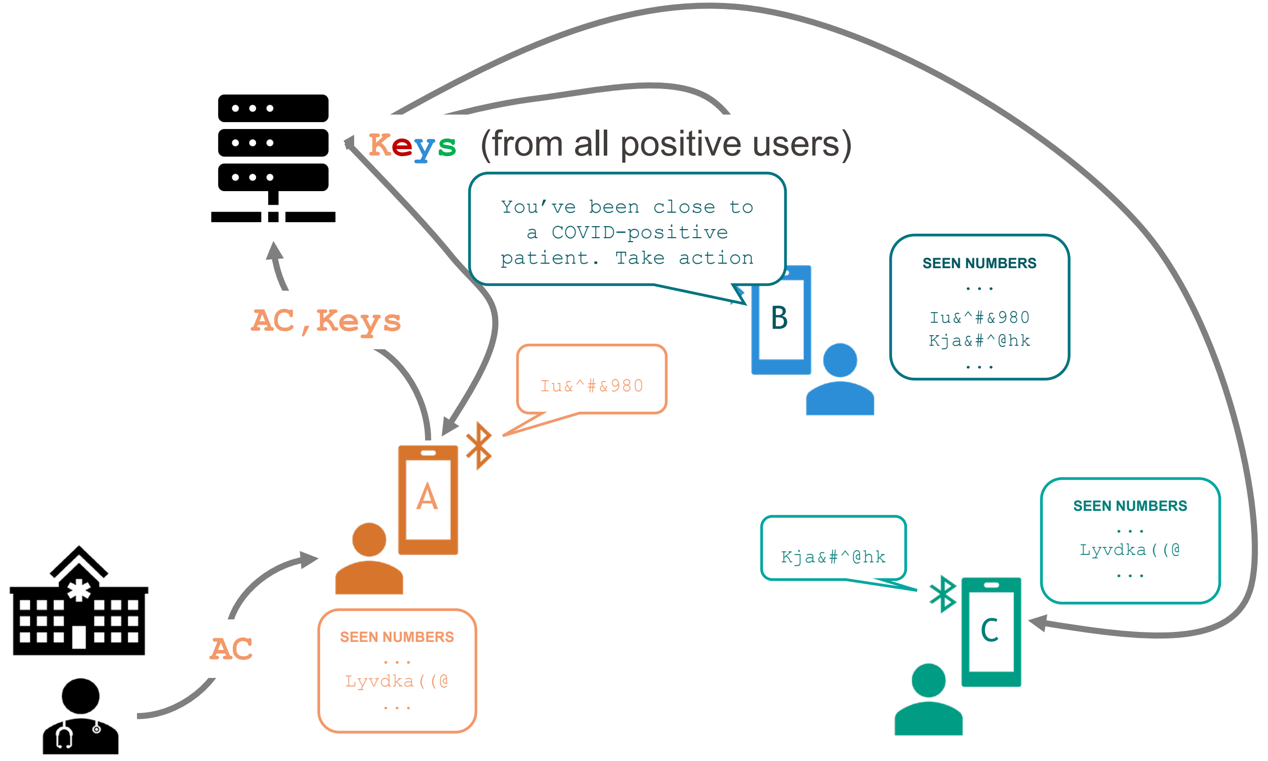
- Run in the background
  - Apple **must** be involved

- Compatibility Android - iOS
  - Google and Apple **must** be involved

- **Consequence:** Google and Apple implement the protocol **and the API**
  - Implications on privacy engineering
  - Implications for epidemiology and exposure estimation (no time in this talk…)
  - Implications for privacy when internationalizing (no time in this talk…)

EPFL

The system design



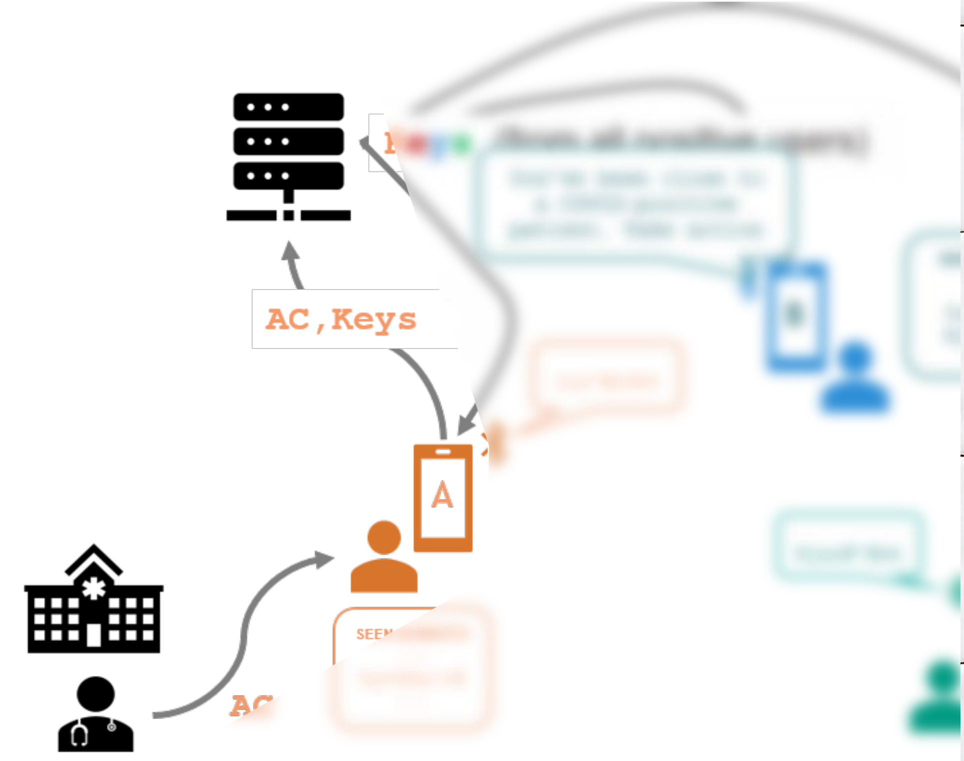
Only information that ever leaves the phone are the **TEKs broadcasted** during the contagious period.

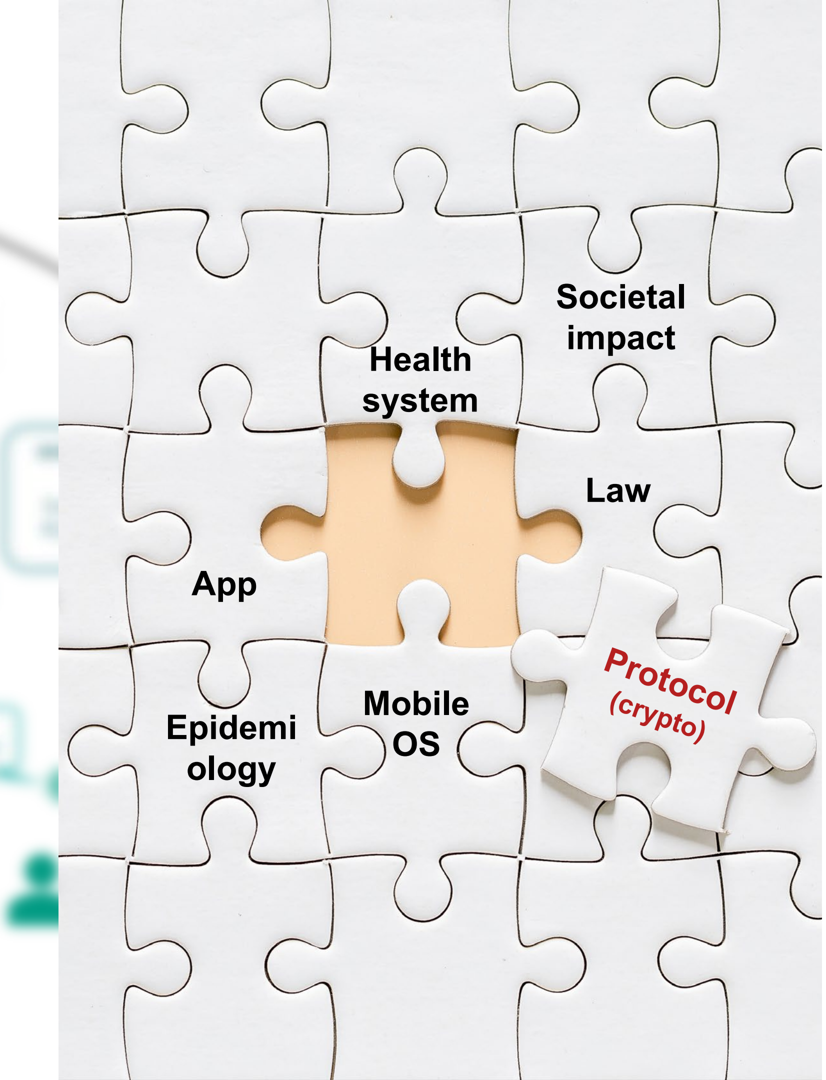
No identity, **no** location, **no** information about others

No information available for abuse

System **sunsets-by-design**

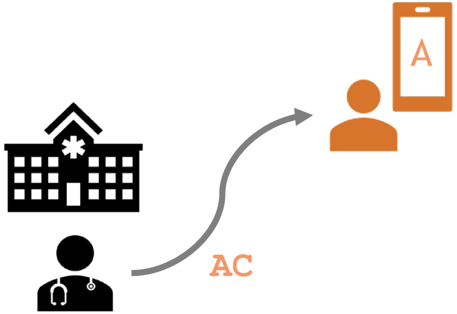
The system design





Authorization mechanism
Our first design

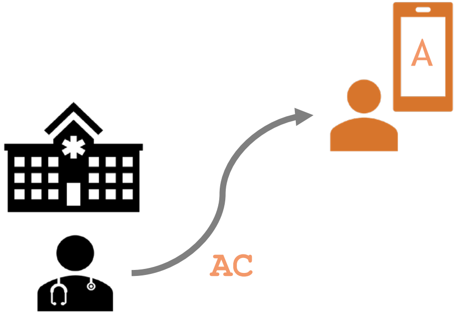
- Crucial for security: only *true* positives can upload
  - Desired properties:
    - Privacy
    - Hard to delegate
  - Crypto FTW! Commit to content in authorization token!



Secure Upload Authorisation for Digital proximity tracing. DP-3T project. https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Upload%20Authorisation%20Analysis%20and%20Guidelines.pdf

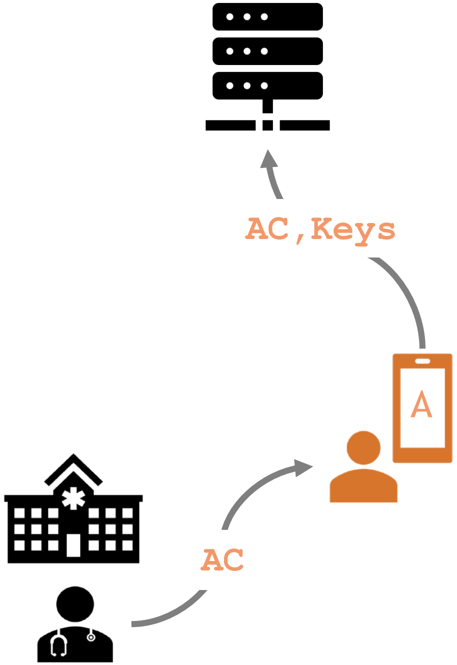
Authorization mechanism

- Crucial for security: only *true* positives can upload
  - Desired properties:
    - Privacy
    - Hard to delegate
  - Crypto FTW! Commit to content in authorization token!
- Health systems/staff are not digitalized everywhere
- EN native popup to request keys (usability nightmare)
  - And for privacy engineering
- Simple activation codes sent via phone/mail/sms
  - Different level of automatization
  - Only Belgium has (light) commitments!

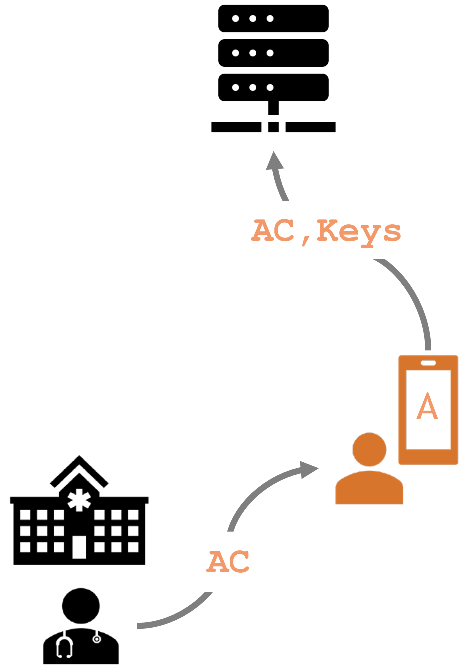


Secure Upload Authorisation for Digital proximity tracing. DP-3T project. https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Upload%20Authorisation%20Analysis%20and%20Guidelines.pdf

Privacy engineering
Are we done?



Privacy engineering
Are we done?

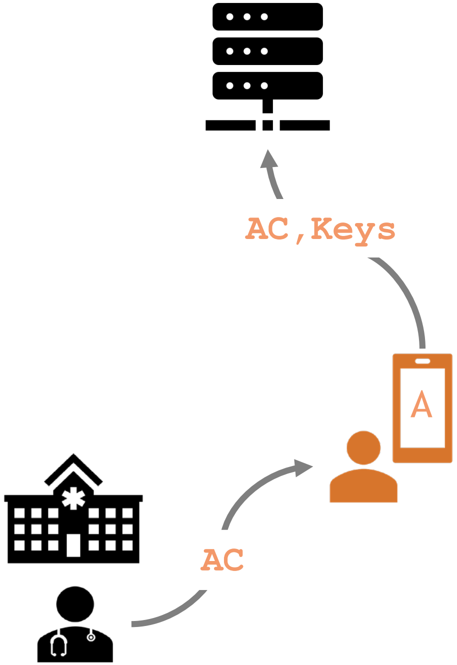


Existence of upload

⇩

the user is COVID+

Privacy of uploads
Our first idea

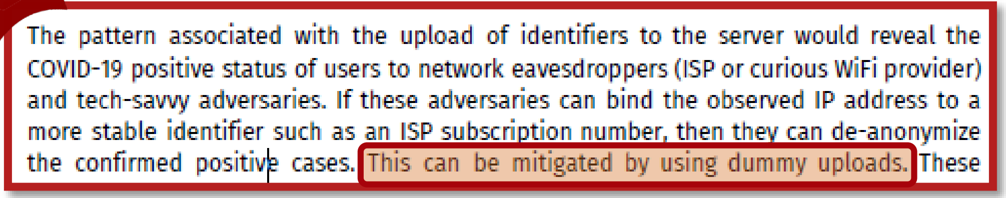


Existence of upload

⇓

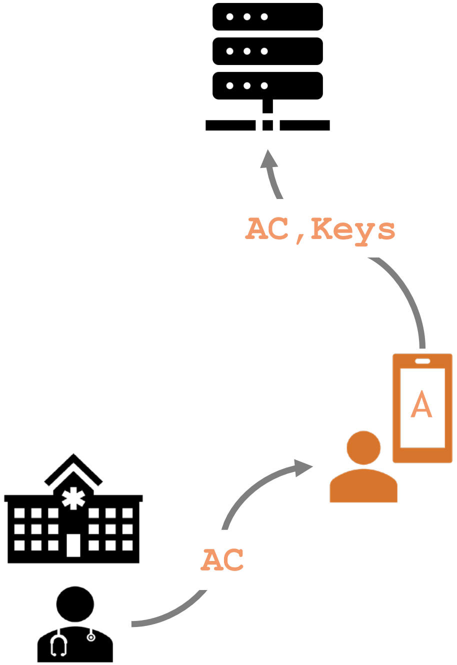
the user is COVID+

DP3T design paper


The pattern associated with the upload of identifiers to the server would reveal the COVID-19 positive status of users to network eavesdroppers (ISP or curious WiFi provider) and tech-savvy adversaries. If these adversaries can bind the observed IP address to a more stable identifier such as an ISP subscription number, then they can de-anonymize the confirmed positive cases. This can be mitigated by using dummy uploads. These

https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf

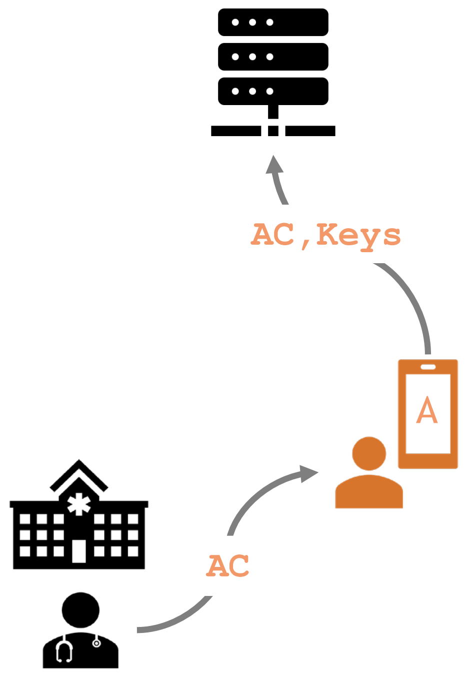
Privacy of uploads
Practice



- Unknown environment
  - What is users' behavior?

- https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Best%20Practices%20for%20Operation%20Security%20in%20Proximity%20Tracing.pdf

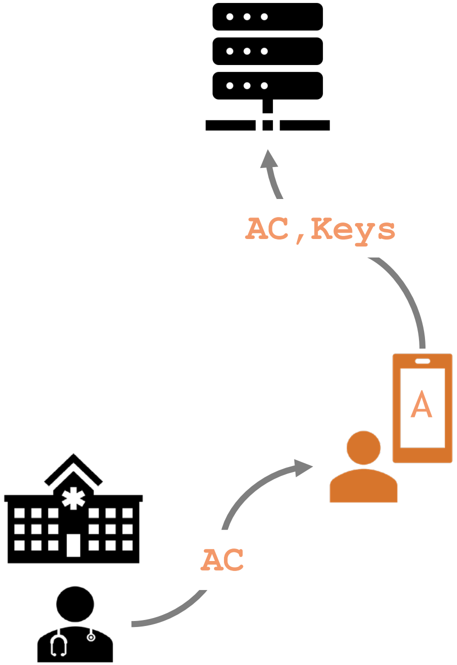
Privacy of uploads Practice



- Unknown environment
  - What is users' behavior?
- Constraints associated to the platform
  - Bandwidth
  - Server capacity
  - Battery
  - OS-mandated user interactions

- https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Best%20Practices%20for%20Operation%20Security%20in%20Proximity%20Tracing.pdf

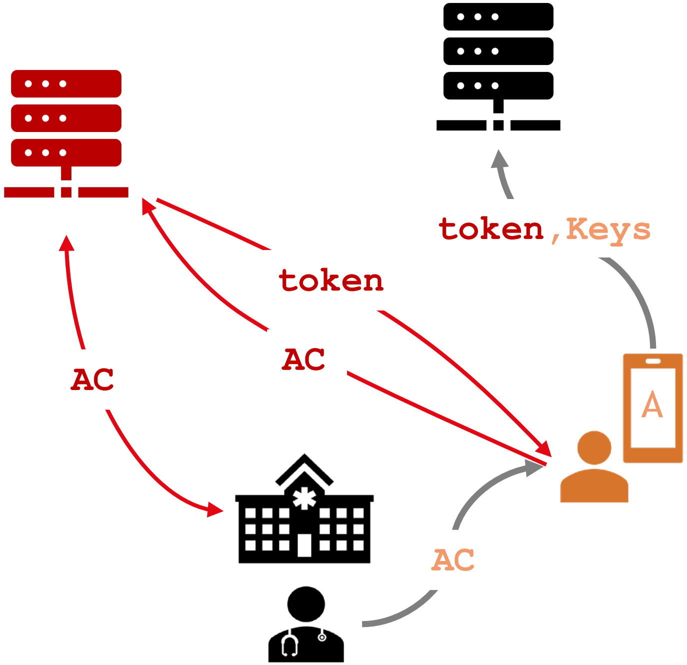
Privacy of uploads Practice



- Unknown environment
  - What is users' behavior?
- Constraints associated to the platform
  - Bandwidth
  - Server capacity
  - Battery
  - OS-mandated user interactions
- Delays and anonymity not possible
  - **Plausible deniability**

- https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Best%20Practices%20for%20Operation%20Security%20in%20Proximity%20Tracing.pdf

Privacy of uploads
Practice – there is authentication!

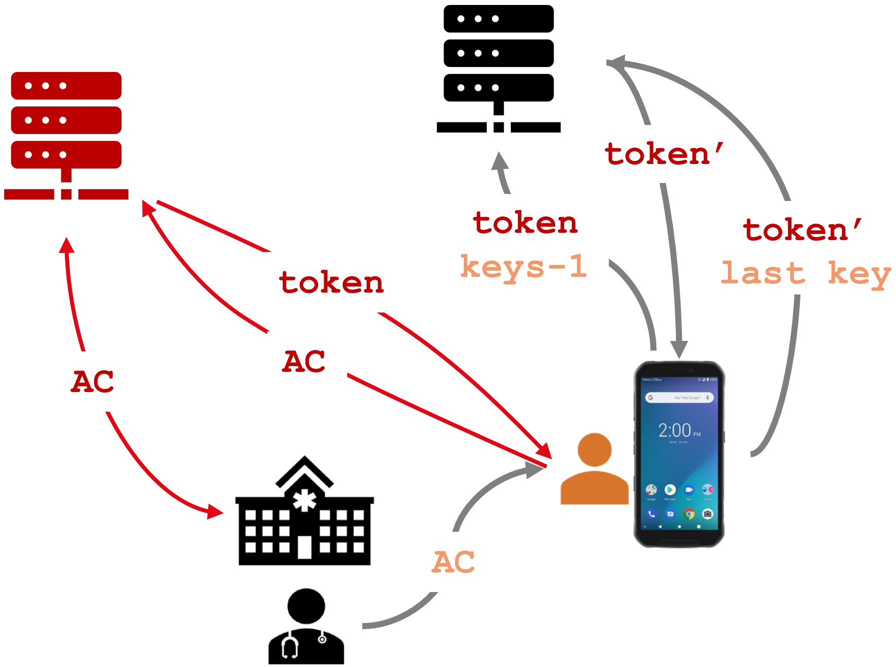


- Dummies also must realize the authentication step
  - Servers must consider dummies
  - Ensure equal timing and volume

- Mandatory pop-up
  - Dummies need delay between receiving token and upload keys

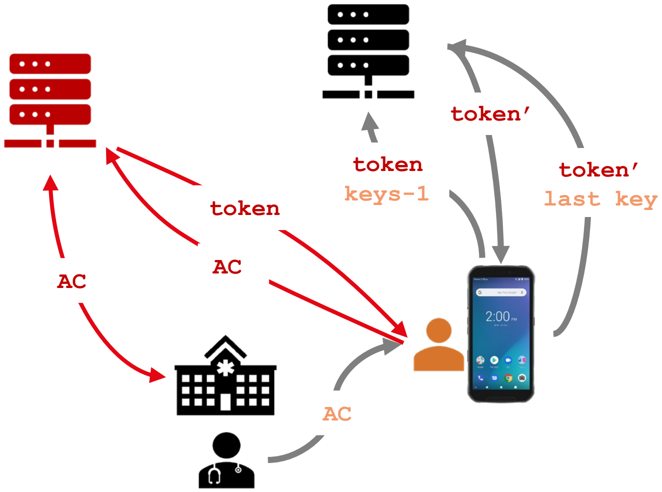
- https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf

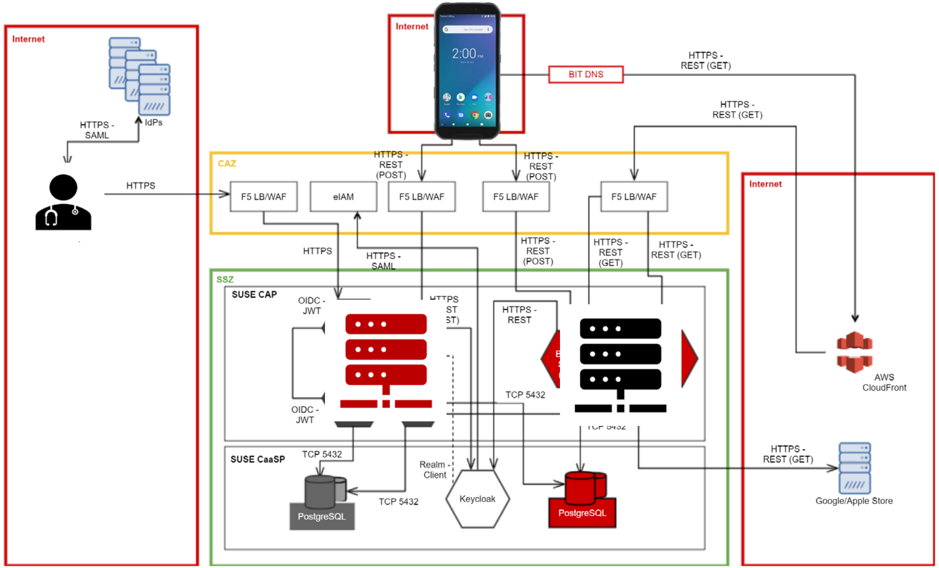
Privacy of uploads Practice –



- Exposure Notification API (<v1.5) had one security mechanism:
  - Only reveal key after it expires
  - (Not needed, it is an implementation decision)
- Implications on authorization and dummy strategy
  - Cannot delay all keys!
  - Need for extra token
  - Dummies must mimic second upload

Privacy of uploads
Practice – servers don't exist in the vacuum





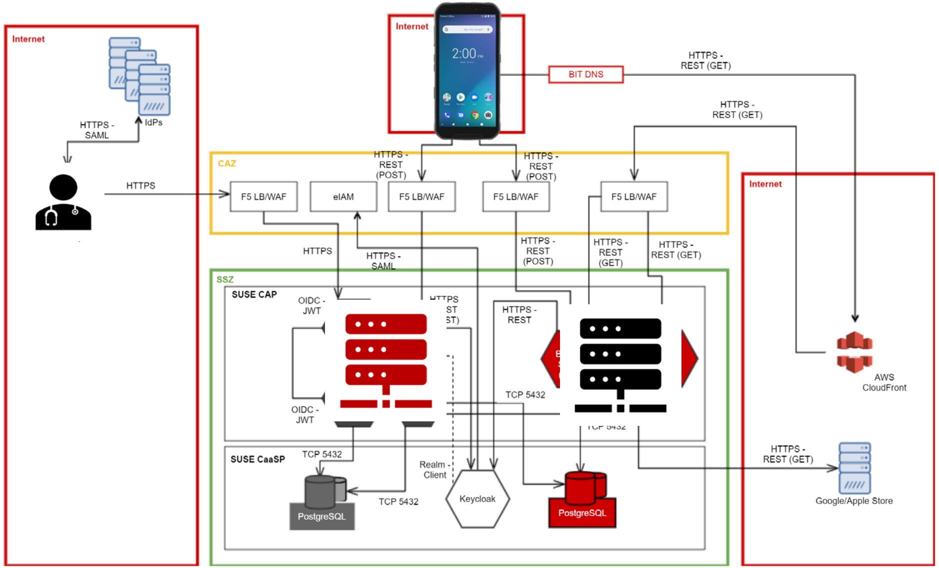
https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Best%20Practices%20for%20Operation%20Security%20in%20Proximity%20Tracing.pdf

Privacy of uploads
Practice – servers don't exist in the vacuum

- Load Balancer, Firewall
  - More information than expected!
  - Off the shelf cloud managing tools

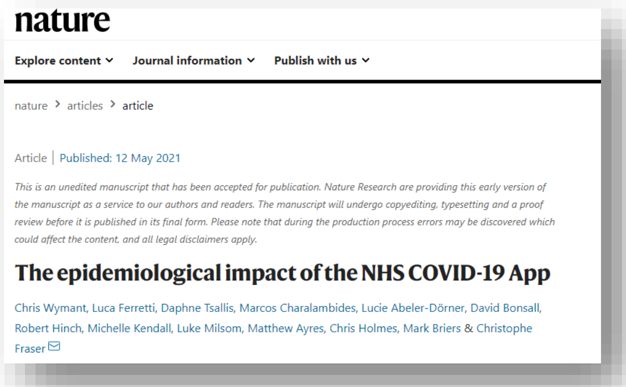
- Careful design of logging to avoid forensics
  - Coarse logging at key server
  - Only counts logged for statistics
    - e.g, active users based on dummy traffic

- Logging strategy re-designed N times



https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Best%20Practices%20for%20Operation%20Security%20in%20Proximity%20Tracing.pdf

Deployment and results



nature

Explore content ⌄ Journal information ⌄ Publish with us ⌄

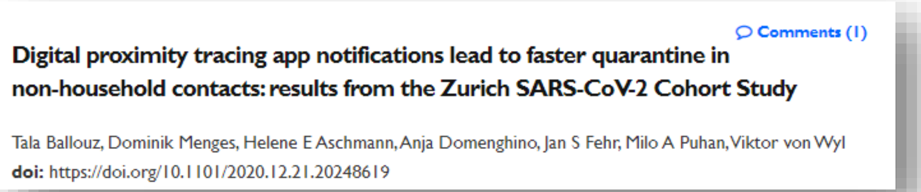
nature › articles › article

Article | Published: 12 May 2021

This is an unedited manuscript that has been accepted for publication. Nature Research are providing this early version of the manuscript as a service to our authors and readers. The manuscript will undergo copyediting, typesetting and a proof review before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers apply.

The epidemiological impact of the NHS COVID-19 App

Chris Wymant, Luca Ferretti, Daphne Tsallis, Marcos Charalambides, Lucie Abeler-Dörner, David Bonsall, Robert Hinch, Michelle Kendall, Luke Milsom, Matthew Ayres, Chris Holmes, Mark Briers & Christophe Fraser ✉

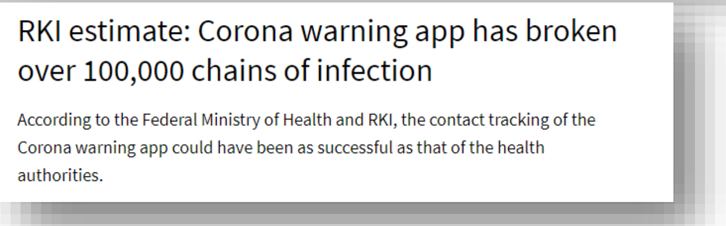


Comments (1)

Digital proximity tracing app notifications lead to faster quarantine in non-household contacts: results from the Zurich SARS-CoV-2 Cohort Study

Tala Ballouz, Dominik Menges, Helene E Aschmann, Anja Domenghino, Jan S Fehr, Milo A Puhan, Viktor von Wyl

doi: https://doi.org/10.1101/2020.12.21.20248619



RKI estimate: Corona warning app has broken over 100,000 chains of infection

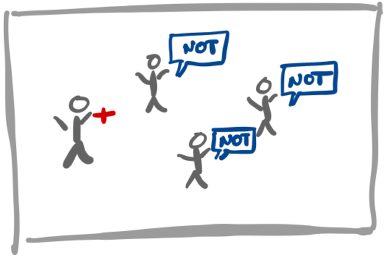
According to the Federal Ministry of Health and RKI, the contact tracking of the Corona warning app could have been as successful as that of the health authorities.

- https://www.experimental.bfs.admin.ch/expstat/en/home/innovative-methods/swisscovid-app-monitoring.html
https://github.com/digitalepidemiologylab/swisscovid_efficacy/blob/master/SwissCovid_efficacy_MS.pdf
https://www.ebpi.uzh.ch/dam/jcr:5fc56fb7-3e7e-40bf-8df4-1852a067a625/Estimation%20of%20SwissCovid%20effectiveness%20for%20the%20Canton%20of%20Zurich%20in%20September%202020_V1.5.pdf
https://www.medrxiv.org/content/10.1101/2020.12.21.20248619v1.full.pdf

Technology to help with pandemic contention

- Airborne transmission in ill-ventilated places can reach beyond 1.5-2 meters

- The need
  - **A complement** to **notify** users that have shared location
  - In a **privacy-preserving** and **abuse-resistant** manner



Goal: **notify** everybody that shared an indoor space with a SARS-CoV-2-positive person

Locations

- Restaurant
- Bar
- Church
- Lecture room

Events

- Party
- AA meeting
- Reading group
- Lecture

SAFE FOOD PRO

Food Safety & Contact Tracing

Welcome to

Sophie's Cafe | Main Entrance

8TMDMR

Please register your visit by scanning the QR Code with your ca
or entering the code 8TMDMR at https://track.safefoodpro.co.nz

Don't enter this building if you are unwell or have any of these symptoms:

- fever
- cough
- shortness of breath
- sneezing or a runny nose

Contact Tracing

Physical Distancing

track.safefoodpro.co.nz | www.covid19.govt.nz

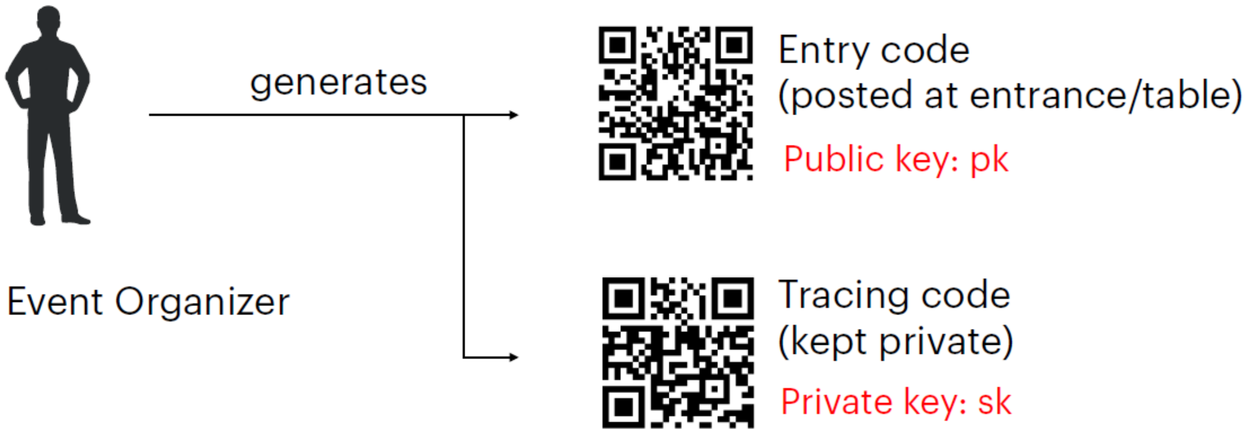
Unite against COVID-19

Centralized implementations appear

- Databases of positive and negative people
- Unique identifiers (phone / name / address)
- Register of (any) events

CrowdNotifier

1. SETUP



Event Organizer

generates

Entry code
(posted at entrance/table)

Public key: pk

Tracing code
(kept private)

Private key: sk

CrowdNotifier

2. USAGE

scans entry code

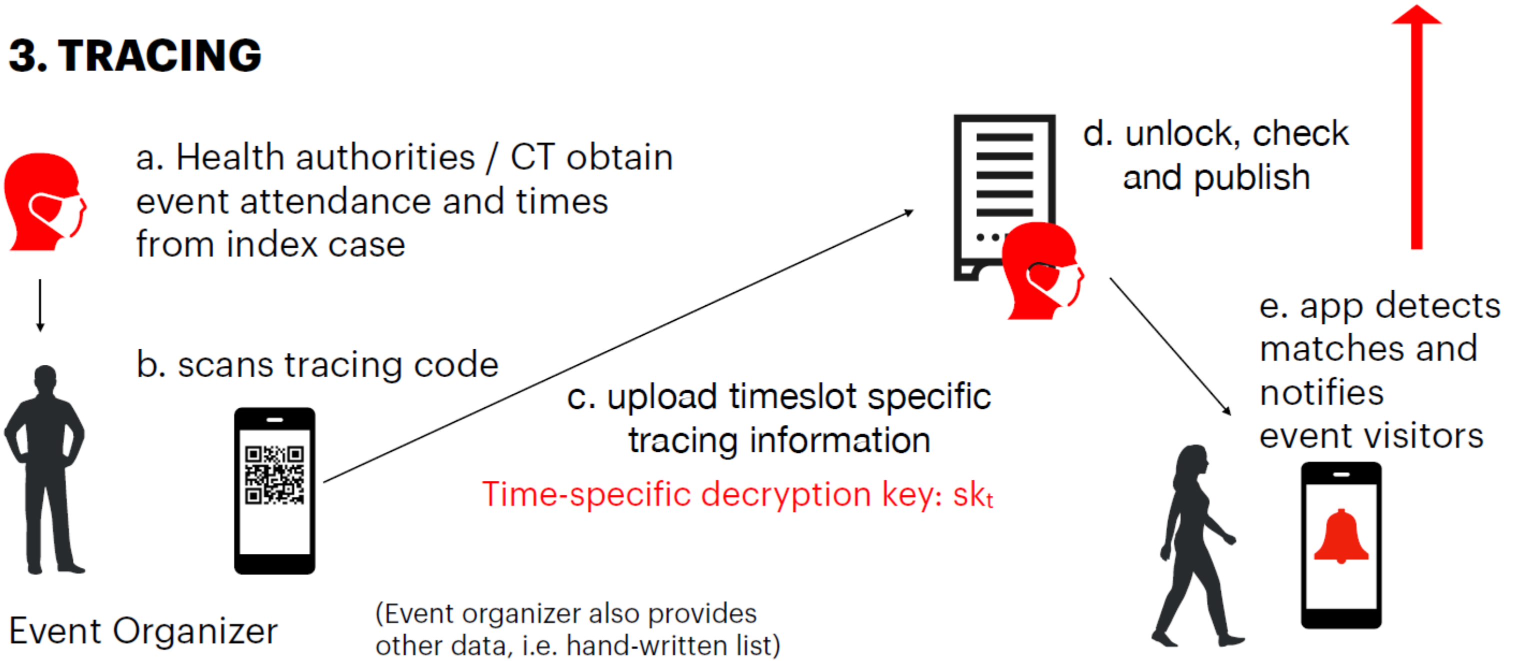
Event Visitor

Enc(pk, timeslot, entry-time & departure-time)

- Visitor stores **encrypted record** of visit containing *entry and exit times* (don't reveal which events were visited)
- (Optional) Diary on phone as memory aid
- Data stays on device, not shared with anyone else.

CrowdNotifier

3. TRACING



a. Health authorities / CT obtain event attendance and times from index case

b. scans tracing code

Event Organizer

c. upload timeslot specific tracing information

Time-specific decryption key: sk_t

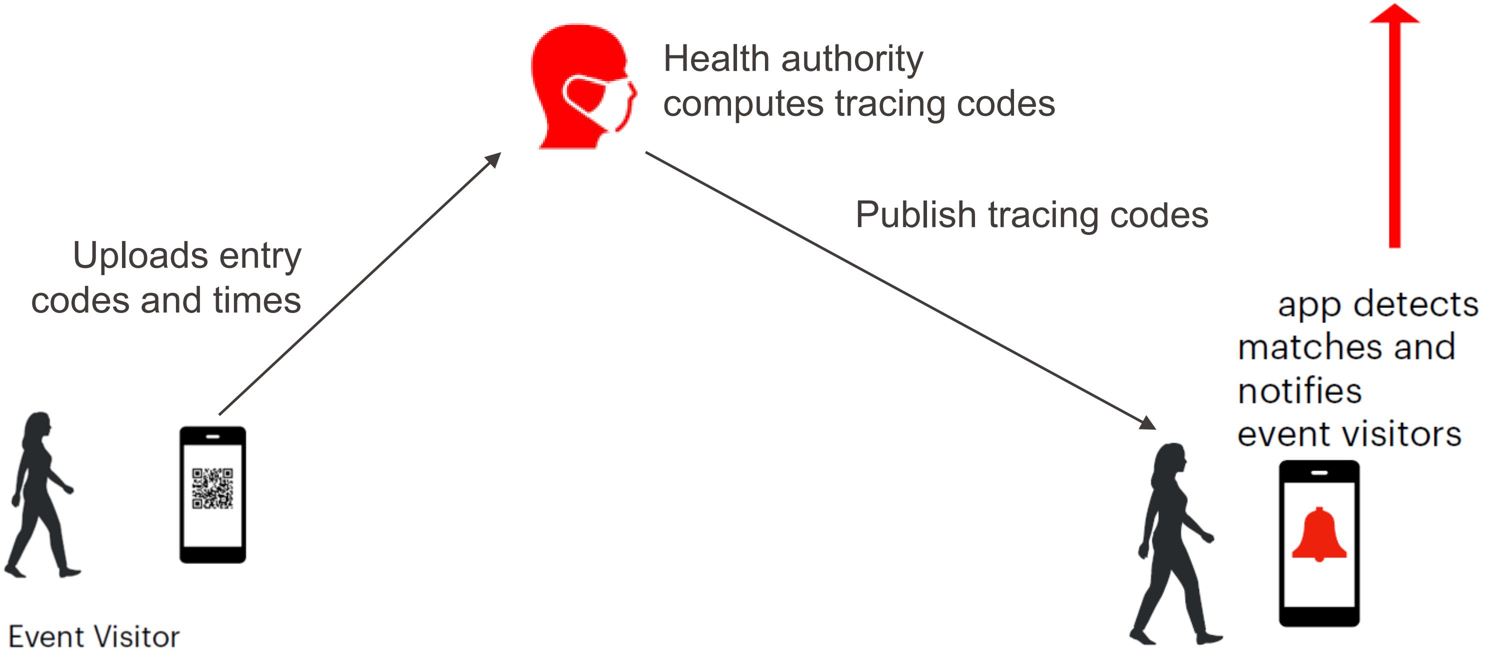
(Event organizer also provides other data, i.e. hand-written list)

d. unlock, check and publish

For each entry:
Try dec(sk_t, entry)

e. app detects matches and notifies event visitors

Server-based CrowdNotifier



For each entry:
Try dec(sk_t, entry)

Health authority
computes tracing codes

Uploads entry
codes and times

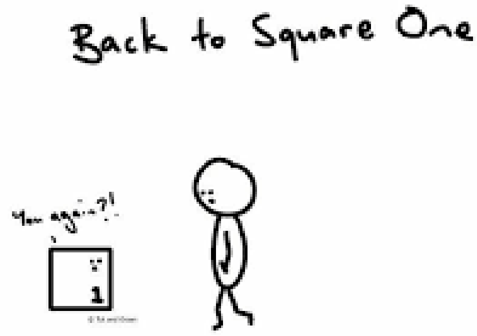
Publish tracing codes

app detects
matches and
notifies
event visitors

Event Visitor

Presence tracing
More privacy engineering

- **New constraints from OS suppliers**
  - Require users to vet uploads
- **Redesign dummy strategy**
  - Redesign authentication: second token
  - Redesign user experience: time for vetting
  - Redesign payload: new padding



Key lessons

- Data is not a must!

- Privacy engineering goes well beyond crypto
  - Good methods to design non-crypto privacy are not available

- Privacy engineering in an agile/service world is exhausting
  - Platforms and requirements continuously change
  - Formal methods not amenable to speed and agility

- Good socio-technical integration is key to success and it is **hard**
  - Purpose limitation and abuse prevention is a must