20/04/2020

Projet « Stop Covid »

1. Présentation du projet « Stop Covid »

Le projet « Stop Covid » est un projet de développement du prototype d'une application de « contact tracing » qui a vocation à s'inscrire dans une stratégie globale de déconfinement afin de réduire la propagation du Covid-19.

Par « contact tracing », on désigne la capacité à pouvoir informer une personne, à travers une application présente sur son smartphone, qu'elle a été à proximité lors des jours précédents (typiquement de deux à trois semaines) de personnes qui ont été diagnostiquées positives au Covid-19. Ce « cas contact » présente en effet un risque d'être porteur du virus et de contribuer à la diffusion de l'épidémie. Cette approche repose sur la capacité de deux smartphones à reconnaitre qu'ils sont à proximité l'un de l'autre, à travers la technologie « bluetooth », opérante seulement à faible distance (quelques mètres). De nombreux projets préfèrent ainsi parler de « proximity tracing », qui a l'avantage d'être plus précis sur le rôle joué par les smartphones. Aucune technologie de géolocalisation (à tel lieu, à telle heure) n'est ainsi mise en œuvre avec une telle approche.

Sous la supervision du Ministère de la Santé et des Solidarités et du Secrétariat d'Etat au numérique, en lien avec le Ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation, et le Ministère de la Justice, Inria pilote la task-force française ayant pour mission de développer un prototype d'application et d'instruire les différentes questions techniques, dans le cadre du projet « Stop Covid ». Les travaux s'appuient également sur l'expertise de l'ANSSI et la Direction du Numérique de l'Etat pour garantir la résilience et la sécurité des solutions étudiées. Ils associent étroitement la CNIL, dans le respect de son indépendance, afin d'apporter toutes les garanties de protection de la vie privée nécessaire.

Les prérequis suivants ont été posés : **une application open source, installée volontairement, protectrice de la vie privée et respectueuse du Règlement Général de Protection des Données.**

Par ailleurs, ces travaux s'inscrivent dans **un cadre européen** afin de garantir une interopérabilité entre les applications nationales qui seront éventuellement déployées. A ce titre, Inria s'implique dans des échanges avec des partenaires académiques comme le Fraunhofer Heinrich Hertz Institut et le Fraunhofer AISEC (Allemagne), l'Ecole Polytechnique Fédérale de Lausanne et l'ETH de Zürich, qui jouent un rôle-clé dans le développement des solutions respectivement allemande et suisse. Des échanges ont été également initiés avec les équipes britanniques (NHXS) et italiennes (Team Digitale). Une partie de ces échanges a lieu au sein d'une initiative, à ce stade informelle (sans cadre conventionnel), Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), qui a pour ambition de donner un cadre d'interopérabilité entre des solutions respectant strictement le cadre européen de respect de la vie privée et de protection des données (Règlement Général de Protection des Données).

De nombreux points techniques critiques étant à instruire afin de lever les incertitudes sur la faisabilité technologique et, partant, l'efficacité sanitaire d'une telle application le projet « Stop Covid » a été lancé le 7 avril afin qu'une technologie adaptée à nos pratiques et législations puisse, le cas échéant, être disponible au moment de la sortie de confinement.

Le déploiement d'une telle solution fera l'objet d'un débat au parlement les 28 et 29 avril. Un avis de la CNIL est attendu avant ce débat.

Le lancement d'un éventuel déploiement ainsi que ses modalités (calendrier, déploiement géographique) feront l'objet d'une décision après ce débat.

Cet outil est envisagé dans une approche intégrée et subsidiaire de la stratégie sanitaire (tests, masques, déconfinement progressif, etc.) pilotée par le Ministère de la Santé et des Solidarités et Jean Castex.

Pour information, le projet « Stop Covid » rassemble des acteurs publics (comme Inria, ANSSI, Inserm pour la partie santé, SPF, etc.) et des entreprises qui interviennent de manière pro bono dans la phase de développement (3DS, Cap Gemini, Orange, Lunabee ; d'autres ont vocation à rejoindre).

2. Principes fixés pour le développement d'un prototype d'application

Le prototype d'application en cours de développement repose sur les principes décrits ci-dessous, et qui pourront être amenés à évoluer suite aux débats parlementaires organisés les 28 et 29 avril prochain.

Finalité et fonctionnement :

- L'objectif est de pouvoir informer l'utilisateur de l'application que son smartphone a été à proximité, récemment (à titre indicatif : lors des deux dernières semaines), avec un smartphone dont l'utilisateur a l'application et a depuis été diagnostiqué positif au Covid-19, cette proximité étant susceptible, en l'état des connaissances médicales, d'avoir généré un risque de transmission du virus.
- L'application permet à cette fin de pouvoir recueillir et conserver des historiques de proximité de façon anonyme.
- L'historique de proximité est constitué des crypto-identifiants éphémères (d'une durée indicative de 15 minutes) des smartphones des personnes utilisatrices de l'application rencontrées. Ces crypto-identifiants sont générés lors du téléchargement de l'application pour chaque smartphone.
- La technologie utilisée pour évaluer la proximité entre deux smartphones est uniquement le bluetooth.
- L'application ne possède que son historique de proximité et aucune autre donnée.
- L'application permet de partager avec un serveur central l'historique de proximité lorsque l'utilisateur de l'application est diagnostiqué positif et rentre une preuve de son diagnostic dans l'application (à ce stade, sous la forme d'un One Time QR code ne contenant aucune information personnelle).
- L'application vérifie auprès du serveur, à intervalles réguliers (typiquement quelques heures), si ses propres crypto-identifiants se trouvent parmi les crypto-identifiants disponibles sur le serveur.
- Si c'est le cas, l'application affiche une notification qui sera affichée à l'utilisateur dans une plage horaire spécifique (par exemple en journée quand les services de santé sont ouverts et joignables). Cette notification peut indiquer la date du dernier contact si ce dernier s'est produit en présence d'autres contacts simultanés.
- La prise en charge des personnes alertées par l'application comme ayant été à proximité d'une personne diagnostiquée positive au Covid-19 devra être définie dans le cadre de la stratégie de déconfinement par le Ministère de la Santé. Elle devra apporter un bénéfice personnel en termes de prise en charge. Ces personnes recevront un message de santé pour être prises en charge de la bonne façon.
- Les données, qui sont toutes anonymisées dans le serveur, pourraient être utilisées de manière statistiques et anonymisées à des fins de recherche sur les modèles de diffusions de l'épidémie
- La finalité est liée strictement à la gestion de l'épidémie de Covid-19.
- La finalité n'est en aucune manière de s'assurer du respect des mesures de confinement ni l'identification des zones dans lesquelles les personnes positives se sont déplacées. A ce titre l'application ne repose pas sur des données de localisation.
- Il ne s'agit pas non plus de faire un suivi du nombre de personnes positives au Covid-19 par ce biais.

Volontariat et consentement :

- L'installation de l'application est volontaire.
- L'activation du bluetooth pour le suivi des contacts à proximité se fait sur une base volontaire.
- Le partage de l'historique de proximité avec un serveur central fait l'objet d'un recueil du consentement.
- Le fait de déclarer un diagnostic positif dans l'application relève du volontariat.
- Le projet étudie les équipements alternatifs qui pourraient être proposés aux personnes non équipées de smartphones.

Données :

- L'architecture doit permettre de limiter au maximum les données stockées et partagées en fonction du modèle de santé qui sera défini :
    - Seuls les identifiants épidémiologiquement pertinents seront conservés (en fonction de la durée du contact, de la distance estimée).
    - Les identifiants qui ne sont plus pertinents d'un point de vue épidémiologique sont effacés. La durée de pertinence d'un contact sera définie en fonction du modèle de santé.
- La protection de la liste des personnes diagnostiquées positives est une priorité :
    - Une donnée associée au diagnostic d'une personne ne peut pas se retrouver sur le smartphone d'une autre personne. A aucun moment cette information lié à un identifiant ne circule ni n'est stockée.
    - Seuls les crypto-identifiants éphémères sont stockés dans l'application.
    - Seuls les crypto-identifiants définissant l'historique de proximité d'un smartphone sont partagés de l'application *vers* un serveur central.
    - Le serveur central ne contient donc que les historiques de proximité des smartphones des personnes ayant téléchargé l'application, ayant activé leur bluetooth et ayant été diagnostiquées positif.

Anonymat :

- Il n'est pas possible de savoir qui utilise un smartphone. La liste des crypto-identifiants générée lors du téléchargement de l'application n'est pas associée à une personne.
- Seuls des crypto-identifiants éphémères sont stockés sur un smartphone et partagés, le cas échéant, d'un smartphone vers un serveur central.
- Il n'y a pas de système d'authentification/inscription au moment de l'installation de l'application.

Confiance :

- Le tiers de confiance est l'Etat.
- Un élément de preuve est demandé pour se déclarer comme ayant été diagnostiqué positif afin de renforcer la confiance dans le système. Il est envisagé à ce stade que cette preuve soit fournie sous la forme d'un One Time QR code ne contenant aucune information personnelle.

Efficacité :

- L'efficacité du « contact tracing », dans le cadre d'un dispositif sanitaire complet, fait l'objet de travaux scientifiques en cours au niveau international. Les travaux de référence sont par exemple ceux du professeur Christophe Fraser (Université d'Oxford) qui montrent d'un point de vue épidémiologique, dans le cadre de simulations numériques de l'évolution de l'épidémie de Covid-19, sur la base des connaissances scientifiques disponibles, la contribution éventuelle que peut avoir le contact tracing dans la lutte contre l'épidémie.

3. Description de l'architecture et du protocole de communication

Le développement du prototype se base sur un protocole de transmission qui garantit les éléments décrits dans la section précédente.

Ce protocole est décrit dans un article scientifique disponible de manière ouverte sous https://github.com/ROBERT-proximity-tracing/, depuis le 18 avril 2020. Il pourra être amené à évoluer notamment suite aux retours de la communauté scientifique après cette publication. Le projet « Stop Covid » prendra en compte le protocole issu de ces travaux, dans le respect strict des principes décrits supra, qui pourront évoluer à l'issue des débats parlementaires.

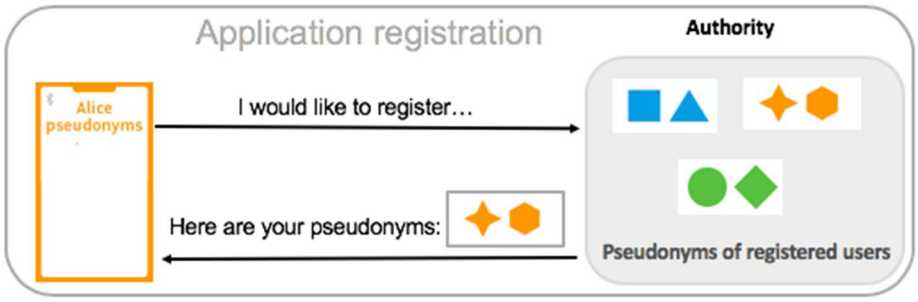
Les travaux ont été menés conjointement par l'équipe Inria Privatics, appuyée par une part significative de la communauté de chercheurs en privacy et en cryptographie d'Inria, et une équipe de l'institut de cybersécurité du Fraunhofer (AISEC).

Ce protocole permet une interopérabilité entre les applications éventuellement déployées en France et en Allemagne. Il est porté comme une contribution conjointe d'Inria et de Fraunhofer/AISEC au sein de l'initiative PEPP-PT.

Description synthétique :

1. Installation

L'utilisateur installe de manière volontaire l'application sur son téléphone. Au moment de l'installation, l'application s'enregistre auprès de l'autorité centrale. Cette autorité génère et partage un ensemble d'identifiants temporaires et anonymes avec l'application de l'utilisateur (« crypto-identifiants »). En pratique, ces identifiants ressemblent à un ensemble aléatoire de chiffres (représentés par des formes dans les schémas ci-dessous). Ce protocole doit permettre de protéger l'utilisateur en s'assurant qu'aucun observateur externe ou utilisateur de l'application ne peut relier ces identifiants ensemble et les utiliser pour suivre l'utilisateur dans le temps. Les identifiants ne peuvent être reliés que par l'utilisateur lui-même et l'autorité centrale (voir le schéma ci-dessous).



2. Création de l'historique de proximité

L'application mobile s'appuie sur les communications bluetooth pour envoyer l'un de ses pseudonymes à tous les autres utilisateurs à proximité. Les autres applications font de même. Tous les pseudonymes ainsi échangés et jugés pertinents d'un point de vue épidémiologiques sont stockés sur les smartphones.

3. Déclaration de diagnostic positif au Covid-19

Un utilisateur de l'application est testé positif. Il partage alors son historique de proximité avec l'autorité centrale à travers l'utilisation d'un QR code (hypothèse retenue à ce stade) qui lui a été remis à l'occasion de la transmission d'information de son test positif, étant entendu que le QR code n'est pas relié à la

personne. L'autorité centrale reçoit ainsi l'historique de proximité, sans aucune information sur l'utilisateur qui les transmet (ni ses pseudonymes ni a fortiori ses informations personnelles). Cet historique de proximité se rajoute ainsi à une liste de crypto-identifiants qui sont « à risque ».

4. Interrogation de l'autorité

Pour vérifier si un utilisateur a été en contact avec un utilisateur s'étant déclaré positif, les applications envoient régulièrement leurs crypto-identifiants à l'autorité centrale. Celle-ci vérifie si les crypto-identifiants font partie de la liste à risque. Si c'est le cas, alors l'autorité centrale renvoie l'information vers l'application et l'utilisateur est alerté.