Lessons from SwissCovid

Serge Vaudenay[1] and Martin Vuagnoux[2]

2020, August 31st

[1] EPFL, Lausanne, Switzerland
[2] base23, Geneva, Switzerland

Abstract. SwissCovid is the Swiss automated contact tracing app based on the Google-Apple Exposure Notification system, inspired by DP-3T. This note is an unofficial comment about problems which were encountered with it. It is mostly based on the content which is available on

https://lasec.epfl.ch/people/vaudenay/swisscovid.html

We review security and privacy issues: false exposure notifications can be maliciously injected; people who report using SwissCovid essentially go public; people using SwissCovid can be traced. We discuss about encountered problems: compliance issues, non-inclusiveness, the lack of attractivity, the involvement of Apple and Google, and the strong opposition by people. We list goals of DP-3T which have not been met in SwissCovid. We question the effectiveness of this tool to reduce the pandemic.

1 SwissCovid

DP-3T is (originally) a Swiss-based project which developed solutions for automated contact tracing.[3] It inspired Apple and Google to ally to offer the Google-Apple Exposure Notification (GAEN)[4] interface.[5] DP-3T gathers researchers who designed the architecture, analyzed its security, developed the software, and tested the software. In normal circumstances, it is unusual that the same people do several of those tasks. In addition to this, some DP-3T members sit in the Swiss National COVID-19 Science Task Force[6] which advises the government on measures to take and systems to deploy. In normal circumstances, this would be called a conflict of interest.

SwissCovid is based on GAEN. This means that most of the code is installed by default on smartphones without the consent of the user (although it remains inactive until SwissCovid or another authorized app is installed). The app which people install is the interface between GAEN, the user, and the servers. It does not do much besides relaying information from one to the other.

One of the remaining tasks of the app is to download from the server the configuration parameters (every 6 hours), to download the diagnosed keys, to upload keys to report, and to finish the calculation of the risk to decide to notify the user or not. The upload operation is essentially the only technical task. Uploading requires the approval from the Health authorities. Approval is given by the medical infrastructure to the user in the form of a 12-digit code (called *covidcode*). This code is a one-time authorization code which remains valid during 24 hours. The user can enter the code in the app. The app will ask verification of this code to a server who will return a JWT authorization token. The app will then send the keys to report to another server together with this JWT.

[3] https://github.com/DP-3T/documents
[4] https://www.google.com/covid19/exposurenotifications/
[5] It seems that the name of GAEN is now changing to ENS.
[6] https://ncs-tf.ch/en/

To avoid showing to the network that the app is reporting diagnosed keys, some fake reports are submitted from time to time. The delay before submitting the next fake report is randomly picked with an exponential distribution of average equal to 5 days.

2 Security and Privacy Issues

We discuss security and privacy issues related to SwissCovid.[7] We stress that most of those threats would apply to many other automated contact tracing systems.

2.1 False Exposure Notifications

One important risk is that people will receive unjustified exposure notifications which will push them to quarantine. Such false positive can occur randomly, by bad luck, but can also be maliciously created by an adversary in order to get an advantage in putting some person in quarantine. We can imagine two types of scenarios:

- Trying to massively spread false notifications in a more-or-less blind way. A terrorist/activist attack would try to make a wide population receive a false notification. Some competitor would try to make many employees of the same company receive notifications.
- Trying to make one target person receive a false notification. A lazy student would try to make his teacher receive an alert.

In the first case, people make a fake app which simulates the genuine one, and synchronizes many devices on the same keys to spread. Broadcasting Bluetooth messages could be done with a higher power than usual to make receivers believe in a close proximity. If eventually one person is diagnosed, then this person can report the keys used by his fake app, which are the keys used by all the devices.

In the second case, there are two attack methods which require to meet the target person.

The first method consists of replaying to the target the Bluetooth messages which were sent by people who are likely to be diagnosed soon, for instance by capturing messages in emergency places in hospitals. In most of contact tracing applications, there are countermeasures against replay attacks. The countermeasure which is used in GAEN still allows replays for about two hours, following the GAEN specifications.

The second method consists in meeting the target person with the genuine app then reporting by breaking the authorization process. Such breaks can be done in many ways. It can be done by corrupting either the medical infrastructure or a just-diagnosed person to get a covidcode. Social engineering is likely to work to retrieve a covidcode.

In the SwissCovid case, there were also two bugs (now fixed) which eased this attack. First, the authorities were uploading some fake diagnosed keys "to exercise the system" but they did it with an emission date in the future. So, someone could use it in the future as a key which was predicted to be reported. Second, the JWT verification could be bypassed by setting the parameter "algorithm" to null. So, we could report keys without any authorization. Such attacks could have been devastating if discovered by the wrong people at the first place.

[7] https://lasec.epfl.ch/people/vaudenay/swisscovid/swisscovid-ana.pdf

2.2 Privacy of Reporting People

The decentralized architecture of SwissCovid creates privacy threats for reporting people.

People who report essentially publish the keys which they used to announce themselves to close-by people. If a malicious person captures their Bluetooth notification (by being close or not), remembers whom it comes from, then see a matching key on the server, then this person can deduce that the sender was diagnosed.

A paparazzi can capture from far away the signal of a celebrity then wait to see if the celebrity reports. This requires neither proximity nor a long lasting contact.

People can also use "enriched apps" which can store more information than the Bluetooth signal they receive. For instance, they can store the location and precise time, as well as notes from the malicious user. Collected data can even be shared or sold. If the Bluetooth signal of a person who is later diagnosed is captured this way, this can reveal where and when this person has been.

The "enriched app" can also run on the phone of the user without the user being aware of it. For instance, there are applications which needs to scan Bluetooth and share collected data together with localisation information with other devices which use the same app. Those apps could easily be changed into a malicious distributed surveillance system.[8]

Any organization which identifies people (hotels at registration desk, companies at entrance doors, shops at cashier) can, at the same time as they identify the person, take a Bluetooth signal from this person and remember it. This way, a hotel/company/shop can sell health information about a visitor to advertisers.

A video-surveillance system can be enriched with Bluetooth captures. Hence, we can recover visual information of people who have been diagnosed.

2.3 Privacy of SwissCovid Users

The Bluetooth technology is inherently creating privacy threats.

First of all, it is frequent that vulnerabilities allowing hackers to enter into a phone by Bluetooth are discovered. This is why people often turn off Bluetooth.

Second, observing the Bluetooth messages can threaten privacy.

It is trivial to detect SwissCovid users and to spot them around.

We can build networks of sensors which can collect Bluetooth signals with position and time. The smartphones of people could also take part of this network. This way, we can link consecutive Bluetooth messages and create a database showing the movement of people. People can be traced this way.

One critical element of this attack is the ability to link Bluetooth messages. When they are consecutive, linking them is trivial. (It is sometimes made clear by desynchronized rotations of the message and the MAC address.)

2.4 Countermeasures

There could be some protocols which avoid some of the attacks but they require to make choices which deviate from the GAEN infrastructure. Most notably, some solutions based on Diffie-Hellman would solve some problems. They however create technological problems (the

[8] As an example of an app which scans and share: Tile
https://www.thetileapp.com/en-us/location-tracking-device

bandwidth to transmit a public key) and require both participants of an encounter — not only the one to be notified — to realize the proximity.[9]

3 Encountered Problems

3.1 Compliance

In Switzerland, SwissCovid required to adapt the law. However, the law was prepared before SwissCovid was fully developed. The law requires that all components of the system to have a publicly available and verifiable source code.[10] But GAEN has no open source, so an ordinance had later to twist the spirit of the law[11] to make an exception to GAEN.[12] The law also requires to provide public specifications which we did not see so far.

The law also requires participation to be voluntary (people are free to install the app or not, to run or stop it, to report after being diagnosed or not, to choose the days to report, and to pay attention to the notification or not; what is not optional is to follow the order of the state physician to quarantine). In practice, we regularly hear politicians willing to revert this option to a mandatory usage. The law additionally prohibits discrimination based on the choice of using the app.

The interpretation about the law about data protection and privacy is not so clear.[13] Indeed, the status of the messages which are transmitted over Bluetooth is debatable: is this a personal data or not? If it was, storing the received messages and posting keys on a public server would be subject to legal regulation such as the right or erasure, which would make the entire system impossible to manage. The Swiss approach is to take those data as no personal data. This implies that the above attacks which collect and store them are perfectly legal.

The regulation about medical devices also applies because the app notifies the user about a possibility of being infected.[14] At the moment, it is not clear if SwissCovid has passed the validation. We only heard that the Decomplix company is in charge of the procedure with Swissmedic.

Finally, international agreements play a role about interoperability. So far, the European Union has blocked interoperability with Switzerland because of discrepancies in laws about privacy.

3.2 Digital Divide

GAEN will not work for everyone. Clearly, it does not work for people who have no smartphone (unless a dedicated hardware is adopted). GAEN only works on Android or iOS. It does not work on too old versions. It does not work on recent Chinese Android phones due to an American ban on technology transfer to China. It does not work on "deGoogled" Android phones either. Therefore, such technological solution cannot be *inclusive*.

We observed that GAEN looks like working in some phones but does not. Hence, the app looks like running well (it does beam Bluetooth messages) but does not receive anything.

[9] https://eprint.iacr.org/2020/531
[10] https://www.admin.ch/opc/fr/classified-compilation/20071012/index.html#a60a
[11] https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-79584.html
[12] However, GAEN later released some source codes. These are not the real ones. For Apple, the codes are *sample* codes. For Google, the codes are *snippets* (incomplete).
[13] https://www.admin.ch/opc/en/classified-compilation/19920153/index.html
[14] https://www.swissmedic.ch/swissmedic/en/home/medical-devices/regulation-of-medical-devices.html

3.3 Lack of Incentives

At the moment, about 15% of people in Switzerland are using SwissCovid, which is a high number. The fraction of people who report keys using SwissCovid among people who have been diagnosed is in the range 10–15%. There are more SwissCovid users who are diagnosed but we have seen in the press that one third of them do not report.[15] This means that the chances for SwissCovid to spot a contaminating encounter is probably lower than 2%.

The Swiss health authorities are making a campaign to bring more users. The campaigns are similar to commercial advertisements, which is quite unusual for a medical device. Actually, the communication usually lack of objectivity.

Experts and politicians often claim that the unwillingness to install is not understandable, specially because SwissCovid has a pretty good privacy protection level while more popular apps such as social networks have not. What is often omitted is that social networks offer a clear functionality to users while SwissCovid does mostly nothing. Actually, what users could expect from SwissCovid is to receive a bad news which would put them into troubles. Having to quarantine often means an income loss, although there are subsidies to mitigate this problem a bit. We believe the fear to be wrongly put in quarantine can explain the unwillingness to use the app. Most likely, the privacy issue is not the obstacle to adoption.

3.4 GAEN Overtaking

SwissCovid is tied by the law to be transparent. However, the app does not do much as most of the tasks are completed by GAEN. GAEN can be updated without any control, based on the wills of Apple and Google. Sometimes, this can deviate from the original goals. For instance, Apple decided that GAEN would send a weekly notification to the user about the number of diagnosed keys which have been encountered. This message can be conflicting with the one of the app.

Having an app based on GAEN has the advantage that many countries are using the same. On the other hand, it is a clear abandonment of sovereignty.

The app is often compared with other apps by the number of permissions it requires in the operating system. This number is actually very low. However, what this comparison hides is the permissions that GAEN uses. In Android, GAEN is part of the Google app called "Google Play Services" (which some people take as being part of the operating system) and this app has a scary list of permissions. Actually, this app is regularly sending over the air the IP address, the phone number, the email address, the IMEI number, etc.

3.5 Opposition of People

SwissCovid also faces an active resistance by people. The law about SwissCovid is currently challenged by a group who is setting up a referendum against it.[16] It is a committee of citizens without any political affiliation who are fighting for liberties and against lies. Their arguments are often mocked or just trashed by calling them as "conspirationists". We believe that the lack of transparency by authorities and the regular unfortunate mistakes that they make is only nurturing the opposition by those groups.

Their arguments usually start by observing that the statistics do not show the high number of deaths which was anticipated. They find the restrictive measures (such as lock down,

[15] https://www.tdg.ch/la-suisse-compte-253-nouveaux-cas-en-24-heures-484366626037
[16] https://www.stop-swisscovid.net/

mandatory masks, gathering prohibition) unproportional to fight against COVID-19, given those numbers. They observe that health authorities and media are entertaining the fear of COVID-19 by showing numbers when they are scary. They also find evidence in documents and declarations that some measures are only made to train people to more care and not to respond to a particular threat. We understand that their greatest fear is that there will be soon a mandatory vaccination campaign, as it is already made possible by the law[17], and that authorities are currently preparing people to accept it.

4 Missed Goals

We review some of the goals from the DP-3T White Paper.[18] DP-3T originally aimed at providing epidemiologists with data.[19] This goal has been dropped. It is not met.

DP-3T aimed at providing *open-source* solutions. Although the app is open-source (although we cannot compile and run it ourselves), most of the tasks are done by GAEN which is not open-source at all. Although DP-3T is calling for an independent audit of GAEN, we have seen no evidence of such audit. Besides, it would be unethical that editors would be involved in the development or the promotion of any exposure notification app. Conflicts of interest should be clear.

DP-3T aimed to be *decentralized* in the sense that data would be stored on the user's device only. What happened is that the data is stored by GAEN, unavailable to other apps, and out of any control. We can say that the data is stored in a decentralized GAEN system which is fully controlled by Apple and Google.

DP-3T aimed to be *privacy-preserving* or to offer "privacy-by-design". The identified threats show that privacy is far from ideal. It is unlikely that any Bluetooth-based solution would be decently privacy preserving.

DP-3T aimed to be *complete* in the sense that all proximity cases would be considered. This is not the case. Some close encountered are not spotted by SwissCovid. There are false negatives.

DP-3T aimed to be *precise* in the sense that only close contacts would be considered. This is not the case either. Sometimes, contacts from far away are taken.

Actually, the reliability of GAEN to spot only contacts at a distance of up to 1.5m has not been publicly evaluated.

DP-3T aimed to have *authenticity* in the sense that only real contacts would be considered. Replay attacks show that this goal is not met.

5 Effectiveness to Reduce the Pandemic

The purpose of DP-3T is to "alert users who have been in close proximity to a confirmed COVID-19 positive case for a prolonged duration". It is explicitly said that tracking positive cases and locating clusters are not the purpose. Furthermore, the latest versions of the DP-3T white paper states that sharing data with epidemiologists is not a purpose either (it used to be in earlier versions). Hence, the role of DP-3T to fight the pandemic is very limited.

[17] https://www.admin.ch/opc/fr/classified-compilation/20071012/index.html#a6
[18] https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf
[19] It was in an earlier version of the White Paper.

The structure of SwissCovid makes it very hard to even measure if it is effective. To measure how many people are using SwissCovid, the Swiss health authorities used two methods.[20] The first one was based on the number of requests to the server to retrieve the configuration parameters. The second one (which is more accurate) is based on the number of fake reports submitted to the server. What is visible is also the number of genuine reports, which is made public every day. Otherwise, we cannot know how many notifications SwissCovid made. We do not know if some users have learned they were at risk to be contaminated from SwissCovid and not by human contact tracers. Hence, *monitoring* SwissCovid is inherently hard.

To determine if SwissCovid is useful, we should measure how many users were in the case satisfying the following conditions:

- the user received a notification and decided to self-isolate;
- the user was not contacted before by a contact tracer or by a relative who was diagnosed;
- the user has later been diagnosed.

Indeed, notifying users who never get diagnosed is useless. Notifying users who were notified otherwise is useless. Notifying users who do not self-isolate is useless too. SwissCovid would start to be useful if one such case exists. Then, the utility would be measured by the typical number of people who would have been infected by those cases if SwissCovid was not used.

A piece of information was given by the Swiss health authorities on July 28.[21] It was said that, since July 20, 13 people were tested positive after being alerted by SwissCovid. We do not know if they satisfy all the above criteria but we can say it is over a period when 7483 new positive cases were reported in Switzerland (hence 0.17%), and during which 857 covidcodes were entered to report through SwissCovid (hence 1.5% found case per entered covidcode). This can improve with the adoption of SwissCovid. However, the same press conference reveals that "over the last 7 days", 250 covidcodes were entered and 150 users who were alerted by SwissCovid contacted the infoline. Assuming more than 650 people contacted the infoline after being alerted since July 20, this means SwissCovid generates for the infoline a population among which 2% are positive. This ratio will *not* increase with the adoption of SwissCovid. Compared the the 5% positiv results among all tests made in Switzerland[22], this is clearly underperforming.

This app also limits itself to exposure notification. It does not give any more useful data. It cannot be used to identify clusters. It cannot be used for surface contamination. It is not made to work with asymptomatic superspreaders. However, asymptomatic superspreaders could be notified by the people they infected, which could help a bit to identify them if they pay attention to their notifications.

It is worrying that the privacy protection is made at the expense of making this tool much less useful than it could have been. Identifying where and when people are likely to have been infected could have been useful. We believe that the privacy design was a nice academic exercise which resulted in a poor tool to fight the pandemic.

[20] https://www.experimental.bfs.admin.ch/expstat/fr/home/methodes-innovation/swisscovid-app-monitoring.html

[21] https://www.srf.ch/play/tv/tagesschau-spezial/video/medienkonferenz-des-bundesamts-fuer-gesundheit-bag?id=6af1ebc6-485c-4b4c-96eb-26626a09e4be

[22] https://covid-19-schweiz.bagapps.ch/fr-3.html