AIPD du module Signal de TousAntiCovid

Version mise à jour le 3 septembre 2021

1 Contexte

1.1 Vue d'ensemble

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

L'AIPD porte sur le **module Signal** (nom d'origine TAC-W) de l'application TousAntiCovid.

Ce module offre aux utilisateurs fréquentant un lieu la possibilité d'enregistrer ce lieu dans leur historique de lieux fréquentés. Si par la suite un utilisateur se déclare ensuite dépisté ou diagnostiqué positif à la Covid-19, les utilisateurs ayant fréquenté le même lieu et dans la même plage horaire recevront une notification comme contact à risque de contamination avec les recommandations sanitaires.

Ce module permet ainsi de maximiser les chances de rompre les chaînes de transmission de la Covid-19.
Il est intégré dans l'application TousAntiCovid, mais il est indépendant des autres fonctionnalités de cette application car il repose sur un protocole spécifique, nous avons donc décidé de rédiger la présente **AIPD dédiée à ce module mais reliée à l'AIPD de TousAntiCovid**.

Pour rappel

- La responsabilité du développement de l'application TousAntiCovid 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.
- Le projet TousAntiCovid rassemble des acteurs publics (Inria, ANSSI, Inserm, Santé Publique France) et privés (Dassault Systèmes, Capgemini, Lunabee Studio, Orange, Withings) ainsi qu'un écosystème de contributeurs.
- 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 jouera 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 en date du 24 avril 2020 le traitement est 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.
- L'application TousAntiCovid est installée librement et gratuitement par un utilisateur

Les principaux enjeux du module Signal 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**

- de collecter de manière centralisée des données personnelles des personnes qui fréquentent un lieu ;
- de déduire des données de localisation ou de co-localisation des personnes qui fréquentent un lieu (notifiées positives ou non) ;
- de collecter sur le lieu du restaurant des données personnelles des clients du restaurant ;
- d'inférer à partir du trafic réseau qu'un utilisateur spécifique a reçu un test ou une notification ;

Les finalités du traitement sont

- informer les utilisateurs qu'ils ont fréquenté, à une date donnée et au cours d'une période donnée, un lieu où se trouvait, pendant tout ou partie de la même plage horaire, une personne diagnostiquée ou dépistée positive à la Covid-19 ;
- permettre l'identification des clusters potentiels dans les lieux.

Il appartient à l'utilisateur d'activer ou non le module Signal.

Le périmètre de cette AIPD concerne le module Signal de l'application mobile, la partie serveur, ainsi que les moyens de communication. Le module Signal est une mise en œuvre du protocole : « The Cluster Exposure Verification (Cléa) Protocol »[1].

1.1.2 Fonctionnement global du traitement

Le responsable du lieu affiche ou met à disposition un QR code aux personnes fréquentant le lieux. Ce QR code doit être spécifique à chaque lieu. Ce QR code peut être soit présenté de façon dite statique (imprimé sur une affiche) soit au travers d'un dispositif matériel qui le régénère périodiquement et automatiquement. Dans le cas statique, il est recommandé que le responsable du lieu génère et change le QR régulièrement (tous les jours et si possible entre les rassemblements ou les

[1] https://hal.inria.fr/hal-03146022 et https://github.com/TousAntiCovid/CLEA-exposure-verification/tree/master/documents

services).

Le visiteur est équipé du module Signal ou l'installe quand il arrive dans le lieu. Il scanne alors le QR code affiché ou mis à disposition par le responsable du lieu.

Si le visiteur se déclare par la suite positif dans l'application TousAntiCovid, et après son accord, son historique de proximité et son historique des lieux fréquentés durant les 14 derniers jours sont remontés au serveur central.

Les visiteurs présents dans ce lieu dans la même date et plage horaire et utilisant le module Signal au sein de TousAntiCovid sont notifiés qu'ils sont contacts à risque de contamination modéré (ou élevé en cas de cluster) avec une approximation de la date de l'exposition à risque.

1.1.3 Quelles sont les responsabilités liées au traitement ?

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 Business Service (OBS) : maintenance et exploitation de l'infrastructure ;
  - Lunabee : développement de l'application TouAntiCovid ;
  - 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 : Foire aux questions[2] (FAQ) de l'application TousAntiCovid ;
  - Reputation squad[3] : Développement du site web de génération des QR codes de lieu[4] affichés à l'entrée ou dans les lieux;
  - Scaleway : Mise à disposition d'un bucket pour les QR Codes de lieux
- **Destinataires**
  - Les utilisateurs du module Signal qui seront notifiés qu'ils ont été présents dans un lieu sur une plage horaire pendant laquelle ils auraient pu être contaminées par une ou plusieurs personnes ultérieurement diagnostiquées ou dépistées positives à la Covid-19 ;
  - Inria en tant que sous-traitant auprès de la DGS du MSS.

1.1.4 Quelles sont les personnes concernées

Les personnes concernées sont les utilisateurs de l'application TousAntiCovid installée avec le module Signal activé et présents sur les lieux.

Les mineurs sont inclus dans le dispositif.

1.1.5 Quels sont les référentiels applicables ?

- Référentiel Général de Sécurité (RGS)
  - Une homologation au RGS de TousAntiCovid a été instruite et a été prononcée par la DGS du MSS préalablement à sa mise en production
- PSSI de l'Etat PSSI-E
- Référentiel SecNumCloud de l'ANSSI pour la partie infra

1.2 Données, processus et supports

1.2.1 Quelles sont les données traitées ?

Aucune donnée personnelle n'est collectée par le module Signal.

Le serveur central Signal est séparé du serveur central ROBERT utilisé par l'application TousAntiCovid. Le module Signal est porté par la même application mais n'en partage pas les données. L'application TousAntiCovid ne s'enregistre pas auprès du serveur Signal.

[2] https://tousanticovid.stonly.com
3 https://www.reputationsquad.com
[4] https://qrcode.tousanticovid.gouv.fr

Données traitées pour l'assistance concernant le module de contact warning

La société IMA[5] est en charge de l'assistance

- Aux utilisateurs du module de Contact warning ;
- Aux responsables des lieux utilisant les QR codes dynamiques.

Les données traitées par IMA sont hébergées sur le territoire français

- les dossiers ouverts lors de la prise en charge des appels sont hébergées et répliquées dans les différents Data-Centre d'IMA sur Niort avec une réplication sécurisée complémentaire chez DARVA à Chauray (à côté de Niort).
- Les dispositifs pris en charge par la plateforme médico-sociale et le service médical d'IMA sont hébergés chez Claranet (certifié HdS) dont le siège est à Londres et les Data-Centres sont basés en France.

Des clauses RGPD ont été signées entre Inria et IMA.

Données traitées dans l'application

- L'historique des lieux fréquentés qui est composé des informations ci-dessous encodées dans un QR code dont la spécification est décrite dans https://hal.inria.fr/hal-03146022v2
    - Une url (deeplink). Pour la France https://tac.gouv.fr?v=0#
    - La partie spécifique au lieu encodée en base64 qui contient ;
        - Version : la version du protocole
        - Type : le type de format supporté
        - LTId : l'UUID sur 128 bits du lieu
        - Une partie encrypté non lisible par l'application.
- Les plages horaires de fréquentation afférentes aux QR codes, ajoutées par le module Signal ;

Données traitées sur le serveur Central

- Liste des lieux exposés, ce qui inclut les données listées ci-dessus pour chaque lieu. Le serveur est en mesure de décrypter la partie cryptée et ainsi avoir en sa possession notamment :
    - Si le QR code est pour le personnel du lieu ou pour les clients
    - Le type de lieu (par exemple restaurant, salle de sport,…)
    - La première catégorie du lieu (restaurant rapide, cafétéria,…)
    - La seconde catégorie du lieu (surface ou jauge suivant le type)
- Plages horaires des lieux exposés

5 https://www.ima.eu

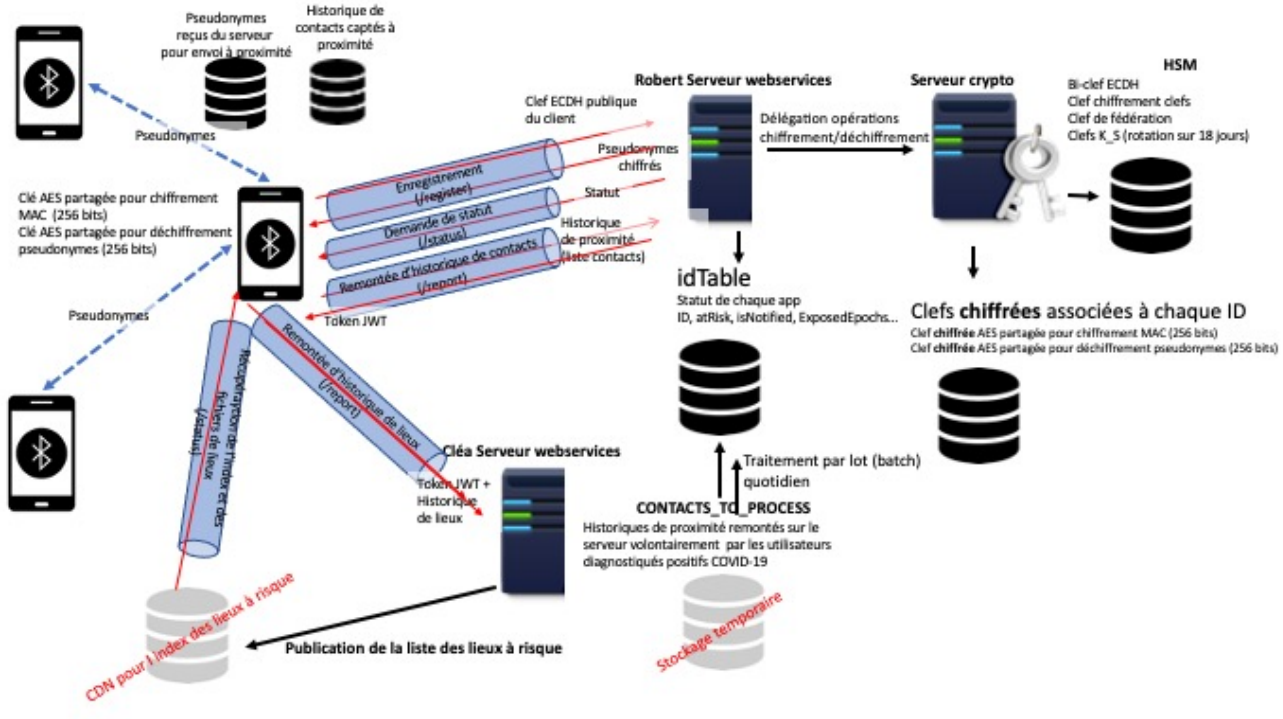


Figure 1 – Schéma des flux de données

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

- **Génération des QR codes du lieu**
  Le responsable du lieu imprime un **QR code** qu'il peut obtenir à partir du site de génération des QR codes[6] puis il l'affiche ou la met à disposition dans ce lieu.
- **Collecte par le module Signal des QR codes des lieux fréquentés**
  - La personne qui fréquente un lieu est invitée à utiliser le module Signal et scanne le QR code lorsqu'elle rentre dans ce lieu ;
- **Action périodique par le module Signal**
  - Le module Signal récupère régulièrement un fichier index qui liste les lieux à risque, leur plage horaire et le niveau de risque afférant. Le module Signal vérifie en local si les lieux qu'il a dans son historique de lieux sont concernés et si oui, le module Signal émet une notification à l'utilisateur.
- **Si un utilisateur se déclare positif à la Covid-19 dans l'application TousAntiCovid**
  - Il reçoit un QR code de SI-DEP qu'il scanne ou un code court donné par un personnel de santé et obtenu auprès de https://pro.tousanticovid.gouv.fr qu'il saisit dans TousAntiCovid ;
  - TousAntiCovid remonte au serveur ROBERT l'historique de proximité et obtient en retour un token;
  - Le module Signal remonte au serveur Signal l'historique des pseudonymes des lieux fréquentés durant les 14 derniers jours et le token précédent qui n'est valable que x minutes.
- **Vérification par le serveur Signal des QR codes de lieux fréquentés**
  - Le serveur Signal tient à jour la liste des pseudonymes des lieux exposés et de leur plage horaire et publie régulièrement un index de ces lieux.

1.2.3 Quels sont les supports des données ?

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

- **Activation du module Signal :** téléphone mobile, serveur, Internet ;
- **Envoi des données au serveur** : téléphone mobile, serveur, Internet
- **Assistance téléphonique pour Signal** : téléphone mobile

[6] https://qrcode.tousanticovid.gouv.fr

2 Principes fondamentaux

2.1 Remarques liminaires

L'utilisation du module Signal repose sur le volontariat, il peut être activé ou désactivé à tout moment par l'utilisateur.

Il n'existe aucun lien entre les données gérées par le module de Contact Tracing de TousAntiCovid et le module Signal. Les services sont totalement indépendants car les flux logiques et les serveurs respectifs sont séparés. En particulier, il n'existe aucun lien entre l'identifiant coté TousAntiCovid et la partie Signal.

Le seul lien fonctionnel indirect entre TousAnticovid et son module Signal apparait lors de la requête « report », lorsqu'un utilisateur décide de se déclarer positif dans l'application et le cas échéant de faire remonter la liste de ses contacts et la liste des lieux fréquentés.

Dans l'application TousAntiCovid, cette remontée est « permise » via un QR-Code donné par SI-DEP (ou un code court donné par https://pro.tousanticovid.gouv.fr) et attestant d'un test positif.

Pour ne pas mélanger les deux services de TousAntiCovid et son module Signal, dans la réponse à une remontée de contacts un jeton JWT (JSON Web Token) est donné afin de permettre au module Signal de remonter les lieux fréquentés vers un autre serveur nommé Signal :

- Aucun lien ni communication n'a lieu entre le serveur ROBERT et le serveur Signal.
- JWT est un standard ouvert défini dans la RFC 75191. Il permet l'échange sécurisé de jetons entre plusieurs parties.

Cette sécurité de l'échange se traduit par la vérification de l'intégrité des données à l'aide d'une signature numérique. Pour résumer, le jeton JWT est juste une preuve donnée à l'application qu'elle a bien fait remonter un QR code valide et que ce jeton peut être transmis à Signal.

2.2 Proportionnalité et nécessité

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

Les données sont générées et collectées pour **fournir le service**, à savoir **alerter les personnes ayant fréquenté les lieux sur une plage horaire similaire à celle d'une ou de plusieurs personnes ultérieurement dépistées ou diagnostiquées positives à la Covid-19**.

Les ERP ciblés par ce dispositif sont définis sur les recommandations de Santé Publique France et visent à intégrer les ERP dans lesquels le port du masque n'est pas possible et les autres mesures barrières difficiles à mettre en œuvre (risque élevé), ainsi que les ERP dans lesquels il existe un protocole sanitaire comprenant l'ensemble des mesure barrières mais dans lesquels une rupture est possible (risque modéré). Le niveau de risque définira le type de notification que l'utilisateur recevra ainsi que la conduite à tenir.

Selon les recommandations de Santé publique France les ERP classés sont les suivants :

- Restaurant
- Restaurant rapide
- Restauration d'un lieu culturel, salle des fêtes, village vacances etc.
- Débit de boisson
- Salle de sports

2.2.2 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.

2.2.3 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 plages

horaires et les informations contenues dans les QR codes des lieux fréquentés par les utilisateurs qui se sont déclarés positifs à la Covid-19 dans l'application.

Les informations contenues dans les QR codes de lieu ne contiennent aucune information de lieu (GPS), de nom ou d'adresse, seule potentiellement la date peuvent être adressées à l'utilisateur concerné dans le cadre de ce dispositif.

Le nom d'un utilisateur fréquentant un lieu n'est jamais remonté au serveur central, ni stocké par ce dernier.

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

Il n'est pas possible de vérifer que le QR code d'un lieu corresponde à ce lieu car :

- Sur le site web de génération des QR code de lieu, le responsable du lieu renseigne le type de l'établissement, sa surface ou sa capacité mais il n'authentifie pas le lieu
- Il est possible à n'importe qui de générer un QR code à l'aide d'outils présents sur Internet.

2.2.5 Quelle est la durée de conservation des données ?

Les données sont conservées

- Dans le module Signal jusqu'à suppression par l'utilisateur à tout moment un ou des lieux fréquentés dans son historique et de façon automatique au bout de 15 jours.
- Sur le serveur central pendant 15 jours à partir de leur enregistrement par le module Signal

2.3 Mesures protectrices des droits

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

Un affichage des mentions d'information à destination des personnes concernées sera réalisé dans

- tous les lieux concernés ;
- les communiqués de presse ;
- les supports de communication (dont les sites web) de la DGS du MSS ;
- les informations dans l'application TousAntiCovid (section à propos, brève, section dédiée) ;
- la présente AIPD.

Les personnes concernées sont informées

- qu'en cas de partage de leur historique de proximité ou de lieux fréquentés sur le serveur central, les personnes identifiées comme leurs contacts à risque de contamination seront informées qu'elles auront, à une date donnée et au cours d'une période donnée, été à proximité d'au moins un autre utilisateur diagnostiqué ou dépisté positif au virus de la Covid-19, ou fréquenté un même lieu au même moment qu'au moins un utilisateur diagnostiqué ou dépisté positif au virus de la Covid-19
- de la possibilité limitée d'identification indirecte susceptible d'en résulter lorsque ces personnes ont, à cette date et au cours de cette période, eu un très faible nombre de contacts ou fréquenté des lieux où se trouvaient un faible nombre de personnes

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

Les personnes concernées donnent leur consentement à utiliser le module Signal à la première ouverture du module dans l'application TousAntiCovid.

Elles peuvent retirer leur consentement à tout moment en désactivant ce module.

2.3.3 Comment les personnes concernées peuvent-elles exercer leurs droit d'accès et droit 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. De plus, by-design, il n'est pas possible de retrouver le ou les lieux fréquentés par un utilisateur donc il n'est pas possible de répondre aux demandes d'exercice de droit d'accès. Enfin, le décret relatif à ce traitement écarte le droit d'accès.

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

2.3.4 Comment les personnes concernées peuvent-elles exercer leurs droit de rectification et droit 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 au 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 : depuis le menu Paramètres de l'application TousAntiCovid, elle a la possibilité de supprimer un ou tous les lieux visités.

Par contre elle ne peut pas supprimer ses données sur le serveur, celles-ci seront effacées automatiquement au bout de 15 jours.

2.3.5 Comment les personnes concernées peuvent-elles exercer leurs droit de limitation et droit 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 au Covid-19. Le décret relatif à ce traitement écarte le droit à la limitation.

Concernant les QR codes des lieux collectés sur son téléphone, la personne concernée peut à tout moment arrêter d'utiliser le module Signal donc exercer son droit de d'opposition.

Dans le cas où la personne concernée a envoyé au serveur les QR codes des lieux fréquentés, 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.

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

- **Inria**
  - un accord cadre a été signé entre MSS et et Inria
- **3DS OutScale : hébergement**
  - un accord de consortium a été signé entre Inria et les partenaires impliqués, dont 3DS Outscale
- **Lunabee**
  - un accord de consortium a été signé entre Inria et les partenaires impliqués, dont Lunabee
- **Orange : maintenance et exploitation**
  - un accord de consortium a été signé entre Inria et les partenaires impliqués, dont Orange
- **IMA**
  - Un cahier des clauses particulières (CCPP) et des clauses RGPD ont été signés entre Inria et IMA

2.3.7 En cas de transfert de données vers des pays tiers, les données sont-elles protégées de manière équivalente ?

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

3 Risques

3.1 Mesures existantes ou prévues

Les mesures existantes ou prévues pour Signal sont les même que pour TousAntiCovid, elles sont décrites dans l'AIPD de TousAntiCovid.

3.2 Analyse de risque

Cette analyse porte sur l'utilisation par les responsables des lieux de QR codes statiques.

Vie privée

- **PU1 - Pas de collecte centralisée de données personnelles**. Le système ne devrait pas exiger la collecte centralisée de données personnelles (par exemple nom, adresse e-mail, numéro de téléphone, lieux fréquentés) des personnes qui fréquentent un lieu. Le système ne devrait pas non plus être en mesure de déduire des données de localisation ou de co-localisation des visiteurs (notifiés positif ou non).
- **PU2 - Pas de collecte de données personnelles sur le lieu du restaurant**. Le système ne devrait pas exiger de collecte sur le lieu du restaurant de données personnelles (par exemple nom, adresse e-mail, numéro de téléphone) des personnes qui ont fréquenté le restaurant.
- **PU3 - Pas d'inférence à partir du trafic réseau**. Le trafic réseau ne doit pas révéler qu'un utilisateur spécifique a reçu un test ou une notification.
- **PU4 - Utilisateurs à risque**. Le système doit minimiser la collecte de données des utilisateurs à risque par les autorités.
- **PU5 - Utilisateurs testés positifs**. Le système doit minimiser la collecte de données des utilisateurs testés positifs par les autorités.

Confidentialité

- **PL1 - Ne pas dévoiler les restaurants où un cas positif a été déclaré**. Un attaquant qui n'a jamais fréquenté un restaurant ou qui a fréquenté un restaurant mais pas pendant l'intervalle de temps où un cas positif était présent, ne devrait pas être en mesure de déterminer si cet emplacement a présenté un cas positif. **Un utilisateur ne doit pas être en mesure de dresser la liste de tous les lieux « à risque » de sa rue, de son quartier, ou de monter un site collaboratif sur google map ou de cibler des types spécifiques d'ERP.**
- **PL2 - Pas de collecte centralisée des lieux**. Le système ne devrait pas créer de base de données centrale capturant des informations sur tous les restaurants.

Sécurité

- **S1 - Pas de fausses notifications**. Le système devrait rendre impossible le ciblage d'individus spécifiques.
- **S2 - Pas de ciblage en fonction du lieu**. Le système devrait rendre impossible le ciblage de personnes fréquentant des lieux spécifiques

	Solution CLEA sans rafraîchissement du QR-code	Solution CLEA avec rafraîchissement du QR-code
Vie privée		
PU1 - Pas de collecte centralisée de données personnelles	Pas de collecte centralisée de données personnelles. Le serveur collecte uniquement les tokens potentiellement exposés (tous ces tokens ne sont pas forcément distribués).	Aucune collecte centralisée de données personnelles. Le serveur reçoit uniquement des PETs qui sont aléatoires et non identifiants lors des requêtes de statut.
PU2 - Pas de collecte d'information dans le lieu visité	Le client ne laisse aucune donnée sur le lieu du restaurant.	Le client ne laisse aucune donnée sur le lieu du restaurant.
PU3 - Le système ne doit pas permettre à une tierce personne d'apprendre les lieux visités par une personne	Aucune remontée des lieux en temps normale. Seules les personnes déclarées positive. Les informatiosn remontées ne sont pas personnelles	Aucune remontée des lieux en temps normale. Seules les personnes déclarées positive. Les informatiosn remontées ne sont pas personnelles

	et la remontée se fait via un canla de communication sécurisée.	et la remontée se fait via un canla de communication sécurisée.
PU4 - Confidentialité des notifications	Décision locale	Décision locale
PU5 -Confidentialité du résultat de positivité d'une personne	Le serveur collecte l'ensemble des QR-codes et les horodatages correspondants. Si le serveur est malicieux, deux clients testés COVID+ ayant fréquenté le même restaurant peuvent être co-localisés après upload de leurs infos au serveur.	Le serveur collecte l'ensemble des QR-codes et les horodatages correspondants. Si les QR-codes sont changé avec une fréquence élevée, cela devient impossible même pour un serveur malicieux.
PL1 - Ne pas dévoiler les restaurants où un cas positif a été déclaré	Un utilisateur ne peut savoir si un ERP était un cluster que s'il était présent sur place pendant le bon intervalle de temps (ou s'il a récupéré un token d'une personne qui était sur place).	Un utilisateur ne peut savoir si un ERP était un cluster que s'il était présent sur place pendant le bon intervalle de temps (ou s'il a récupéré un token d'une personne qui était sur place). Le fait que les QR-codes changent mitige ce risque.
PL2 - Pas de collecte centralisée des lieux	Le serveur collecte uniquement les LTID des restaurants identifiés comme clusters et uniquement pendant la période de contamination.	Le serveur collecte uniquement les LTID des restaurants identifiés comme clusters et uniquement pendant la période de contamination. Les QR-codes changeant il faut être en mesure de récupérer tous les QR-codes d'un même lieu.
S1 - Pas de fausses notifications	Difficile de cibler quelqu'un sauf d'aller dans le même ERP que lui au même moment pour récupérer un token, puis donner ce token à un utilisateur possédant un QR-code de test à la Covid19.	Difficile de cibler quelqu'un sauf d'aller dans le même ERP que lui au même moment pour récupérer un token, puis donner ce token à un utilisateur possédant un QR-code de test à la Covid19. Si les QR-codes sont uniques par utilisateur cela est encore plus difficile.
S2 - Pas de ciblage en fonction du lieu	Difficile de cibler un endroit, sauf d'aller à plusieurs dans un ERP au même moment pour récupérer des tokens et les donner à des	Ciblage impossible si l'attaquant n'est pas physiquement dans le même restaurant au même moment.

	personnes en possession d'un QR-code de test à la Covid19.	

Les différents risques sont les suivants :

- **Accès illégitimes aux données concernées**
  - Impact sur les personnes
    - Sentiment d'intrusion dans la vie privée
    - Affectation psychologique mineure de type diffamation/réputation.
    - Difficultés relationnelles avec l'entourage personnel comme professionnel
  - Menaces permettant réalisation du risque
    - Altération du code de l'application côté backend et frontend
    - Intrusion sur le serveur TAC Signal
    - Intrusion dans la base de données
    - Vol des serveurs
  - Sources de risque
    - Personnels interne au projet et ayant accès au système
    - Cybercriminel
  - Mesures contribuant à traiter ou limiter le risque
    - Cloisonnement
    - Sécurisation des canaux informatiques
    - Sécurisation matérielle
    - Contrôle des accès logiques
    - Supervision
    - Audits de code
    - Tests d'intrusion
    - Journalisation
    - Gestion des postes de travail
    - Sécurité physique
    - Traçabilité
    - Éloignement des sources de risque
    - Gestion des personnels
    - Gestion des mots de passe
    - Exploitation
    - Authentification
    - Contrat de sous-traitance
    - Gestion des tiers accédant
    - Organisation de la politique de protection de la vie privé
  - Gravité du risque pour les personnes (négligeable / limitée / Importante / maximale)
    - Limitée
  - Vraisemblance du risque (négligeable / limitée / Importante / maximale)
    - Négligeable
- **Modification non désirée des données**
  - Impact sur les personnes concernées
    - Impossibilité d'alerter les personnes ayant fréquenté un lieu à la même date et sur une même plage horaire qu'une personne qui s'est déclarée positive
    - Alerte intempestive des personnes ayant fréquenté un lieu à la même date et sur une même plage horaire qu'une personne qui s'est déclarée positive
    - Affectation psychologique mineure.
    - Sentiment d'atteinte à la vie privée
  - Menaces permettant réalisation du risque
    - Interception des données en transit avec altération à la volée
    - Altération du code de l'application côté backend et frontend
    - Intrusion sur le serveur TAC Signal
    - Intrusion dans la base de données
  - Sources de risque
    - Personnels interne au projet et ayant accès au système
    - Personne malveillante qui afficherait/remplacerait un code à barres différent de celui du propriétaire des lieux

        - Cybercriminel
    - Mesures contribuant à traiter ou limiter le risque
        - Cloisonnement
        - Sécurisation des canaux informatiques
        - Sécurisation matérielle
        - Contrôle des accès logiques
        - Supervision
        - Audits de code
        - Tests d'intrusion
        - Journalisation
        - Gestion des postes de travail
        - Sécurité physique
        - Traçabilité
        - Sauvegarde
        - Éloignement des sources de risque
        - Gestion des personnels
        - Gestion des mots de passe
        - Exploitation
        - Authentification
        - Gestion des tiers accédant au SI
        - Organisation de la politique de protection de la vie privé
        - Analyse du certificat papier
    - Gravité du risque pour les personnes (négligeable / limitée / Importante / maximale)
        - Importante
    - Vraisemblance du risque (négligeable / limitée / importante / maximale)
        - Limitée
    - Plan d'action
        - Communiquer aux ERP sur une possible malveillance par remplacement de leurs codes à barres.
- **Disparition des données**
    - Impact sur les personnes concernées
        - Impossibilité d'alerter les personnes ayant fréquenté un lieu à la même date et sur une même plage horaire qu'une personne qui s'est déclarée positive
    - Menaces permettant réalisation du risque
        - Suppression des données figurant dans la base des établissements à risque
        - Incendie dans les datacenters
        - Vol des serveurs

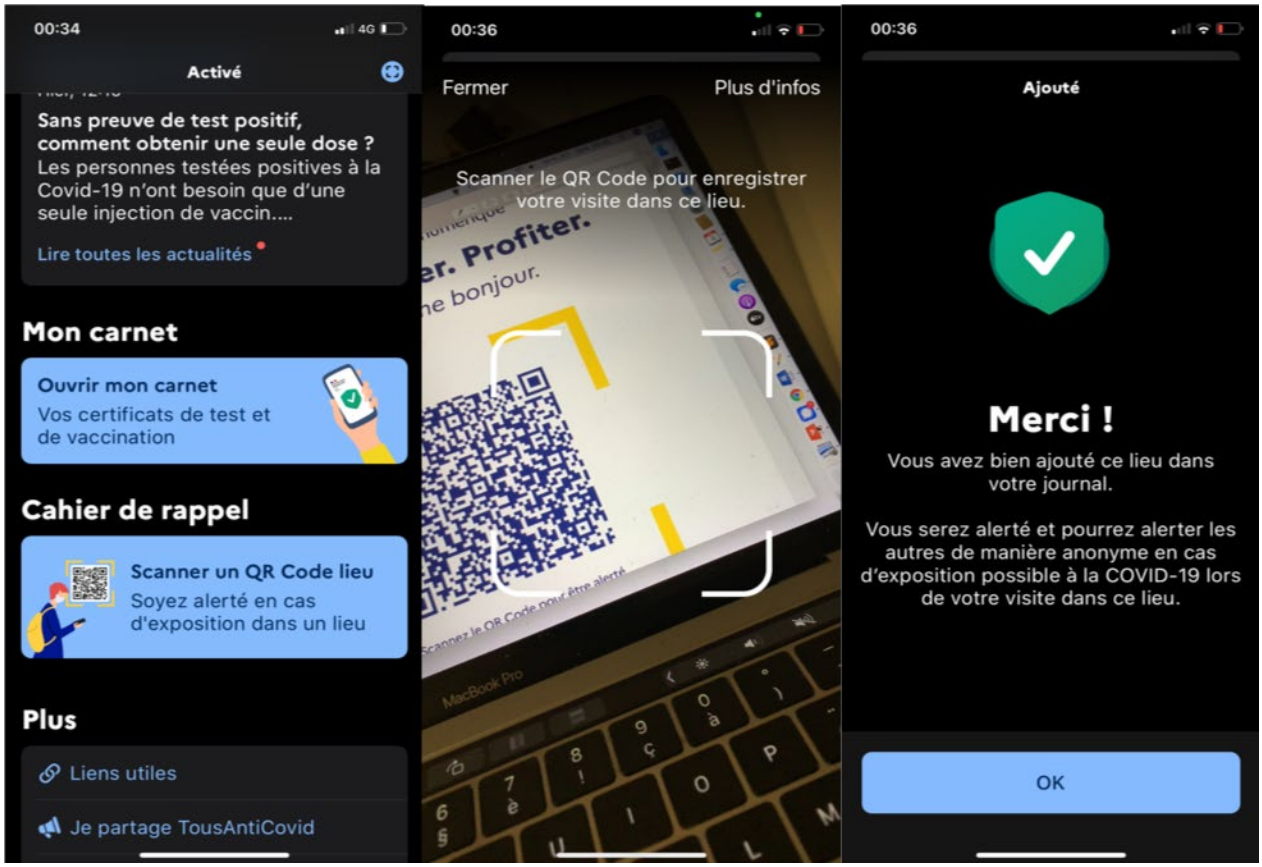
      Mesures contribuant à traiter ou limiter le risque
        - Cloisonnement
        - Sécurisation des canaux informatiques
        - Sécurisation matérielle
        - Contrôle des accès logiques
        - Supervision
        - Audits de code
        - Tests d'intrusion
        - Journalisation
        - Gestion des postes de travail
        - Sécurité physique
        - Traçabilité
        - Sauvegarde
        - Éloignement des sources de risque
        - Gestion des personnels
        - Gestion des mots de passe
        - Exploitation
        - Authentification
        - Gestion des tiers accédant au SI
        - Organisation de la politique de protection de la vie privé
    - Gravité du risque pour les personnes (négligeable / limité / Important / Maximale)
        - Limitée
    - Vraisemblance du risque (négligeable / limité / Important / Maximale)
        - Limitée

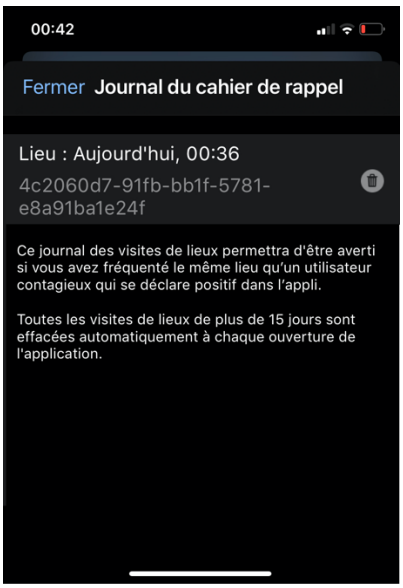
- Plan d'action
  - Restauration de la base de données

4 Annexes

4.1 Information des personnes concernées

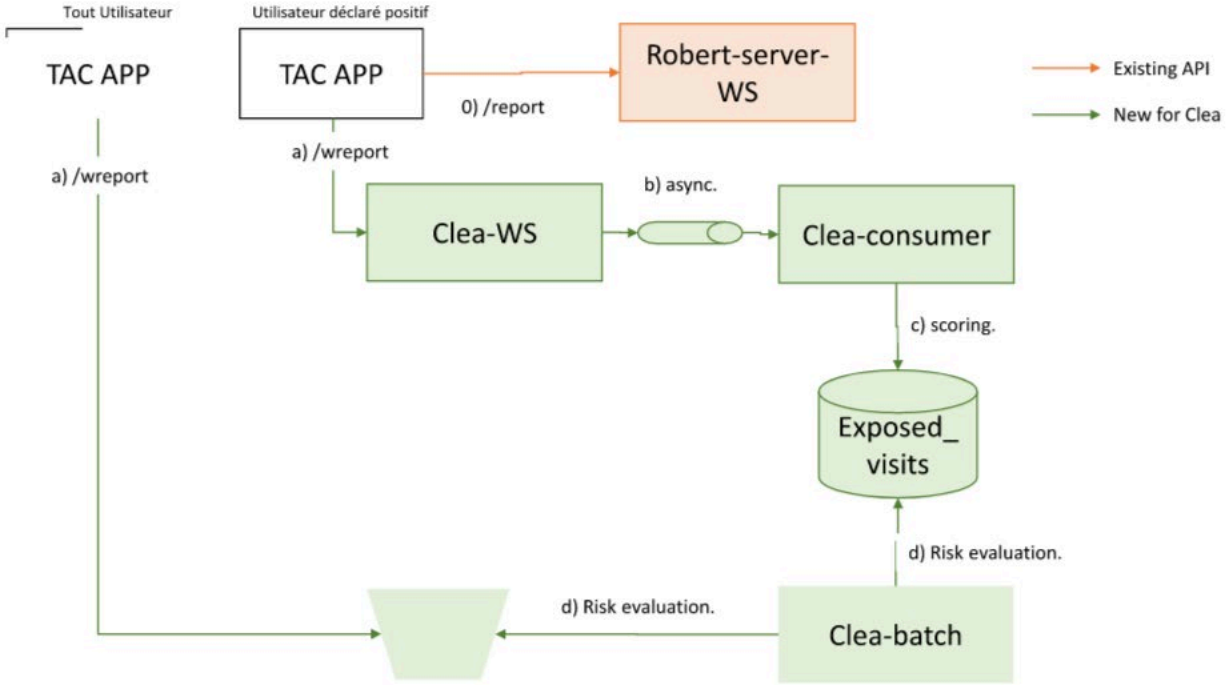
4.1.1 Écrans de travail de Signal





4.2 Architecture de Signal

Le schéma ci-dessous donne une vision globale de l'architecture mise en place pour le module fonctionne du module Signal (Cléa)



4.3 Format d'un deeplink dans l'historique des lieux

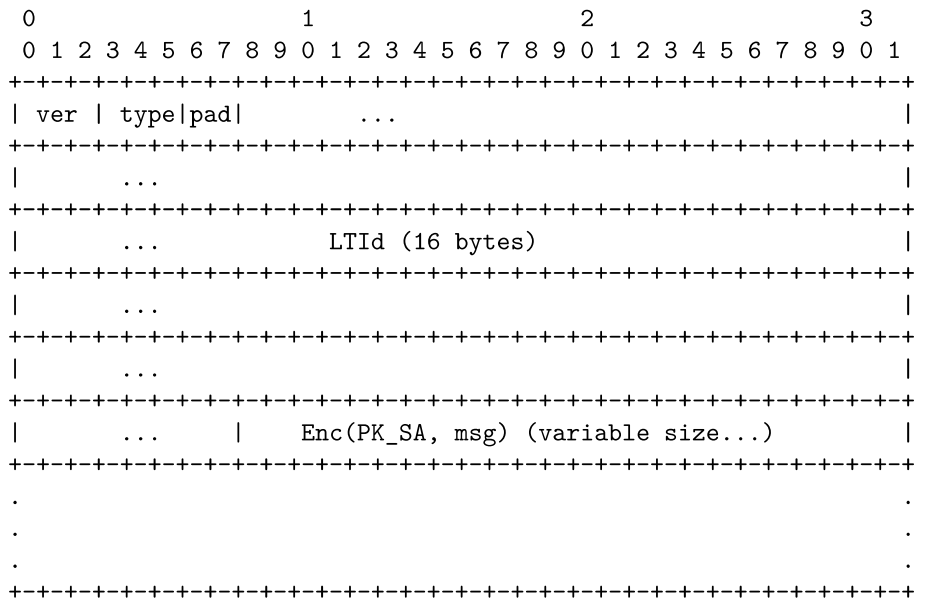
Le deeplink à utiliser pour ajouter un lieu dans l'historique des lieuxest de la forme suivante.

The QR code of a location, at any moment, contains a URL ("deep link"), structured as:

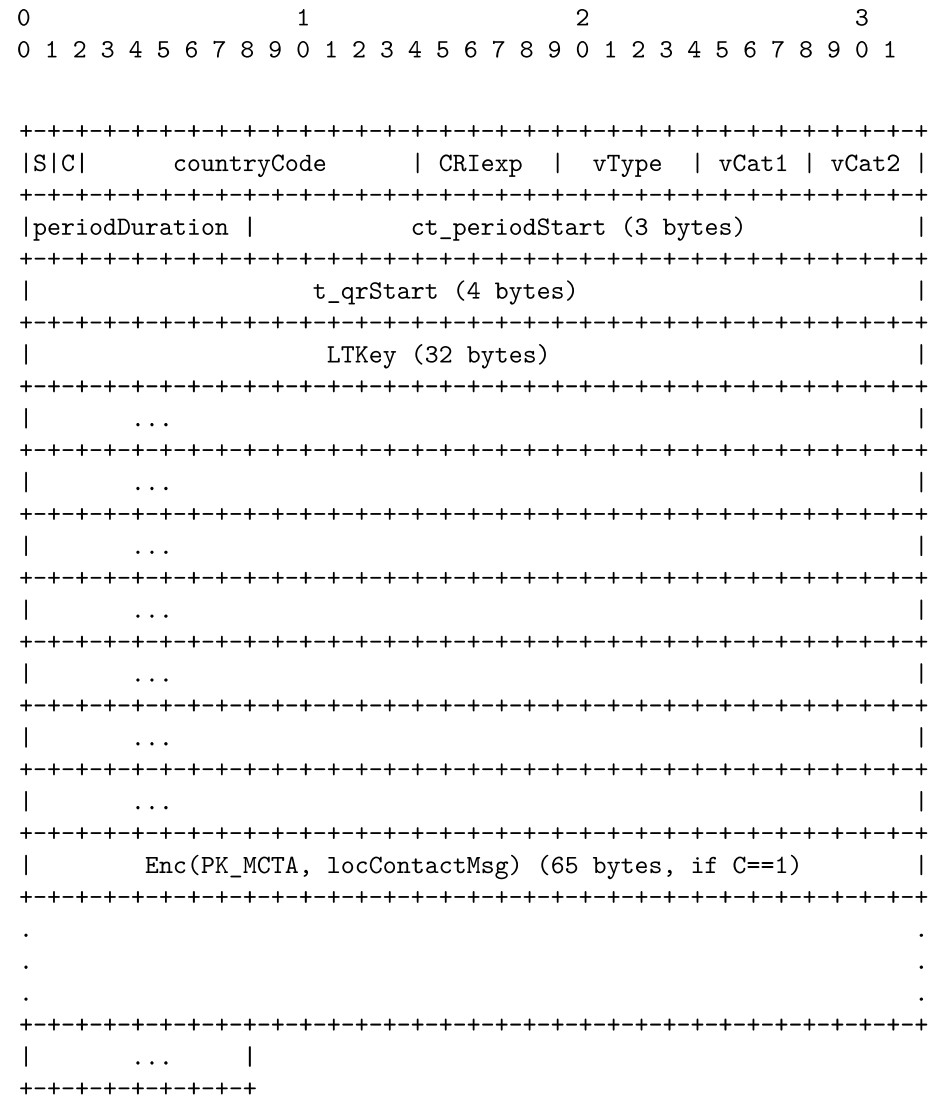
`"country-specific-prefix" / "Base64(location-specific-part)"`

For instance, the country specific prefix is: `https://tac.gouv.fr/` in case of France.

The following binary format must be used for the location specific part:



The following binary format for the `msg` message must be used:



Ce deeplink est encodé dans le QR code.

Le QR code peut être flashé dans l'application TousAntiCovid, ou sur iOS, directement par l'appareil photo sans avoir besoin de passer par l'application TousAntiCovid.