AIPD de l'Application TousAntiCovid

Version mise à jour le 17 février 2021

1 Informations de l'AIPD

Nom de l'auteur
Déléguée à la protection des données d'Inria, Anne COMBE
Nom de l'évaluateur
RSSI de la DGS, Olivier VANDEWYNCKELE
Nom du validateur
Jérôme SALOMON
Date de création
08/05/2020
Nom du DPD
Daniela PARROT
Recherche de l'avis des personnes concernées
RSSI de la DGS, Olivier VANDEWYNCKELE

2 Contexte

2.1 Vue d'ensemble

2.1.1 Quel est le traitement qui fait l'objet de l'étude ?

L'AIPD porte sur l'application TousAntiCovid de « suivi de contacts » (ou « contact tracing ») dont la responsabilité du développement d'une version prototype a été confiée le 8 avril 2020 à Inria par le Gouvernement, sous la supervision du Ministère des Solidarités et de la Santé et du Secrétariat d'Etat au numérique.

Dans ce contexte, le projet StopCovid (développement, modèle, diffusion) a été rendu public le 26 avril 2020 : il rassemble des acteurs publics (Inria, ANSSI, Inserm, Santé Publique France) et privés (Capgemini, Dassault Systèmes, Lunabee Studio Orange, Withings) ainsi qu'un écosystème de contributeurs.
Le 22 octobre 2020, il a été décidé de remplacer l'application StopCovid par une nouvelle application baptisée TousAntiCovid dont le mode de fonctionnement est assez similaire à StopCovid mais pour laquelle des améliorations, en terme d'information et de fonctionnement, ont été apportées.

Comme le projet s'inscrit dans le cadre d'une stratégie sanitaire globale, le Ministère des Solidarités et de la Santé (MSS) est le Responsable de traitement. Du fait de son rôle lors du développement du projet, Inria joue le rôle d'appui à travers un accord-cadre qui précise son engagement en assistance à la maitrise d'œuvre.

Comme précisé par la CNIL dans sa délibération 2020-046 en date du 24 avril 2020, le traitement serait fondé sur l'**exécution d'une mission d'intérêt public** au sens des articles 6.1.e) du RGPD et 5.5° de la loi « Informatique et Libertés », dans le cadre du plan gouvernemental de lutte contre la pandémie Covid-19.

De nombreuses études épidémiologiques, comme par exemple celles de Christophe Fraser[1] à Oxford, montrent l'intérêt pour les autorités sanitaires de pouvoir disposer d'applications de « suivi de contacts », en appui au suivi manuel de propagation des chaines de transmission.

L'utilisation de telles applications permet en effet de pouvoir alerter, en complément du travail de traçage manuel, avec une véritable plus-value envisagée pour d'une part alerter les contacts anonymes, par exemple dans les transports ou dans les commerces, et qui représentent un risque non négligeable, et d'autre part, alerter de manière précoce et automatisée les contacts, ce qui constitue un gain de temps et de ressources.

Si le retour d'expériences à partir d'applications déjà déployées ne permet pas à la date de rédaction de cette AIPD d'avoir suffisamment de recul sur l'impact des applications de contact tracing dans la gestion de l'épidémie de Covid-19, beaucoup d'experts soutiennent l'utilité de cette application dans le cadre de la stratégie de contact tracing.

Les travaux d'un des groupes de travail sur le développement de TousAntiCovid mené par Vittoria Colizza démontrent par le biais de simulations numériques l'apport d'une application dès les premiers téléchargements pour réduire les chaines de transmissions. En effet, les résultats des modélisations suggèrent que l'efficacité est faible si l'adoption est limitée, mais elle

[1] Christophe Fraser et al. Modelling the Covid-19 epidemic and simulating the use of a contact tracing app in the UK

n'est pas nulle, elle sera donc utile même avec une adoption faible. L'application permettra d'informer de manière précoce les personnes ayant été en contact avec une personne diagnostiquée positive dès notification du test positif par le cas confirmé. Cette précocité et cette réactivité sont essentielles dans le succès de la stratégie d'identification et de suivi des contacts puisque la proportion de transmission pré-symptomatique est estimée à 44%. Elle contribue de ce fait à alerter rapidement les individus à la suite d'un contact et de mettre en place plus rapidement les gestes barrières et de les informer des conduites à tenir telles que préconisées par le MSS. Les contacts identifiés via l'application TousAntiCovid pourront être réintégrés dans le parcours de soins et devront suivre les mesures en termes de dépistage et de quatorzaine telles que préconisées par le MSS.

Par ailleurs, le Conseil Scientifique rappelle l'utilité de l'outil numérique comme étant complémentaire et touchant un public différent du contact tracing manuel (avis du 20 avril[2] et 20 octobre[3]), et parce qu'elle permet de renforcer l'efficacité du contrôle sanitaire de l'épidémie, et également, dans le cadre d'une application interopérable au niveau européen (ce qui est le cas de TousAntiCovid), de prendre en considération les cas de transmission transfrontalière. L'Académie de médecine s'est également prononcée de manière favorable à l'utilisation d'une application du type TousAntiCovid dans le cadre du déconfinement afin de permettre une participation active de la population dans la lutte contre la pandémie tout en respectant l'anonymat et la règlementation européenne et nationale du RGPD.

Enfin, l'ECDC soutient également l'utilisation des application de contact tracing comme outil complémentaire au contact tracing manuel puisqu'elle permet d'identifier et d'alerter plus de contacts que via le contact manuel (les contacts inconnus et ceux qui sont omis), et permet d'identifier les contacts transfrontaliers. Si l'application ne peut pas remplacer la méthode manuelle, pour l'ECDC il est également essentiel que les autorités sanitaires soient impliquées dans toutes les étapes de développement de l'application et que cette dernière soit utilisée sur une base volontaire.

Les principaux enjeux en matière de respect du RGPD sont de s'appuyer dès la conception de l'application sur l'état de l'art des recherches en sécurité et en protection de la vie privée afin de **supprimer ou de réduire au mieux le risque**

- d'identifier les utilisateurs de manière directe ou indirecte ;
- de les géolocaliser ou tracer leurs parcours ;
- d'inférer qu'un utilisateur est diagnostiqué ou dépisté positif ;
- de reconstituer les intéractions sociales ;

Il est entendu que la réponse à ces enjeux repose sur des hypothèses d'attaque du système qui sont détaillées dans les sections 4.2, 4.3 et 4.4.

Les finalités du traitement sont :

1. D'informer les personnes utilisatrices de l'application qu'il existe un risque qu'elles aient été contaminées par le virus de la Covid-19 en raison du fait qu'elles se sont trouvées à proximité d'un autre utilisateur de cette application ayant été diagnostiqué positif à cette pathologie. Les personnes exposées à ce risque sont désignées ci-après comme « contacts à risque » ;
2. De sensibiliser les personnes utilisatrices de l'application, notamment celles identifiées comme contacts à risque, sur les symptômes de ce virus, les gestes barrières et la conduite à adopter pour lutter contre sa propagation ;
3. De recommander aux contacts à risque de s'orienter vers les acteurs de santé compétents aux fins que ceux-ci les prennent en charge et leur prescrivent, le cas échéant, un examen de dépistage ;
4. De réaliser des analyses statistiques à partir des données anonymes issues de l'application afin d'adapter les mesures de gestion nécessaires pour faire face à l'épidémie et d'améliorer les performances de l'application ;
5. D'informer les personnes utilisatrices de l'application qu'il existe un risque qu'elles aient été contaminées par le virus du covid-19 en raison du fait qu'elles ont fréquenté un lieu dans lequel se trouvait au même moment une personne ayant été diagnostiquée ou dépistée positive à la Covid-19. ;
6. De permettre aux personnes utilisatrices, sur présentation du statut "contact à risque" dans l'application, de bénéficier d'un examen ou test de dépistage dans des conditions de réalisation prioritaire, au même titre que les autres personnes à risque d'infection ;
7. D'informer les personnes utilisatrices de l'application sur la situation sanitaire nationale et locale, ainsi que sur des mesures ou actions de promotion, de prévention et d'éducation pour la santé ou de les orienter vers des applications ou des sites internet mis en œuvre pour la gestion de l'épidémie de la Covid-19 et de leur fournir des informations sur les données d'utilisation de l'application ;
8. De permettre aux personnes utilisatrices de l'application de stocker des données à caractère personnel sur leur téléphone mobile en vue de générer des justificatifs requis par les autorités publiques. » ;

[2] Sortie progressive de confinement prérequis et mesures phares : https://solidarites-sante.gouv.fr/IMG/pdf/avis_conseil_scientifique_20_avril_2020.pdf
[3] Un nouvel ensemble numérique pour lutter contre le SARS-CoV-2 : https://solidarites-sante.gouv.fr/IMG/pdf/avis_conseil_scientifique_20_octobre_2020.pdf

L'application TousAntiCovid est installée librement et gratuitement par un utilisateur. Il appartient à l'utilisateur d'activer ou non la fonctionnalité de l'application permettant de constituer un historique de proximité avec d'autres utilisateurs de l'application. En cas de résultat positif à un examen de dépistage au Covid-19, l'utilisateur de l'application est libre de notifier ou non ce résultat dans l'application. L'application peut être désinstallée à tout moment et les données collectées sont alors immédiatement détruites.

Le périmètre de cette AIPD concerne l'application mobile, la partie serveur, ainsi que les moyens de communication.

Les aspects strictement liés aux structures médicales, comme les comptes rendus de test ne sont pas pris en compte dans cette AIPD dans la mesure où ils font l'objet de systèmes distincts et séparés du point de vue des informations.

Nous décrivons pour information la partie mise en place pour délivrer des jetons aléatoires temporaires à usage unique qui seront joints aux comptes rendus de test au Covid-19 délivrés au patient ou qui pourront aussi être délivrés par un médecin à un patient suite à un diagnostic clinique au cours d'une consultation dans son cabinet médical, à domicile ou par téléconsultation.

2.1.2 Quelles sont les responsabilités liées au traitement ?

A compter du 7 avril 2020, le Gouvernement français a confié à Inria le pilotage opérationnel du projet de recherche et développement baptisé « TousAntiCovid » qui réunit l'expertise d'acteurs nationaux, publics comme privés, au sein de cette équipe-projet TousAntiCovid qui rassemble : Inria, l'ANSSI, Capgemini, Dassault Systèmes, l'Inserm, Lunabee Studio, Orange, Santé Publique France et Withings.

L'ensemble de ces acteurs contribue aux travaux déjà engagés pour mettre à disposition de tous les Français un outil permettant de mieux les protéger contre le Covid-19, dans l'éventualité où une décision politique serait prise pour autoriser le déploiement effectif du système.

La Direction Générale de la Santé (DGS) du Ministère des Solidarités et de la Santé (MSS) détermine les finalités et les moyens du traitement et est responsable de TousAntiCovid.

Inria exerce un rôle d'appui à la DGS à travers un accord d'assistance à maitrise d'ouvrage (AMO) de manière à déterminer les obligations et rôles respectifs, conformément à l'article 28 du RGPD.

Par ailleurs, un accord de consortium a été signé entre Inria et les acteurs privés du projet StopCovid (renommé en TousAntiCovid) afin de préciser les éléments relatifs d'une part à l'exploitation opérationnelle de TousAntiCovid et d'autre part aux projets de développement et de R&D afférents.

Les différents niveaux de responsabilité sont les suivants :

- **Responsable de traitement**
  - La DGS du Ministère des Solidarités et de la Santé (MSS)
- **Sous-traitant public** / assistance à maitrise d'œuvre (AMO) :
  - Inria
- **Sous-traitants privés**
  - 3DS Outscale : hébergement de l'infrastructure ;
  - Orange : maintenance et exploitation de l'infrastructure ;
  - Webhelp Medica : support utilisateurs de l'application ;
  - Inter Mutuelle Assistance (IMA) : assistance téléphonique aux utilisateurs du module de contact warning et des établissements recevant du public et utilisant des QR codes dynamiques ;
  - Stonly[4] : Foire aux questions (FAQ) de l'application TousAntiCovid ;
  - Reputation squad[5] : génération des QR codes de lieu affichés à l'entrée ou dans les lieux.
- **Destinataires**
  - Les utilisateurs qui
    - sont notifiés par l'application comme étant à risque d'avoir contracté le Covid-19 sont destinataires de l'information selon laquelle ils ont été à proximité d'au moins un autre utilisateur diagnostiqué ou dépisté positif au Covid-19 ;
    - génèrent des attestations de déplacement dérogatoire ;
    - obtiennent des informations sanitaires sur les actualités en lien avec la Covid-19 relativement à un lieu d'intérêt

[4] https://stonly.com
[5] https://www.reputationsquad.com

        - obtiennent des conseils relatifs à l'isolement
    - Les autorités publiques auxquelles attestations de déplacement dérogatoire seront présentées ;
    - Inria en tant que sous-traitant auprès de la DGS du MSS.

2.1.3 Quelles sont les personnes concernées

La population concernée est toute celle qui est couverte par le plan de maitrise de l'épidémie de l'État. L'application n'est qu'un outil au service de ce plan, en complément du traçage manuel.

L'application est téléchargeable sur les stores applicatifs officiels Google et Apple en France. Les taux d'utilisabilité des versions des systèmes Android et iOS sont les suivants :

- Android : 89,5 % des versions d'Android sont supportées (support à partir d'Android 5)
- iOS : 94% des versions iOS sont supportés (support à partir de iOS 11.5).

Les mineurs sont inclus dans le dispositif.

- En application du 1 de l'article 8 du règlement (UE) 2016/679 du 27 avril 2016, un mineur peut consentir seul à un traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information à compter de l'âge de quinze ans. Lorsque le mineur est âgé de moins de quinze ans, le traitement n'est licite que si le consentement est donné conjointement par le mineur concerné et le ou les titulaires de l'autorité parentale à l'égard de ce mineur. Toutefois, l'article 8.1 du RGPD précise que les dispositions s'appliquent au traitement entrant dans le champ de l'article 6.1.e du RGPD, donc les traitements fondés sur le consentement, ce qui n'est pas le cas en l'espèce puisque TousAntiCovid est fondé sur l'exécution d'une mission d'intérêt public.

- A l'occasion de la première ouverture de l'application, il est proposé à l'utilisateur de cocher une case pour indiquer s'il a moins de 15 ans ou non. Sur cette base déclarative, il sera alors indiqué à ce mineur de moins de 15 ans qu'il doit avertir au moins l'un de ses représentants légaux qu'il souhaite utiliser cette application afin que celui-ci y consente. Une deuxième case à cocher dans l'application lui sera alors proposée pour s'assurer qu'il a bien eu le consentement d'au-moins l'un de ses représentants légaux.

2.1.4 Quels sont les référentiels applicables ?

- Référentiel Général de Sécurité (RGS)
    - Une homologation au RGS de StopCovid puis TousAntiCovid a été instruite et a été prononcée par la DGS du MSS préalablement à la mise en production de StopCovid.
- PSSI des ministères sociaux– PSSI-MCAS
- Référentiel SecNumCloud de l'ANSSI pour la partie infra
- Hébergement de Données de Santé (HdS)

2.2 Données, processus et supports

2.2.1 Quelles sont les données traitées ?

Données traitées pour le support utilisateurs de l'application

La société Webhelp Medica[6] est en charge du support utilisateur et traite les mails envoyés par les utilisateurs de TousAntiCovid à contact@tousanticovid.gouv.fr et contact@stopcovid.gouv.fr.

Les données traitées par Webhelp Medica sont hébergées en France par l'hébergeur CIS Valley certifié HDS[7]

Des clauses RGPD ont été signées entre Inria et Webhelp Medica.

Données traitées uniquement dans l'application

- **Pour l'attestation de déplacement dérogatoire**
    - Prénom, Nom, Date de naissance, Lieu de naissance, Adresse, Ville. Code postal, Date de sortie, Heure de sortie, Motif de déplacement, Signature (représentée par le QR code)
    - Ces informations saisies dans ce générateur d'attestation de déplacement ne font l'objet d'aucun traitement par le Ministère des Solidarités et de la Santé. Ces données personnelles sont exclusivement stockées dans le

[6] http://webhelpmedica.com/qualite-et-securite/
[7] https://www.cis-valley.fr/cloud-et-infogerance/hebergement-de-donnees-de-sante/

téléphone mobile de l'utilisateur afin de lui permettre de remplir plus aisément la prochaine attestation de déplacement dérogatoire.

- **Pour l'obtention des informations sanitaires sur les actualités en lien avec la Covid-19 relativement à un lieu d'intérêt**
    - Le code postal (lieu d'intérêt) saisi par l'utilisateur de l'application
    - Cette information
        - est stockée dans l'application mais elle est effaçable
        - n'est pas traitée pas le Ministère des Solidarités et de la Santé
- Pour l'obtention des conseils relatifs à l'isolement
    - Le statut Covid-19 sélectionné par l'utilisateur de l'application
    - La date de début des symptômes
    - La date de prélèvement positif
    - La présence de fièvre après 7 jours
    - La date de dernier contact (pour les personnes contact)
    - Le partage du foyer avec un cas COVID-19
    - La date de fin de symptômes du cas malade
    - La date de fin de symptômes du cas malade (cas indexd'une personne contact)

    Ces informations
        - sont stockées dans l'application mais elle est effaçable
        - ne sont pas traitées pas le Ministère des Solidarités et de la Santé

Données traitées sur le serveur Central pour le contact tracing

- **Données générées par le serveur**
    - Une clé d'au moins 128 bits, partagée entre l'application et le serveur (ci-après **clé partagée**) qui sert à authentifier les messages de l'application ;
    - Un identifiant de 40 bits (ci-après **identifiant de l'application**), unique pour chaque application qui s'enregistre et généré de façon aléatoire. Cet identifiant est seulement connu du serveur ;
    - Les pseudonymes aléatoires et temporaires (ci-après **pseudonymes**) de 64 bits que le serveur envoie à l'application à chaque requête journalière de l'application. Ils sont utilisés pour constituer les historiques de proximité définis ci-dessous ;
    - Les codes pays.
- **Données collectées et enregistrées par l'application sur le téléphone mobile de l'utilisateur**
    - Les pseudonymes émis via la technologie Bluetooth par les applications sur des téléphones mobiles à portée radio du téléphone mobile de l'utilisateur. La durée de vie de ces pseudonymes enregistrés est de 14 jours à compter de leur première émission. Ces pseudonymes enregistrés, avec leur horodatage d'émission et les niveaux de puissance reçue (RSSI), constituent **l'historique de proximité** qui est stocké dans l'application ;
- **Données stockées sur le serveur**
    - L'historique de proximité des personnes diagnostiquées ou dépistées positives au virus Covid-19 et qui ont consenti à envoyer volontairement leur historique de proximité au serveur ;
    - Le statut "à risque" de l'identifiant de l'application ;
    - Le statut « à risque d'avoir contracté le virus Covid-19 » de l'identifiant de l'application ;
    - La date de dernière notification d'un risque d'exposition par le serveur à un utilisateur notifié d'un risque ;

- Le device token et la time zone utilisés pour réveiller les applications sous iOS par un serveur d'Apple appelé Apple Push notification service (APNs). Le device token est généré au moment de l'installation de l'application sur un iPhone Il est stocké sur le serveur central afin que celui-ci puisse demander au serveur APNs de notifier les applications.

Pour simplifier la lecture, ces données seront identifiées par les sigles suivants :

Acronyme	**Description**
ID_A	Pseudonyme permanent associé à l'utilisateur A.
K_A	Clef partagée entre le serveur et l'application de l'utilisateur A.
EBID	Pseudonyme temporaire diffusé en Bluetooth.
$EBID_{A,i}$	Pseudonyme temporaire diffusé en Bluetooth par l'utilisateur A à la période i.
ECC	Code de pays chiffré.
LEE	Liste des périodes où l'utilisateur A est indiqué comme exposé sur le serveur.
UN_A	Variable binaire stockée sur le serveur indiquant si l'utilisateur A a déjà été notifié d'un risque d'exposition.
SRE_A	Variable stockée sur le serveur indiquant quand l'utilisateur A a envoyé la dernière requête pour connaître son statut "à risque" au serveur.

Pour information, il est mis à disposition des personnes diagnostiquées positives, en fonction du type de diagnostic (laboratoire ou consultation médicale) deux types de jetons, aléatoires, à usage unique qui ne sont en aucun cas stockés sur le serveur :

- Un QR code qui est un « mot de passe à usage unique » (One Time Password) aléatoire, émis par SI-DEP, avec un code et un lien « deeplink ». Il est remis à un patient dépisté lorsque ce dernier récupère son compte rendu d'analyse biologique du laboratoire et que ce dernier indique la présence du virus SARS-Cov2 (virus de la Covid-19). Le patient peut alors le scanner afin d'être en mesure d'autoriser le partage de son historique de proximité. Ce QR code n'est lié ni au patient, ni au test, ni au smartphone, il est à voir comme un certificat permettant de confirmer un diagnostic positif dans l'application.
- Un code aléatoire de 6 caractères alpha numérique qui est un « mot de passe à usage unique » (One Time Password) à durée de vie limitée (1 heure) donné par le médecin traitant à son patient suite à un diagnostic clinique positif à la Covid-19 pour qu'il soit autorisé par le serveur à partager son historique de proximité.

L'utilisation d'un de ces jetons par l'utilisateur lui permet, après avoir donné son consentement, et sa Date de Début des Symptômes (DSS), s'il la connait, d'envoyer son historique de proximité au serveur (uniquement les données collectées 2 jours avant la DDS). Cette DDS est une donnée locale au téléphone mobile.

Des statistiques ou KPI (*Key Performance Indicator*) sont calculées pour suivre l'évolution de l'épidémie et mieux adapter les paramètres de l'application TousAntiCovid. Elles sont les suivantes :

- Nombre de nouveaux utilisateurs s'étant enregistrés sur le serveur avec succès (si 1 utilisateur = 1 mobile)
- Nombre de nouveaux enregistrements ayant échoué. La cause pouvant être une erreur logicielle ou bien une tentative hors application mobile mal effectuée
- Nombre de nouveaux enregistrements non effectifs dus à un échec du Captcha Orange
- Nombre de demandes de status d'exposition à une personne s'étant déclarée positive effectuées avec succès
- Nombre de demandes de status d'exposition à une personne s'étant déclarée positive en échec. La cause pouvant être une erreur logicielle ou bien une tentative hors application mobile mal effectuée
- Nombre de demandes de status d'exposition à une personne s'étant déclarée positive effectuées par un utilisateur non authentifié hors application mobile
- Nombre d'utilisateurs ayant été exposés à une personne s'étant déclarée positive, jugés à risque mais pas encore notifiés
- Nombre cumulé d'utilisateurs exposés à une personne s'étant déclarée positive, jugés à risque et notifiés pour la première fois

- Nombre d'utilisateurs ayant été exposés à une personne s'étant déclarée positive, jugés à risque, notifiés et de nouveau en contact avec une personne s'étant déclarée positive
- Nombre cumulé d'utilisateurs exposés à une personne s'étant déclarée positive, jugés à risque ou non (agrégation des colonnes H + I + J et du nombre d'utilisateurs exposés mais non jugés à risque)
- Nombre de demandes de suppression de l'historique d'exposition effectuées depuis l'application mobile réussies
- Nombre de demandes de suppression de l'historique d'exposition effectuées depuis l'application mobile en échec. La cause pouvant être une erreur logicielle ou bien une tentative hors application mobile mal effectuée
- Nombre de demandes de suppression de l'historique d'exposition effectuée par un utilisateur non authentifié hors application mobile
- Nombre de désenregistrements réussis, depuis la fonction Me désinscrire de l'application
- Nombre de désenregistrements en échec. La cause pouvant être une erreur logicielle ou bien une tentative hors application mobile mal effectuée
- Nombre de désenregistrements effectués par un utilisateur non authentifié hors application mobile
- Nombre d'utilisateurs ayant saisi un code avec succès grâce à l'application mobile
- Nombre de saisie de code grâce à l'application mobile ayant échoué. La cause pouvant être une erreur logicielle ou bien une tentative hors application mobile mal effectuée
- Nombre de saisie de code effectuée par un utilisateur non authentifié hors application mobile
- Nombre de codes courts utilisés avec succès
- Nombre de codes longs utilisés avec succès
- Nombre de codes longs n'étant plus valides
- Nombre de codes courts n'étant plus valides
- Nombre de codes courts généré
- Nombre de tentatives d'utilisation d'un code déjà utilisé
- Nombre de tentatives d'utilisation d'un code n'étant pas encore valide ou n'étant plus valide
- Nombre de vérifications d'un code n'ayant pas été fourni par un laboratoire ou un médecin

Le serveur n'est pas en mesure d'initier une connexion vers une application et donc de la contacter. Le serveur n'a pas pour objet de réaliser un suivi ou d'identifier les zones dans lesquelles ces personnes se sont déplacées.

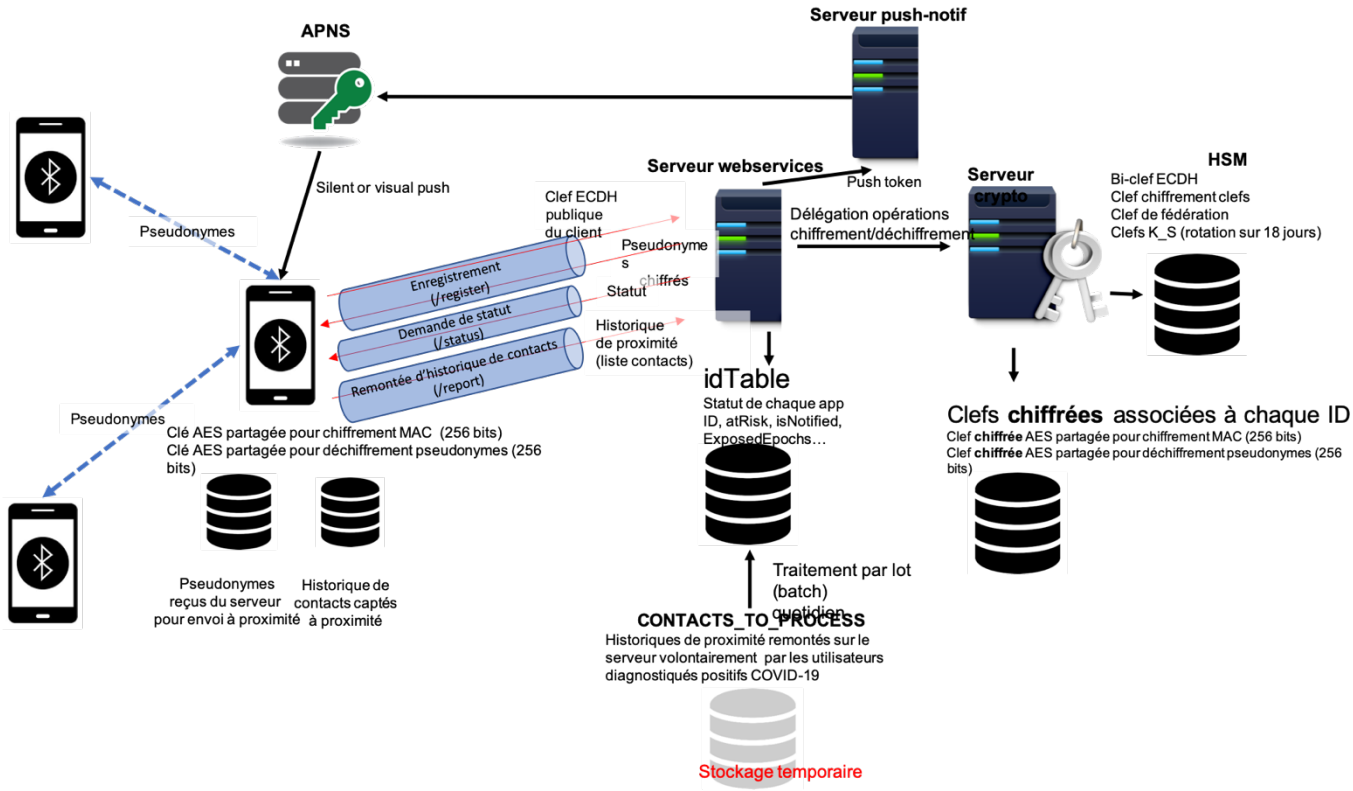


Figure 1 - Schéma des flux de données

2.2.2 Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?

- **Génération par le serveur**
  - D'une clé partagée entre l'application et le serveur qui sert à authentifier les messages de l'application.
  - D'un identifiant unique et généré de façon aléatoire, pour chaque application qui s'enregistre auprès du serveur. Cet identifiant est seulement connu du serveur.
  - De pseudonymes :
    - Aléatoires et temporaires : ils ne correspondent à aucun identifiant connu de la personne.
    - Vérifiables : la clé partagée (voir plus haut) permet d'authentifier les pseudonymes transmis au serveur.
- **Collecte par l'application de l'historique de proximité.** Aucune remontée de cet historique vers le serveur n'est effectuée tant que l'utilisateur ne se déclare pas positif au sein de l'application suite à un diagnostic positif à la COVID-19.
- **Émission périodique des pseudonymes par l'application** afin que ces pseudonymes soient collectés par les applications voisines pour constituer leur historique de proximité.
- **Demande de statut journalière au serveur** afin de savoir si des pseudonymes de l'application sont à risque :
  - Si le serveur répond par l'affirmative
    - Cela implique que le téléphone de l'utilisateur a été à proximité du téléphone d'au moins une personne diagnostiquée positive.
    - L'application émet alors une notification à l'utilisateur du téléphone.
- **Si la personne est diagnostiquée positive, envoi au serveur de son historique de proximité** après authentification donnée par l'autorité de santé et après consentement de la personne. La date de début de symptôme (DDS) lui sera demandée afin de restreindre l'envoi des contacts à 2 jours avant la DDS.

2.2.3 Quels sont les supports des données ?

Les supports des données associés à chaque étape du cycle de vie des données sont les suivants :

- **Installation de l'application :** téléphone mobile, serveur, Internet ;
- **Collecte des pseudonymes** : téléphone mobile, Bluetooth, serveur, Internet ;
- **Envoi des pseudonymes au serveur** : téléphone mobile, serveur, Internet

Évaluation : Acceptable **Commentaire d'évaluation :** Evaluations dans le document.

3 Historique des évolutions majeures

3.1 Juin 2020

3.1.1 Arrêt de la remontée de l'historique au serveur Central

Depuis le 26 juin 2020, il est impossible à toutes les applications TousAntiCovid (anciennement StopCovid) de remonter des données au serveur central sans le filtre. En effet, la mise à jour vers la version 1.1 est consécutive à toute ouverture de l'application, nécessaire si quelqu'un rentre un code lié à un test positif.

3.1.2 Arrêt de l'utilisation du reCaptcha Google

Depuis le 26 juin 2020, les utilisateurs de l'application TousAntiCovid (anciennement StopCovid) téléchargée depuis les stores utilisent le Captcha d'Orange et ne peuvent plus s'enregistrer avec reCaptcha de Google
De plus les appels au webservice reCaptcha de Google ont été désactivés depuis le le 31 aout 2020

3.2 Septembre 2020

3.2.1 Réveil des applications sous iOS par un « Push server »

Jusqu'au 15 septembre 2020, l'application TousAntiCovid (anciennement StopCovid) pour iOS effectuait en background (arrière-plan) et de manière erratique, en cas de non interaction régulière avec l'utilisateur, des requêtes *status* vers le serveur. Ce comportement qui n'avait pas été anticipé est lié au mode « background » et aux algorithmes (non connus) de priorisation des processus sur iOS permettant de faire basculer une application localisée en arrière-plan , au premier plan.

Pour rappel, la requête *status* permet de récupérer de nouveaux pseudonymes et de savoir si l'utilisateur a été à risque depuis le dernier *status* (dont la fréquence d'appel est paramétrable). Son bon fonctionnement est donc essentiel.
L'évolution consiste à s'appuyer sur une « push *notification* » journalière pour que l'application TousAntiCovid pour iOS se fasse réveiller de manière fiable, prédictible et puisse, pendant le temps CPU octroyé par iOS, effectuer un *status* au serveur de manière certaine.

Apple propose une solution basée sur un *serveur de push notifications* nommée APNS[8] (Apple Push Notification service) pour qu'un serveur puisse envoyer une notification aux applications.
L'APNS est décrit comme « un service robuste, sécurisé et très efficace permettant aux développeurs d'applications de propager des informations vers iOS ».

Les données transmises sont des données techniques et propres à toutes les applications tournant sous iOS.
Lors du lancement initial de l'application sur le téléphone mobile d'un utilisateur, le système établit automatiquement une connexion IP accréditée, chiffrée et persistante entre l'application et les APNS. Cette connexion permet à l'application d'effectuer la configuration pour lui permettre de recevoir des notifications de la part du serveur APNS.

L'information en question, nommée « token » ou jeton, est générée par Apple. Ce token est transmis au provider TAC qui est alors en mesure de demander à l'APNS de notifier les applications. Aucune autre donnée que ce token n'est envoyée à l'APNS. Il est à noter que l'APNS peut émettre de nouveaux tokens pour différentes raisons :

8 https://developer.apple.com/library/archive/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/APNSOverview.html#//apple_ref/doc/uid/TP40008194-CH8-SW1

- L'utilisateur installe son application sur un nouvel appareil ;
- L'utilisateur restaure le dispositif à partir d'une sauvegarde ;
- L'utilisateur réinstalle le système d'exploitation ;
- Autres événements définis par le système

L'architecture technique réalisée est la suivante :

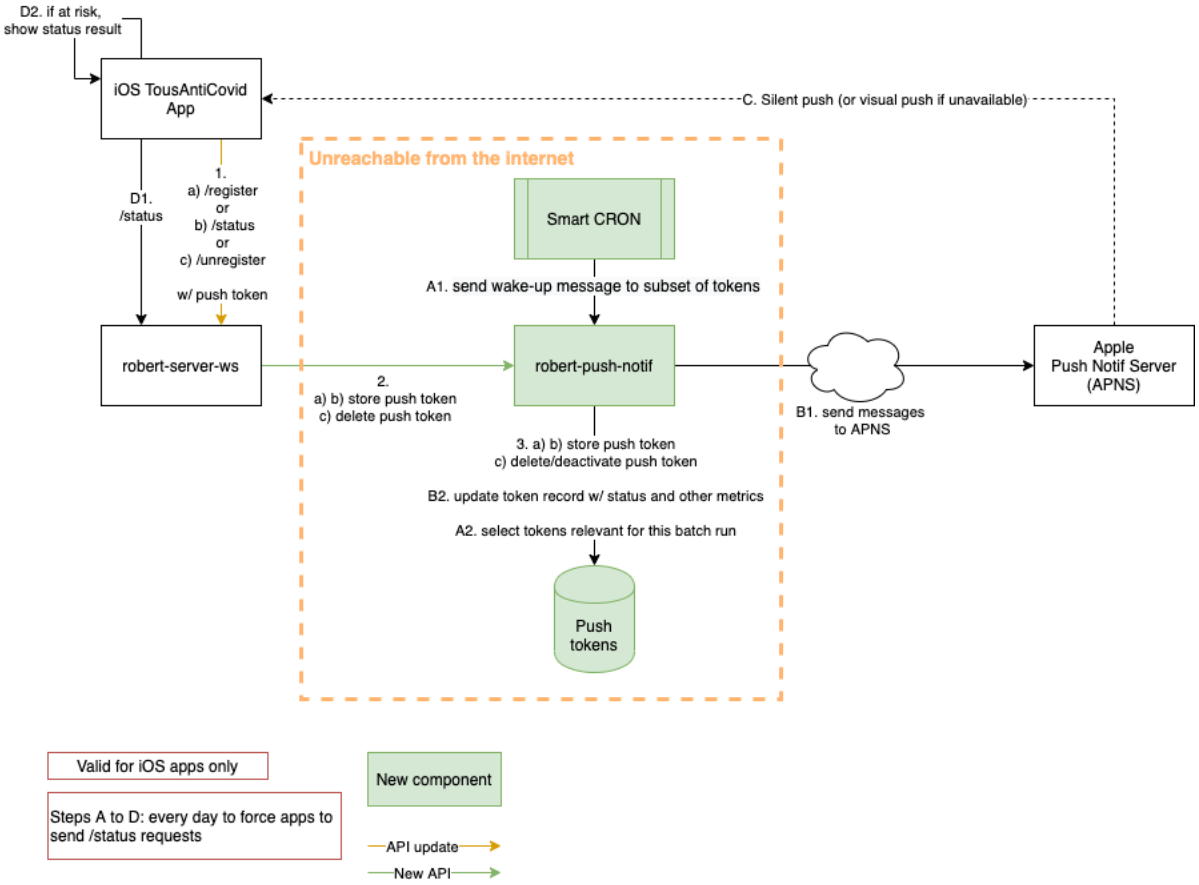


Figure 2 – Architecture Push Server

Cette solution s'appuie sur les webservices existants (*register*, *status* et *unregister*) dans lesquels l'application TousAntiCovid iOS fournit en plus un *device token* qui correspond à un token de l'application sur cet iPhone, généré par iOS et *Apple Push notification service* (APNs) au moment de l'installation de l'application. Le *device token* est une suite de caractères permettant à Apple d'identifier une application mobile sur un téléphone mobile donné).
Et pour bien notifier l'utilisateur pendant des heures en journée (entre 7h et 20h), il est passé également la *timezone* de l'utilisateur. Et en cas de message visible à l'utilisateur, il est passé la *locale* du smartphone pour le notifier dans la bonne langue.

Le serveur Robert *robert-server-ws* passe alors le *device token* au Push Server TousAntiCovid *robert-push-notif* pour qu'il le stocke dans la base de *push tokens*.

Ensuite, à une fréquence donnée, une tâche automatisée interne (*Smart CRON*) parcourt cette base de *push tokens* afin de notifier les téléphones mobiles qui doivent être réveillés à ce moment-là.

Le serveur *robert-push-notif* demande alors au serveur APNs d'envoyer une *notification push* aux iPhones correspondant à ces *push tokens* et leur permettre ainsi de réaliser un appel à *status*.

Tous ces nouveaux composants « Push server » sont placés dans une zone dédiée, complètement isolée du serveur Robert *robert-server-ws*, et non accessible de l'extérieur, au même titre que le serveur de QR codes.

3.3 Novembre 2020

3.3.1 Nouvelle version de StopCovid nommée « TousAntiCovid »

Dans le cadre du volet numérique de gestion de la crise, la décision a été prise, pour renforcer l'adoption, d'une version 2.0 de StopCovid, nommée « TousAntiCovid », plus ancrée dans le champ sanitaire (sa raison d'être), et qui prend en compte de nombreux retours d'utilisateurs.

Cette nouvelle version

- Est plus dynamique :
  - un nouveau design graphique, sur un seul écran, qui est plus lisible et éditorialisé. Il a été conçu suite à des interactions avec des groupes de tests ;
  - une insertion dans un ensemble d'outils numériques. En pratique, des liens web dans les rubriques **Mes conseils Covid**[9] et **Où me faire dépister**[10], et aussi un lien vers l'observatoire Géodes SPF (taux d'incidence sur carte française)
- Donne des informations sur l'épidémie :
  - Une section **Infos** a été créée pour informer l'utilisateur avec un fil de brèves et des chiffres clés. S'il y a de nouvelles actualités, elles sont envoyées à l'utilisateur. Pourquoi ? Donner à l'utilisateur des informations fiables sur l'épidémie.
- Montre qu'elle est utile et utilisée :
  - Une section **Chiffres-clés** a été rajoutée, ils renseignent
    - sur la situation de l'épidémie (nouveaux cas, Patients en réanimation, Nouveaux patients en réanimation, Tension des réanimations, R effectif, taux d'incidence, taux de positivité)
    - sur les métriques de l'application (enregistrements, déclarations de positivité, notifications d'expositions au risque)
  - Ces chiffres clés trouvent leur source sur data.gouv.fr pour la partie épidémiologique, avec un rafraîchissement trois fois par jour. Les différentes sources sont détaillées sur cette page web : https://bonjour.tousanticovid.gouv.fr/app.html#chiffres

3.3.2 Génération des attestations de déplacement dérogatoire

L'utilisateur peut générer et gérer ses attestations dans l'application.

- Elles sont conservées dans le téléphone, et à la prochaine ouverture de l'application, l'application supprime automatiquement toutes les attestations de plus de 24 heures. L'utilisateur peut aussi les supprimer à tout moment, soit une à une, soit toutes les informations dans la section « Paramètres » de l'application ;
- Lorsqu'il remplit une attestation l'utilisateur a la possibilité de sauvegarder dans son téléphone mobile son Prénom, Nom, Date de naissance, Lieu de naissance, Adresse, Ville, Code postal et le motif de déplacement, pour lui éviter de les saisir de nouveau dans les prochaines attestations. Il peut supprimer à tout moment ces données de son téléphone dans la section « Paramètres » de l'application.
- Ces données ne sont pas remontées au serveur central.

3.3.3 Obtention des Informations sanitaires par lieu d'intérêt

L'utilisateur peut saisir dans l'application un lieu d'intérêt sous la forme d'un code postal pour obtenir des indications sanitaires par département.

Cette donnée est stockée uniquement dans l'application (exemple : 73100) et n'est pas remontée vers le serveur central.

3.4 Décembre 2020

3.4.1 Obtention de conseils relatifs à l'isolement

L'utilisateur peut obtenir des informations sur le recours à l'isolement, en sélectionnant ou en saisissant des données.

Ces données sont stockées uniquement dans l'application et ne sont pas remontées vers le serveur central.

Elles sont conservées jusqu'à ce que l'utilisateur choisisse de les supprimer en indiquant qu'il souhaite les supprimer depuis le menu Paramètres > Effacer sur mon téléphone de la section Mes données « isolement »

[9] https://mesconseilscovid.sante.gouv.fr
[10] https://sante.fr/recherche/trouver/DepistageCovid

4 Principes fondamentaux

4.1 Remarques liminaires

L'utilisation de l'application TousAntiCovid repose sur le volontariat.

Pour les personnes diagnostiquées positives, le partage de l'historique de proximité avec le serveur repose sur le consentement.

Les technologies utilisées reposent sur le Bluetooth et excluent l'usage de toute technologie de géolocalisation.

4.2 Proportionnalité et nécessité

4.2.1 Les finalités du traitement sont-elles déterminées, explicites et légitimes ?

Les données sont générées et collectées pour **fournir le service**, à savoir **informer une personne du risque qu'elle a encouru les 15 derniers jours.**

La définition de contact à risque donnée par Santé Publique France (SPF) est évolutive. A ce jour, elle est la suivante :

En l'absence de mesures de protection efficaces pendant toute la durée du contact :

- *séparation physique isolant la personne-contact du cas confirmé en créant deux espaces indépendants (vitre, Hygiaphone®);*
- *masque chirurgical ou FFP2 ou grand public en tissu fabriqué selon la norme AFNOR SPEC S76-001 de catégorie 1 ou masque grand public en tissu réutilisable possédant une fenêtre transparente homologué par la Direction générale de l'armement, porté par le cas ou le contact.*

Un contact à risque est une personne

1. *Ayant partagé le même lieu de vie que le cas confirmé ou probable ;*
2. *Ayant eu un contact direct avec un cas, en face à face, à moins de 2 mètres, quelle que soit la durée (ex. conversation, repas, contact physique). En revanche, des personnes croisées dans l'espace public de manière fugace, même en l'absence de port de masque, ne sont pas considérées comme des personnes-contacts à risque;*
3. *Ayant prodigué ou reçu des actes d'hygiène ou de soins;*
4. *Ayant partagé un espace confiné (bureau ou salle de réunion, véhicule personnel…) pendant au moins 15 minutes consécutives ou cumulées sur 24h avec un cas ou étant resté en face à face avec un cas durant plusieurs épisodes de toux ou d'éternuement.*

L'application TousAntiCovid vise plus particulièrement les troisième et quatrième types de contact à risque .

Les données générées et collectées avec l'accord de l'utilisateur ont donc pour unique but d'estimer de manière statistique des proximités et leur durée. L'usage du Bluetoooth a été retenu et l'usage de toute technonlogie de géolocalisation écartée.

En termes de rattachement au parcours de santé du sujet contact, à travers le « rattachement du contact TousAntiCovid vers/ via les médecins généralistes » : le contact TousAntiCovid sera invité à consulter son médecin traitant, par télésurveillance de préférence. Le numéro de la plateforme nationale sera également mis à disposition pour orienter la personne vers un service téléphonique lui permettant de trouver un médecin s'il n'a pas de médecin traitant ou n'est pas en mesure de le joindre. Le médecin lui indiquera les mesures à suivre telles que préconisées par le MSS. Cette plateforme téléphonique pourra également rappeler les messages de conduite à tenir.

Évaluation : Acceptable
Plan d'action / mesures correctives :
Commentaire d'évaluation :
Evaluations dans le document.

4.2.2 Quel(s) est(sont) les fondement(s) qui rend(ent) votre traitement licite ?

Conformément à l'article 6 e. du RGPD, le traitement est nécessaire à l'exécution d'une mission d'intérêt public contre l'épidémie de la Covid-19 dont est investi le responsable du traitement. Il s'appuie en cela sur le décret n° 2020-650 du 29 mai 2020

Le traitement des données de santé est fondé sur des motifs d'intérêt public dans le domaine de la santé (article 9 2.i RGPD).

Évaluation : Acceptable
Commentaire d'évaluation :
Aucun commentaire.

4.2.3 Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?

En matière d'identification possible, toute l'architecture du dispositif envisagée fait remonter au serveur uniquement les pseudonymes aléatoires et temporaires générés par les applications associées aux personnes avec lesquelles un individu diagnostiqué positif a été en contact, et non le pseudonyme de ce dernier.

L'information "un pseudonyme est diagnostiqué positif" n'est jamais remontée au serveur, ni stockée par ce dernier, et n'est jamais communiquée aux autres applications. Une personne est informée du risque non pas parce qu'elle reçoit l'information de qui est infecté, mais parce que la personne diagnostiquée positive accepte de partager la liste des pseudonymes collectés, et qu'elle peut potentiellement s'y trouver. Ce n'est pas le serveur qui notifie une personne : c'est l'application de la personne qui interroge le serveur, au cours de la journée et qui alerte la personne de son exposition éventuelle au risque lors des jours écoulés. Le serveur n'est pas en mesure de contacter une application.

Nous avons suivi un procédé qui réduit au maximum le risque de ré-identification de la personne diagnostiquée positive à l'origine d'une remontée de ses contacts dans le respect des principes de protection des données personnelles.

Évaluation : Acceptable
Plan d'action / mesures correctives :
Commentaire d'évaluation :
Evaluations dans le document.

4.2.4 Les données sont-elles exactes et tenues à jour ?

L'application émet et collecte des pseudonymes qui sont

- aléatoires : ils ne correspondent à aucun identifiant connu de la personne,
- temporaires : leur durée de vie est de 15 minutes,
- vérifiables : la clé partagée permet d'authentifier les pseudonymes auprès du serveur.

Quand une personne est diagnostiquée positive au Covid-19, et après qu'elle ait donné à nouveau son consentement, son historique de proximité est chargé sur le serveur sécurisé après vérification d'un jeton aléatoire à usage unique (code ou QR code, voir supra) donné par l'autorité de santé. Une personne ne peut pas se déclarer « positive elle-même » et ainsi fausser la base centralisée., puisqu'elle doit avoir à sa disposition un tel jeton. La base centralisée contient la liste des pseudonymes des historiques de proximité des personnes diagnostiquées positives. Elle ne contient pas les pseudonymes des personnes diagnostiquées positives.

Sur le plan technique : les données mesurées et enregistrées sont des séries temporelles de paquets échangées entre téléphones mobiles, et qui donnent un RSSI (Received Signal Strength Indicator) pour chaque paquet échangé. Le RSSI est une mesure de la puissance en réception d'un signal reçu d'une antenne. En Bluetooth, les valeurs usuelles de RSSI pour un terminal varient de −60 dBm (niveau élevé de réception) à −90 dBm (niveau minimum permettant d'exploiter le signal). Le RSSI varie selon la distance avec l'antenne émettrice. C'est cette corrélation à la distance entre l'émetteur et le récepteur qui permet d'inférer un proxy/une classification de la proximité entre les deux terminaux émetteur et récepteur.

Le calibrage, nécessaire pour tenir compte des gains en émission et réception pour le signal Bluetooth et qui dépend des terminaux, est réalisé sur le téléphone mobile. Une première classification est également réalisée sur le téléphone mobile à la remontée des contacts, notamment à travers la suppression des contacts beaucoup trop courts ou beaucoup trop faibles. Le calcul de risque se

fait sur le serveur (qui est le seul à pouvoir valider les paquets de type « Hello » et à permettre l'intégration pour une même application exposée) à l'aide d'un algorithme de classification statistique qui a été paramétré en fonction de résultats de tests terrain (menés auxniveauxeuropéen et français).

Il n'est pas envisagé, dans la mise en oeuvre de TousAntiCovid, d'introduire des fauxpositifs dans les notifications transmises aux personnes, ce qui aurait permis de limiter les risques de ré-identification dans certains types d'attaques mais présente des inconvénients du fait des conséquences sur les personnes recevant des fauxpositifs. Ce point a été souligné dans la délibération 2020-046 de la CNIL.

Évaluation : Acceptable
Plan d'action / mesures correctives :
Commentaire d'évaluation :
Evaluations dans le document.

4.2.5 Quelle est la durée de conservation des données ?

Le traitement est mis en œuvre jusqu'au 31 décembre 2021.

La clé d'authentification partagée et l'identifiant aléatoire permanent sont conservés jusqu'à ce que l'utilisateur se désinscrive et désinstalle l'application TousAntiCovid, et au plus tard pour la durée mentionnée au premier alinéa.

Les données de l'historique de proximité enregistrées par l'application sur le téléphone mobile et stockées sur le serveur sont conservées au maximum quatorze jours à compter de leur émission.

Les données mentionnées au 4° de l'article 2 du présent décret ne sont pas conservées dans l'application TousAntiCovid. Elles ne sont traitées qu'une seule fois afin que l'utilisateur de l'application soit autorisé par le serveur à partager son historique de proximité.

Une purge systématique des pseudonymes périmés stockées à la fois sur les téléphones mobiles et sur le serveur est effectuée quotidiennement. Toutes les données, tous les pseudonymes éphémères de proximité qui sont enregistrés dans l'historique de proximité des téléphones mobiles ou qui sont remontés sur le serveur sont effacés au bout de 14 jours à compter de leur date d'émission par une application. L'effacement a lieu par une suppression quotidienne du jour le plus ancien.

Il est nécessaire de borner cette durée pour englober la recommandation de Santé Publique France (SPF) et du MSS : 2 jours avant la date de début des symptômes ou 7 jours avant la date de prélèvement à laquelle il faut ajouter la durée d'envoi, la réalisation du test, et la durée à recevoir le compte rendu et de choisir de se déclarer. 15 jours étaient aussi la durée admise de contagion (14 jours de contagion après le jour où la personne est infectée).

Cette durée devra donc être comprise entre 10 jours et 15 jours, laissant le temps à une personne pour se déclarer dans l'application. La durée de 15 jours est retenue.

L'utilisateur de TousAntiCovid peut décider à tout moment dans l'application d'effacer son d'historique de proximité local, ses données sur le serveur et ses alertes, ou encore de supprimer l'application.

Évaluation : Acceptable
Plan d'action / mesures correctives :
Commentaire d'évaluation :
Evaluations dans le document.

4.3 Mesures protectrices des droits

4.3.1 Comment les personnes concernées sont-elles informées à propos du traitement ?

Quand une personne installera l'application TousAntiCovid, elle sera informée du traitement via les mentions d'information RGPD respectant l'article 13 du RGPD ainsi que le paragraphe 3 de l'article 48 de la Loi Informatique et Libertés.

Par ailleurs, le fonctionnement de l'application TousAntiCovid et le traitement seront présentés sur les supports de communication (dont les sites web) de la DGS du MSS.

TousAntiCovid sera intégré aux communications sur les gestes barrières à adopter.

Les éléments communiqués à la population seront présentés d'une manière compréhensible et accessible à toutes et à tous notamment à travers des infographies permettant de vulgariser les concepts technologiques sous-jacents.

Les écrans de travail en Annexe donnent un exemple de ces mentions d'informations.

Évaluation : Acceptable
Plan d'action / mesures correctives :
Commentaire d'évaluation :
Evaluations dans le document.

4.3.2 Si applicable, comment le consentement des personnes concernées est-il obtenu ?

Lorsqu'une personne installe l'application TousAntiCovid, elle donne son consentement pour :

- L'activation du Bluetooth ;
- La réception des notifications de risque de transmission du virus suite à un contact avec des personnes diagnostiquées ou dépistées positives à la COVID-19 ;
- L'activation de l'envoi de ses pseudonymes et la mémorisation de ceux de ses voisins (historique de proximité).

Si une personne est diagnostiquée ou dépistée positive :

- Par un laboratoire : elle scanne le QR code transmis par SI-DEP pour que son historique de proximité soit envoyé au serveur avec son consentement.
- Par un médecin : elle saisit sur le serveur le code que lui a communiqué le médecin et donne son consentement pour que son historique de proximité soit envoyé au serveur.

Évaluation : Acceptable
Plan d'action / mesures correctives :
Commentaire d'évaluation :
Evaluations dans le document.

4.3.3 Comment les personnes concernées peuvent-elles exercer leurs droits d'accès et droits à la portabilité ?

En application des articles 11 et 23 i) du règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 susvisé, les droits d'accès, de rectification et de limitation prévus aux articles 15, 16 et 18 de ce même règlement ne peuvent s'exercer auprès du responsable de traitement dès lors que les données traitées sont pseudonymisées, et que l'exercice de ces droits nécessiterait une identification de la personne concernée et pourrait permettre à cette même personne d'identifier des utilisateurs diagnostiqués ou dépistés positifs à la Covid-19. Le décret relatif à ce traitement écarte le droit d'accès.

En outre, un usage détourné du droit d'accès pourrait permettre d'obtenir indirectement des informations et être une manière détournée d'identifier des personnes avec lesquelles la personne a été en contact

Le droit à la portabilité ne peut pas être exercé dans le cadre de l'exécution d'une mission d'intérêt publique.

Évaluation : Acceptable
Plan d'action / mesures correctives :
Commentaire d'évaluation :
Evaluations dans le document.

4.3.4 Comment les personnes concernées peuvent-elles exercer leurs droits de rectification et droits à l'effacement (droit à l'oubli) ?

En application des articles 11 et 23 i) du règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 susvisé, les droits d'accès, de rectification et de limitation prévus aux articles 15, 16 et 18 de ce même règlement ne peuvent s'exercer auprès du responsable de traitement dès lors que les données traitées sont pseudonymisées, et que l'exercice de ces droits nécessiterait une identification de la personne concernée et pourrait permettre à cette même personne d'identifier des utilisateurs diagnostiqués ou dépistés positifs à la Covid-19. Le décret relatif à ce traitement écarte le droit de rectification.

Concernant l'exercice du droit d'effacement, en application de l'article 17 paragraphe 3, le droit à l'effacement n'est pas applicable lorsque le traitement est nécessaire pour exécuter une mission d'intérêt public dont est investi le responsable du traitement ou pour des motifs d'intérêt public dans le domaine de la santé publique. Par ailleurs, l'exercice du droit à l'effacement auprès du RT aboutirait à la nécessaire réidentification de la personne concernée, ce qui doit être écartée pour les mêmes raisons qu'évoquées précédemment.

La personne concernée peut elle-même procéder à l'effacement de ses données de la manière suivante :

- Effacer toutes les données stockées sur son téléphone mobile : les pseudonymes des téléphones mobiles qui ont été à proximité du sien et qui sont enregistrés dans l'historique de proximité de son téléphone mobile ;
- Effacer et/ou désactiver les notifications affichées par l'application ;
- Effacer toutes les données stockées sur le serveur : les pseudonymes de son téléphone qui ont été enregistrés dans l'historique de proximité des téléphones mobiles qui sont passés à proximité du sien et que le ou les utilisateurs ont accepté de communiquer au serveur car ils ont été diagnostiqués ou dépisté positif à la Covid-19 ;
- Effacer les attestations de déplacement dérogatoires ;
- Modifier ou effacer le lieu d'intérêt ;
- Modifier ou effacer le statut Covid-19 sélectionné permettant l'obtention de conseils sur le recours à l'isolement ;
- Se désinscrire du serveur, cela efface toutes les données sur le serveur y compris les pseudonymes et les autres données sur son téléphone mobile.

Évaluation : Acceptable
Plan d'action / mesures correctives :
Commentaire d'évaluation :
Evaluations dans le document.

4.3.5 Comment les personnes concernées peuvent-elles exercer leurs droits de limitation et droits d'opposition ?

En application des articles 11 et 23 i) du règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 susvisé, les droits d'accès, de rectification et de limitation prévus aux articles 15, 16 et 18 de ce même règlement ne peuvent s'exercer auprès du responsable de traitement dès lors que les données traitées sont pseudonymisées, et que l'exercice de ces droits nécessiterait une identification de la personne concernée et pourrait permettre à cette même personne d'identifier des utilisateurs diagnostiqués ou dépistés positifs à la Covid-19. Le décret relatif à ce traitement écarte le droit à la limitation.

Concernant les pseudonymes générés ou collectés sur son téléphone, la personne concernée peut à tout moment arrêter d'utiliser l'application donc exercer son droit de d'opposition. Elle peut à tout moment arrêter d'émettre des pseudonymes et/ou désactiver le Bluetooth.

Dans le cas où la personne concernée a envoyé au serveur les pseudonymes temporaires des téléphones mobiles qui sont passés à proximité du sien et qui sont enregistrés dans l'historique de proximité de son téléphone elle ne peut pas exercer son droit de d'opposition, car par conception, ces données ne sont rattachées, sur le serveur, à aucun de ses propres pseudonymes temporaires.

La personne peut décider à tout moment de ne pas être notifiée par l'application du fait qu'elle est à risque car son historique de proximité contient une personne diagnostiquée ou dépistée positive.

Évaluation : Acceptable
Plan d'action / mesures correctives :
Commentaire d'évaluation :
Evaluations dans le document.

4.3.6 Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?

- **3DS OutScale : hébergement**
    - Pendant la phase de **développement** du projet une convention a été signée entre Inria et 3DS Outscale pour héberger le développement du prototype. Il s'agit de la convention de service SecNumCloud signée entre 3DS Outscale et Inria le 29/04/2020, ainsi que les Conditions Générales d'Utilisation et de vente de 3DS Outscale acceptée par Inria le 29/04/2020.
    - Pour la phase de **production**,

        - un accord cadre sera signé entre MSS et et Inria
        - un accord de consortium a été signé entre Inria et les partenaires impliqués, dont Outscale
- **Orange : maintenance et exploitation**
    - Pour la phase de développement, une convention de Sous-traitance est en cours de signature entre Cap Gemini et Inria
    - Pour la phase de production,
        - un accord cadre a été signé entre MSS et et Inria
        - un accord de consortium a été signé entre Inria et les partenaires impliqués, dont Orange
- **Webhelp Medica**
    - Des clauses RGPD ont été signées entre Inria et Webhelp Medica
- IMA
    - Des clauses RGPD ont été signées entre Inria et IMA

Évaluation : Acceptable
Plan d'action / mesures correctives :
Commentaire d'évaluation :
Evaluations dans le document.

4.3.7 En cas de transfert de données en dehors de l'Union européenne, les données sont-elles protégées de manière équivalente ?

Il n'est pas prévu de transférer de données personnelles hors de l'Union Européenne.

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

5 Risques

5.1 Mesures existantes ou prévues

5.1.1 Mesures organisationnelles

Organisation de la politique de protection de la vie privée

- Pour l'hébergement, 3DS Outscale :
    - S'engage depuis le 25 mai 2018 à respecter la conformité au RGPD dans ses services de Cloud computing.
    - Est également adhérent et respecte les prescriptions du Code de Conduite de l'association Cloud Infrastructure Services Provider (CISPE).
    - Applique des processus certifiés ISO 27001:2013 permettant la mise en œuvre de procédures propres à garantir la confidentialité et la protection des données de ses clients.
- Prise en compte du principe de « Privacy by Design » dès la conception du protocole.

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Gérer la politique de protection de la vie privée

- La définition et la mise en œuvre de la politique de protection de la vie privée repose sur l'implication de la DPO de MSS et l'Inria. Cette mise en œuvre passe notamment par l'inscription du traitement dans le registre de traitement du MSS et d'Inria.

Evaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Gérer les risques

Durant toute la durée de conception de l'architecture et de l'application :

- Mise en œuvre et vérification des bonnes pratiques de la sécurité dans le code ;
- Vérification automatique via une chaîne Intégration continue / déploiement continu (CI/CD) des vulnérabilités en appliquant le top 10 Open Web Application Security Project (OWASP Zed Attack Proxy) ;
    - L'intégration continue couvre la première moitié de la chaîne. Elle vise à organiser au mieux et automatiser les opérations de développement et leurs transitions.
    - Le déploiement continu prend la suite : il consiste pour l'équipe infrastructures à scripter et automatiser les étapes de déploiement en production afin qu'une version livrée par le serveur CI puisse sans attendre se déployer en production ;
- Le Top 10 de l'OWASP est un document de sensibilisation standard pour les développeurs et la sécurité des applications web ; Broken Authentication. ; Sensitive Data Exposure ; XML External Entities (XXE) ; Broken Access Control ; Security Misconfiguration ; Cross-Site Scripting XSS ; Insecure Deserialization ; Using Components with Known Vulnerabilities ; Insufficient Logging & Monitoring.

Pendant la phase d'exploitation

- Le Sous-Traitant chargé de la maintenance prendra en charge l'organisation de veille et de gestion des vulnérabilités pour maintenir un bon niveau de sécurité de l'application mobile et du serveur durant toute la durée d'utilisation de l'application (veille des publications des vulnérabilités par les Internautes / qualification / correction / communication) est mise en œuvre.

Evaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Intégrer la protection de la vie privée dans les projets

La CNIL a été consultée en amont sur le projet StopCovid (renommé en TousAntiCovid) et a rendu un premier avis (délibération n°2020-046 du 24 avril 2020) sur le protocole sous-jacent, le protocole Robert.

Elle a rendu un deuxième avis (Délibération n° 2020-056 du 25 mai 2020) sur le projet de décret relatif à l'application mobile StopCovid (renommée en TousAntiCovid).

Evaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Gérer les incidents de sécurité et les violations de données

Les points clés du RGPD que 3DS Outscale s'engage à respecter sont les suivants :

- Signalement des failles de sécurité, engendrant un risque aux personnes concernées, au RSSI de la DGS (dgs-ssi@sante.gouv.fr), le FSSI (ssi@sg.social.gouv.fr) ainsi que la DPO du ministère (dpd-minsociaux@sg.sociaux.gouv.fr).
- Le Sous-traitant s'engage à informer sans délai (et au maximum dans un délai de 24 heures après en avoir pris connaissance)
    - le RSSI de la DGS (dgs-ssi@sante.gouv.fr), le FSSI (ssi@sg.social.gouv.fr) ainsi que la DPO du ministère

- Inria, dans le cadre de son contrat de sous-traitance en appui à la DGS

Il est constitué à cette fin une cellule conjointe entre la DGS et Inria impliquant leurs RSSI et DPO respectifs pour un traitement efficace et approprié de ce type d'incident impliquant toute violation de données à caractère personnel avérée ou supposée, susceptible d'engendrer un risque pour les personnes concernées.

Si des données à caractères personnelles sont concernées, le référent RGPD du ministère et la DPO sont informés par le RSSI de la DGS ou la FSSI MCAS.

L'information du responsable de traitement est accompagnée de toutes les documentations utiles permettant de comprendre l'incident, les mesures envisagées et si nécessaire les éléments permettant de notifier à la CNIL dans les 72 heures une violation de données à caractère personnel.

Évaluation : Acceptable
Commentaire d'évaluation :
- une organisation de veille et de gestion des vulnérabilités doit être mise en œuvre par le Responsable de Traitement

Gestion des personnels

Les points clés du RGPD que 3DS Outscale et les autres sous-traitants s'engagent à respecter sont les suivants :

- Formation et sensibilisation du personnel aux exigences de confidentialité et de protection des données personnelles
- Nomination d'un délégué à la protection des données (DPO) dont la désignation est effective depuis le 25 mai 2018
- Habilitations des personnes accédant au serveur

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Gestion des tiers accédant aux données

L'accès aux systèmes de stockages des données clients de 3DS Outscale est strictement limité aux équipes en charge des opérations de la plateforme. Tout accès à ces systèmes est journalisé afin de pouvoir détecter les éventuels accès illégitimes.

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Superviser la protection de la vie privée

Les points clés du RGPD que 3DS Outscale s'engage à respecter sont les suivants :

- Audits réguliers et actualisation des stratégies de traitement des données
- 3DS Outscale est certifié ISO 27001 et attesté conforme ISO 27017 et ISO 27018. Et à ce titre, a mis en œuvre des mesures de sécurité visant à protéger les données personnelles de toutes les parties prenantes en relation avec elle.

Evaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

5.1.2 Mesure sur les données

Chiffrement et précisions sur les clés utilisées

- Sécurisation du stockage des clés de chiffrement (HSM / Vault en Appliance virtuelle)
- Nous avons mis en œuvre le chiffrement des pseudonymes en employant l'algorithme de chiffrement SKINNY-CIPHER64/192 afin de remplacer 3DES, comme préconisé dans la délibération 2020-046 de la CNIL. Mise en œuvre du Certificate pinning (offert par l'API Android et sur iOS) sur les applications clientes qui est un mécanisme de sécurité

qui protège les sites internet de l'usurpation d'identité contre les certificats frauduleux émis par des autorités de certification compromises.

- Nous avons programmé les applications Android et iOS afin de stocker ou wrapper le secret partagé au moyen des API qui permettent l'utilisation du composant crypto du téléphone (secure enclave pour iOS, hardware backed keystore pour Android)
- Que cela soit pour le serveur backend ou pour les applications mobiles, nous avons utilisé une source d'aléa dont la qualité permet l'usage pour des opérations cryptographiques.

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Anonymisation

- Accès APIs protégé par API Gateway / Reverse proxy
- De plus, nous avons nettoyé les méta-données non-utiles au protocole ROBERT (IP, ports, token d'authentification etc.) au niveau du frontal web
- Une attention particulière est portée sur le fait qu'aucune information relative aux développeurs de l'application ne doit être enregistrée dans les journaux en mode « release » (codes erreurs explicites, informations techniques relatives aux téléphones mobiles, etc.)

Evaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Cloisonnement

- Découpage du système en plusieurs niveaux cloisonnés
- Cloisonnement et sécurisation des réseaux (VPC, VLAN et subnet)
- Mise en œuvre de groupes de sécurité, ACL sur les ressources IaaS
- L'architecture de tout le système intègre un cloisonnement entre le backend de l'application, le service de génération/validation des QR codes et le service Pro TousAntiCovid. De plus, il est mis en place un filtrage réseau entre tous ces services.
- Nous avons aussi mis en œuvre, sur un principe similaire, une segmentation du backend de l'application en plusieurs zones avec des rôles différents (front-office, middle-office, back-office, alerting/reporting/monitoring, développement/déploiement). Là aussi, un filtrage réseau entre ces zones est assuré.

Evaluation : Acceptable
Commentaire d'évaluation :
Toutes ces protections ont été listées dans les recommandations de l'ANSSI pour la sécurisation de TousAntiCovid. Le document listant l'ensemble des recommandations est donné en pièce jointe. Nous avons appliqué l'ensemble des recommandations majeures et modérées. Comme indiqué dans la politique de sécurité, tout le développement a fait l'objet d'un processus d'audit continu avec des points d'audit spécifique également.

Contrôle des accès logiques

- Mise en œuvre d'un service de gestion des identités et des accès (IAM -- Identity and Access Management) pour les administrateurs techniques et les administrateurs fonctionnels
- Les permissions d'accès sont basées sur RBAC (Role-Based Access Control)
- Mise en œuvre de groupes de sécurité, ACL sur les ressources IaaS du Cloud 3DS Outscale

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Journalisation

Mise en œuvre logging, supervision & monitoring avec des logs chiffrés et des mécanismes d'audit de l'imputabilité et de la traçabilité des actions menées sur le système, avec les points suivants :

- Existence d'un serveur de journalisation dédié, configuré en écriture seule ;
- Des journaux signés et chiffrés (priorité modérée) ;
- Accessibilité par une autorité de contrôle.

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Archivage

- Archivage des sauvegardes / snapshots basé sur les services proposés nativement par le Cloud 3DS Outscale
- Le Responsable de traitement précisera à 3DS Outscale
  - La fréquence des archivages,
  - Le responsable des archivages.
- Conformément à l'article L. 213-2 du Code du patrimoine, le sort final retenu pour les données à l'issue de la durée d'utilité administrative (DUA) est l'élimination. Compte tenu de la durée de conservation courte, il n'est pas prévu de processus d'archivage intermédiaire.

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Minimisation des données

- Mise en œuvre de la pseudonymisation pour limiter la réidentification : les pseudonymes générés et collectés sur les téléphones mobiles ainsi que ceux stockés ceux sur le serveur sont des **pseudonymes aléatoires et temporaires.**

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

5.1.3 Mesure générale de sécurité du système

Sécurisation de l'exploitation

- Plateforme hébergée par 3DS Outscale en France et qualifiée SecNumCloud, par ailleurs certifiée HdS
- IAM pour les administrateurs techniques et les administrateurs fonctionnels
- Accès SSH par Bastion pour les administrateurs de la plateforme
- Afin de répondre aux recommandations de l'ANSSI, un dispositif de détection des incidents de sécurité est mis en place. Le mécanisme prévu se compose de :
  - Une protection anti-DDoS capable de contrer une attaque massive vis-à-vis du front-office exposé sur Internet ; le recours à un service spécialisé a été effectué au travers de l'anti-DDos (Cybersécurité Orange).
  - Mécanismes Blackhole et anti-DDoS de 3DS Outscale.
  - API Gateway permettant de mettre en place un rate-limiting (caper les appels APIs pour protéger le middle-end)
  - Cela s'accompagne de la minimisation de la surface d'attaque des serveurs centraux en procédant à la désactivation de tous les services inutiles.
- Nous avons basé nos développements en utilisant au maximum les mécanismes de sécurité offerts par le framework, notamment Spring Security, qui est un framework d'authentification et de contrôle d'accès puissant et hautement

personnalisable pour les applications Java Il s'agit de la norme de facto pour la sécurisation des applications basées sur Spring. Ceci comprend notamment l'authentification et l'autorisation ; la protection contre les attaques telles que la fixation de session, le "clickjacking", la falsification de demandes de sites croisés, etc.

Évaluation : Acceptable
Commentaire d'évaluation :

- On peut encore renforcer l'architecture en mettant en place une détection d'intrusion ce qui implique une détection d'attaque en continue.

- Une solution telle que Gatewatcher a été évoquée. A noter qu'il n'est pas envisageable que la sonde réseau de détection d'intrusion soit une appliance matérielle car non compatible avec l'hébergement 3DS Outscale. De plus l'hébergement de TousAntiCovid Back-End se situant dans la région SecNumCloud, cela nécessiterait une nouvelle procédure de certification / homologation.

- Une solution de type appliance virtuelle / logicielle sera à privilégier.

Lutte contre les logiciels malveillants

- Utilisation du Captcha d'Orange à l'enregistrement pour limiter les attaques de logiciels malveillants / robots.
- Anti-DDoS Orange Cyberdéfense
    - L'architecture applicative mise en œuvre repose sur l'utilisation d'Internet pour assurer le routage et la transmission des informations. Lors d'une communication entre le téléphone mobile et le serveur, les flux de données sont encapsulés et transmis par paquets en utilisant le protocole IP.

      Il apparait nécessaire de mettre en œuvre des protections contre les attaques les plus communes observées. Ainsi selon le document disponible sur le site de l'ANSSI[11], les attaques par déni de service distribué (Distributed Denial of Service ou DDoS) sont aujourd'hui fréquentes, notamment du fait de la relative simplicité de leur mise en œuvre, et de leur efficacité contre une cible non préparée. Afin d'éviter l'interruption de service et anticiper cette menace, le choix a été fait de mettre en œuvre une solution anti-DDoS, pour se protéger d'attaques DDoS.
    - Le dispositif anti-DDOS mis en œuvre pour protéger le serveur central de TousAntiCovid est composé de 2 phases :
        - en phase de monitoring, la solution anti-DDoS traite des échantillons de paquets IP (1 pour 4000) afin d'identifier la nature d'un trafic malveillant ;
        - en phase de protection, le trafic est dévié et analysé en temps réel, à ce stade il existe des solutions d'analyse par prélèvement d'échantillons dans un fichier contenant 5000 paquets IP.
    - Si un paquet IP contient bien les adresses de destination et d'envoi, cet élément n'est pas l'objet du traitement qui consiste à vérifier l'éventuelle malveillance des paquets IP.
- Nous n'avons pas utilisé de code natif (NDK) ou des bibliothèques natives sur Android
- Dans tous les développements, et la liste est disponible en annexe, nous avons veillé et nous nous sommes assurés que pour toutes les dépendances externes nous étions à jour et utilisions les dernières versions disponibles. Nous nous sommes aussi assurés de choisir des bibliothèques maintenues et respectueuses des présentes recommandations. Nous avons aussi appliqué un principe de frugalité, en réduisant au strict nécessaire, l'utilisation bibliothèques externes, pas de superflu.
- Dans la programmation sur Android, nous avons veillé à supprimer les dépendances au Play Services ainsi que l'usage des bibliothèques Google (Cloud, Firebase, Crashlytics, ...) sur Android
- Dans tous les développements de l'application mobile, nous avons exporté aucun service, aucune activité à l'exclusion de l'activité principale et avons réduit au strict minimum les permissions requises.
- Les possibilités de débogage en mode « release » ont été désactivées et nous avons supprimé tout code mort, obsolète, ou inaccessible.
- Des tests de pénétration ainsi que des audits de code et de configuration doivent être réalisés avant la mise en production.

[11] https://www.ssi.gouv.fr/uploads/2015/03/NP_Guide_DDoS.pdf

Evaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Protection des sites web

- 3DS Outscale et le Sous–traitant en charge de la maintenance et de l'exploitation mettrons en œuvre une stratégie de détection avec des alarmes reposant sur la collecte des journaux d'événements sur l'infrastructure d'hébergement.

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Sauvegarde des données

- 3DS Outscale garantit l'intégrité des snapshots réalisés par le Responsable de traitement et en assure le backup.
- Le Responsable de traitement
  - Réalisera les snapshots de ses volumes s'il souhaite avoir un backup de ses données par 3DS Outscale.
  - Précisera à 3DS Outscale les fréquences et le responsable de l'activation de ces snapshots.
- Une procédure et des dispositifs de sauvegarde et de restauration sont mis en œuvre.

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Maintenance

- **Hébergement du serveur**
  - 3DS Outscale est responsable du Maintien en Condition Opérationnelle (MCO) et Maintien en Condition de Sécurité (MCS) de la plateforme de IaaS en 24/7 ;
  - 3DS Outscale en tant que fournisseur de IaaS fournit des images systèmes au Responsable de traitement afin de pouvoir déployer ses infrastructures. 3DS Outscale est responsable de fournir régulièrement des images à jour de ses systèmes d'exploitation et notifiera le Responsable de traitement à chaque fois qu'une mise à jour sera réalisée avec l'identifiant de la nouvelle image. A partir du moment où un volume est créé à partir de cette image, le Responsable de traitement a la charge du MCO et du MCS du système déployé.
- **Maintenance / exploitation du serveur** : afin de sécuriser les données dans le cadre des opérations de maintenance
  - Insertion d'une clause de sécurité et de confidentialité dans les contrats de maintenance effectuée par des prestataires ;
  - Enregistrement des interventions de maintenance dans une main courante (contenant notamment les dates, la nature des opérations et les noms des Intervenants) ;
  - Installation des dernières versions applicatives à jour ainsi que des patchs de sécurité.
  - Les mesures de sécurité seront définies par le Responsable du traitement avec l'aide de se(s) sous-traitant(s) désigné(s), sur la base des exigences de l'ANSSI et des standards de sécurité qu'ils jugeront applicables en la matière
- **Maintenance de l'application**
  - Correction des failles de sécurité et des bugs autant que de besoin
  - Si une faille de sécurité est découverte, il est possible d'obliger une application à se mettre à jour pour fonctionner
  - Il n'est pas possible de désinstaller l'application mais il est possible de faire passer l'application dans un mode où elle est inactive avec désinscription de l'application et effacement de toutes les données

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Contrat de sous-traitance

- Pendant la phase de développement du projet une convention a été signée entre Inria et 3DS Outscale pour héberger le développement du prototype

- Pour la phase de production :
  - un accord cadre a été signé entre MSS et et Inria
  - un accord de consortium a été signé entre Inria et les partenaires impliqués, dont Outscale

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Sécurisation des canaux informatiques

- Chiffrement (HTTPS, SSL/TLS) de tous les flux échangés entre les applications mobiles et le Back-End TousAntiCovid et entre le Back-End ;
- L'accès au serveur de QR code par les professionnels de santé est sécurisé en protégeant la couche transport (IPsec de préférence) et en authentifiant les accès API entre le serveur de génération de QR codes (pro.tousanticovid.gouv.fr) et les postes clients des professionnels de santé ;
- Les communications entre le serveur *robert-push-notif* et APNs sont chiffrées en utilisant un certificat au format PKCS#12

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Sécurité physique

3DS Outscale met en œuvre des datacenters certifiés ISO 27001 localisés en France et assurant un contrôle d'accès conforme au référentiel de qualification SecNumCloud de l'ANSSI.

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Traçabilité

- L'architecture Back-End TousAntiCovid met en œuvre des solutions d'administration technique et fonctionnelle et des outils de supervision & monitoring permettant d'exploiter le système.
- Mise en œuvre des mécanismes d'audit de l'imputabilité et de la traçabilité des actions menées sur le système :
  - Mise en place d'un serveur de journalisation dédié, configuré en écriture seule ;
  - Accessibilité par une autorité de contrôle.
- Ceci s'accompagne de la mise en œuvre d'une collecte centralisée des journaux d'événements de sécurité sur l'infrastructure d'hébergement serveurs

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Sécurisation des matériels

- L'architecture Back-End TousAntiCovid met en œuvre des solutions d'administration technique et fonctionnelle et des outils de supervision & monitoring permettant d'exploiter le système.
- Les mécanismes de haute-disponibilité (composants redondés, répartition de charge, tolérance aux pannes), l'extensibilité, l'élasticité et les performances des solutions proposées pour le système Back-End TousAntiCovid permettent de se conformer au niveau de qualité de service demandé et de garantir la résilience du système en conformité avec le Plan de Reprise d'Activité et de Plan de Continuité d'Activité (PRA/PCA).
- L'hébergement du système Back-End TousAntiCovid chez le fournisseur de Cloud 3DS Outscale couplé à une automatisation de la création des instances et des environnements (Infrastructure as Code) permet d'offrir une extensibilité et une élasticité du système Back-End TousAntiCovid.

Évaluation : Acceptable
Commentaire d'évaluation :

Pour des raisons de timing, la mise en œuvre de l'orchestration de conteneurs (Kubernetes) n'a pas été retenue. Kubernetes est un système open source qui vise à fournir une « plate-forme permettant d'automatiser le déploiement, la montée en charge et la mise en œuvre de conteneurs d'application sur des clusters de serveurs ». Il fonctionne avec toute une série de technologies de conteneurisation, et est utilisé avec Docker

Eloignement des sources de risques

- Processus d'audit de sécurité (code, architecture, tests d'intrusion) et d'amélioration continue
- Sécurisation du stockage des clés de chiffrement (HSM / Vault en Appliance virtuelle)
- Nous avons, via l'utilisation d'un HSM, restreint l'accès aux éléments cryptographiques au back-office, ainsi que l'accès aux éléments cryptographiques au back-office.

Évaluation : Acceptable
Commentaire d'évaluation :
Evaluations dans le document.

Protection contre les sources de risques non humaines

- Les acteurs systèmes s'interfaçant avec le système Back-End TousAntiCovid sont les suivants :
  - **Service Génération Code**
    - Le service Génération Code (QR Code) est situé dans une zone dédiée hébergée dans Outscale (région SecNumCloud).
    - Codes courts
      - L'accès à l'API de génération de code court par le serveur Pro TousAntiCovid est sécurisé par l'API Gateway ([redacted]) et utilise un Token JWT généré par l'IAM ([redacted]). Le canal d'échange est sécurisé HTTPS, SSL/TLS.
      - Le Back-End TousAntiCovid accède à l'API de vérification de code court par l'API Gateway ([redacted]) et utilise un Token JWT généré par l'IAM ([redacted]). Le canal d'échange est sécurisé HTTPS, SSL/TLS.
    - Codes longs
      - L'échange entre SI-DEP et le service Génération Code est assuré par la mise à disposition quotidienne des codes longs dans un fichier compressé généré par le service Génération Code. Le fichier est déposé dans le répertoire du serveur SFTP.
      - SI-DEP télécharge le fichier [redacted] via un accès VPN.
  - **Site Web Pro StopCovid** (via le service Génération Code) (renommé en Pro TousAntiCovid)
    - Le site Web Pro TousAntiCovid est situé dans une zone dédiée hébergée chez Outscale (région SecNumCloud).
    - L'accès au site Web Pro StopCovid (renommé en Pro TousAntiCovid) par les médecins nécessite une authentification sur Pro Santé Connect ([redacted]). Une mire d'authentification fournie par Pro Santé Connect est affichée au médecin. Lors de la première connexion du médecin au site Web Pro TousAntiCovid avec sa carte CPS ou application eCPS, une demande d'autorisation est formulée au médecin pour que le site Web Pro StopCovid (renommé en Pro TousAntiCovid) puisse accéder aux informations basiques de son profil.
    - Dans le cas où le médecin ne s'est pas authentifié au préalable, il est redirigé vers la mire d'authentification de Pro Santé Connect. Une fois authentifié, le médecin est redirigé vers le site Web Pro StopCovid (renommé en Pro TousAntiCovid) et fournit le token pour vérification (vérification que le token est valide et que le profil de l'utilisateur est bien de profession 'médecin').
  - **Service CAPTCHA**
    - Solution de protection autonome des sites web contre les attaques par bots utilisant une solution proposée par Orange

Évaluation : Acceptable
Plan d'action / mesures correctives :
Commentaire d'évaluation :
Evaluations dans le document.

5.2 Accès illégitime à des données

5.2.1 Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Les impacts diffèrent selon les types de données concernées :

- I_1 : **Informations sur l'état de santé d'une personne** (diagnostiquée positive, à risque) : harcèlement, stigmatisation, discrimination, difficultés relationnelles, refus de continuer à utiliser l'application.
- I_2 : **Informations sur les déplacements des personnes ou sur le motif du déplacement** : sentiment d'atteinte à la vie privée sans préjudice irrémédiable, refus de continuer à utiliser l'application.
- I_3 : **Information sur le graphe de proximité d'une personne** : sentiment d'atteinte à la vie privée sans préjudice irrémédiable, refus de continuer à utiliser l'application, installation de difficultés relationnelles (hypochondrie agiographie).
- I_4 : **Informations sur les données personnels** : sentiment d'atteinte à la vie privée sans préjudice irrémédiable, refus de continuer à utiliser l'application.

5.2.2 Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Les menaces peuvent se décliner par type de support ciblé[1] (téléphone mobile, serveur, communications) :

- M_1 : Utilisation d'informations disponibles sur le téléphone mobile et résultant d'une utilisation conforme du protocole pour avoir des informations sur l'état de santé d'une personne (par exemple, obtention du statut "à risque" après avoir utilisé l'application en présence d'une seule personne). Cette information peut être obtenue fortuitement (personne qui rencontre peu d'autres personnes) ou de manière délibérée (activation de l'application ou de Bluetooth seulement en présence de la personne cible). Ce risque peut difficilement être annihilé puisqu'il peut correspondre à une utilisation normale de l'application (fonctionnalité). Cependant, l'utilisateur devient alors « à risque » et ne peut pas réitérer cette menace.
- M_2 : Utilisation d'informations disponibles sur le serveur pour construire le réseau d'interactions sociales des personnes diagnostiquées positives ou à risque à partir des pseudonymes de leurs contacts (à travers l'analyse des listes de contacts et des estampilles temporelles associées).
- M_3 : Négligence sur le serveur conduisant à une fuite de données ou exploitation de vulnérabilité pour déterminer les pseudonymes correspondant à une même personne et son risque d'exposition.
- M_4 : Observation de communications Bluetooth et recoupement avec des pseudonymes présents sur le serveur (à l'aide d'une collusion avec le gestionnaire du serveur ou via une fuite de données M_3) pour tracer les parcours d'utilisateurs de l'application.
- M_5 : Observation de l'écran de l'utilisateur à son insu pour y lire les information rentrées ou affichées.

[1] Notons cependant que certaines menaces peuvent impliquer plusieurs supports (serveur et communications Bluetooth par exemple).

5.2.3 Quelles sources de risques pourraient-elles en être à l'origine ?

Il faut considérer trois catégories principales de sources de risques :

- S_1 : Les utilisateurs de l'application qui peuvent tenter de détecter si une personne est diagnostiquée positive, rendre le service indisponible, tromper les mécanismes d'authentification, générer de fausses alertes, de faux contacts, etc. Ils peuvent aussi tenter de décompiler l'application et d'en changer le comportement, ou installer une version de l'application différente de celle qui figure sur les plateformes officielles (volontairement ou pas)[1].
- S_2 : Le gestionnaire du serveur qui peut accéder à toutes les données stockées sur celui-ci et potentiellement modifier son code. Il peut vouloir combiner et corréler toutes les informations obtenues (et d'autres informations publiques), par exemple pour obtenir des informations sur le réseau d'interactions sociales.
- S_3 : Les tiers malicieux qui peuvent intercepter ou observer des communications par exemple Bluetooth (éventuellement avec une grande antenne pour couvrir une plus grande zone) ou réseau (ISP, faux AP Wifi ouvert,…), pour déterminer notamment le pseudonyme utilisé par une application ou tenter d'inférer d'autres informations comme l'état d'une personne (à risque, diagnostiquée positive, etc.). Ils peuvent aussi tenter de pénétrer dans un système et d'exploiter ses vulnérabilités pour obtenir des informations, les modifier ou les effacer.
- S_4 : Les tiers malicieux ou curieux qui peuvent lire les informations affichées sur un écran qui n'est pas le leur.

On peut distinguer pour chaque catégorie des sources de risques dotées de moyens plus importants (par exemple, utilisateur profane ou expert, malicieux ou simplement curieux) ou agissant de manière individuelle, en groupe (collusions) ou pour le compte d'un État (doté de prérogatives spécifiques, par exemple pour exiger certains accès dans le cadre d'enquêtes judiciaires). Ces distinctions, qui ont une incidence sur la vraisemblance du risque, sont présentées dans l'Annexe 1. On précise ici pour

chaque menace les moyens dont doit disposer la source de risque pour la réaliser.
S'agissant des menaces identifiées dans la partie 4.2.2, elles peuvent être mises en œuvre par les sources de risques suivantes :

- M_1 : S_1
- M_2 : S_2
- M_3 : S_2, S_3
- M_4 : collusion entre S_2 et S_3 (par exemple, une agence de renseignement déployant des antennes Bluetooth et exigeant l'accès aux données du serveur)
- M_5 : S_4

[1] Le fait qu'un utilisateur modifie son application ou utilise une application qui diffère de la version officielle ne conduit pas à des risques nouveaux par rapport aux menaces de rejeu puisque les seules actions possibles de l'application consistent à envoyer des pseudonymes (déclarations de positivité ou requêtes) : si ces pseudonymes sont réels mais proviennent d'autres applications, la menace est identique à celle d'un rejeu ; s'ils sont fabriqués par l'application, ils ne correspondent à aucune entité existante et ne sont pas reconnus.

5.2.4 Quelles sont les mesures initiales, parmi celles identifiées, qui contribuent à traiter le risque ?

- C_1 : Les pseudonymes utilisés par l'application changent périodiquement afin d'éviter de tracer le propriétaire du téléphone mobile en observant uniquement les messages diffusés en Bluetooth.
- C_2 : Une publication du code en open source et un audit régulier du serveur peuvent permettre de s'assurer de son bon comportement. De plus, un cloisonnement et une segmentation du backend en plusieurs zones avec des rôles différents ainsi qu'une information temporelle restreinte liée aux contacts permet de limiter le croisement d'information. En outre, les personnes diagnostiquées positives pourraient envoyer de manière anonyme les pseudonymes de leurs contacts séparément (un par un) et dans un ordre aléatoire à travers un nœud relais (proxy) pour dissimuler les liens entre ces contacts. La sécurité de ce proxy pourrait également être renforcée par l'usage d'un environnement sécurisé (TEE).
- C_3 : Les informations stockées sur le serveur pourraient être chiffrées avec une clef possédée par l'application. Le choix d'un hébergeur certifié permet de s'assurer d'une réduction des négligences d'exploitation.
- C_4 : Les données sont enregistrées dans des zones chiffrées (Keychain).

5.2.5 Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

En prenant comme référence l'échelle de gravité proposée par la CNIL dans son document « Analyse d'impact relative à la protection des données – Les bases de connaissances », on obtient les niveaux de gravité suivants pour les impacts identifiés dans la partie 4.2.1 :

- I_1 : Informations sur l'état de santé d'une personne : harcèlement, stigmatisation, discrimination, difficultés relationnelles.
  Gravité 3 (importante) : conséquences significatives que les personnes devraient pouvoir surmonter mais avec des difficultés réelles et significatives.
- I_2 : Informations sur les déplacements des personnes : sentiment d'atteinte à la vie privée sans préjudice irrémédiable, refus de continuer à utiliser l'application.
  Gravité 2 (limitée) : désagréments significatifs que les personnes pourront surmonter malgré quelques difficultés.
- I_3 : Information sur le graphe de proximité d'une personne : sentiment d'atteinte à la vie privée sans préjudice irrémédiable, refus de continuer à utiliser l'application
  Gravité 2 (limitée) : désagréments significatifs que les personnes pourront surmonter malgré quelques difficultés.
- I_4 : **Informations sur les données personnels** : sentiment d'atteinte à la vie privée sans préjudice irrémédiable, refus de continuer à utiliser l'application.
  Gravité 2 (limitée) : désagréments significatifs que les personnes pourront surmonter malgré quelques difficultés.

5.2.6 Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

- I_1 : Informations sur l'état de santé d'une personne : harcèlement, stigmatisation, discrimination, difficultés relationnelles.
  Vraisemblance 2 (limitée) : Ce risque est lié à la menace M_1 qui est simple à mettre en œuvre mais qui comporte des inconvénients pour la source de risques (classée « à risque »). Ce risque d'isoler une personne via sa propre application est bornée en temps et donc en surface d'impact.

- I_2 : Informations sur les déplacements des personnes : sentiment d'atteinte à la vie privée sans préjudice irrémédiable, refus de continuer à utiliser l'application.
  Vraisemblance 1 (négligeable) : Ce risque est lié à la menace M_4 qui requiert une collusion entre S_2 et S_3 ainsi que des moyens importants et n'est possible que dans des contextes très spécifiques.
- I_3 : Information sur le graphe de proximité d'une personne : sentiment d'atteinte à la vie privée sans préjudice irrémédiable, refus de continuer à utiliser l'application
  Vraisemblance 1 (négligeable) : Ce risque est lié à la menace M_2 qui est possible uniquement si le code du serveur est modifié afin de stocker et manipuler plus de données, de plus le résultat est incertain et de faible intérêt pour la source de risques.
- I_4 : **Informations sur les données personnels** : sentiment d'atteinte à la vie privée sans préjudice irrémédiable, refus de continuer à utiliser l'application.
  Vraisemblance 1 (négligeable) : Ce risque est lié à la menace M_5 inhérente si on laisse son téléphone à la vue de tous. Les informations personnelles sont aussi disponible sur la version papier des attestations qui est tout aussi "lisible" par-dessus l'épaule qu'un écran de téléphone.

Evaluation : Acceptable
Plan d'action / mesures correctives :
Commentaire d'évaluation :
Evaluations dans le document.

5.3 Modification non désirées de données

5.3.1 Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

- I_4 : **Déclenchement d'une fausse alerte :** Engendrer éventuellement des troubles psychologiques pour une personne ou engendrer des incidences sur ses conditions de vie (personnelle et professionnelle, notamment en réduisant ses déplacement, ses contacts) avec la réception d'une notification de conduite à tenir liée à un risque non effectif.

5.3.2 Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Les principales menaces sont les suivantes

- M_5 : Rejeux des communications Bluetooth d'une personne diagnostiquée positive.
- M_6 : Modification des informations d'une personne donnée suite à une intrusion sur le serveur ou à un abus de droits.
- M_7 : Utilisation du QR code fournit par SI-DEP (communiqué aux utilisateurs diagnostiqués positifs afin qu'ils puissent s'ils le souhaitent envoyer leur historique de proximité au serveur) par une tierce personne et non par la personne réellement diagnostiquée positive.
- M_8 : menaces en lien avec l'application : compromission du code source

5.3.3 Quelles sources de risques pourraient-elles en être à l'origine ?

On considère les mêmes sources de risques que dans la partie précédente (4.2.3).
S'agissant des menaces identifiées dans la partie 4.3.2, elles peuvent être mises en oeuvre par les sources de risques suivantes :

- M_5 : S_1, S_3
- M_6 : S_2, S_3
- M_7 : S_1, S_3

5.3.4 Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

- C_4 : Durée de vie limitée des pseudonymes échangés avec d'autres applications et mécanisme anti-rejeux.
- C_5 : Un QR code ne peut être utilisé qu'une fois et a une durée de vie limitée
- C_6 : mesures pour s'assurer que les applications qui communiquent avec les serveurs en back end sont bien les applications conformes à celle mises en ligne sur les stores

5.3.5 Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

- I_4 : Déclenchement d'une fausse alerte : Rendre anxieux une personne ou engendrer des incidences sur ses conditions de vie (personnelle et professionnelle) avec la réception d'une notification de conduite à tenir liée à un risque non effectif.

Gravité 2 (limitée) : désagréments significatifs que les personnes pourront surmonter malgré quelques difficultés.

5.3.6 Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

- I_4 : Déclenchement d'une fausse alerte : Rendre anxieux une personne ou engendrer des incidences sur ses conditions de vie (personnelle et professionnelle) avec la réception d'une notification de conduite à tenir liée à un risque non effectif.
  Vraisemblance 2 (limitée) : Ce risque est lié aux menaces M_5 et M_6 qui requièrent des moyens importants. La faible durée de vie du QR code rend M_7 également limité.

Evaluation : Acceptable **Plan d'action / mesures correctives :** **Commentaire d'évaluation :** Evaluations dans le document.

5.4 Disparition de données

5.4.1 Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

- I_5 : **Absence de notification de risque** : ne pas prévenir une personne du risque encouru, et perdre par la même l'opportunité éventuelle d'être diagnostiquée le cas échéant de manière anticipée.

5.4.2 Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

- M_8 : Brouillage des communications Bluetooth interdisant à des applications de capturer les pseudonymes diffusés.
- M_9 : Panne matérielle ou logicielle sur le serveur
- M_{10} : Panne réseau rendant le serveur indisponible
- M_{11} : Attaque par déni de service rendant le serveur indisponible
- M_{12} : Modification ou suppression des informations d'une personne donnée suite à une intrusion sur le serveur ou à un abus de droits

5.4.3 Quelles sources de risques pourraient-elles en être à l'origine ?

On considère les mêmes sources de risques que dans la partie précédente (4.2.3).
S'agissant des menaces identifiées dans la partie 4.4.2, elles peuvent être mises en oeuvre par les sources de risques suivantes :

- M_8 : S_1, S_3
- M_9 : S_2
- M_{10} : S_3
- M_{11} : S_3
- M_{12} : S_2, S_3

5.4.4 Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

- C_6 : Redondance des connexions réseau pour traiter le risque de panne réseau rendant le serveur indisponible
- C_7 : Protection anti DDoS pout traiter le risque d'attaque par déni de service du serveur rendant le serveur indisponible
- C_8 : Mise en place d'une architecture haute-disponibilité pour traiter le risque des pannes matérielle rendant le serveur indisponible

5.4.5 Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

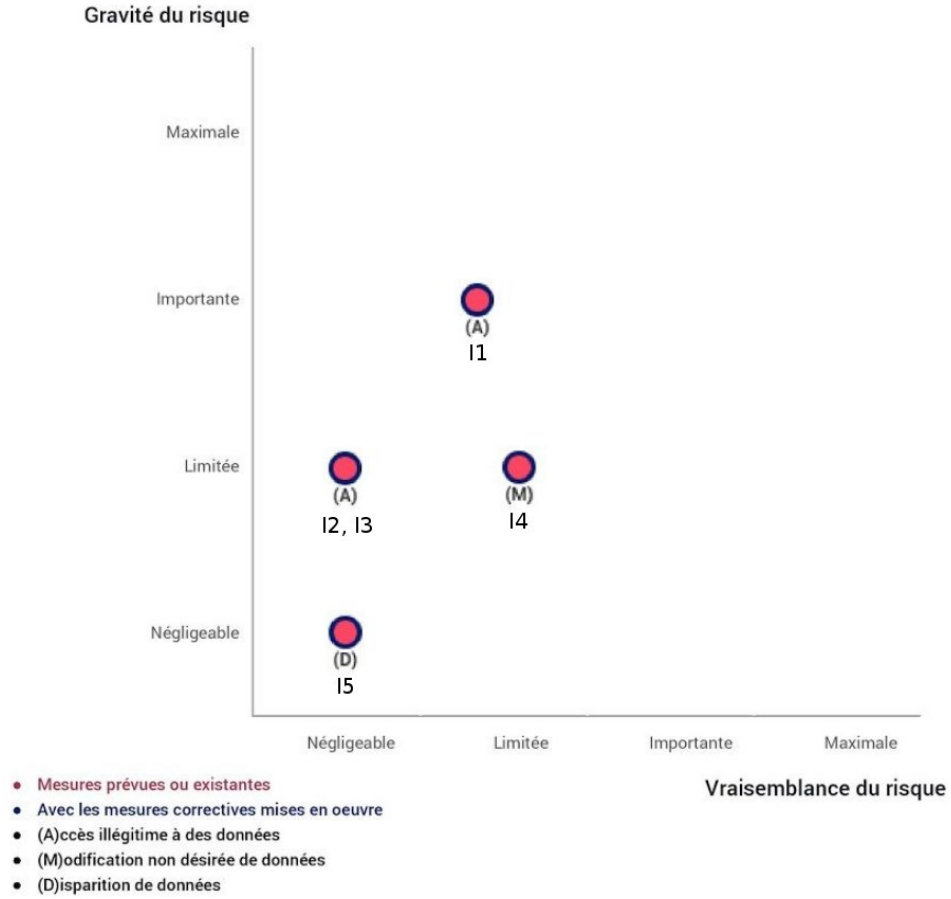
- I_5 : Absence de notification de risque : ne pas prévenir une personne du risque encouru.
  Gravité 2 (limitée) : désagréments significatifs que les personnes pourront surmonter malgré quelques difficultés.

5.4.6 Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

- I_5 : Absence de notification de risque : ne pas prévenir une personne du risque encouru. Vraisemblance 1 (négligeable) : Ce risque est lié aux menaces M_8, M_9, M_{10} et M_{11} qui si-ont traitées par les mesures C_6, C_7 et C_8. M_{12} requière des moyens importants.

5.5 Cartographie des risques

Le graphique suivant montre la cartographie des risques identifiés en section 4.2, 4.3 et 4.4.



Évaluation : Acceptable
Plan d'action / mesures correctives :
Commentaire d'évaluation :
Evaluations dans le document.

6 Annexes

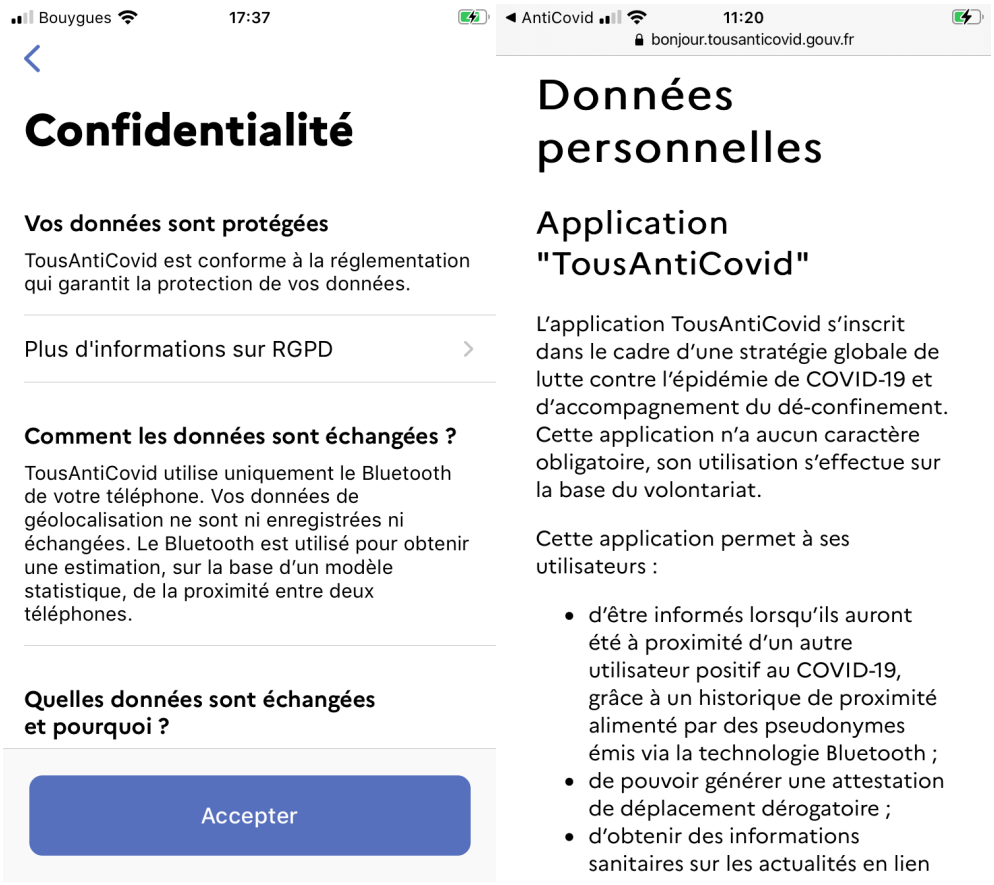
6.1 Information des personnes concernées

6.1.1 Écrans de travail présentant les données échangées et la politique de confidentialité.

NB : Ces écrans de travail sont donnés à titre indicatif car ils sont amenés à évoluer

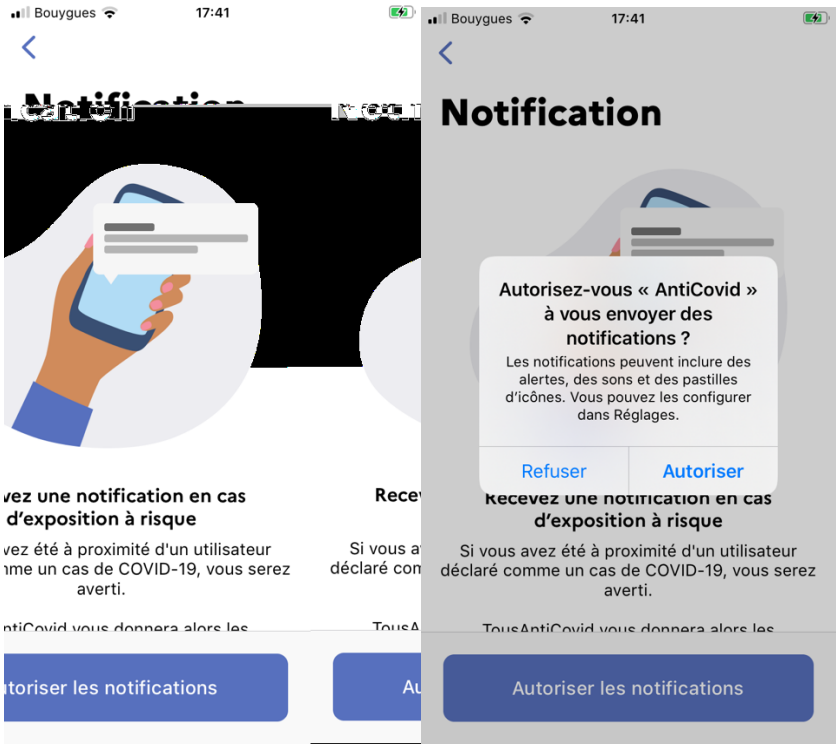
Écrans de travail d'installation de l'application TousAntiCovid

Écrans de travail présentant les données échangées et leur confidentialité / protection



Ecran de travail présentant et demandant l'autorisation de construire un historique de proximité

Ecrans de travail présentant et demandant l'autorisation de s'informer de son risque et de recevoir des notifications de l'application

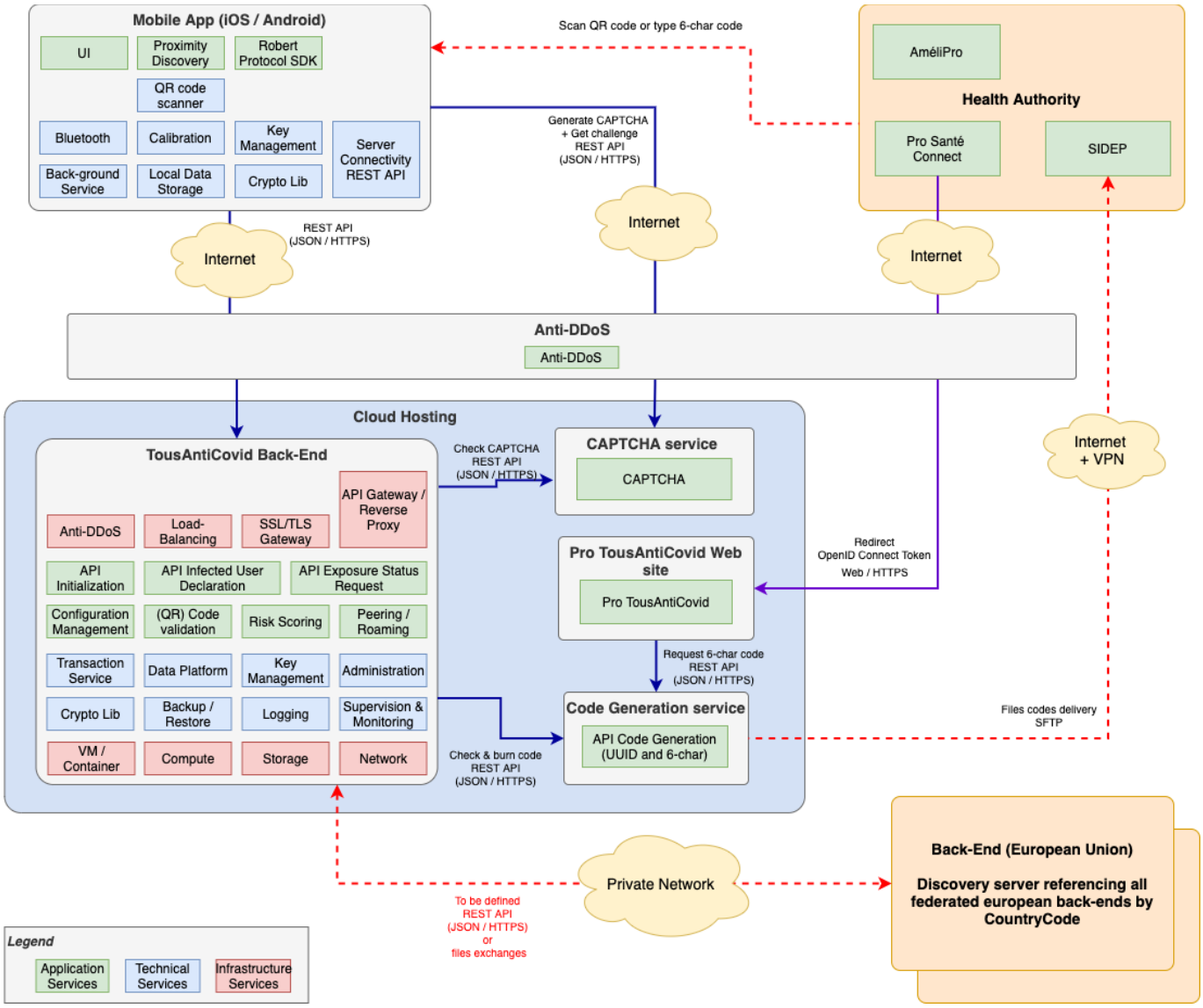


Écran de travail informant l'utilisateur qu'il a désactivé l'application

Ecran de travail permettant de gérer ses données : effacement des attestations, effacement local de l'historique de proximité, effacement local de la notification reçue, effacement de ses données sur le serveur et désinscription sur le serveur

6.2 Architecture

Le schéma ci-dessous donne une vision globale de l'architecture mise en place.



[redacted].

6.3 Flux de données

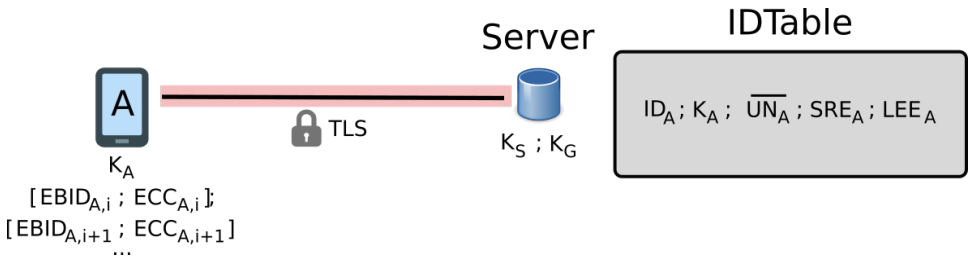
Ce tableau liste les termes utilisés dans les figures de cette sous-section.

Acronyme	Description
ID_A	Pseudonyme permanent associé à l'utilisateur A.
K_A	Clef partagée entre le serveur et l'application de l'utilisateur A.
EBID	Pseudonyme temporaire diffusé en Bluetooth.
$EBID_{A,i}$	Pseudonyme temporaire diffusé en Bluetooth par l'utilisateur A à la période i.
ECC	Code de pays chiffré.
LEE	Liste des périodes où l'utilisateur A est indiqué comme exposé sur le serveur.

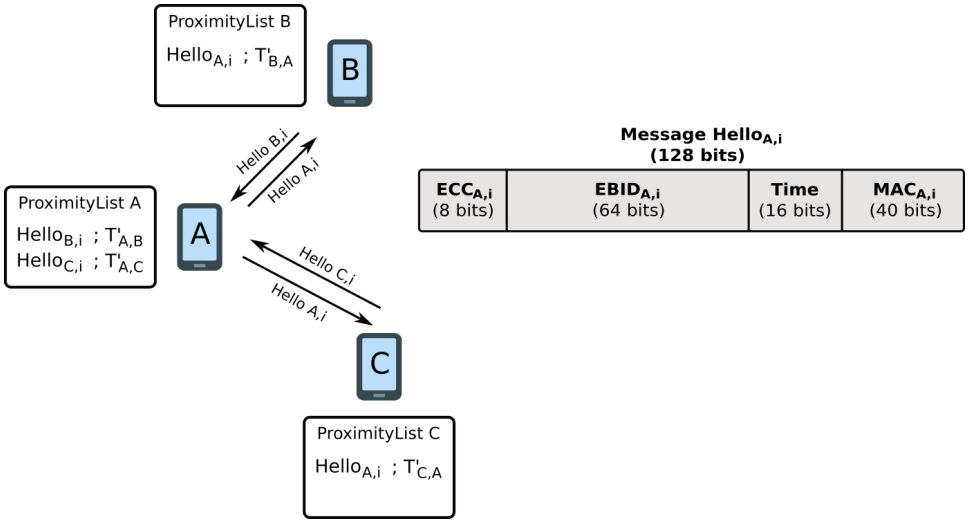
UN_A	Variable binaire stockée sur le serveur indiquant si l'utilisateur A a déjà été notifié d'un risque d'exposition.
SRE_A	Variable stockée sur le serveur indiquant quand l'utilisateur A a envoyé la dernière requête pour connaître son statut "à risque" au serveur.

Les schémas ci-dessous résument les grandes phases du cycle de vie au sein de l'application.

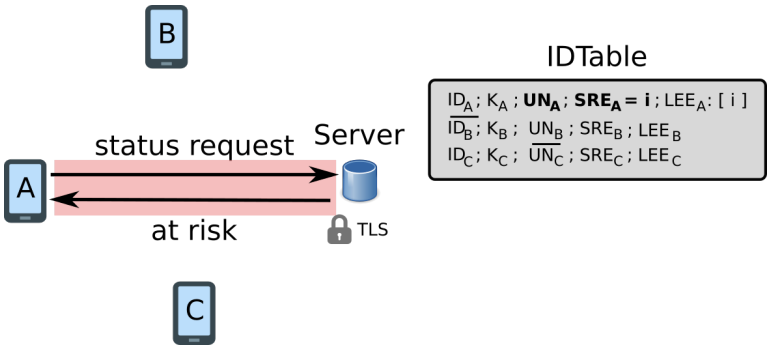
1°) L'initialisation de l'application.



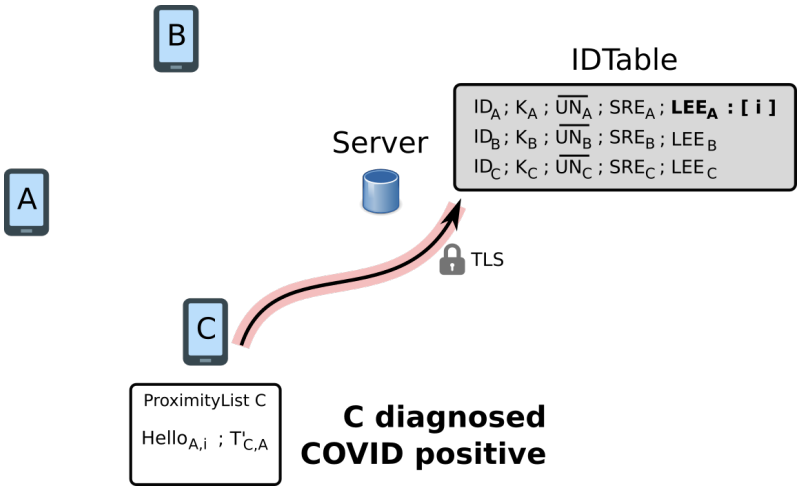
2°) La diffusion de ses pseudonymes, la réception des pseudonymes des autres téléphones à proximité et la construction d'historique de proximité.



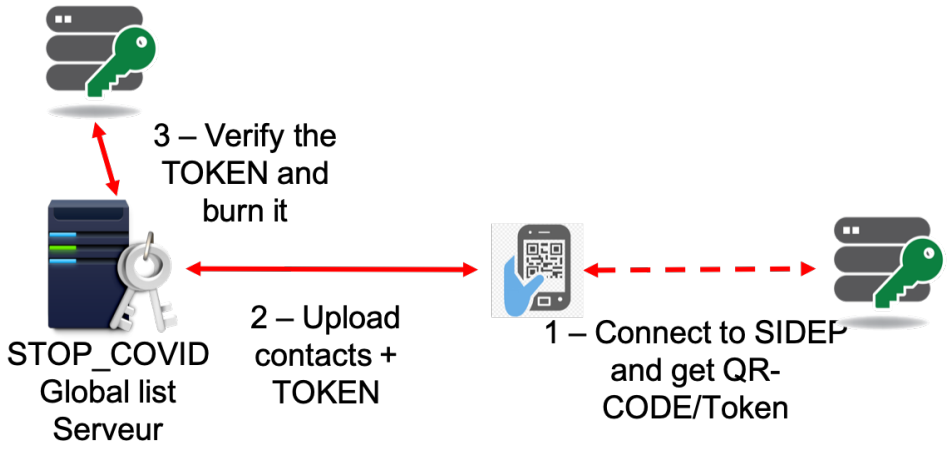
3°) L'application demande périodiquement son statut "à risque" au serveur Ce dernier est une valeur binaire.



4°) La remontée d'un historique de proximité quand un utilisateur est testé positif COVOD-19 et donne son consentement pour sauvegarder son historique de proximité sur le serveur.



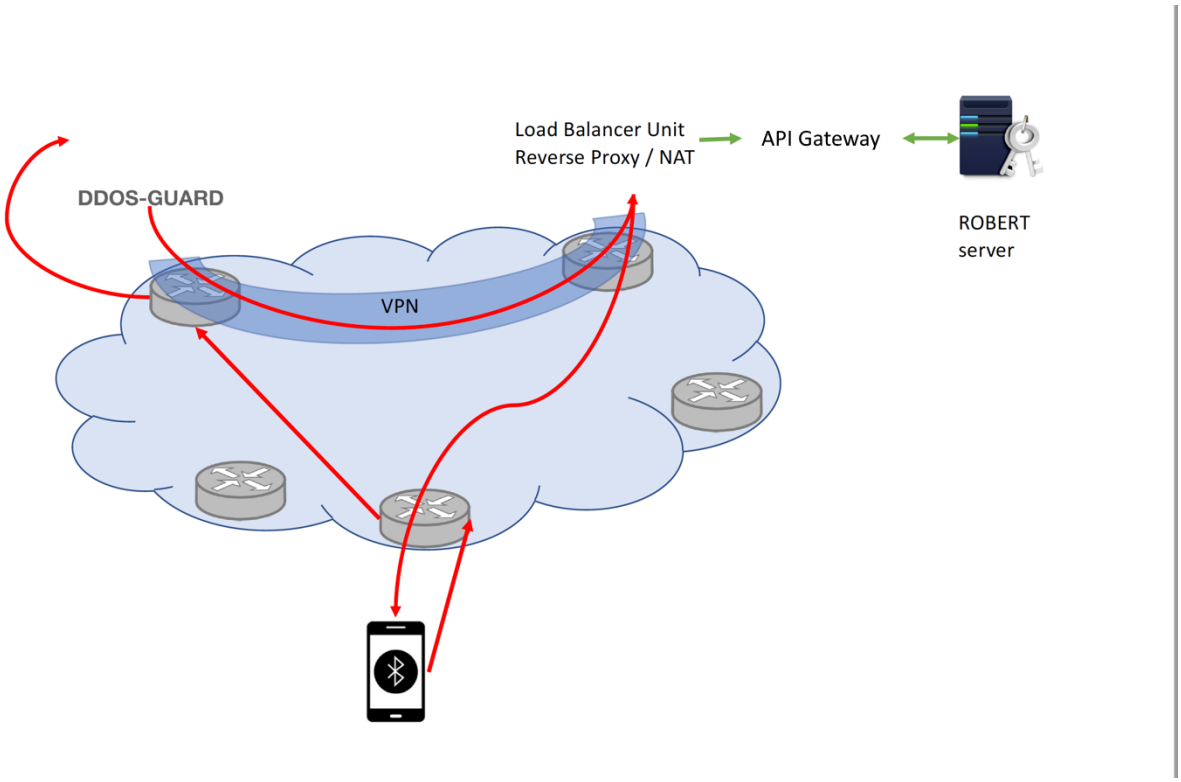
Le schéma ci-dessous donne un aperçu des flux en intégrant le token aléatoire à usage unique.



Ces différents flux sont résumés dans la matrice de flux ci-dessous :

Schéma effacé

La figure ci-dessus détaille la vue logique du parcours d'une requête depuis le téléphone mobile vers le serveur central.



6.4 Mécanismes de cryptographie

1/ **Initialisation du serveur :**
- Il a une clé K_S

2/ **Lors de l'inscription d'une application A** sur le serveur central sont générées
- Un identifiant connu du seul serveur (40 bits) : ID_A
- Une clé partagée connue du serveur et de l'application (128 bits) : K_A

3/ Tous les 4 jours (c'est paramétrable), **l'application récupère sa liste d'identifiants Bluetooth éphémères** (Ephemeral Bluetooh IDentifier = EBID, 64 bits) :
- EBID_A (à indicer par le temps, toutes les 15 s).
- EBID_A = F(K_S, ID_A)

NB : EBID_A est calculé à partir de la clé du serveur K_S et de ID_A à l'aide d'une fonction encryptée, Skinny 64/192 (initialement 3DES). Au pire, si c'est cracké, quelqu'un qui récupère ID_A à partir de l'observation de EBID_A n'en fera rien, à moins de cracker le serveur et de connaître K_S).

4/ **Lors d'un échange entre deux smartphones A et B** est récupéré par B un message Hello_A qui est constitué :
- D'un code pays (8 bits)
- Du temps (16 bits)
- EBID_A (64 bits)
- MAC_A : un code d'authentification du message (40 bits) qui va permettre de vérifier l'intégrité du message reçu par B (voir infra, sur le serveur).

MAC_A = G (EBID_A, K_A) est calculé à partir d'une fonction de hachage SHA256.

5/ **Lorsque Hello_A est remonté sur le serveur**, celui-ci :
- Récupère EBID_A et MAC_A
- A partir de EBID_A, il récupère ID_A grâce à sa clé K_S (voir 3/).
- Il vérifie qu'ID_A existe (que ce n'est pas une fausse application)
- Connaissant ID_A, il peut alors récupérer K_A, la clé partagée entre le serveur et l'application A
- Il vérifie alors que MAC_A est bien valide (intégrité du message, voir 4/).

6/ **La protection des clés (K_S, K_A) est donc majeure** et c'est toute la faiblesse potentielle d'un système « centralisé » s'il y a détournement de la mission (mission creep) par le détenteur du serveur ou s'il est hacké.

Une rotation des clefs K_S est ainsi mise en place afin de renforcer la sécurité. Quand bien même la clefs K_S est volée, elle est changée périodiquement : on ne peut donc pas l'utiliser très longtemps (elle devient caduque), empêchant une surveillance de masse, à grande échelle et en temps long.

Par ailleurs, **on met également en place un coffre-fort (HSM : Hardware Security Module**), qui est implémenté sous forme logicielle (Software HSM). En pratique, trois organisations (Inria, Inserm, Académie des Technologies) se sont partagés une partie de la serrure chiffrée du coffre-fort dans lequel sont mises les clés (K_S, K_A) à travers une « cérémonie des clés » pour éviter tout dévoiement éventuel de la finalité (qui a eu lieu le 30 mai 2020 dans le cadre d'un protocole impliquant l'ANSSI comme témoin).

6.5 Développement

A partir du 22 octobre 2020, nous prévoyons de faire des release mineurs et des améliorations de présentation toutes les 2 ou 3 semaines.

6.6 Paramètres et mise en oeuvre du protocole

Les paramètres retenus dans la mise en œuvre de l'implémentation du protocole ROBERT sont :

- Fréquence de changement des pseudonymes : toutes les 15 minutes
- Durée de vie de l'historique des proximités contenant les pseudonymes : 15 jours

Par rapport à la description scientifique du protocole ROBERT des choix de mise en œuvre ont été effectués :

- Remontée en une seule fois de l'historique de proximité. Afin de prévenir tout risque de création de lien à des vues de reconstruction de graphe des pseudo identifiants par le serveur, un serveur de proxy a été mis en place. Remonter les pseudonymes un par un implique d'avoir un token valide pour chaque pseudo identifiant remonté, une application peut alors "mentir" sur son nombre et acquérir le droit de faire remonter les futurs identifiants qu'elle va mémoriser, ou "donner" ce token à une autre application invalidant le fait que pour un test positif il n'y a qu'une seule déclaration au sein de TousAntiCovid.
- Une application qui reçoit une indication positive suite à une demande de statut, continue à faire des demandes de statut les jours suivants. Les pseudonymes qui ont été pris en compte dans le calcul de la première réponse ne sont plus pris en compte dans les réponses potentielles ultérieurs. Cela n'a pas d'impact direct sur la privacy, un utilisateur pouvant dans tous les cas, désinstaller et réinstaller son application.
- Quand un utilisateur souhaite faire remonter son historique de proximité, l'application lui demande sa DDS (Date de Début de Symptômes) afin de préciser la fenêtre temporelle à employer pour faire remonter les contacts. SPF conseille de prendre 2 jours avant la DDS.
- Remplacement de 3DES par Skinny-cipher 64.
- Pour avoir des KPI objectives sur l'application, il est souhaité pouvoir :
    - Faire remonter le nombre de jours entre la date du test et la DDS et la date de la dernière notification.
- Pour mieux informer l'utilisateur, il serait souhaitable d'avoir la date du dernier contact en cas de réponse positive à une demande de statut. Ceci permet d'ajuster en conséquence la durée de la période d'affichage des CAT (Conduite à tenir) et la période durant laquelle il est recommandé à l'utilisateur d'effectuer un test. (cf le rattachement au parcours de santé du sujet contact dans la section 3.1.1)

6.7 Principe général de publication

Pour permettre aux différentes communautés de développeurs et de spécialistes d'expertiser les algorithmes implémentés et la façon dont cette application est programmée, en particulier si elle met en œuvre correctement le protocole ROBERT, Le code source est publié sur https://gitlab.inria.fr/stopcovid19

Le code source présenté est le résultat d'un processus de développement collaboratif impliquant de nombreuses personnes et

organisations. Il permet de proposer des évolutions à l'application, de signaler des bugs, de proposer des changements pour la documentation et de suivre la prise en compte ou non de ces propositions. C'est aussi l'objet de ce projet Gitlab.

Les contributions attendues par la communauté des développeurs permettront de faire évoluer l'ensemble des briques logicielles afin d'améliorer la qualité de l'application. Pour contribuer, il est demandé de prendre connaissance du fichier contributing.md disponible sur le projet Gitlab dédié. La plateforme Gitlab n'a pas vocation à héberger les débats d'ordre plus général, politique ou sociétal.

La politique de publication dans le cadre du projet repose sur trois catégories :

- Une partie (restreinte) qui n'est pas publiée car correspondant ou à des tests ou à des parties critiques pour la sécurité sur les paramétrages du serveur (la documentation donnera alors les grands principes) ;
- Une partie qui est rendue publique sans qu'un appel à contribution ne soit attendu (les propositions seront bien entendu étudiées) : cela correspond par exemple à des parties qui implémentent directement des spécifications très précises ;
- Une partie qui relève à strictement parler de l'open source, avec des appels à contribution qui sont attendus : cela concerne le cœur de l'application, notamment l'implémentation du protocole ROBERT.

L'équipe-projet TousAntiCovid a décidé de publier le code en deux phases. Ce phasage ne remet pas en question les principes fondamentaux de publication ouverte du code mais permet une meilleure gestion de la montée en charge pour une mise à disposition éventuelle d'une application opérationnelle fin mai/début juin.

Phase 1 : transparence
Une première partie des briques logicielles est publiée le 12 mai. Désormais visible, le code peut être revu par tous ceux qui le souhaitent. En le rendant public, l'équipe-projet TousAntiCovid respecte son engagement de transparence.
Les personnes externes à l'équipe-projet TousAntiCovid peuvent, à ce stade, donner un avis, faire remonter des suggestions ou des commentaires. Selon la pertinence technique de ces premiers retours, elles seront invitées à rejoindre le pool de contributeurs du projet pour gagner en efficacité. La durée de cette phase 1 sera dépendante des contraintes liées aux phases de tests et au calendrier de mise en disponibilité de l'application

Phase 2 : contribution
La partie logicielle qui implémente le protocole ROBERT sera mise en Open Source. La phase de contribution permettra à la communauté de contribuer au logiciel tout en respectant les mécanismes de régulation qui seront mis en place (essentiellement via de la revue de code et une acceptation ou un rejet par un comité de validation).