

COMMUNIQUÉ DE PRESSE
Paris, le 27/04/2020

Application StopCovid – L'ANSSI apporte à Inria son expertise technique sur le volet sécurité numérique du projet

Pilote du projet d'application StopCovid, à la demande du Secrétaire d'Etat chargé du numérique, Cédric O, l'Institut national de recherche en sciences et technologies du numérique (Inria) est accompagné par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) sur les aspects de sécurité numérique.

En tant qu'autorité nationale référente en matière de sécurité du numérique, l'ANSSI est régulièrement sollicitée par les autorités compétentes pour émettre un avis sur la sécurité de certains systèmes d'information sensibles.

Face à la réalité de la menace cyber actuelle, la sécurisation de l'application apparaît primordiale pour veiller à sa fiabilité et à la confiance que les professionnels de santé chargés de gérer la crise sanitaire et les utilisateurs lui accorderont.

Afin d'anticiper le risque numérique, l'ANSSI a été intégrée au projet d'application StopCovid, outil numérique s'inscrivant dans une stratégie globale de gestion de la crise sanitaire et du suivi épidémiologique, pour conseiller Inria sur le volet sécurité numérique, lui transmettre un ensemble de recommandations techniques et évaluer au fil de l'eau la sécurité des développements.

Recommandations de l'ANSSI

Prenant en compte les spécifications techniques imposées par les fondements du projet StopCovid, l'ANSSI recommande :

- l'utilisation d'un coffre-fort électronique, matériel ou logiciel, pour protéger de manière robuste sur le serveur central, les informations pseudonymisées envoyées par le téléphone ;
- la mise en œuvre sur l'ensemble des composants du dispositif de mesures pour concevoir une architecture sécurisée et permettre le bon fonctionnement du traitement des informations tel qu'envisagé ;
- l'application de mesures de sécurité visant à se protéger des attaques informatiques de type DDOS (https://www.ssi.gouv.fr/uploads/2015/03/NP_Guide_DdoS.pdf) ;
- l'utilisation de mécanismes d'audit de l'imputabilité et de la traçabilité des actions menées sur le système (https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Journalisation_NoteTech.pdf) ;
- la réalisation d'audits et de contrôles de sécurité réalisés par l'ANSSI tout au long de la conception de l'application. L'agence recommande également qu'un audit de type bug bounty soit mené en parallèle. Conçue en mode agile, l'application devra être régulièrement mise à jour par ses utilisateurs ;
- la création d'un dispositif de gestion des vulnérabilités pour maintenir un bon niveau de sécurité de l'application et du serveur central durant toute la durée d'utilisation de l'application ;

- la mise en place d'un dispositif de détection des cyberattaques pour réagir au plus tôt en cas de tentatives de compromission du système.

Choix du Bluetooth

Le protocole de communication ROBERT, sur lequel repose le projet d'application StopCovid, utilise le réseau sans fil de proximité Bluetooth.

Le rôle de l'ANSSI est d'accompagner ce choix en recommandant des mesures de sécurité efficaces et adaptées au contexte.

L'application StopCovid est destinée, sur la base du volontariat, à un usage personnel. L'ANSSI recommande donc fortement aux futurs utilisateurs de mettre régulièrement à jour leur téléphone pour limiter les risques liés à l'usage de cette technologie.

Chiffrement des pseudonymes

Le projet d'application StopCovid repose sur la construction d'un historique de contacts pseudonymisés, en utilisant les signaux Bluetooth.

Le protocole ROBERT a défini des spécifications techniques de communication par Bluetooth limitant la taille des informations transmises entre les téléphones disposant de l'application.

Dans ce contexte, concernant le chiffrement des pseudonymes, l'ANSSI recommande l'utilisation de l'algorithme de chiffrement SKINNY-64/192. Bien que récent, cet algorithme a été largement étudié et son analyse n'a révélé aucune faiblesse en termes de sécurité. Il offre de plus, d'excellentes performances.

Publication sous licence open source

Tous les travaux menés dans le cadre du projet StopCovid seront publiés sous licence open source afin de garantir l'amélioration continue du dispositif et la correction d'éventuelles vulnérabilités.

À PROPOS DE L'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée par le décret n°2009-834 du 7 juillet 2009 sous la forme d'un service à compétence nationale.

L'agence assure la mission d'autorité nationale en matière de défense et sécurité des systèmes d'information. Elle est rattachée au secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP

www.ssi.gouv.fr - communication@ssi.gouv.fr



CONTACTS PRESSE

Margaux Vincent

margaux.vincent@ssi.gouv.fr / 06 49 21 63 80

Baptiste Grégoire

baptiste.gregoire@ssi.gouv.fr