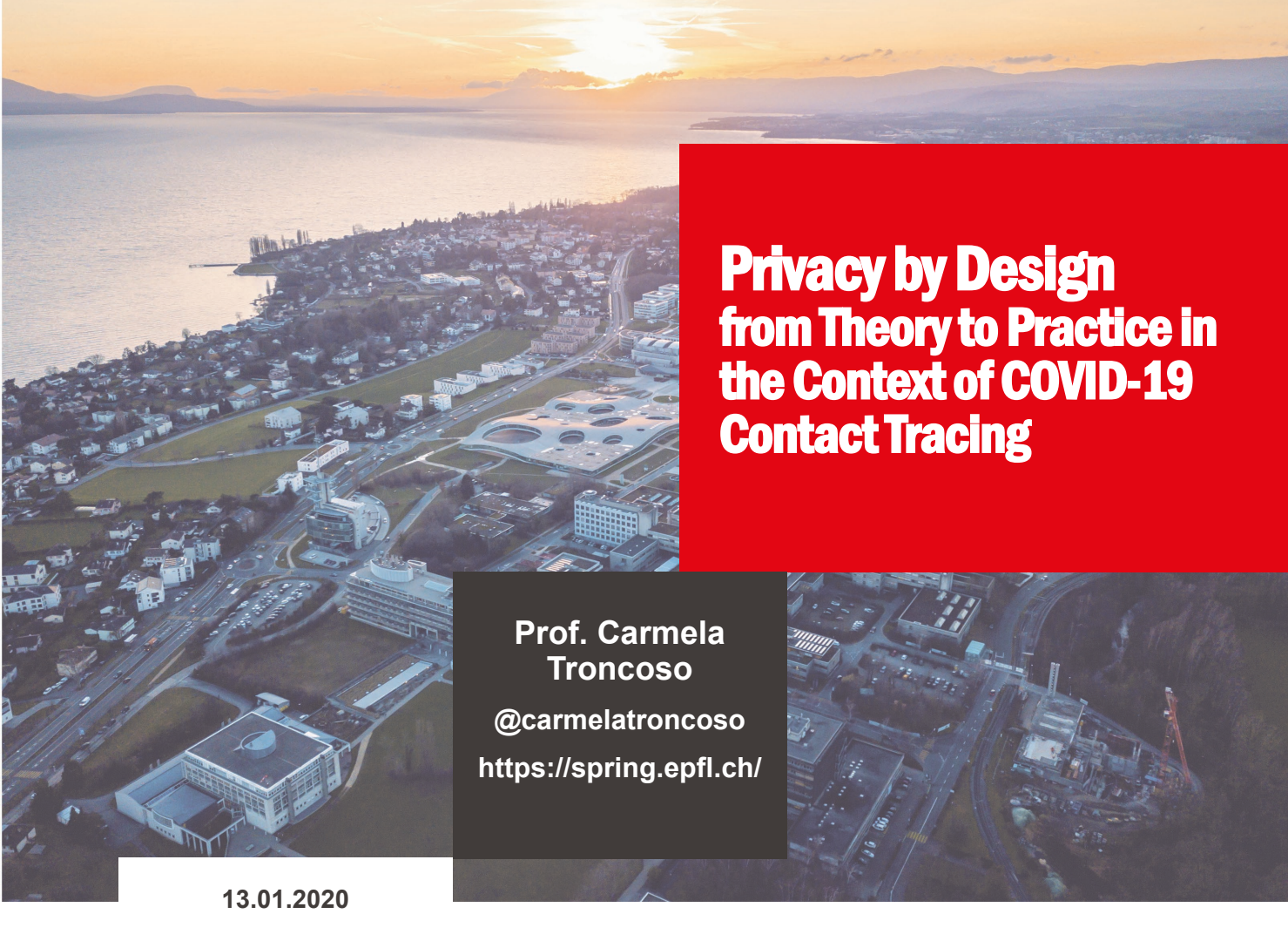


The background of the slide is an aerial photograph of a city, likely Lausanne, taken at sunset. The sun is low on the horizon, casting a warm orange glow over the city and the surrounding water. The city features a mix of residential and commercial buildings, with a prominent modern building with a circular design in the foreground. The water is calm, reflecting the sunset colors.

Privacy by Design from Theory to Practice in the Context of COVID-19 Contact Tracing

Prof. Carmela
Troncoso
@carmelatroncoso
<https://spring.epfl.ch/>

13.01.2020

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 constraints: Security and Privacy

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



The constraints: Security and Privacy

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 • NEWS 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

Comment

Covid 19 coronavirus: Subway worker 'harassed' woman customer after getting details for contact tracing

14 May, 2020 08:23 PM

© 3 minutes to read

BBC Sign in Home News Sport Reel Worklife Travel Future Cult

NEWS January 2021

Home Coronavirus Video World UK Business Tech Science Stories Entertainment & Arts Health

Asia China India

Singapore reveals Covid privacy data available to police

Top Story
Indonesia

The constraints: Security and Privacy

Apple launches COVID-19 'Exposure Notification Express' with iOS 13.7 — Android to follow later this month

Darrell Etherington @etherington / 6:00 PM GMT+2 • September 1, 2020

Comment

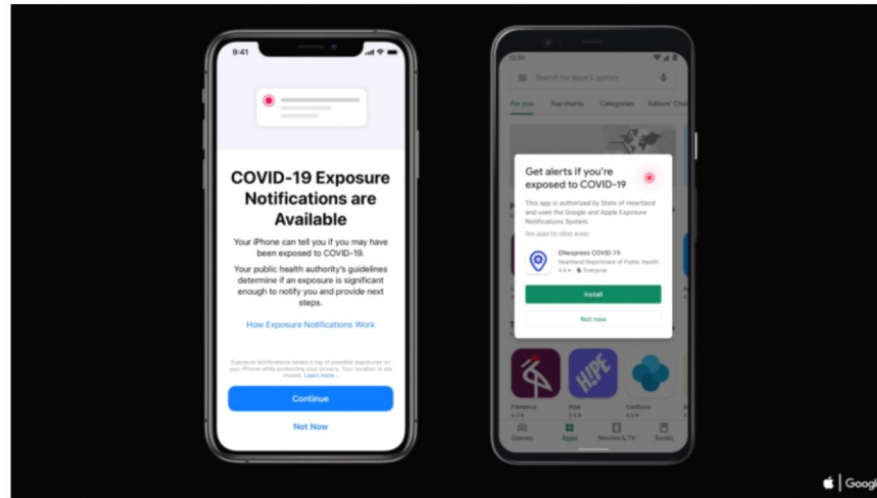


Image Credits: Apple / Google

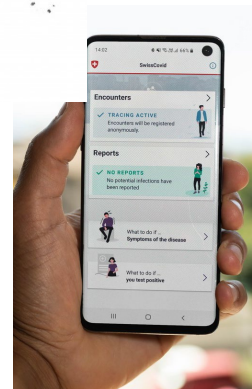
The constraints: Security and Privacy

- 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



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



Apps Maintenance
and support

March 2020 – **Start DP3T**

April 2020 – **GAEN is announced**

May 2020 – **Final version DP3T**

June 2020 – **Pilots EU apps**

July/August 2020 – **CT Apps launching**

August/September 2020 – **Towards EU interoperability**

Since September – **Presence tracing**
(some members) **Immunity Certificates**

Decentralized Privacy-Preserving Proximity Tracing

Version: 25 May 2020.

Contact the first author for the latest version.

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 Čapkun, Prof. David Basin, Dr. Jan Beutel, Dr. Dennis Jackson, Dr. Marc Roeschlin, Patrick Leu

KU Leuven: Prof. Bart Preneel, Prof. Nigel Smart, Dr. Aysajan Abidin

TU Delft: Prof. Seda Gürses

University College London: Dr. Michael Veale

CISPA: 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

IMDEA Software Institute: Prof. Dario Fiore

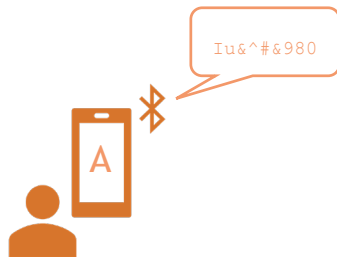
INESC TEC: Prof. Manuel Barbosa (FCUP), Prof. Rui Oliveira (UMinho), Prof. José Pereira (UMinho)

Key ideas:

- BLE beacons broadcast/ recorded by devices
- Cryptography for unlinkability
- Decentralization of matching operations for privacy and purpose limitation

The system design

The theory...



- The App creates a **secret key (SK)** and from this key it derives **identifiers (EphID)** broadcasts via Bluetooth
- Secret keys are updated every day
 $SK_{t+1} = H(SK_t)$
- $EphID_1 || \dots || EphID_n$ (where SK_t , "broadcast key"))
- A random identifier is generated for a limited amount of time
- Without the key, no-one can link two identifiers

Reality

Use existing infrastructure

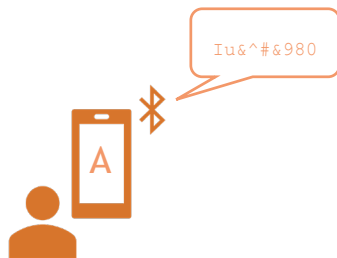
- Battery and CPU usage
 - Limited round trips
 - Google and Apple **must** be involved
- Run in the background
 - Apple **must** be involved
- Compatibility Android - iOS
 - Google and Apple **must** be involved
- Google and Apple implement the protocol **and the API**
 - Implications on privacy engineering
 - Implications for epidemiology and exposure estimation (no time in this talk...)
 - Implications for privacy when internationalizing (no time in this talk...)



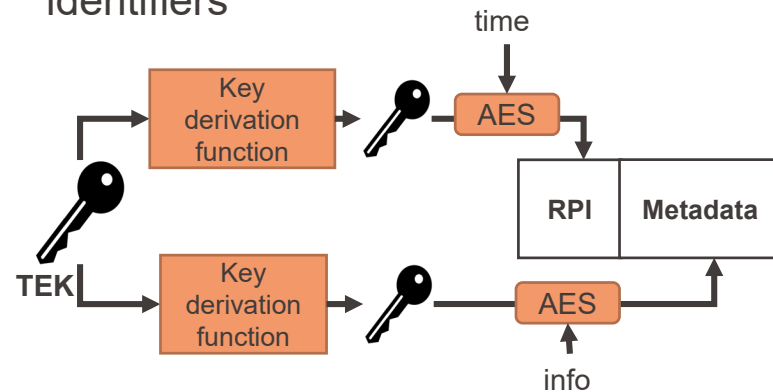
The system design

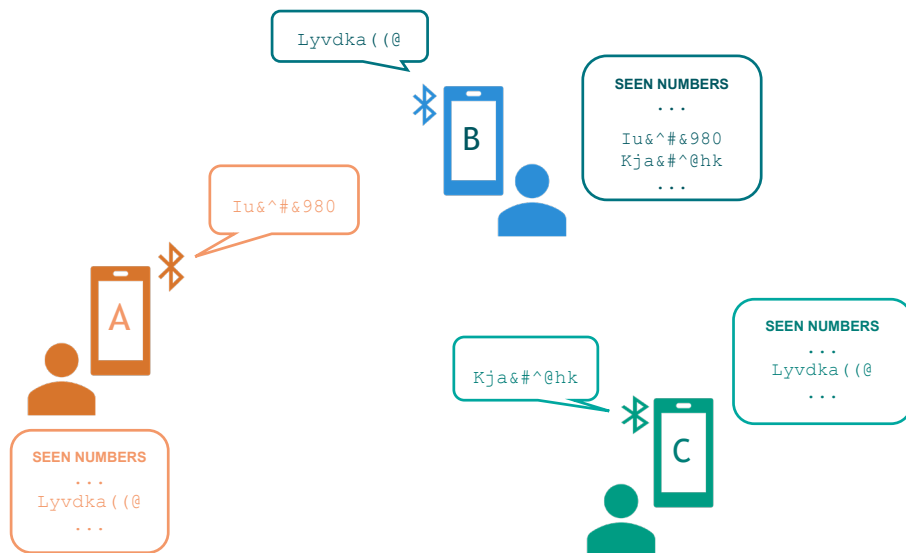
The practice

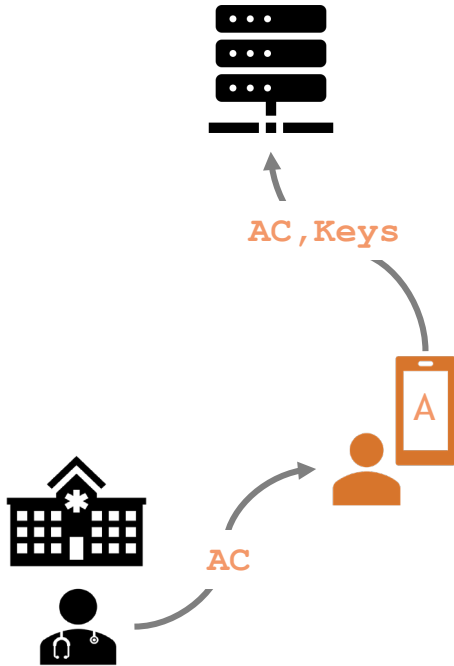
Google and Apple decide



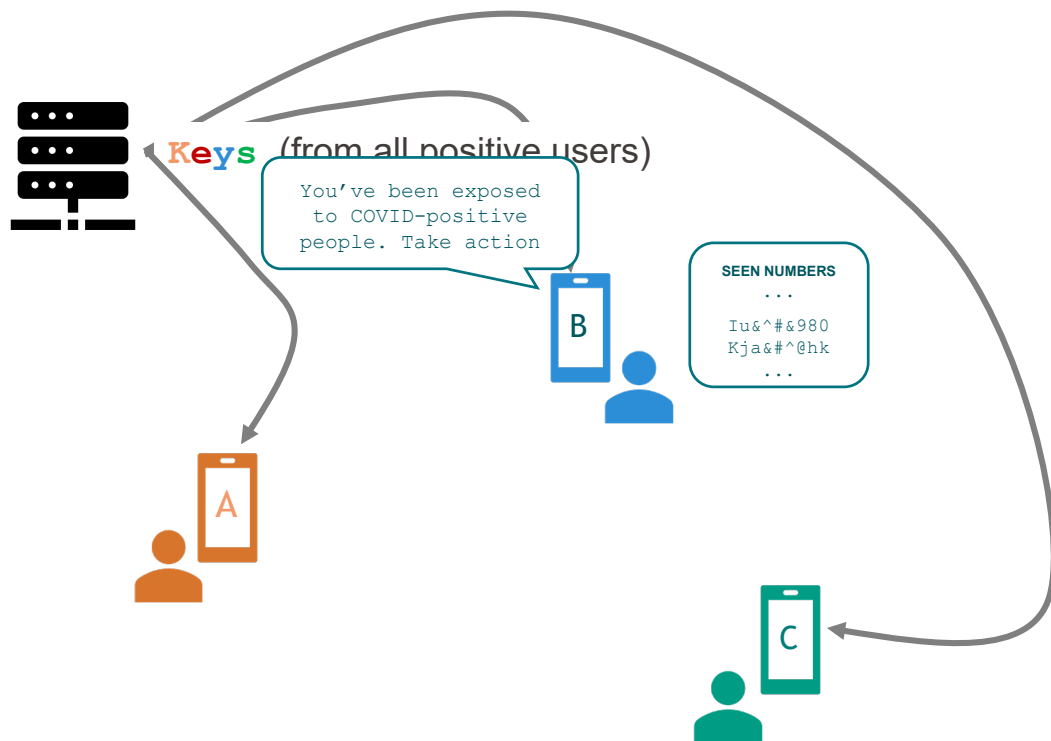
- The App creates a **secret every day (TEK)** and from this key it derives **random identifiers (RPIs)** that it broadcasts via Bluetooth
- A random identifier is used for a limited amount of time
- Without the key, no-one can link two identifiers



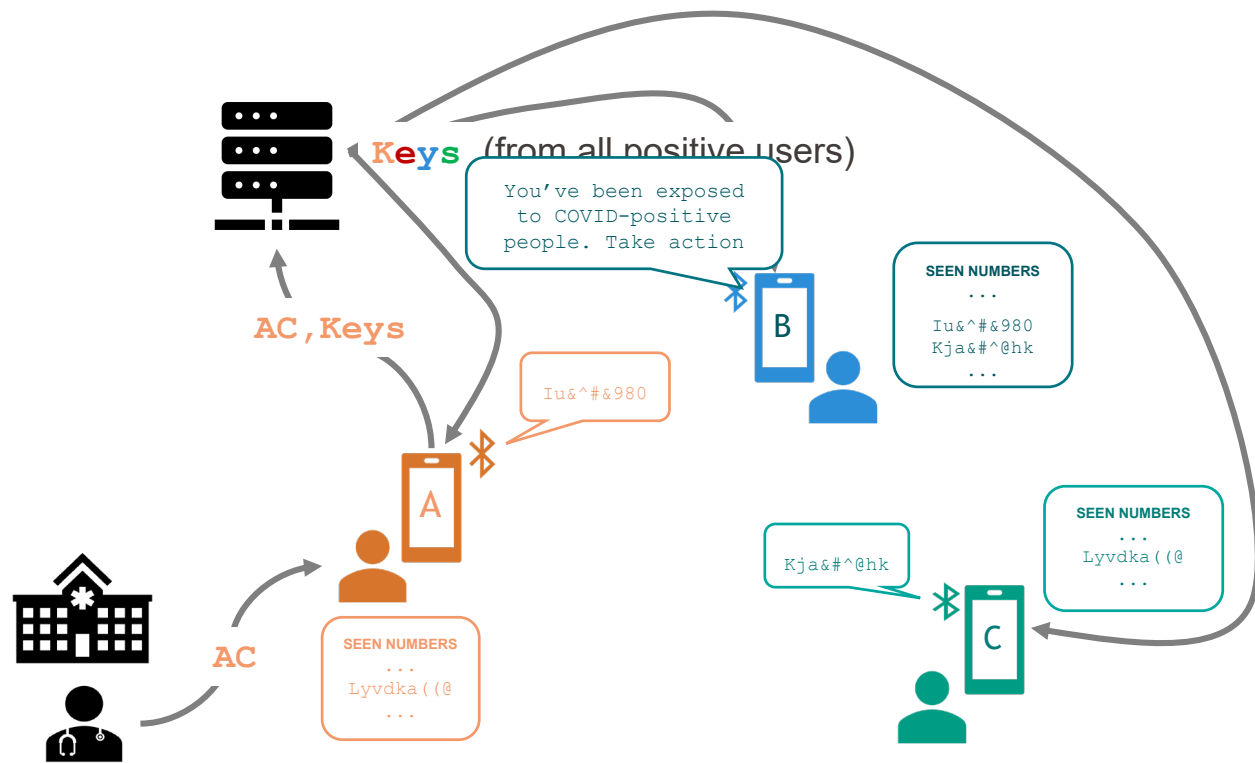




The system design



The system design



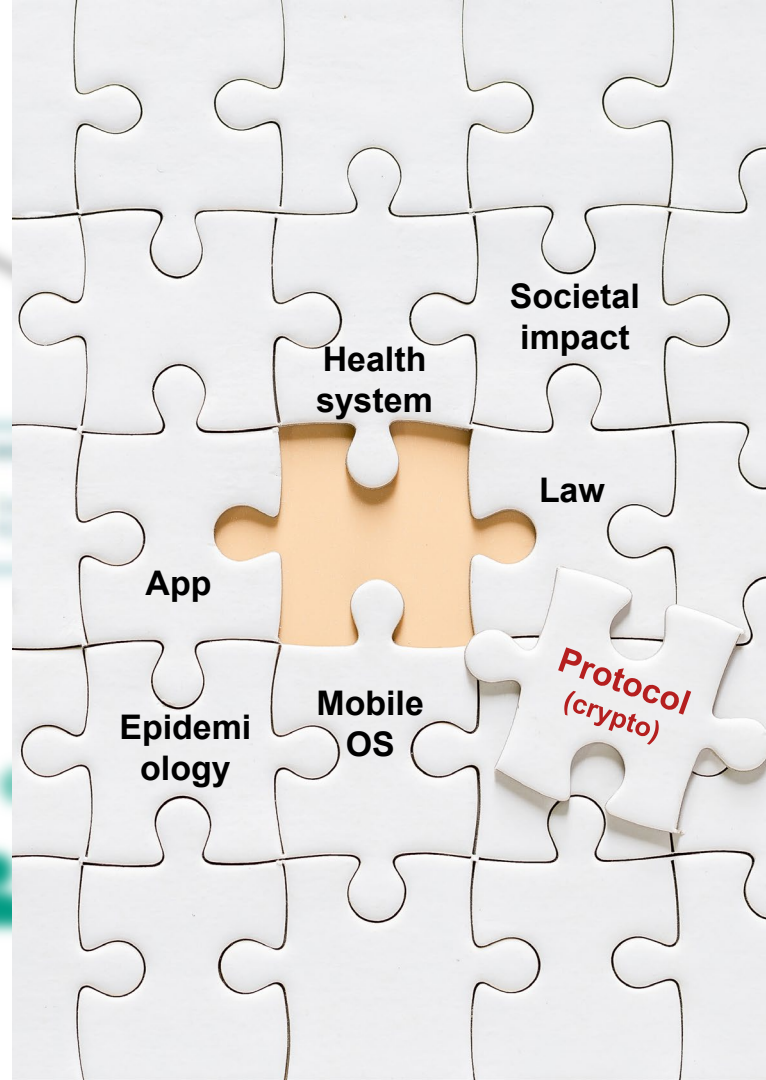
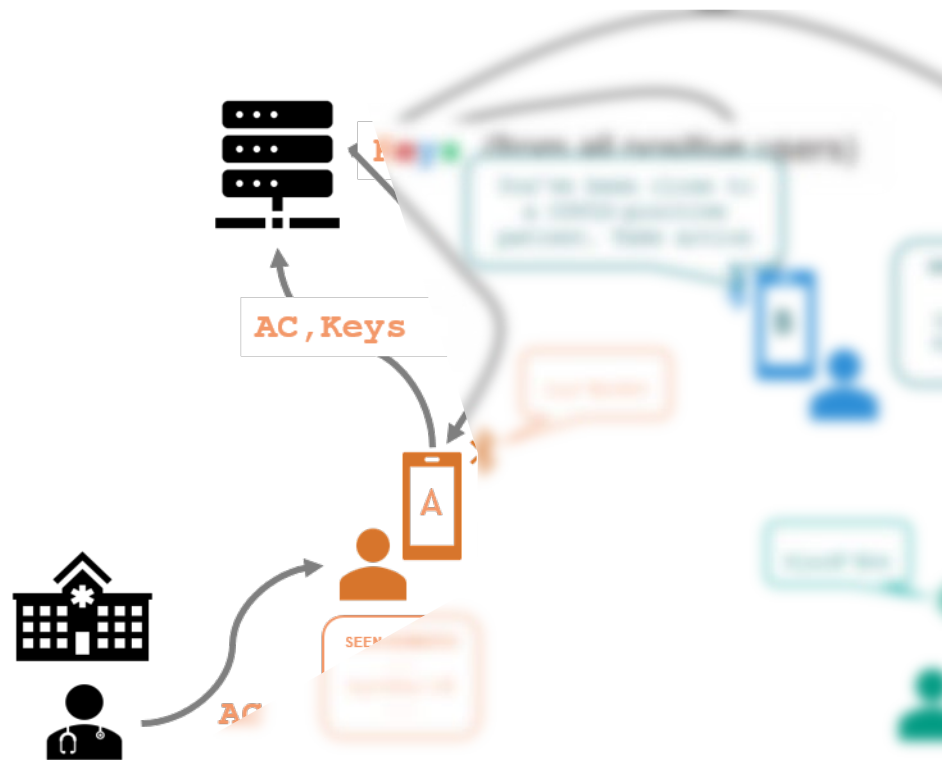
Only information that ever leaves the phone are the **TEKs broadcasted** during the contagious period.

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

No information available for abuse

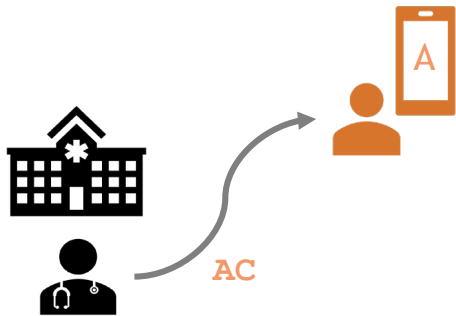
System **sunsets-by-design**

The system design



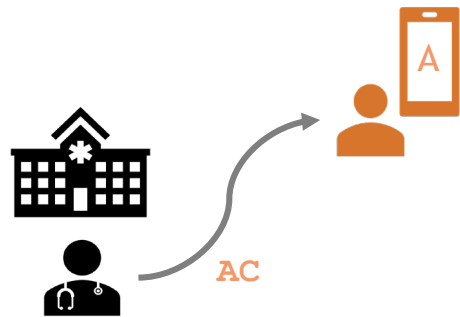
Authorization mechanism Theory

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



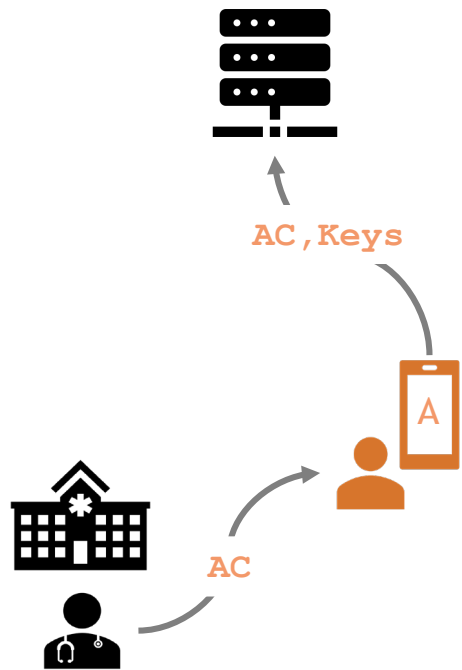
Authorization mechanism Practice

- 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
 - Simple activation codes sent via phone/mail/sms
 - Different level of automatization
 - Belgium went for (light) commitments!

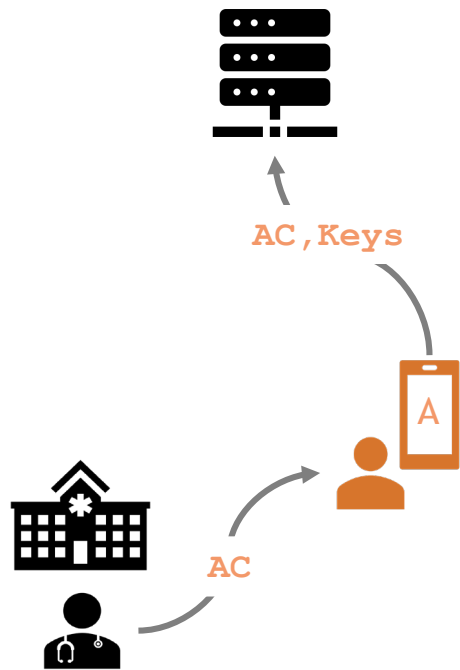


Privacy engineering

Are we done?



Privacy of uploads Theory



Existence of upload

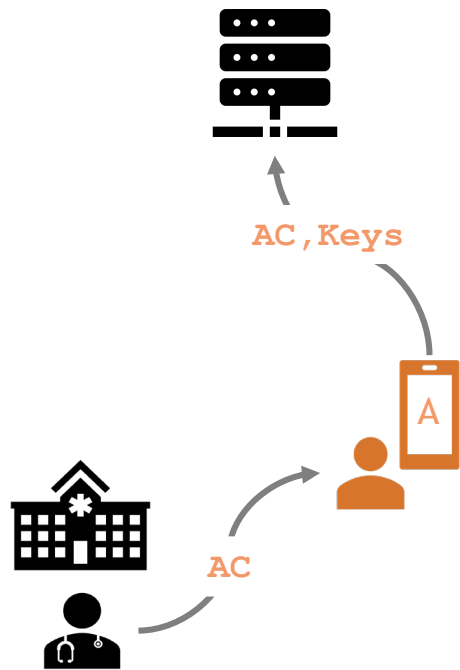


the user is COVID+

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

Privacy of uploads Practice



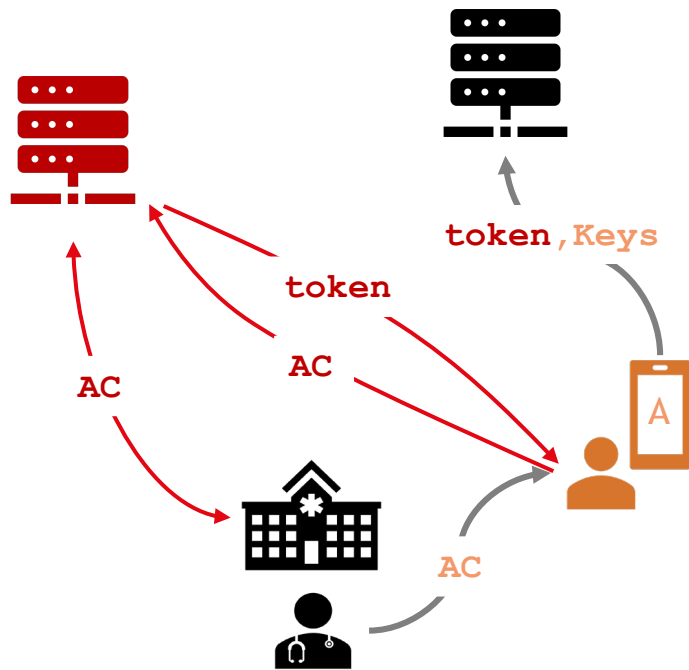
- Unknown environment
 - What is users' behavior?
- Constraints associated to the platform
 - Bandwidth
 - Server capacity
 - Battery
- Anonymity and delays not possible



Plausible deniability
(constant time & size)

Privacy of uploads

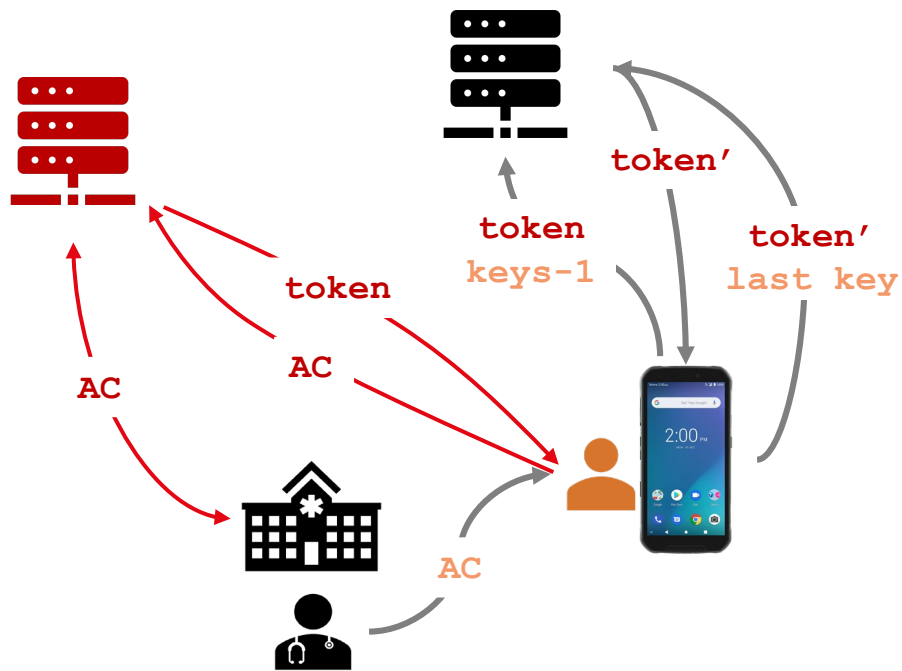
Practice – there is authentication!



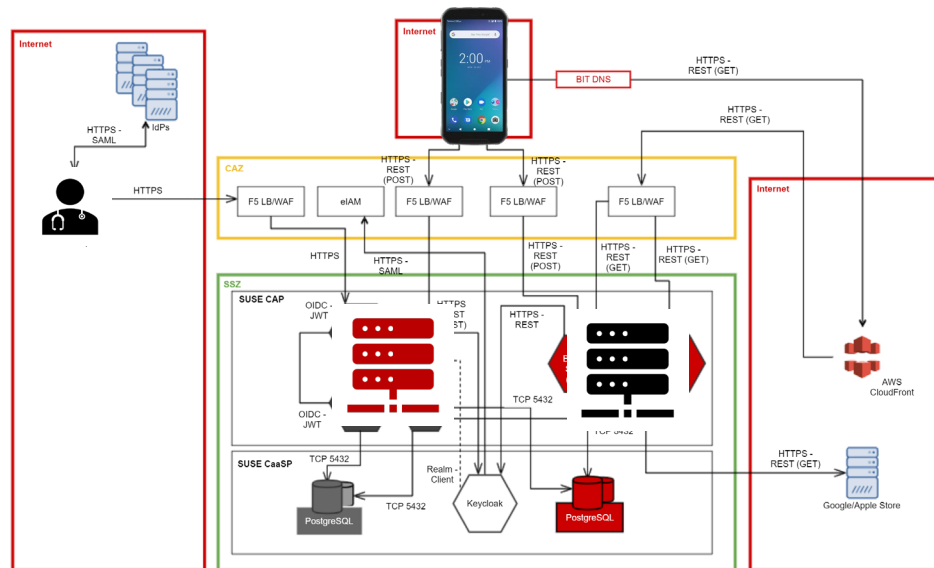
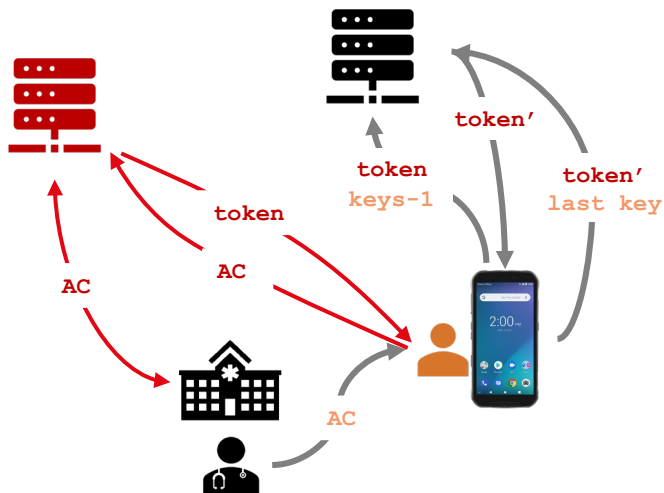
- Dummies also must realize the authentication step
 - Servers must consider dummies
 - Ensure equal timing and volume

Privacy of uploads

Practice -



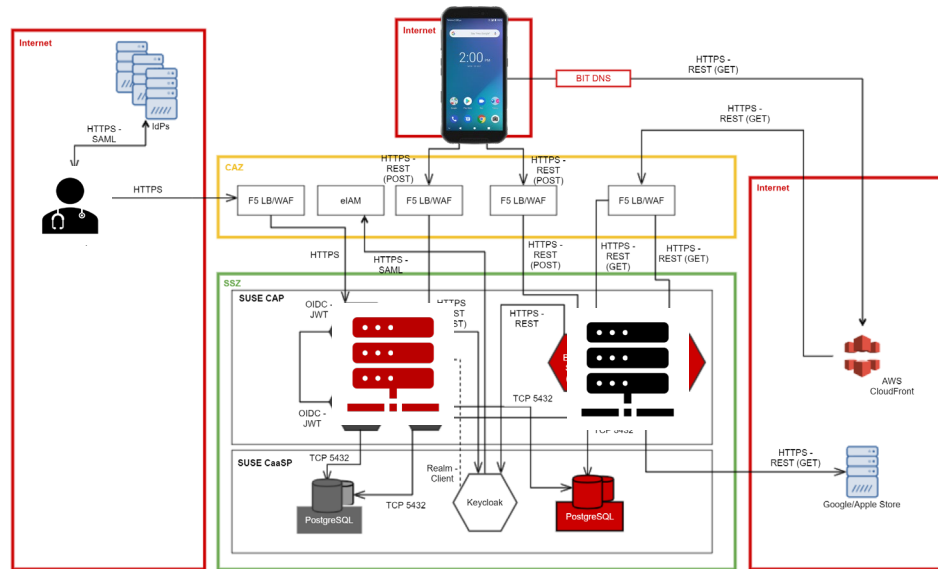
- Exposure Notification API (<v1.5) had one security mechanism:
 - Only reveal key after it expires
 - (Not needed, it is an implementation decision)
- Implications on authorization and dummy strategy
 - Cannot delay all keys!
 - Dummies must mimic second upload
- Phone does not always wake up...



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



Where is this deployed?

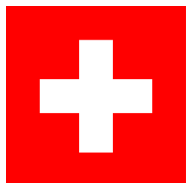


1.87 Million active users (~22% population)

~18000 COVID-positive users uploaded their keys in December (15% of PCR in Switzerland)

Field experiment in Zurich October 2020

- 80% COVID-positive app users upload their codes
- 22% sent quarantine
- 1 in 10 tested positive after notification
- 5% of positives with respect to Manual Contact Tracing in Zurich
- Speed: ~1 day faster notification for non-household exposures (70% of the cases)



<https://www.experimental.bfs.admin.ch/expstat/en/home/innovative-methods/swisscovid-app-monitoring.html>

https://github.com/digitalepidemiologylab/swisscovid_efficiency/blob/master/SwissCovid_efficiency_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>

Key lessons

- Data is not a must!
- Privacy engineering goes well beyond crypto
- Privacy engineering in an agile/service world is exhausting
 - Platforms and requirements continuously change
- Good socio-technical integration is key to success and it is **hard**
 - Purpose limitation and abuse prevention is a must

-

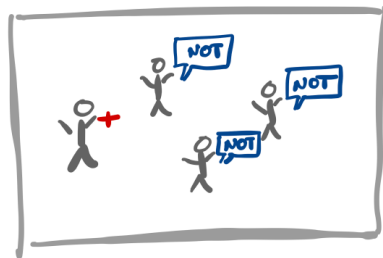
Where to go from here

Digital contact tracing solved?

- Google/Apple dependency (and also Amazon!)
 - Can it be eliminated?
 - Device-based contact tracing is a possibility? (free from Bluetooth?!)
- At least reduce trust?
 - Can we verify the randomness of the keys?
 - Can we verify their libraries without seeing them?
- Can we eliminate beacon-authentication related attacks?
 - Without Google and Apple's collaboration?

The pandemic is still here

More technologies to the rescue



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

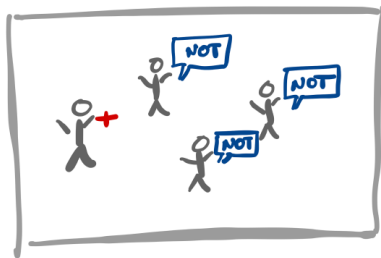
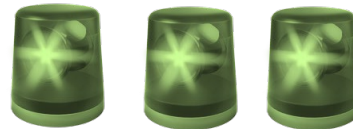


Implementations appearing

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

The pandemic is still here

More technologies to the rescue



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

Our proposal

- Privacy for users (from locations, databases)
- Privacy for SARS-CoV-2-positive location
- Abuse prevention by design

<https://notify-me.ch/en>

(link to white paper at the bottom)
(new pairing-based version soon!)

The pandemic is still here

More technologies to the rescue



Implementations ???

- Danger of...
 - central database
 - global tracking of users
 - discrimination
 - function creep

The pandemic is still here

More technologies to the rescue



**Cannot limit the
purpose by design**
(nor the longstanding
impact)



Post-doctoral position SPRING Lab



Do you want to use your crypto skills to deploy socially-responsible technologies?

Come help us in our privacy-engineering efforts. Example partners:

Position for 1 year (extendable)



ICIJ

THE INTERNATIONAL CONSORTIUM
OF INVESTIGATIVE JOURNALISTS

More info: <https://spring.epfl.ch/>

Our projects: <https://github.com/spring-epfl>

Applying: email carmela.troncoso@epfl.ch