Traduction d'un extrait du rapport SwissCovid du LASEC (EPFL)

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

Conformité (Episode II)

Le 24 juin 2020, le Conseil fédéral a publié une *ordonnance sur le système de dépistage de proximité des coronavirus (OSTP)*. Elle affine le LEp (*ndt: Loi fédérale sur la lutte contre les maladies transmissibles de l'homme*) sur SwissCovid. De manière assez prévisible, l'OSTP définit les composantes du système en excluant le GAEN (art.2). Le système est composé de serveurs et de l'application SwissCovid que les utilisateurs installent sur leur téléphone. Nous avons déjà qualifié cela d'astuce pour exclure GAEN de l'obligation de divulgation du code source.

De manière assez surprenante, l'article 5 al.2 décrit les fonctions que l'application SwissCovid remplit *à l'aide d'une interface du système d'exploitation*. Nous comprenons cela comme une référence à GAEN (bien que GAEN ne fasse pas partie du système d'exploitation, comme nous l'avons déjà mentionné). Nous observons ci-dessous que presque aucune des 5 fonctionnalités énumérées n'a de ligne de code correspondante dans le code source disponible, pour la simple raison que ce sont les fonctionnalités qui sont remplies par ("avec l'aide de") GAEN.

- Génération d'une nouvelle clé du jour.
    - Ceci est fait par GAEN. L'application n'y a accès que si l'utilisateur est diagnostiqué et reçoit un code pour la déverrouiller.
- Échange d'identifiants éphémères via Bluetooth.
    - Ceci est fait par GAEN. L'application ne le voit jamais.
- Stockage des identifiants éphémères reçus.
    - Ceci est fait par GAEN. L'application ne le voit jamais.
- Téléchargement des clés diagnostiquées et comparaison.
    - L'application télécharge mais la comparaison est faite par GAEN. L'application ne voit que les résultats correspondants.
- Notification en cas de concordance.
    - Ceci est fait par l'application sur la base des données fournies par le GAEN.

Il s'agit en fait de la liste des tâches de GAEN. Ce que l'application fait réellement n'est pas énuméré ici.

L'OSTP renforce également l'exclusion de GAEN de l'obligation de divulgation du code source du LEp en ajoutant une exception explicite à la loi pour les fonctions du système d'exploitation qui sont utilisées via l'interface, donc GAEN (Art.5 al.3). L'ajout d'une exception à la loi pour une partie qui n'est pas reconnue comme un composant est assez gênant. Il est clair que le travail de l'application (qui est soumise au LEp) est presque totalement sous-traité à GAEN (qui est exempté du LEp par l'OSTP). Il est évident que cela n'est pas conforme à l'esprit du LEp.

En résumé, la loi LEp du 19 juin 2020 stipule que tous les composants du système SwissCovid doivent avoir un code source accessible au public et laisse au Conseil fédéral la responsabilité de régler les détails

du déploiement. L'ordonnance du Conseil fédéral du 24.6.2020 définit les composants en excluant ce qui est fourni par Google-Apple et met en œuvre les fonctionnalités de DP3T. Par conséquent, **la mise en œuvre du DP3T a contourné la loi.** Nous pensons que l'ordonnance était déjà en préparation alors que le Conseil des Etats et le Conseil National discutaient de la nécessité de disposer d'un code source accessible au public et que notre analyse était censurée. Les citoyens et le Parlement ont été trompés. Que ce soit pour de bonnes raisons (par exemple pour empêcher la seconde vague), il s'agit d'une tricherie flagrante. À notre avis, l**a loi, qui a été faite pour protéger les gens pour avoir dû utiliser un système opaque, s'est avérée insuffisante 5 jours après son adoption**.

Auteur: Serge Vaudenay - LASEC/EPFL
Traduit de l'anglais avec www.DeepL.com/Translator (version gratuite), relecture Emmanuelle Germond

Texte d'origine

Compliance (Episode II)

On June 24, 2020, the Federal Council released an Ordinance on the proximity tracing system for coronavirus (OSTP). It refines LEp about SwissCovid. Quite predictably, OSTP defines the components of the system by excluding GAEN (Art.2). The system is composed of servers and of the SwissCovid app that users install on their phone. We already qualified this as a trick to exclude GAEN from the source code disclosure requirement.

Quite surprisingly, Art.5 al.2 describes the functions that the SwissCovid app is fulfilling with the help of an interface of the operating system. We understand this as a reference to GAEN (although GAEN is not part of the operating system, as already discussed). We observe below that nearly none of the 5 listed functionalities have any corresponding line of code in the available source code, for the simple reason that these are the functionalities which are fulfilled by ("with the help of") GAEN.

- Generation of a new key of the day.
    - This is done by GAEN. The app has no access to it unless the user is diagnosed and receives a code to unlock it.
- Exchange of ephemeral identifiers via Bluetooth.
    - This is done by GAEN. The app never sees it.
- Storage of received ephemeral identifiers.
    - This is done by GAEN. The app never sees it.
- Download of diagnosed keys and comparison.
    - The app downloads but comparison is made by GAEN. The app only sees the matching results.
- Notification in case of matching.
    - This is done by the app based on the input from GAEN.

This is actually the list of the tasks of GAEN. What the app is really doing is not listed here.

OSTP also strengthens the exclusion of GAEN to the source code disclosure requirement of LEp by adding an explicit exception to the law for the functions of the operating system which are used via the interface, hence GAEN (Art.5 al.3). Adding an exception to a law for a part which is not recognized as a

component is quite awkward. What is clear it that the job of the app (which is subject to LEp) is nealry totally outsourced to GAEN (which is exempted from LEp by OSTP). Obviously, this is not compliant with the spirit of LEp.

In a nutshell, the 19.6.2020 LEp law says all components of the SwissCovid system must have a publicly available source code and lets the Federal Council the responsibility to address the deployment details. The 24.6.2020 ordinance from the Federal Council defines the components by excluding what is provided by Google-Apple and is implementing the DP3T functionalities. Consequently, the implementation of DP3T has bypassed the law. We believe that the ordinance was already in preparation while the Council of States and the National Council were discussing on the necessity to have a publicly available source code and our analysis was censored. Citizens and the parliament have been deceived. May it be for good reasons (e.g. to hit the second wave), it is a blatant cheat. In our opinion, the law, which was made to protect people for having to use an opaque system, has proven itself to be insufficient 5 days after adoption.

Author: Serge Vaudenay
Translated with www.DeepL.com/Translator (free version), proofreading Emmanuelle Germond