From ROBERT to DESIRE exposure notification: situation and lessons learned

Vincent Roca

From ROBERT to DESIRE exposure notification: situation and lessons learned

Vincent Roca, Inria, PRIVATICS team, FR
vincent.roca@inria.fr, https://team.inria.fr/privatics/
Workshop on Security and Privacy in Contact Tracing, September 11th, 2020
https://visp.wien/news/contact-tracing-workshop/

Guiding design objectives

1. Be **efficient** (it's the primary goal)

2. Be **sovereign** (keep control of choices and citizens' data)

3. Be **privacy friendly** (it's a high responsibility, tool is sensitive)

4. Be **flexible** (which country you want to deploy the app does matter a lot… there's n o single answer)

Outline

- ROBERT and StopCovid

- What about GAEN? Would it be an option?
- DESIRE, a 3rd way for a European exposure notification system

ROBERT and StopCovid

- early April, decision to propose a “centralized” approach for France
  - risk analysis carried in a **central server** that necessarily keeps some information (e.g., pseudonyms of users potentially at risk)
  - under the control of the **Health Authority** (data controller)
  - audited by our **Data Protection Agency** (CNIL)

- still convinced it is the best option for France

#1 Efficiency considerations

- being centralized is a plus from an epidemiological viewpoint
  - real-time knowledge of epidemic spread
  - monitoring of the number of warnings sent
  - full control on warning criteria (e.g., to adjust to PCR testing capacity)

Can be critical in crisis time!

- StopCovid official statistics not yet available (expected soon)
  - … but the situation changed quite a bit since June
  - end of August: in spite of low app usage, **currently approx. 100 uploads/day** (user tested COVID+ who volunteer to share data) **and 10 notifications/day**

#2 Sovereignty considerations

- sovereignty is the only reasonable approach
  - keep control of citizen's **health data**
    - "Alphabet's Verily Plans to Use Big Data for Health Insurance", Bloomberg, 2020/08/25
    - Q: what's the price to pay for the free GAEN system?
  - keep control of **technology**
    - choose what is the best option, freely
    - minimize dependence on G&A (e.g., with Orange new sovereign captcha service in place of Google re-captcha, as asked by CNIL)

- … despite difficulties (it requires more work, from all viewpoints)

#3 Privacy considerations

- user privacy is not an option, data is sensitive… High responsibility
- lesson learned: ask your DPA as soon as possible!
  - we did it for ROBERT **specifications** (in April)
    - Deliberation N°. 2020-046 of April 24, 2020 delivering an opinion on a proposed mobile application called "StopCovid"
  - for app **development** work (in May)
    - Deliberation N° 2020-056 from 25 May 2020 delivering an opinion on a draft decree relating to the mobile application known as StopCovid
  - for StopCovid **deployment** (audit in June… App v1.1 validated in Sept. 3rd)
    - Décision n°2020-015 du 3 septembre 2020 - Clôture de la décision n°2020-015 du 15/07/2020 mettant en demeure le ministère des Solidarités et de la Santé
  - periodic audits will continue to take place

CNIL says current StopCovid is GDPR compliant ☺

Outline

- ROBERT and StopCovid
- What about GAEN? Would it be an option?

- DESIRE, a 3rd way for a European exposure notification system

No, GAEN has major privacy issues

- Google/Apple Exposure Notification (GAEN), being **decentralized**, creates IOHO unacceptable discrimination risks

reason: ”making public a pseudonymized database containing health data is risky”

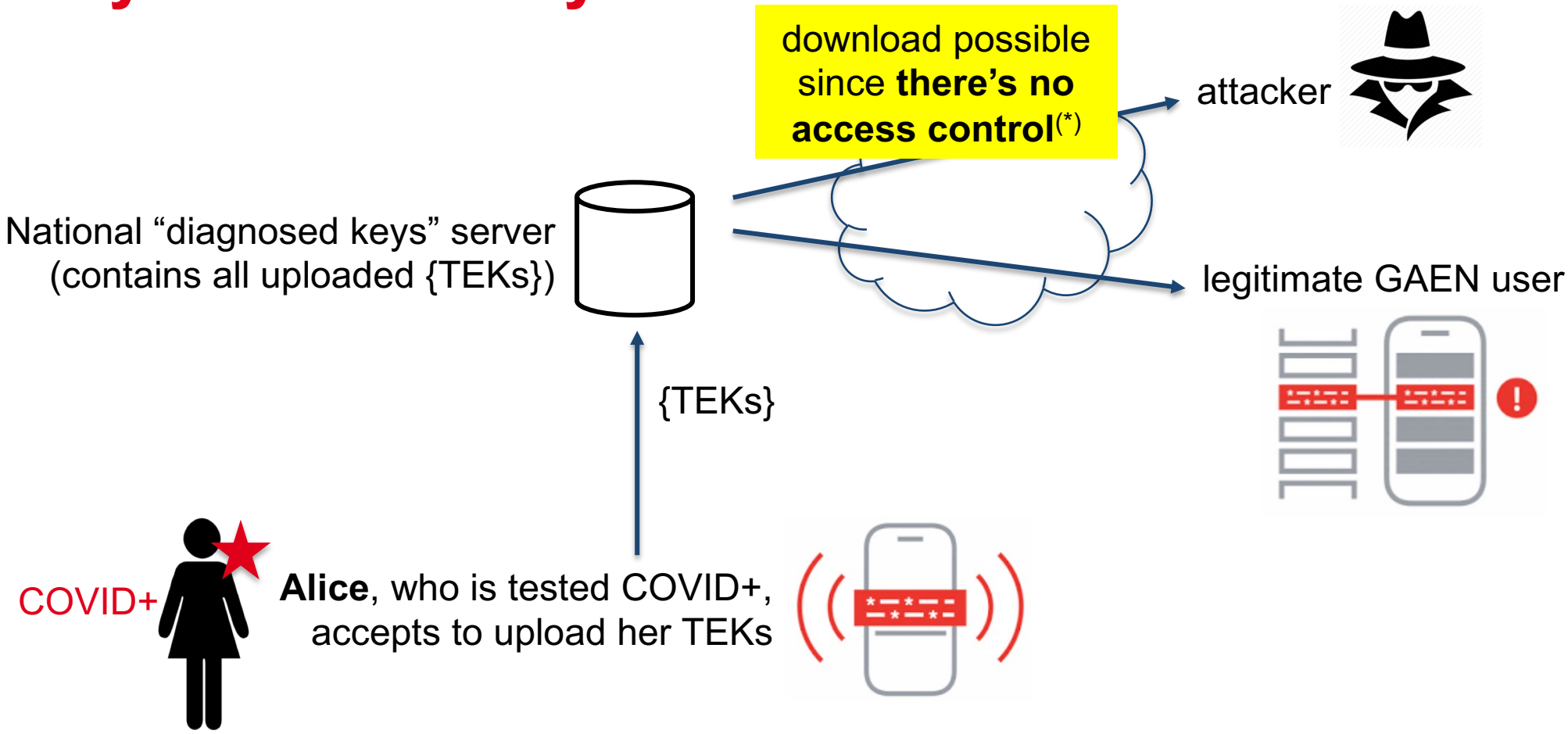
this entry is for a COVID+ GAEN user

(NB: we redacted TEK data)

Listing 4: Content extracted of the `export.bin` of KeyFile with the `TEKs` redacted

```
start_timestamp: 1593561600
end_timestamp: 1593568800
region: "ch"
batch_num: 1
batch_size: 1
signature_infos {
  verification_key_version: "v1"
  verification_key_id: "228"
  signature_algorithm: "1.2.840.10045.4.3.2"
  1: "ch.admin.bag.dp3t"
}
keys {
  key_data: "REMOVED"
  transmission_risk_level: 0
  rolling_start_interval_number: 2655936
  rolling_period: 144
}
keys {
  key_data: "REMOVED"
  transmission_risk_level: 0
  rolling_start_interval_number: 2655936
  rolling_period: 144
}
...
```

Why is GAEN risky?



(*) S. Farrell, D. Leith, « Transparency in the Deployment of Coronavirus Contact Tracing Apps » https://down.dsg.cs.tcd.ie/tact/transp.pdf

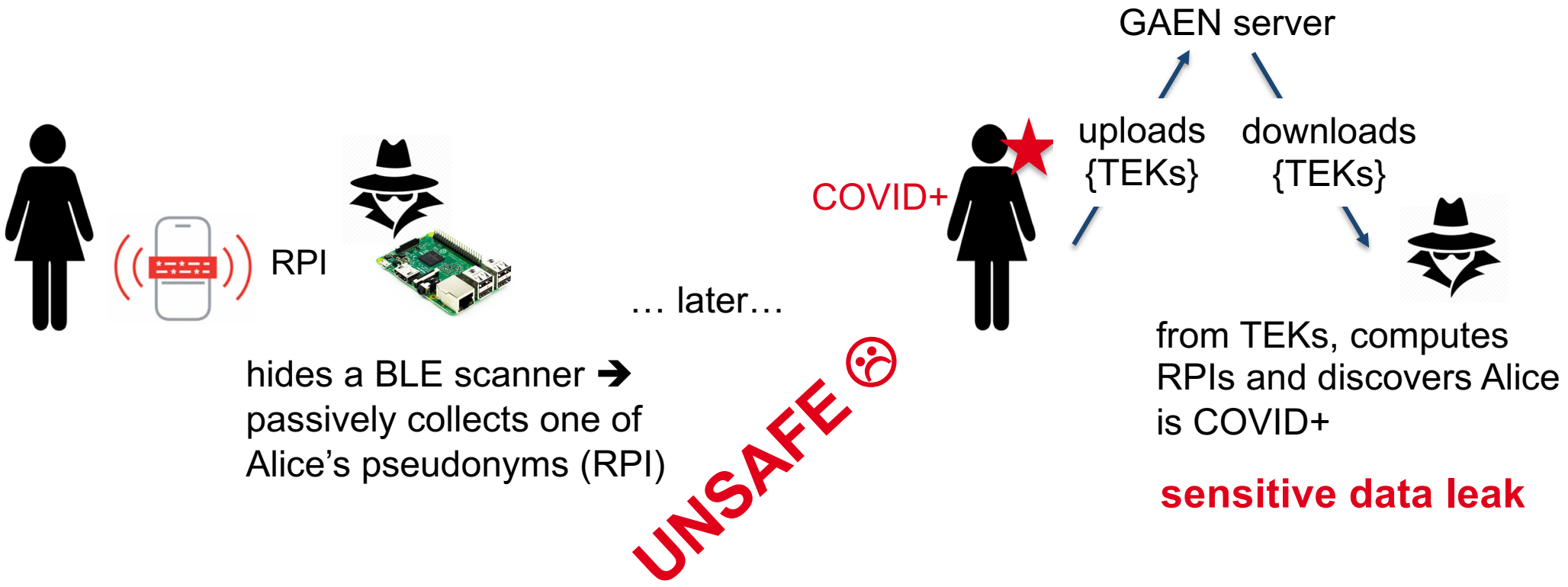
Why is GAEN risky? (2)

- Summary: database contains **pseudonyms** (since TEKs enable to compute the associated daily pseudonyms, the RPIs) **attached to health data** (i.e., persons tested COVID+)

➔ Key question: can an attacker re-identify Alice?

- No if the attacker only collects TEKs from the national server, and **nothing else**
  - TEKs are for days in the past, associated RPIs won't be used any more, useless for re-identification purposes

It’s different if the attacker did BLE scans



- The attacker anticipated and **started collecting RPIs in an area of interest**…
- … then he **immediately knows** if someone associated to the RPIs collected has uploaded her TEKs after being tested COVID+

Many variants possible depending on…

- … the attacker's **area of interest**
  - a building, a shop, a company, an administration
- … his **motivations**
  - compute statistics (how many COVID+ persons living in my building | in my shop | at my competitor…)
  - re-identify people
- … his **capabilities**
  - deploy a camera along with the BLE scanner (an employer want's to know) to easily re-identify infected users
  - use a fidelity card information

Is it difficult? No

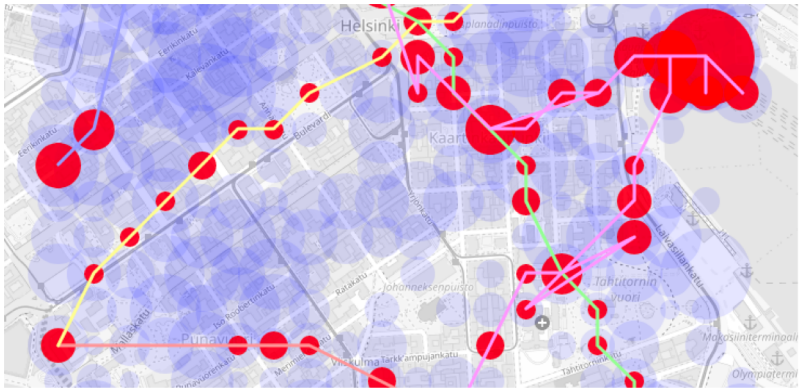
- very **cheap devices**
  - old smartphones, dedicated devices (10 Euros or so)
- very **easy to hide**
  - anywhere (e.g., in a mailbox)
- very **easy to setup**
  - plug and play softwares (free BLE scanners available)

BLE scanners already exist for GAEN

- https://github.com/oseiskar/corona-sniffer (Android sniffer app now available)

BLE contact tracing sniffer PoC

How "anonymous" is the semi-decentralized BLE contact tracing provided by Apple & Google (*GAEN* a.k.a. *ENS*) or DP-3T?



- for additional information and “paparazzi attack”

  “The Dark Side of SwissCovid”, Prof. S. Vaudenay, https://lasec.epfl.ch/people/vaudenay/swisscovid.html

A known problem, without known solution

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

- "Replay Attacks", June 14th, 2020

> "**Unmasking users by eavesdropping EphIDs**
>
> […] It is important to keep the app running whenever infection situations with unknown people can occur, but it is better to turn it off at home, which reduces the replay attack risk on the receiving side, when in places that should later not be exposed, or when at work if a risk of BLE collectors operated by the employer exists."

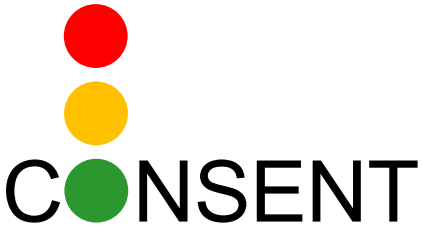
- "Security Report Proximity Scanning", May 28th, 2020
  - **Feasibility** of the "secret sharing" mitigation is **uncertain** [VR: it has been removed from DP-3T May 25th spec.] and anyway depends on Google / Apple willingness

- "Best Practices: Operational Security for Proximity Tracing", June 2020, DP-3T
  - DP-3T authors suggest the privacy leak is of lower importance because it's difficult given the low number of uploaded infected keys, propose a mitigation but conclude "**we do not currently recommend**".

Would GAEN be applicable to France? Probably not

- reason 1: IOHO we think our Data Protection Agency would not validate GAEN as GDPR compliant
  - NB: this is only an opinion
  - threats are practical and concern sensitive data

- reason 2: users must be aware of discrimination risks while agreeing to upload their “diagnosed keys” for a valid, informed consent
  - this obligation will probably **discourage** most users



Outline

- ROBERT and StopCovid
- What about GAEN? Would it be an option?
- DESIRE, a 3rd way for a European exposure notification system

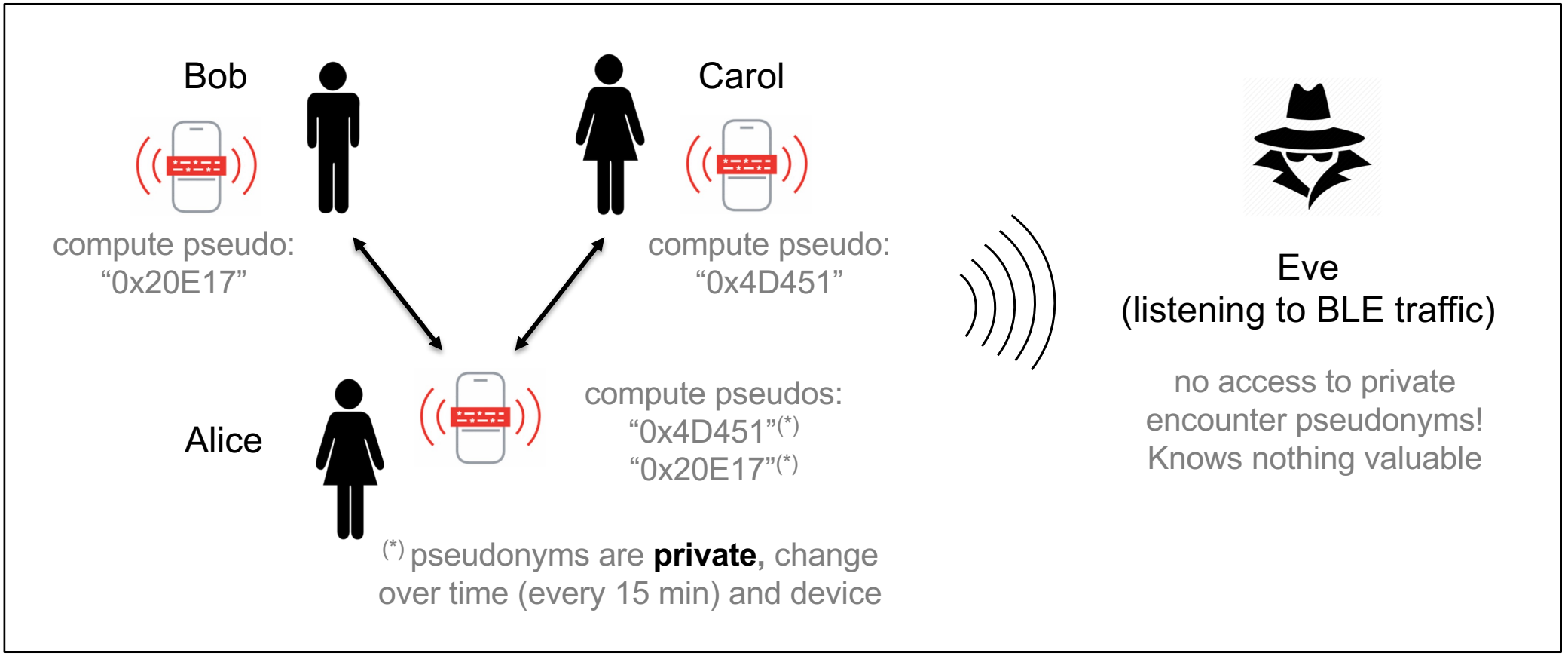
DESIRE: share private encounter pseudonyms

paradigm shift: from **public device** pseudonyms to **private encounter** pseudonyms

- pseudonyms are called ”Private Encounter Tokens” (PET):
  - **change** across time and devices
  - are **private** to users who meet, eavesdroppers cannot recompute them
- based on well-known Diffie-Hellman crypto

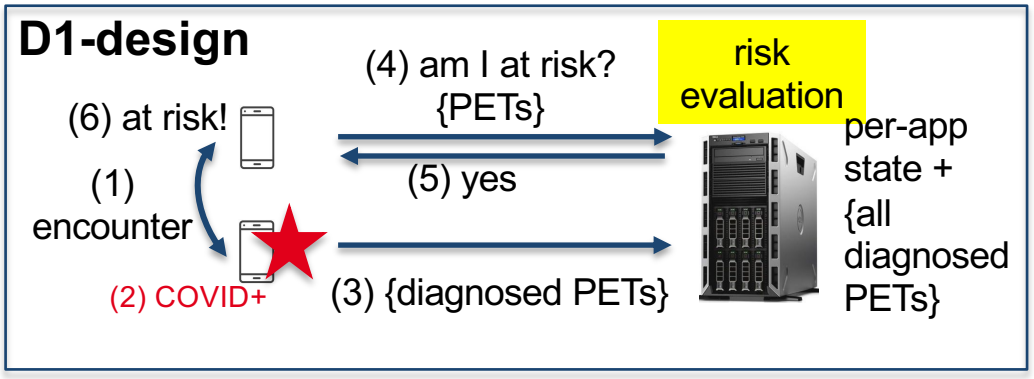
(NB: for privacy reasons, we derive two different PETs per encounter, on for status query, the other one in case of COVID+ diagnosis)

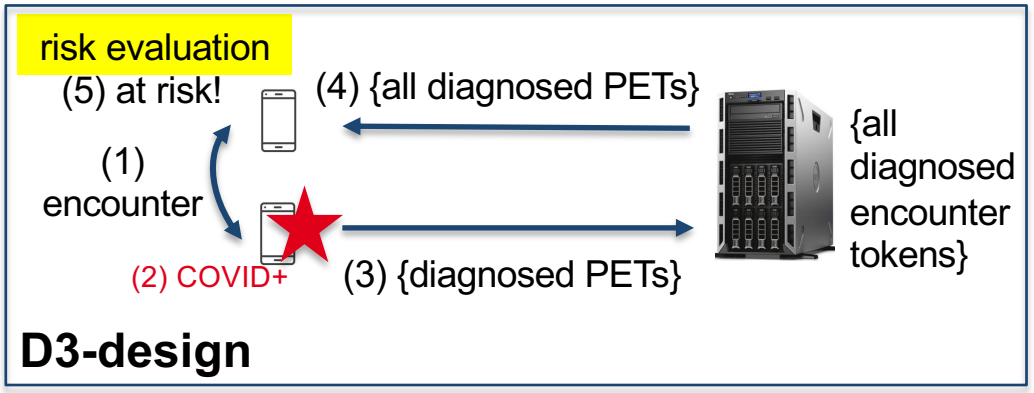
DESIRE: share private encounter pseudo. (2)



DESIRE can be (cen/decen/*)tralized

- (D1-design) **centralized** risk evaluation
- (intermediate D2-design)
- (D3-design) **decentralized** risk eval.





#4 Flexibility criteria: choose what deployment you want, freely

- each country chooses what to do, in a **sovereign** manner
  - citizens don't trust their institutions and are not afraid of discrimination risks (limited with DESIRE)? ➔ decentralized
  - citizens trust their DPA and institutions? ➔ centralized
- all DESIRE deployments fully **interoperate**, seamlessly
- Matches Criteria #4: flexibility ☺
  - it's not the case of ROBERT or GAEN

Beyond paper work: our Proof-of-Concept

Smartphone side (Kotlin Android app)

- **BLE**
  - done: tested 3 options, carousel mode is fine for maximum compatibility
  - no consumption/acquisition time issue found
- **Asymmetric crypto computations**
  - done: no latency/power issue found
- **Protocol**
  - done
  - supports centralized and dec. modes

- **TODO:** assess traffic load, probably the price to pay for privacy

Server side (Python, emulated server)

- **App registration**
  - done
- **Protocol**
  - done
  - supports centralized and dec. modes

Conclusions

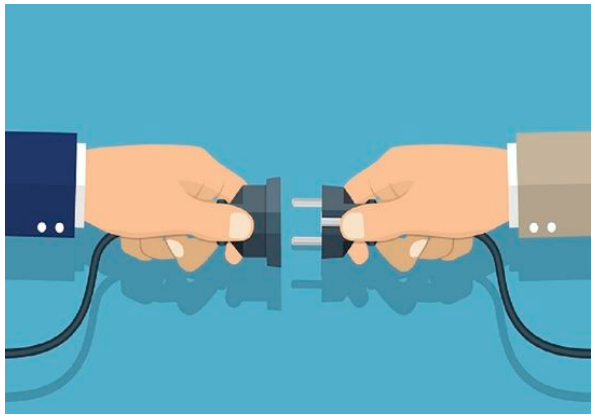
Conclusions and lessons learned

- no perfect security and privacy
  - special situations (e.g., US votes) may require to suspend the service for some time
- yet digital tracing may be effective
  - proposing something was the **only valid option**
- very **proud** of ROBERT/StopCovid
  - being centralized and sovereign were key decisions for FR
  - asking our DPA (CNIL) opinion immediately was key
    - CNIL said current StopCovid is GDPR compliant ☺
  - StopCovid app works fine and helps…
    - …even if it was not easy and if it could work better with Apple help
  - raises many side questions (e.g., OS and big tech companies neutrality)
    - Shoshana Zuboff (https://www.youtube.com/watch?v=NOKxAIyPLpo -- offset: 30:46 - 35:38)

Conclusions and lessons learned (2)

- DESIRE goes beyond, by adding flexibility to the other 3 criteria
  - choosing between (cen/decen)tralized depends on the target country
    - with **trusted institutions**, being centralized is IOHO preferable

      (current GAEN to avoid because of discrimination risks and IOHO hazardous GDPR compliance)
    - in **authoritarian** countries, being decentralized is preferable
  - leave each country the **sovereign choice** of the model, while guaranteeing **full interoperability** between them ☺



Thank you!

- “Asterix and Obelix and the Covix Tracing App”, C. Castellix, Inria Privatix, Eurocrypt 2020 panel on “contact tracing”
- ROBERT docs.: https://github.com/ROBERT-proximity-tracing/documents
- DESIRE docs.: https://github.com/3rd-ways-for-EU-exposure-notification/project-DESIRE
- StopCovid source code: https://gitlab.inria.fr/stopcovid19

Additional slides

Can ROBERT solve GAEN privacy issues (slide #9)?

- BLE scanners exist (e.g., Stop Covid Detector 3000) but it is essentially used to check if StopCovid app is working fine

- **no link to user health data possible!**

  StopCovid being centralized, information is not available to the public ☺

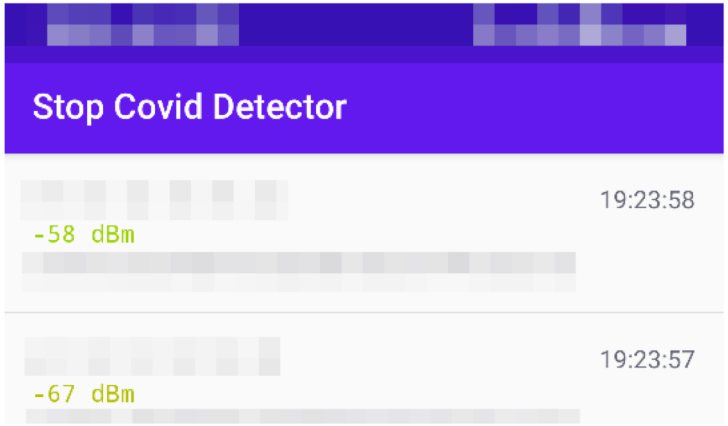
Usage

This app can be used to check whether the Stop Covid app is really working as intended (sending beacons), for example when your phone is in sleeping mode or in standby. Of course, you'd need another phone to check, as your phone cannot detect the beacons it sends.

You can also use this app to illustrate the inner working of the application, as it underlines it's possible to check (without any contact) if someone is using the Stop Covid application or not.

It can also be used to check if your phone changes of MAC address regularly to avoid tracking.

Screenshots



Can DESIRE solve GAEN privacy issues (slide #9)?

- A “centralized” deployment of DESIRE is **immune by design**

- A “decentralized” deployment of DESIRE **prevents passive** BLE scans by design
  - identifying encounters rather than endpoints helps: requires an **active** BLE component,
    - attack is more difficult and more easily identifiable
  - attacker must remain close to Alice approx. 50 sec to compute the PET, limits risks
    - de facto “secret-sharing” feature… see DESIRE PoC