Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Report by NCSC with annotated remarks in red from
Serge Vaudenay and Martin Vuagnoux. 17.6.2020

We thank NCSC for feedbacks on our report.

Federal Department of Finance FDF

National Cyber Security Centre (NCSC)

Security Issue Submission [INR-4434]. Detailed analysis.

Below you will find the major security concerns about the SwissCovid System submitted by Prof. Serge Vaudenay, EPFL and the corresponding risk assessment of NCSC.

Finding of Prof. Serge Vaudenay and Dr. Martin Vuagnoux	Risk assessment of NCSC
Availability of the source code	
It was initially hard to obtain the source code. We regret it is not documented. The fact that it is constantly updated made it impossible to make any real analysis. In general, complete technical specifications are missing. We fear that the entire system will be adopted without any real public security analysis (such as what was made for e-voting).	NCSC has the lead of the Public Security Test. On its website, you will find all necessary information: https://www.melani.admin.ch/SwissCovid_de
The source codes have nearly no comment at all.	We acknowledge that source code documentation can be improved and this is an ongoing process.
We wonder if the current plan is to deploy a dangerous and controversial system without giving time to a proper public security audit on the final version.	We do not agree with this statement. The submitted test result have shown that the public security test is useful and produces good and helpful results. All results you will find on our webpage: https://www.melani.admin.ch/melani/en/home/public-security-test/current_findings.html We did not find our own report there and we wonder if others are also missing. What criteria does NCSC apply to publish a report?
Open Source	
There is a misconception on the meaning of open source. SwissCovid is not open source and will unlikely be. Actually, having the API closed gives some security advantage. Assuming that Google-Apple did this job well and can be trusted, this provides a high level of security and defeats some of the attacks which have been proposed in the past. It is however very risky to count on this type of security as this has been shown to fail in the past.	Open source always refers to the application itself and never to the underlying operating system. For example there are open source windows programs. GAEN is not part of the operating system (at least on Android). It is correct that SwissCovid App uses the new technical possibilities of Google and Apple's API. In fact, Google and Apple have used the concepts and preliminary work of the EPFL/ETHZ for the development. Above all, the optimization of energy consumption by "Bluetooth Low Energy" can only be achieved directly by the manufacturer at this low

This implies that - the work of EPFL/ETHZ was installed in phones of people who did not consent to use SwissCovid - NCSC denies any responsibility for potential misuse of data by GAEN and cannot offer guarantees to the user - while NCSC offers openness guarantees on the app itself and kindly relies on users' consent, there is no similar thing about GAEN We don't find that the privacy of the users has been increased by outsourcing a big part of the protocol to an opaque implementation which was installed without users' consent and did not pass any independent audit.	technical level. While it is true that this component is neither Open Source nor has been thoroughly tested by NCSC, this does not mean that it is implemented in a way that affects the privacy in a negative way. As Google and Apple both have adhered to the design of EPFL, the robustness and privacy preserving elements are still in place. We have looked at how both versions behave (the pre-GAEN and the GAEN versions) and did document our findings in our report. The usage of GAEN does not affect the exposure of the Swisscovid users negatively. In our view, a deeper analysis of these APIs does not change the risk significantly as - presuming that Apple and Google want to violate the privacy of its users - they can do that on lower levels within the kernel as well. OS does have much more information about your device (for example Geolocation, …) as it could learn from the app One concern is that either Apple or Google might collect the information for their own purposes and thus might violate the privacy of its users. This is true for any usage of any application on a smart phone. As the data is now stored by the OS, it is not directly accessible by other apps which in our opinion increases security and privacy. As there is a separation of duties in place the privacy for the users has been increased: Health care organizations may apply to Google/Apple for getting access to the API and thus are limited to what information the API provides.
SwissCovid requires users to give personal information to Google-Apple while SwissCovid is forbidden to collect such information from users. The GAEN heart of the system is not subject to any independent audit. Consequently, the decentralized DP3T system has now become a non-transparent centralized one	The solution remains a decentralized system, no mattter if GAEN is used or not. GAEN is only the interface, not the communication protocol. GAEN implements the DP3T protocol and is much more than a communication interface.
Location of the Server	
Some SwissCovid servers are hosted by Amazon.	A content delivery network, or content distribution network (in this case Amazon AWS) is a geographically distributed network of proxy servers and their data centers. The goal is to provide high availability and performance by distributing the service spatially relative to end

This is insufficient to claim that the use of CDN brings no security/privacy risk. While we acknowldge it may be harmless, we need proper specifications of the architecture to be able to assess.	users. There is no distribution of sensitive data through Amazon. Sensitive POST requests are provided directly to the backend and not to the CDN. The use of the CDN is documented by us. Risk-Estimation-Proximity-Tracing_Appendix_Signed: https://www.melani.admin.ch/melani/de/home/public-security-test/current_findings.html

Replay Attacks

The metadata which is broadcasted by Bluetooth can be maliciously modified. This may ease false at-risk alert injection attacks.	The risk of replay attacks is known and documented. Replay-Attacke-Risk-Estimation_Public_Signed.pdf https://www.melani.admin.ch/melani/de/home/public-security-test/current_findings.html This document mentions relay attacks are possible during the epoch of a beacon. We say during epoch + 2h on average.
Replay attacks work during two hours and could be used to inject false at-risk alerts.	
Making many phones believe that they met the sender of a given beacon is possible	
One question is how to prove that he received the at-risk notification to claim for subsidies.	In a decentralized approach, it is conceptually impossible for the app alone to prove an at-risk notification to another party, like an employer or a test center. This can only be implemented by involving a trusted third party, like a hotline, that validates the claim by non.technical means and subsequently issues a digital certificate or TAN. Only centralized approaches, like manual contact tracing, could provide such a proof a priori.

Tracking

A passive Bluetooth sensor can easily keep track on how many active SwissCovid phones are present in its covering cell in real time. By disseminating sensors in a building, we can locate a phone in the intersection of cells and track moving phones from cell to cell.	Where? The risk is known and documented. The risk of tracking exists with any wireless technology that regularly sends beacons. The risk assessment must also take into account whether there is a benefit and ROI for someone who takes advantage of it. Users can always turn off tracing if they are in what they consider to be a sensitive environment.
It is likely that a good fraction of SwissCovid users are identifiable by Bluetooth	The risk is known and documented. Where?
Another interesting question is whether the app is still scanning although tracing is on but Bluetooth is off. It is well known that turning off Bluetooth only turns off the sending functionality in Bluetooth. Bluetooth scanning can still be done by apps when Bluetooth is off. We could not verify this.	This is an academical question as continues scanning for BLE beacons does not constitute a risk for the user. Only emitting BLE beacons would constitute such a risk. We assume scanning would also be turned off in order to save battery. GAEN (or other apps) may silently continue to store encounters even through the user does not want SwissCovid to. This is a risk for users. This recommendation should be made very visible by users.

Interoperability

Making SwissCovid interoperable across borders may not be easy.	In the future, the other country apps should be interoperable with the Swiss SwissCovid app, assuming that at least technically the new Apple/Google Exposure Notification API is used and that there are bilateral agreements between the countries that define the common standards for data protection, processes and data security. Germany for example is working on a solution with this new API. The apps will not interfere with each other; users will later have to choose with which other country apps to communicate for interoperability.

Dataprotection

With regard to your data, you have the right to information, rectification, erasure or disclosure. You also have the right to restrict or object to data processing. It would be more transparent to ask the user for the explicit unrevocable consent to publish their pseudonym for a period of 21 days.	The FDPIC has confirmed his assessment that the Swiss proximity tracing system operated by the Federal Office of Public Health and the SwissCovid app are data protection compliant. https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news.html#-796881893
Anyone who captured one of your Bluetooth signals recently and who made the association with you can figure out that you reported. Identifying reporting people is essentially easy for anyone/anything who has seen those people before.	By looking at a captured beacon, you don't know yet which person belongs to the beacon and if the person has reported yet. You can make a database of such beacons with personal information and later on recognize reported ones.
Although no personal data relating to you is sent out, it may well be that someone remembers their encounter with you from the date.	The FDPIC has confirmed his assessment that the Swiss proximity tracing system operated by the Federal Office of Public Health and the SwissCovid app are data protection compliant. https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news.html#-796881893

We wish FDPIC explicitely confirmed that the reported pseudonym information on the server are not subject to the regulation on data protection.

Threats Related to Malicious Apps

	This is not a problem of the app but is a general risk of all mobile phones.

This is a risk for society coming from an infrastructure which has been put in place by SwissCovid, with many users beaming beacons all the time. A person who did not consent in SwissCovid may have an app collecting data from those beacons. Such app could sell the information that this non-consenting person is at risk of being infected.