Investigating Third Ways for Exposure Notifications in Europe

Searching for mid-term European interoperable solutions, beyond the centralized/decentralized vain debate

A contribution of Bruno Sportisse, Inria, CEO and Chairman

Today, this is the Europe Day.

The situation as of May the 9th, 2020

It is now clearly recognized that there are two families of approaches for proximity/contact tracing in Europe: the so-called "centralized" and the so-called "decentralized" protocols.

Both rely on backend servers operated by "Authorities" and user devices (smartphones), which underlines the vain debate about the words ("centralized" versus "decentralized").

From a rigorous perspective, the major difference consists in the nature of the data that are transmitted: crypto-IDs of exposed people in the so-called "centralized" approach (from the devices of the infected users to the central server), crypto-IDs of infected users in the so-called "decentralized" approach (from the devices of the infected people to a central server to all devices). Then, the risk exposure is computed either on the server or on the device.

Both architectures result in consequences for the ability to a Health Authority to manage the pandemic interventions, especially for the regulation and the feedback loops, which are in its hand by design in the "centralized" approach, which have to be dealt with the OS manufacturers (Apple-Google) in the "decentralized" approach.

There is also a strong link between the so-called "decentralized" approach and the API proposed by Apple and Google, which makes the implementation of the "decentralized" approach easier.

Concerning cybersecurity and privacy issues, I like the conclusion in one recent scientific article[1] of Serge Vaudenay, a renowned Professor at EPFL, who does not support any approach (he is making his job of an independent researcher):

« Against a powerful adversary, the privacy of a reporting user breaks as follows:
– (centralized system) it reveals its identity and the one of his reported contacts, but the adversary can only be the server;
– (decentralized system) it reveals its identity, but the adversary can be anyone. »

Of course, a State which is not a democratic State would have a very powerful tool for massive surveillance (even if it has much more efficient other tools) with a centralized approach. The centralized approach requires actually high trust in the health authority that is deploying the system (by the way, if you do not trust your national health authority, you might have other more serious issues).

On the other hand, as demonstrated recently with the first attack simulation against decentralized systems, these systems can be exploited by any malicious user to re-identify infected users and trace

[1] https://eprint.iacr.org/2020/531.pdf

their locations[2]. Decentralized systems require high trust toward citizens. Considering that a malicious authority can use the exact same attack, this means that decentralized systems require high trust *both* toward malicious users and malicious authority. Also, widely acknowledged by the scientific community (including one of the principal investigators of the "decentralized" approach[3]), decentralized systems have to make some fundamental trade-off between availability, privacy, and integrity. They also have to make strong and questionable assumptions about the platform security and computing environment of end-users or devices.

The situation faces therefore a system that requires trusting the authority because they might use the system to trace users, and another one that requires trusting users *and* the authority because they might use the system to trace infected users.

Which one to choose?

As a European citizen living in a democratic State (France), I prefer without hesitation a so-called centralized protocol. For me, decentralized citizens' medical data into all mobile devices is too risky and inappropriate. This is my choice and the one of some European countries.

If I were a citizen of a non-democratic State, I would prefer to use (or not to use) a decentralized protocol. Meanwhile, I also understand that other citizens and other European countries would prefer a so-called decentralized protocol.

Following what Paul Francis, a Director of the Max Planck Institute for software systems, has written in his blog[4]: this can be discussed. This has to be discussed. As a researcher and as a citizen, I cannot accept that the debate should be closed "without further discussion".

To summarize: both approaches have advantages and drawbacks.

The issue of interoperability

The issue of interoperability is a growing concern regarding the future expected increase of travels in Europe and the day-to-day life of the cross-boarders.

To date, the situation has to be stated and said very clearly: it is very difficult to build the interoperability between both systems because the nature of the information that travels within the networks is not the same one (infected keys in the "decentralized" approach versus exposed keys in the "centralized" approach).

A lot of works is under progress: under the umbrella of the European Commission (following the "Toolbox" that recognizes the existence of both approaches and within the eHealth network), with existing standardization bodies (announcements will be done next week), etc.

This also includes the recent paper written by the founders of the so-called "decentralized" approach[5]. It is not the point but I regret that such papers, that should be only "technical papers" are also "political papers" by pushing the usual claim in favour of the so-called "decentralized" approach ("We also show

[2] https://twitter.com/podehaye/status/1257977489965625345

[3] C. Troncoso and al, "Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments", https://www.petsymposium.org/2017/papers/issue4/paper87-2017-4-source.pdf.

[4] https://medium.com/@francis_49362/the-joint-statement-on-contact-tracing-is-irresponsible-627f347a0cd5

[5] As seen in https://www.reuters.com/article/us-health-coronavirus-europe-tech/european-coalition-takes-shape-on-coronavirus-contact-tracing-idUSKBN22J1N8, giving a link to the paper.

that interoperability with systems in which risk computation is performed by a central server significantly impact user privacy", " Decentralized systems, which provide strong privacy guarantees and have in-built resistance to mission creep", "Consequently, centralized risk calculation cannot be used without severely weakening the privacy of users of the decentralized system", etc.) or even **false statements** ("The centralized risk calculation mechanism relies on the central server being able to recover the list of user identities from the records of a device reporting an infection").

To summarize: it will be very difficult to achieve interoperability with both approaches.

It could also be seen as a consequence of the existence of national apps, due to the requirements of the National Health Authorities, but, as researchers and engineers, we have to propose solutions.

We need a third way, leveraging the so-called "centralized" and "decentralized" solutions

Each national team is fully committed in the development of a short-term solution for its country. Some countries have postponed the deployment of a proximity tracing app (eg Switzerland, Germany, etc.), some are currently achieving major tests (eg UK).

However, I think that this is mandatory to investigate a third way which could be able to gather the advantages of both approaches and to propose a mid-term fully interoperable approach at the European level. There is rising number of voices in favor of such a third way[6][7][8].

That is feasible.

This is why one team of my research institute, Inria, is putting on the table, today, the Europe Day, one example of such a third way: DESIRE (which could be the acronym of a "DEcentralized System for Information of Risk Exposure").

The first scientific paper can be found at https://github.com/3rd-ways-for-EU-exposure-notification/project-DESIRE**.**

To date, the French national roadmap is not based on this protocol, for the reasons explained above. The *mid-term* situation could perhaps change if there were a European move to such third ways.

This is not a paper to promote a given solution.

This is not a paper to push another approach against another one.

This is the opening of a credible third way to find an acceptable *mid-term* solution for Europe.

The core idea of DESIRE is to generate the crypto-identifier of an encounter between two phones, in a symmetric yet fully confidential manner: **this generation is fully decentralized on devices and, as such, it can be viewed as a decentralized[9] approach.** Rather than collecting the crypto-identifier of smartphones, the application then generates and collects the crypto-identifiers of all encounters.

This approach drastically reduces the impact of an attack that could be achieved by a central server.

---

[6] https://eprint.iacr.org/2020/531.pdf
[7] https://eprint.iacr.org/2020/493.pdf
[8] https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Centralised%20and%20decentralised%20systems%20for%20contact%20tracing.pdf
[9] I do not want to enter into the debate about the definition of what a "decentralized" approach is for contact tracing: the recent weeks have proven that we are not always in a scientific debate.

On this basis, one can keep the advantages of the so-called centralized approaches: no broadcasting of infected keys but broadcasting of meeting crypto-identifiers (to remove the major risks of leakage as already pointed out by some publications[10]), full control by the Health Authorities on the pandemic management system.

Different implementations are also possible: one fully decentralized approach can also be implemented with one drawback, namely the loss of the feedback loop for the Health Authority. This is a possible choice for some countries but this does not prevent interoperability, the major issue.

Moreover, as this option answers the privacy concern of Apple and Google (the ability of a non-democratic State to use the "centralized" approach), this could lead to an evolution of the joint API, giving the possibility to generate the crypto-identifier of the encounter in the application.

This is a possible candidate for a third way: this is not the only one.

There are probably other options for a third way in Europe, that could ensure full interoperability in the mid-term: welcome to other projects under `https://github.com/3rd-ways-for-EU-exposure-notification/project-***!`

If national teams go beyond the current artificial debate about centralized versus decentralized approaches, I am sure that we can work to find a third way to be implemented in the mid-term.

One month after the French-German partnership which resulted in the protocol ROBERT, I think that we should open this truly European approach, to build a European protocol, able to solve the requirements of interoperability and to be proposed to the Tech giants.

This post has then to be seen as an open call for further investigation of third ways at the European level, to build a European fully interoperable protocol which could be deployed in the mid-term.

Today, this is the Europe Day.

[10] https://github.com/oseiskar/corona-sniffer