AIPD de TousAntiCovid Pass sanitaire

Version mise à jour le 9 juin 2021

1 INFORMATIONS DE L'AIPD 2

2 CONTEXTE 2

2.1 VUE D'ENSEMBLE 2
2.2 DONNÉES, PROCESSUS ET SUPPORTS 5

3 COMPOSANTS DU PASS SANITAIRE 7

3.1 MODULE CARNET DE L'APPLICATION TOUSANTICOVID 7
3.2 APPLICATION TOUSANTICOVID VERIF 7
3.3 APPLICATION WEB TOUSANTICOVID VERIF POUR LA POLICE AUX FRONTIERES 8
3.4 CONVERTISSEUR DE CERTIFICAT 2D-DOC / DCC 8
3.5 CONNEXION AUX PORTAILS SI-DEP ET VACCIN-COVID 9
3.6 CONNEXION AU PORTAIL EUROPEEN DCC-G 9

4 PRINCIPES FONDAMENTAUX 9

4.1 REMARQUES LIMINAIRES 9
4.2 PROPORTIONNALITÉ ET NÉCESSITÉ 9
4.3 MESURES PROTECTRICES DES DROITS 11

5 RISQUES 13

5.1 MESURES EXISTANTES OU PRÉVUES 13
5.2 ANALYSE DE RISQUE 13

6 ANNEXES 15

6.1 INFORMATION DES PERSONNES CONCERNEES 15
6.2 CERTIFICATS DE VACCINATION OU DE TEST OU DE RETABLISSEMENT A LA COVID-19 22
6.3 AJOUT DE CERTIFICAT DE TEST COVID-19 DANS LE MODULE CARNET DE TOUSANTICOVID 22
6.4 MESURES DE SECURITE 24

1 Informations de l'AIPD

Nom de l'auteur
Déléguée à la protection des données d'Inria, Anne COMBE
Nom de l'évaluateur
RSSI/Référent RGPD de la DGS, Olivier VANDEWYNCKELE
Référente RGPD de la DGS Selma FAHLGREN
Nom du validateur
Jérôme SALOMON
Date de création
20/05/2020
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 ?

Afin de permettre aux personnes concernées de prouver l'état de leur protection/immunité face à la Covid-19, lors d'un contrôle par une autorité habilitée au sein de l'Union Européenne, il a été décidé de développer des applications permettant de vérifier l'émetteur et l'authenticité des preuves de vaccination ou test de dépistage présentés par les personnes souhaitant voyager ou participer à un événement regroupant plus de 1000 personnes.

Ces applications sont au nombre de trois :

L'application mobile TousAntiCovid Verif

Cette application a été développée à la demande de la DGS par la société IN Groupe pour permettre aux autorités de contrôle ou aux organisateurs d'événement rassemblant plus de 1000 personnes(compagnie aérienne, douane, police, etc.):

- D'identifier l'organisme émetteur et l'intégrité du des données contenues dans le code à barres 2D-Doc ou DCC d'un certificat de vaccination, d'un résultat de tests ou de rétablissement à la Covid-19
- D'interpréter ces éléments aux regards des règles sanitaires du pays de destination;
- De réaliser des statistiques anonymes pour améliorer l'efficacité de l'application et du modèle de santé utilisé par l'application

L'Application web TousAntiCovid Verif

Du fait de l'absence d'équipement en téléphonie mobile de la Police aux Frontières, la direction générale de la santé à demander à la société IN Groupe de développer une version web de l'application TousAntiCovid Verif permettant aux agents de la PAF de réaliser les mêmes actions de contrôle que dans la version mobile

Toutefois, cette version Web dispose d'un mécanisme complémentaire permettant d'interroger un service web du ministère de l'intérieur afin de vérifier les certificats présentés par les voyageurs.

Un service de conversion des codes à barres 2D-Doc en DCC

Ce service, développé par IN Groupe, permet à SI-DEP, VACCIN-COVID et TousAntiCovid de demander la conversion d'un code à barre 2D-Doc vers le format Digital Covid Certificate (DCC) ou vers un format international (IATA par exemple). Cette opération est réalisée par l'intermédiaire d'un appel à une API.

La passerelle européenne DCCG

Cette passerelle permet aux pays membre de l'Union Européenne d'obtenir les certificats oémis par les autres pays afin de permettre l'identification de l'organisme émetteur ainsi que l'intégrité des données contenues dans le code à barres d'un certificat DCC de vaccination, d'un test de dépistage COVID-19 ou de rétablissement à la Covid-19 produit par un de ces pays. Elle est également responsable du contrôle de la validité des certificats émis par les différents pays européens.

Le module Carnet de l'application TousAntiCovid

Le module Carnet entre dans le dispositif « Pass sanitaire » au même titre que les documents au format numérique ou papier. Ce module Carnet de l'application TousAntiCovid permet à son utilisateur de conserver de façon sécurisée, dans un format numérique signé, ses certificats de vaccination ou résultats de tests ou de rétablissement à la Covid-19.

La présente **AIPD est dédiée au Pass sanitaire mais reliée à l'AIPD de TousAntiCovid**.

Alors que la pandémie impose des mesures sanitaires d'ampleur aux frontières et parfois des restrictions de circulation, le 17 mars dernier, la Commission européenne a fait la proposition d'un DCC dont l'objectif est de permettre, aux autorités de contrôle de disposer d'un mécanisme commun pour contrôler, de manière fiable et sécurisée, tout document produit par les autorités du pays relatif à la Covid-19 qu'un citoyen européen circulant au sein de l'Union européenne, pourrait lui présenter.

La France s'inscrit pleinement dans cette démarche avec « le Pass sanitaire» et sa connexion avec la DCCG d'identifier l'organisme émetteur, l'intégrité des données contenues dans le code à barres présent dans les certificats de test de dépistage COVID-19 et de vaccination et d'appliquer une règle sanitaire.

Le Gouvernement répond ainsi à la proposition faite par la Commission européenne pour aider à une reprise plus large des déplacements entre les pays de l'Union européenne en proposant 3 types de certificats : le certificat de test négatif, le certificat de rétablissement de la Covid-19 et l'attestation de vaccination. L'objectif est de rendre la vérification des certificats interopérable au niveau européen avant le 17 juin, puis plus largement à l'international autour de standards communs.

Cela se traduit par la certification officielle des fiches résultats de tests RT-PCR et antigéniques négatifs et positifs (dès le 19 avril) ainsi que des attestations de vaccination (dès le 29 avril). Les fiches de résultats de tests et preuves de vaccination réalisés en France sont désormais signés de façon numérique, avec un code à barres 2D-Doc employée par l'administration française pour certifier ses documents. Ceci permet de garantir l'intégrité du document électronique et d'en authentifier l'auteur. Ce procédé évite ainsi les fraudes possibles liées à la présentation de faux résultats de tests.

Les autorités en charge des contrôles aux frontières en France et à l'étranger pourront lire les informations certifiées du code à barres DCC grâce au partage de la clef publique permettant de vérifier la signature de l'empreinte numérique (hash) des données présentes dans le code à barres 2D-Doc/DCC. Une application de lecture appelée TousAntiCovid Verif développée par la société IN Groupe à la demande de la DGS équipe les entités autorisées à vérifier les certificats vaccination ou de test ou de rétablissement à la Covid-19 (compagnies aériennes, police, douanes, etc. contenues dans les codes à barres 2D-Doc/DCC des documents produits par SI-DEP ou VACCIN-COVID.

Le module Carnet de l'application TousAntiCovid, permet de sauvegarder le document numérique contenant le code à barres 2D-Doc/DCC afin d'en simplifier le stockage et permettre sa présentation lors de déplacements ou voyages. Ce document est également toujours disponible au format PDF et papier.

Courant avril 2021, le Gouvernement lance l'expérimentation de l'utilisation de la fonctionnalité TousAntiCovid Carnet sur des vols à destination de la Corse puis, dans les semaines suivantes, étendra l'expérimentation aux vols vers les Outre-Mer. L'objectif est de garantir la bonne utilisation de TousAntiCovid Carnet par les passagers et de l'application de lecture TousAntiCovid Verif par les personnes en charge du contrôle de ces preuves, ainsi que le bon fonctionnement des certificats de tests avant leur déploiement sur l'ensemble des vols. Ces expérimentations permettent

- D'améliorer l'ergonomie de l'application TousAntiCovid Verif et de s'assurer de l'adhésion à l'application par les personnels des compagnies aériennes,
- D'intégrer au mieux les mesures sanitaires aux procédures très contraintes des transporteurs aériens,
- D'évaluer la sensibilité du public à ces mesures sanitaires, améliorer la communication vis-à-vis du public,
- De s'assurer des performances du service de vérification TousAntiCovid Verif.

Le 29 mai 2021 s'est tenu à l'Accord Hôtel Aréna un évènement test qui a rassemblé 5 000 spectateurs à l'occasion d'un concert de musique. Les preuves sanitaires des participants ont été systématiquement vérifiées à l'aide de TousAntiCovid Verif, l'objectif étant d'évaluer l'impact sur la gestion de flux de personnes et les dispositions à prévoir dans l'organisations de futurs évènements rassemblant des publics importants.

En parallèle, le gouvernement participe au programme européen Digital Green Certificate (renommé dorénavant Digital Covid Certificate - DCC), qui harmonise la production et la vérification de certificats entre les états membres de l'Union européenne. Ce programme standardise le format des certificats et met en œuvre une infrastructure d'échange de clés publiques qui permet à chaque État de vérifier l'ensemble des certificats émis sur le territoire européen. A partir du 23 juin tous les certificats émis le seront au format DCC, les infrastructures d'émission et vérification seront adaptées en conséquence. Le DCC reprend la même structure que les 2D-DOC mais diffère sur les points suivants :

- Le BAR-CODE émis suit le standards QR-Code et non plus Datamatrix ;
- L'organisation des données diffère ;

- Les données sont compressées avant d'être intégrées dans le QR code.

Les détenteurs de certificats émis avant le 23 juin, donc au format 2D-DOC, devront pouvoir les convertir au format DCC s'ils veulent les voir reconnaitre sur le territoire européen. Et plus généralement un certificat DCC doit pouvoir être converti vers des formats internationaux spécifiés par des organismes tels que l'OACI, l'OMS ou l'IATA. Pour s'inscrire dans le cadre du programme DCC, le gouvernement prépare un mécanisme de conversion disponible à l'ensemble des usagers. Ce mécanisme pourra être invoqué à partir de l'application TousAntiCovid Carnet pour convertir les certificats s'y trouvant ou par scan direct du bar code à convertir.

Afin de doter les personnels de la Police aux Frontières d'un outil permettant de réaliser les contrôles des certificats des voyageurs, une API (interface de programmation) a été spécifiquement développée. Elle est interfacée avec les équipements spécifiques de la PAF (qui n'est pas dotée de smartphone, mais de PC Windows équipés de douchette avec lecteur laser), pour permettre de réaliser - dans le cadre de sa mission de contrôle - la vérification des certificats présentés par les voyageurs, selon les règles de gestion sanitaires particulières pour les déplacements hors du territoire de la métropole. Cette application devrait être disponible courant juillet.

Les principaux enjeux du module du Pass sanitaire 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 falsification des certificats de vaccination ou résultats de tests ou de rétablissement à la Covid-19 ;
- De perte des certificats papier de vaccination ou résultats de tests ou de rétablissement à la Covid-19 ;
- De réduire l'erreur humaine et d'uniformiser l'interprétation des règles sanitaires ;

Les finalités du traitement sont

- De proposer un service simple et gratuit pour tous ;
- D'assurer la sécurité des données sanitaires traitées ;
- De garantir un accès égalitaire avec la possibilité d'obtenir son certificat en version papier comme en numérique.

Il appartient à l'utilisateur d'enregistrer ou non un certificat de vaccination ou de test de dépistage Covid-19 ou de rétablissement à la Covid-19.

2.1.2 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**
  - In Groupe : éditeur de l'application TousAntiCovid Verif et de la plateforme de conversion des certificats du format 2D-Doc au format DCC ou International.
  - Lunabee : développement de l'application TousAntiCovid et du Module Carnet ;
- **Destinataires**
  - Les utilisateurs du module TousAntiCovid Carnet qui enregistrent leur certificat de vaccination ou de test ou de rétablissement à la Covid-19 ;
  - Les utilisateurs de l'application TousAntiCovid Verif qui scanneront les certificats de vaccination ou de test ou de rétablissement à la Covid-19 afin de vérifier l'authenticité de ces certificats;
  - Inria en tant que sous-traitant auprès de la DGS du MSS.

2.1.3 Quelles sont les personnes concernées

Les personnes concernées sont

- les utilisateurs de l'application TousAntiCovid installée et qui enregistrent leur certificat de vaccination ou de test ou de rétablissement à la Covid-19
- les personnes possédant un certificat de vaccination ou de test ou de rétablissement à la Covid-19 en fichier PDF ou en version papier

2.1.4 Quels sont les référentiels applicables ?

- Référentiel Général de Sécurité (RGS)
  - Une homologation au RGS de StopCovid (renommé en TousAntiCovid) a été instruite et a été prononcée par

la DGS du MSS préalablement à la mise en production de StopCovid.

- PSSI de l'Etat PSSI-E
- 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 dans le module Carnet de l'application TousAntiCovid et affichées par l'application TousAntiCovid Verif

Les données contenues dans le module Carnet de l'application TousAntiCovid et les données affichées sur l'écran de l'utilisateur de TousAntiCovid Verif qui scanne un certificat de vaccination ou de test ou de rétablissement à la Covid-19 d'une personne concernée sont les suivantes :

- Certificat de vaccination
    - Prénoms, Nom ;
    - Date de naissance ;
    - Producteur du vaccin ;
    - Type de vaccin ;
    - Date d'injection ;
    - Dose courante ;
    - Dose totale attendue ;
    - Statut du vaccin (en cours, fini).
- Certificat de test
    - Prénoms, Nom ;
    - Date de naissance ;
    - Genre ;
    - Code du test (LOINC) ;
    - Résultat du test ;
    - Date du test.
- Identifiant de l'autorité de certification ;
- Identifiant du certificat ;
- Date d'émission du document ;
- Date de création de la signature ;

La connaissance du statut vaccinale ou du résultat d'un test ou de rétablissement à la Covid-19 est important pour les personnes en charge par exemple de la régulation des déplacements.

Une redirection vers la page d'accueil au bout de 20 secondes. Permettre de contrôler, avec des éléments supplémentaires comme une pièce d'identité, que les données affichées sont bien celles associées à la personne qui présente le code à barres 2D-Doc/DCC.

Données traitées par le convertisseur de certificat 2D-Doc en DCC

Les données sont les même que les données traitées par TousAntiCovid verif

Données traitées par la passerelle européenne DCCG

La passerelle européenne DCC-G ne traite que les clefs publiques des autorités de santé des Etats membre.

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

- **Collecte par le module Carnet des certificats**

- L'utilisateur de l'application TousAntiCovid enregistre dans le module Carnet son certificat de vaccination ou de test ou de rétablissement à la Covid-19, en scannant le code à barres 2D-Doc/DCC qui figure sur le document papier, le fichier numérique ou le deeplink en provenance de SI-DEP ou VACCIN-COVID.

- **Collecte par l'application mobile TousAntiCovid Verif**
  - Préalablement à la lecture du code à barres 2D-Doc/DCC, l'application TousAntiCovid Verif sur le téléphone mobile de l'autorité de contrôle ou de l'organisateur d'événement de plus de 1000 personnes nécessite le recueil du consentement de l'utilisateur pour accéder à la caméra du téléphone mobile aux fins de scanner un certificat de vaccination ou de test ou de rétablissement à la Covid-19 ;
  - Ensuite, les données ne sont pas stockées sur le téléphone mobile de l'autorité de contrôle ou de l'organisateur d'événement de plus de 1000 personnes et aucune capture d'écran n'est possible avec ce téléphone mobile. L'application se contente de lire les informations contenues dans le code à barres 2D-Doc/DCC et de les afficher sur l'écran de l'autorité de contrôle ou de l'organisateur d'événement de plus de 1000 personnes. Une redirection automatique vers la page d'accueil de l'application est également réalisée au bout de 20 secondes.
  - La vérification du code à barres 2D-Doc/DCC est possible du fait que l'application TousAntiCovid Verif dispose du certificat et de la clé publique associé à la clé privée qui a permis de signer l'empreinte numérique qui figure dans le code à barres.
  - le certificat au format 2D-Doc est transmis au serveur d'IN Groupe pour
    - vérification de la signature du certificat ;
    - décodage du certificat grâce à la clé de chiffrement préservée au niveau du serveur ;
    - application des règles de gestion sanitaire en fonction du type de preuve présenté et du contexte du contrôle. Le résultat du contrôle est renvoyé vers l'écran de l'équipement de l'utilisateur.

- **Conversion du certificat au format DCC** si le certificat est au format 2D-Doc
  L'utilisateur de l'application TousAntiCovid peut générer un certificat au format DCC
  - soit à partir d'un certificat 2D-Doc enregistré dans le module Carnet, l'application TousAntiCovid se connecte au service de conversion.
  - soit à partir d'un certificat 2D-Doc obtenu sur VACCIN-COVID et SI-DEP

  Le moteur de gestion des règles techniques vérifie la validité et la pertinence du 2D-Doc ; si les vérifications sont positives, le certificat est converti du format 2D-Doc au format européen DCC qui est signé par IN Groupe et à terme dans n'importe quel format international interopérable.

  Les étapes de la conversion sont les suivantes
  - Le décodage : extraction des informations du 2D-Doc et vérification de l'authenticité et de l'intégrité du 2D-Doc
  - la conversion de champ
  - l'encodage : génération de la structure JSON pour la transformer au format CBOR[1] (format utilisé par le DCC), signature de ce format par IN Groupe, et envoi de la chaine coté TousAntiCovid Carnet,.

  Aucune donnée n'est stockée dans l'application ou sur le serveur central d'IN Groupe, l'appel et la réponse se font dans un temps système. Aucun log applicatif ou des informations d'IP ou de contenu des requêtes au serveur de conversion ne sont mis en place.

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 :

- **Utilisation du module Carnet de TousAntiCovid:** téléphone mobile, système d'exploitation (Android/iOS), Internet, réseau GSM ;
- **Application TousAntiCovid Verif** : téléphone mobile, serveur, Internet, autorité de certification, liste de révocation (CRL), certificat type « cachet serveur » contenant une clé publique permettant la vérification de la signature.
- **Convertisseur de certificat :** téléphone mobile, serveur, Internet.

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

[1] Concise Binary Object Representation

3 Composants du Pass sanitaire

3.1 Module Carnet de l'application TousAntiCovid

Ce module permet à l'utilisateur d'enregistrer les certificats de vaccination ou de test ou de rétablissement à la Covid-19 provenant d'un tiers de confiance (VACCIN-COVID ou SI-DEP). Ces certificats sont certifiés selon la norme 2D-Doc[2]/DCC (représenté sous forme d'un Data Matrix) et ajoutés via un deeplink dans TousAntiCovid, soit en appuyant sur le deeplink (ex sur le portail patient SI-DEP), soit en le scannant sur le certificat papier (VACCIN-COVID ou SI-DEP).

Le flux des données pour un certificat de Test Covid-19 est le suivant (cf le schéma en Annexe) :

- SI-DEP envoie au patient un SMS ou un e-mail contenant un lien vers le portail SI-DEP, ou bien le patient scanne le QR Code apposé sur le document de le certificat du Test Covid
- Le patient obtient alors une page du portail SI-DEP et renseigne sa date de naissance (ou celle de la personne pour laquelle il récupère le certificat)
- Le portail SI-DEP affiche un bouton pour ajouter le certificat du Test Covid dans TousAntiCovid. Le patient peut également avoir accès au certificat au format PDF (qu'il peut alors télécharger ou imprimer).
- Lorsque le patient clique sur le bouton, l'utilisateur déclenche alors la génération du deeplink qui contient les informations de son certificat au format attendu, selon la norme 2D-Doc/DCC avec les données présentées dans la section du document traitant de ce sujet,
- Lorsque le patient clique sur le deeplink et confirme l'ajout dans TousAntiCovid, la signature du 2D-Doc/DCC est vérifiée, et si la signature est valide, les données sont enregistrées dans le Carnet de TousAntiCovid. Si le patient ne possède pas TousAntiCovid, la page https://bonjour.tousanticovid.gouv.fr s'affiche pour inciter à télécharger TousAntiCovid, puis un second clic une fois installée envoie les données du 2D-Doc/DCC vers TousAntiCovid ;
- TousAntiCovid génère dans le Carnet le Data Matrix associé au 2D-Doc/DCC ;
- Les autorités publiques ou les organisateurs d'événement de plus de 1000 personnes scannent le Data Matrix via des lecteurs qui disposent de la clé publique pour vérifier la certification.

Les contraintes sur le Carnet de vaccination et de test Covid-19 sont :

- Avoir une alternative papier pour toute solution présentée dans TousAntiCovid (documents de preuves) intégrant lui aussi le 2D-Doc/DCC;
- Intégrer dans TousAntiCovid des certificats de plusieurs personnes (d'une même famille par exemple) ;
- Assurer une interopérabilité européenne/internationale en termes de règles sanitaires et lecture.

3.2 Application TousAntiCovid Verif

L'application TousAntiCovid Verif permet de vérifier l'authenticité du certificat de vaccination ou de test ou de rétablissement à la Covid-19 au format 2D-Doc/DCC.

L'application TousAntiCovid Verif s'inscrit dans le périmètre de la certification ISO 27001 d'IN Groupe. Le code source de l'application, dans sa version initiale, a fait l'objet d'un audit et de tests techniques par l'ANSSI permettant de garantir la sécurité de l'application

Le flux des données pour une opération de contrôle d'un certificat est le suivant : (cf schéma en annexe)

- L'utilisation de l'application TousAntiCovid Verif est réservé aux seules personnes limitativement prévues au décret XX (article 2, II, 1° et suivants). Chaque utilisateur s'engage à respecter les règles d'utilisation de l'application.
- L'utilisateur scanne un certificat au format 2D-Doc/DCC grâce au lecteur dans l'application, et appelle l'application sur le serveur central.
- La requête est relayée par les serveurs d'Akamaï qui assurent une protection (bouclier) entre l'application et Internet et prévient les attaques en déni de service : il n'y a pas de stockage sur disque des requêtes, elles sont déchiffrées à la volée en mémoire puis transférées vers le serveur central d'IN Groupe
- Le certificat est transmis au serveur central d'IN Groupe pour 3 opérations :

[2] https://ants.gouv.fr/Les-solutions/2D-Doc

- Vérification de la signature du certificat ;
- Décodage du certificat grâce à la clé de déchiffrement qui est conservée dans le serveur central ;
- Application des règles de gestion sanitaire qui sont fonction (i) du type de preuve présenté et (ii) du contexte dans lequel est réalisé le contrôle

- Le résultat du contrôle, sous la forme d'un statut vert ou rouge, le nom, prénom et la date de naissance du détenteur du certificat est renvoyé vers l'équipement de l'utilisateur de l'application ;
- Aucun log identifiant l'utilisateur ou son équipement n'est collecté ou généré : l'application fonctionne en session active qui envoie la requête et réceptionne la réponse, seuls des logs a vocation de facturation sont réalisés;
- Aucune donnée personnelle n'est conservée ni au niveau du serveur central, ni dans l'application. Des données statistiques sont agrégées (date/heure du contrôle, résultat, type d'équipement utilisé pour réaliser le contrôle, type de certificat contrôlé)

Les contraintes sur l'application TousAntiCovid Verif sont :

- Ne conserver aucune donnée relative aux preuves présentées à l'issue de la vérification sur le serveur central

Ne pas échanger avec le serveur central les opérations de contrôle du passe sanitaire sur le territoire national, qui doivent alors se réaliser en local dans l'application.

3.3 Application web TousAntiCovid Verif pour la Police aux Frontières

L'API TousAntiCovid Verif équipe spécifiquement les personnels de la Police aux Frontières pour leur permettre d'effectuer les opérations de vérification d'authenticité du certificat de vaccination ou de test ou de rétablissement à la Covid-19 au format 2D-Doc ou DCC. La Police aux Frontières n'est pas équipée de Smartphone, mais de PC Windows auxquels sont connectés des lecteurs laser (douchettes).

Le flux des données pour une opération de contrôle d'un certificat est le suivant :

- L'utilisation de l'API TousAntiCovid Verif est réservée aux seuls personnels de la Police aux Frontières.
- L'utilisateur scanne un certificat au format 2D-Doc ou DCC grâce à un lecteur laser, et via l'API, se connecte au moyen d'un canal sécurisé par identification de l'adresse IP du terminal appelant sur le serveur central d'IN Groupe. Seuls les équipements sur le réseau proxy du Ministère de l'Intérieur sont des « utilisateurs » autorisés et peuvent se connecter à l'API par reconnaissance de l'adresse IP du proxy.
- Le certificat est transmis au serveur central d'IN Groupe pour 3 opérations :
  - Vérification de la signature du certificat,
  - Décodage du certificat grâce à la clé de déchiffrement qui est conservée dans le serveur central
  - Application des règles de gestion sanitaire spécifique du contexte « voyage »
- Le résultat du contrôle, en affichage détaillé pour les personnels de la Police aux Frontières (c'est-à-dire, toutes les données contenues dans le certificat) est renvoyé vers l'équipement de l'utilisateur.
- Aucun log identifiant l'utilisateur ou son équipement n'est collecté ou généré : l'application fonctionne en canal sécurisé par identification et reconnaissance d'adresse IP.
- Aucune donnée personnelle n'est conservée ni au niveau du serveur central.

Les contraintes sur l'API TousAntiCovid Verif sont :

- Ne conserver aucune donnée relative aux preuves présentées à l'issue de la vérification sur le serveur central

3.4 Convertisseur de certificat 2D-Doc / DCC

Ce service, développé par IN Groupe, permet notamment à l'application TousAntiCovid, à SI-DEP et VACCIN-COVID de demander la conversion d'un certificat au format 2D-Doc vers le format DCC ou international. Cette opération est réalisée par l'intermédiaire d'un appel à une API.

3.5 Connexion aux portails SI-DEP et VACCIN-COVID

Les personnes concernées se connectent au portail SI-DEP[3] et VACCIN-COVID[4] ces portails pour récupérer les certificats de vaccination ou de test ou de rétablissement à la Covid-19 au format 2D-Doc/DCC.

Une AIPD sur SI-DEP ainsi qu'une AIPD sur VACCIN-COVID ont été rédigées.

3.6 Connexion au portail européen DCC-G

Dans ce portail, les prestataires de chaque État membre de l'Union Européenne qui émettent des certificats DCC déposent les clés de vérification publiques des DCC crées ou convertis.

Aucune donnée personnelle n'est transmise à ce portail

4 Principes fondamentaux

4.1 Remarques liminaires

L'enregistrement des certificats de vaccination ou test ou rétablissement à la Covid-19 dans le module Carnet de l'application TousAntiCovid repose sur le volontariat.

Le scan via l'application TousAntiCovid Verif d'un certificat de vaccination ou test ou rétablissement à la Covid-19 d'une personne, situé dans le module Carnet ou dans un fichier PDF ou en version papier, par une autorité ou un organisateur d'évènement de plus de 1000 personnes doit se faire avec l'accord de cette personne.

Il n'existe aucun lien entre l'application TousAntiCovid développée par Lunabee et l'application TousAntiCovid Verif développé par IN Groupe.

4.2 Proportionnalité et nécessité

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

Les finalités du traitement sont déterminées et explicites

- Le module Carnet de l'application TousAntiCovid permet à l'utilisateur de l'application TousAntiCovid de conserver, dans format numérique et sécurisé, ses certificats de vaccination ou résultats de tests ou de rétablissement à la Covid-19.
- L'application TousAntiCovid Verif permet à une autorité ou un organisateur de contrôler, avec des éléments supplémentaires comme une pièce d'identité, que les données affichées sur l'écran de l'utilisateur sont bien celles associées à la personne qui présente le certificat 2D-Doc/DCC et que le contenu des informations affichées n'a pas été altéré et a bien éé émis par une source authentifiée.
- Ces deux applications, le fichier pdf et la version papier permettent aux personnes concernées de prouver l'état de leur protection/immunité face à la Covid-19, lors d'un contrôle par une autorité habilitée au sein de l'Union Européenne.

Ces finalités sont légitimes, elles sont décrites dans le décret XX.

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.

Évaluation : Acceptable
Commentaire d'évaluation :
Aucun commentaire.

[3] https://sidep.gouv.fr/
[4] https://attestation-vaccin.ameli.fr/

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) ?

A partir du 8 juin au soir pour la version Android et du 10 juin soir pour la version iOS, TousAntiCovid Verif fonctionnera en mode off-line sans transmettre de données personnelles aux serveurs de IN Groupe.

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 ?

Pour le module Carnet de l'application TousAntiCovid

L'exactitudes des données et la tenue à jour sont du ressort de la personne concernée qui accepte de communiquer les données contenues dans ses certificats de vaccination ou de test ou de rétablissement à la Covid-19 situés dans le module Carnet de l'application TousAntiCovid ou dans un fichier PDF ou en version papier.

Pour l'application TousAntiCovid Verif

L'exactitudes des données et la tenue à jour sont du ressort de la personne qui accepte de communiquer ses données. Toutefois, et afin de vérifier la véracité des données affichées, l'application TousAntiCovid Verif pourra s'appuyer sur le code à barres 2D-Doc/DCC.

Afin de vérifier les certificats de vaccination ou de test ou de rétablissement à la Covid-19, l'application TousAntiCovid Verif se connectera au portail européen DCC.

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.

Pour le module Carnet de l'application TousAntiCovid

Les données sont conservées tant que l'utilisateur ne décide pas du contraire. Il est seul responsable de l'enregistrement et la suppression des données de preuve dans le Carnet de TousAntiCovid.

Pour l'application TousAntiCovid Verif

Seul l'autorité de contrôle ou l'organisateur d'évènement de plus de 1000 personnes utilisant l'application TousAntiCovid Verif a accès aux informations lues dans le code à barres 2D-Doc/DCC du certificat de vaccination ou de test ou de rétablissement à la Covid-19 qui lui est présenté par la personne qui accepte de communiquer ses données.
L'application lit les informations stockées dans le code à barres 2D-Doc/DCC et les affiche à l'écran de l'utilisateur pendant 20 secondes.
Elle et ne permet pas le stockage des informations sur le téléphone mobile de l'utilisateur de TousAntiCovid verif.

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 ?

Pour le module Carnet de l'application TousAntiCovid

Une information est affichée au niveau du module Carnet (cf document en Annexe)

Pour l'application TousAntiCovid Verif

Une information sera effectuée sur le site du ministère des solidarités et de la santé ainsi qu'auprès des utilisateurs de TousAntiCovid Verif (Politique de confidentialité, CGU). Les conditions générales d'utilisation mentionnent également ce besoin de notifier les personnes concernées mais il sera très difficile de demander à un agent de contrôle de le faire verbalement.

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 ?

Pour le module Carnet de l'application TousAntiCovid

L'utilisateur du module Carnet de l'application TousAntiCovid est libre d'ajouter un certificat de vaccination ou de test ou de rétablissement à la Covid-19.

Pour l'application TousAntiCovid Verif

Pas de consentement nécessaire. La personne peut si elle le souhaite présenter à l'autorité de contrôle ou à l'organisateur d'événement de plus de 1000 personnes un document papier, un document numérique ou sa représentation dans le Carnet TousAntiCovid mais toujours en accord avec elle.

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 droit d'accès et droit à la portabilité ?

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 droit de rectification et droit à l'effacement (droit à l'oubli) ?

Pour le module Carnet de l'application TousAntiCovid

L'utilisateur peut lui-même procéder à l'effacement de ses certificats enregistrés dans le module Carnet de l'application TousAntiCovid.

Pour l'application TousAntiCovid Verif

Etant donné qu'aucune information n'est stockée, ce droit de rectification et d'effacement ne s'applique pas pour les données contenues dans le code à barres 2D-Doc/DCC ni pour les statistiques anonymes remontées par l'application, à IN Groupe.

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 droit de limitation et droit d'opposition ?

Pour le module Carnet de l'application TousAntiCovid

L'utilisateur peut lui-même procéder lui-même à son droit d'opposition ou de limitation en effaçant ses certificats enregistrés dans le module Carnet de l'application TousAntiCovid.

Pour l'application TousAntiCovid Verif

La personne concernée peut refuser que ces certificats soient vérifiés, donc elle ne pourra pas participer au voyage ou à l'événement qui impose cette vérification.
Elle ne peut pas exercer ses droits de limitation ou d'opposition car le traitement se termine dès que le résultat est affiché sur l'écran de l'utilisateur de TousAntiCovid Verif

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 ?

- **Inria**
  - un accord cadre a été signé entre MSS et Inria
- **Lunabee**
  - un accord cadre a été signé entre Inria et Lunabee
- **IN Groupe**
  - Un accord-cadre entre Inria et IN Groupe est en cours de signature

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

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

Pour le module Carnet de l'application TousAntiCovid

Aucun transfert de données à caractère personnel en dehors de l'Union Européenne n'est réalisé dans le cadre de ce traitement et toutes les informations relatives aux statistiques sont localisées en France.

Pour l'application TousAntiCovid Verif

Un transfert de données hors UE peut avoir lieu lors de l'utilisation d'Akamai, c'est le serveur le plus proche de la requête qui répond

- pour toutes les requêtes effectuées en métropole, ce seront les serveurs français ou UE d'Akamai qui répondront
- si la requête est réalisée depuis un territoire outre-mer, c'est un serveur hors UE qui pourra répondre.

Les contremesures mises en place sont les suivantes

- Rédaction d'un accord RGPD entre IN Groupe et Akamai conforme suite à l'invalidation PrivacyShield réalisé
- Pas de stockage de données par Akamai, mais un simple transit de données.
- L'infrastructure Akamai est sécurisée de telle manière que les serveurs n'ont pas de mémoire morte (disque dur) mais uniquement de la mémoire vive (RAM)

Akamai n'est pas un fournisseur de services de communication électronique, selon les lois applicables aux Etats-Unis, il n'est donc pas soumis aux demandes d'accès en vertu de la loi FISA 702 ou E.O 12333.

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

5 Risques

5.1 Mesures existantes ou prévues

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

Les mesures de sécurité pour TousAntiCovid Verif en place sont communiquées en Annexe.

5.2 Analyse de risque

Cette analyse porte sur l'utilisation du module Carnet de l'application TousAntiCovid, l'application TousAntiCovid Verif et le convertisseur 2D-Doc / DCC

.

Les différents risques sont les suivants :

- **Accès illégitimes aux données concernées**
  - Impact sur les personnes
    - Utilisation des informations relatives à l'identité et aux données de santé (elles permettent de savoir que la personne concernée a réalisé des tests, a eu la Covid-19, a été vaccinée par une marque de Vaccin)
    - Diffusion de données hors du périmètre prévu
  - Menaces permettant réalisation du risque
    - espionnage des communications entre appli et serveur IN Groupe
    - intrusion dans serveur central IN Groupe
    - intrusion dans le smartphone (cheval de Troie permettant de s'introduire dans appli)
    - accès interne au serveur
    - interception des informations coté serveur central
    - Compromission de la clé de conversion
    - Fausse application TousAntoCovidVerif qui ne fait que lire les données, les enregistrent et les envoie vers un autre serveur, ou les stocke en local sur une mémoire flash.
  - Sources de risque
    - Personnel interne ayant accès au système
    - Pirate informatique
  - Mesures contribuant à traiter ou limiter le risque
    - Cloisonnement
    - Sécurisation des canaux informatiques
    - Sécurisation matérielle
    - Contrôle des accès logiques
    - Journalisation
    - Gestion des postes de travail IN Groupe
    - Gestion des postes de travail IN
    - Sécurité physique
    - Traçabilité
    - Éloignement des sources de risque
    - Gestion des personnels
    - Gestion des mots de passe
    - Exploitation
    - Authentification
    - Gestion des tiers accédant
    - Organisation de la politique de protection de la vie privé
  - Gravité du risque pour les personnes (négligeable / limité / Important / Maximale)
    - Important
  - Vraisemblance du risque
    - Importante
  - Plan d'action

        - Passage de l'application en mode offline
    - Révision des échelles de gravité et vraisemblance
        - Gravité reste: importante
        - La vraisemblance du risque devient limitée
        - Source du risque est la défaillance ou attaque interne
- **Modification non désirée des données**
    - Impact sur les personnes concernées
        - Porter atteinte à liberté de mouvement en ne permettant pas l'accès à un évènement, à un moyen de transport…
        - Risque sanitaire en permettant par exemple à un voyageur de se rendre dans un pays alors qu'il est contaminé à la Covid-19
    - Menaces permettant réalisation du risque
        - espionnage des communications entre appli et serveur central d'IN Groupe
        - intrusion dans serveur central d'IN Groupe
        - intrusion dans le smartphone (cheval de Troie permettant de s'introduire dans application TAC Verif)
        - accès interne au serveur
        - interception des informations coté serveur central d'IN Groupe
        - Cheval de Troie embarqué dans 2D-Doc
        - Compromission de la clé de conversion
    - Sources de risque
        - Personnel interne ayant accès au système
        - Pirate informatique
    - Mesures contribuant à traiter ou limiter le risque
        - Cloisonnement
        - Sécurisation des canaux informatiques
        - Sécurisation matériel
        - Contrôle des accès logiques
        - Journalisation
        - Gestion des postes de travail d'IN Groupe
        - Sécurité physique
        - Traçabilité
        - 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 / limité / Important / Maximale
        - Important
    - Vraisemblance du risque
        - Importante
    - Plan d'action
        - Passage de l'application en mode offline
    - Révision des échelles de gravité et vraisemblance
        - Gravité reste: importante
        - La vraisemblance du risque devient limitée
        - Source du risque est la défaillance ou attaque interne
- **Disparition des données**
    - Impact sur les personnes concernées
        - Impossibilité d'utiliser l'application TAC Verif
        - Porter atteinte à liberté de mouvement en ne permettant pas l'accès à un évènement, à un moyen de transport…
        - Retards
        - Risque sanitaire en permettant par exemple à un voyageur de se rendre dans un pays alors qu'il est contaminé à la Covid-19
    - Menaces permettant réalisation du risque
        - indisponibilité des services et des serveurs sur le serveur central d'IN Groupe

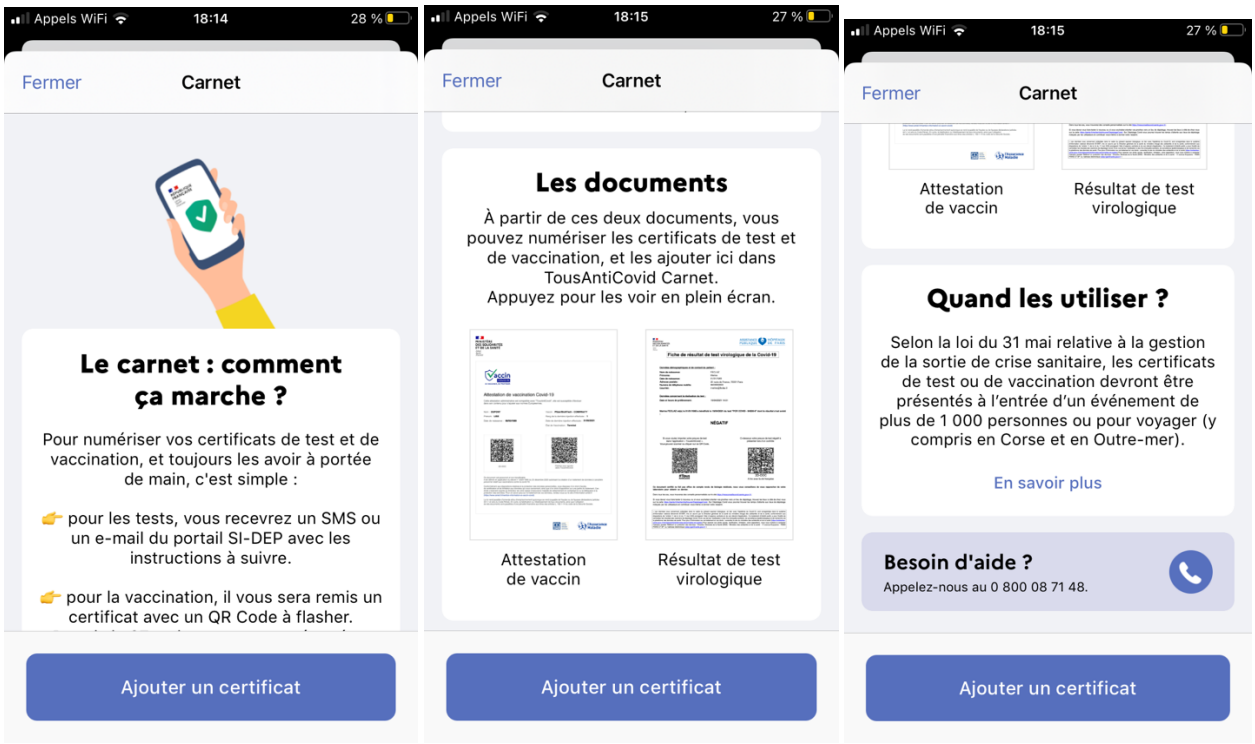
- Mesures contribuant à traiter ou limiter le risque
  - Redondance des serveurs et des services au niveau du serveur central d'IN Groupe
  - Les données ne sont pas stockées sur le serveur central d'IN Groupe
- Gravité du risque pour les personnes (négligeable / limité / Important / Maximale
  - Important
- Vraisemblance du risque
  - Importante
- Plan d'action
  - Passage de l'application en mode offline

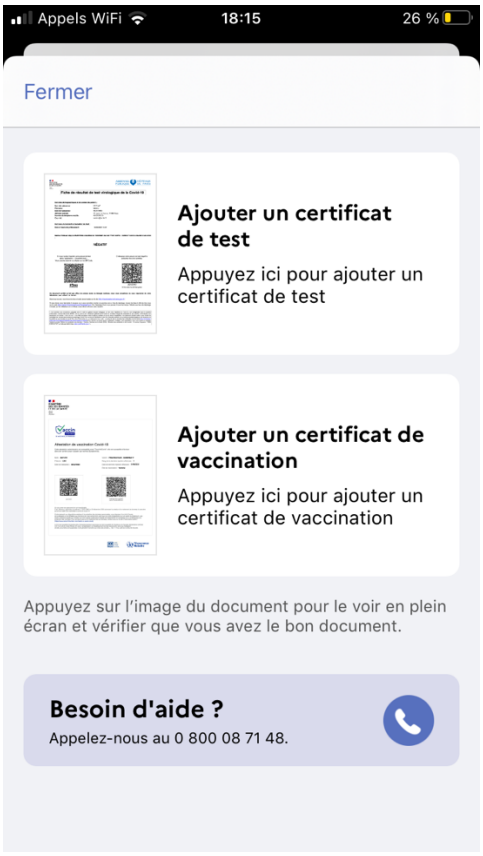
6 Annexes

6.1 Information des personnes concernées

6.1.1 Écrans de travail du module Carnet de l'application TousAntiCovid

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

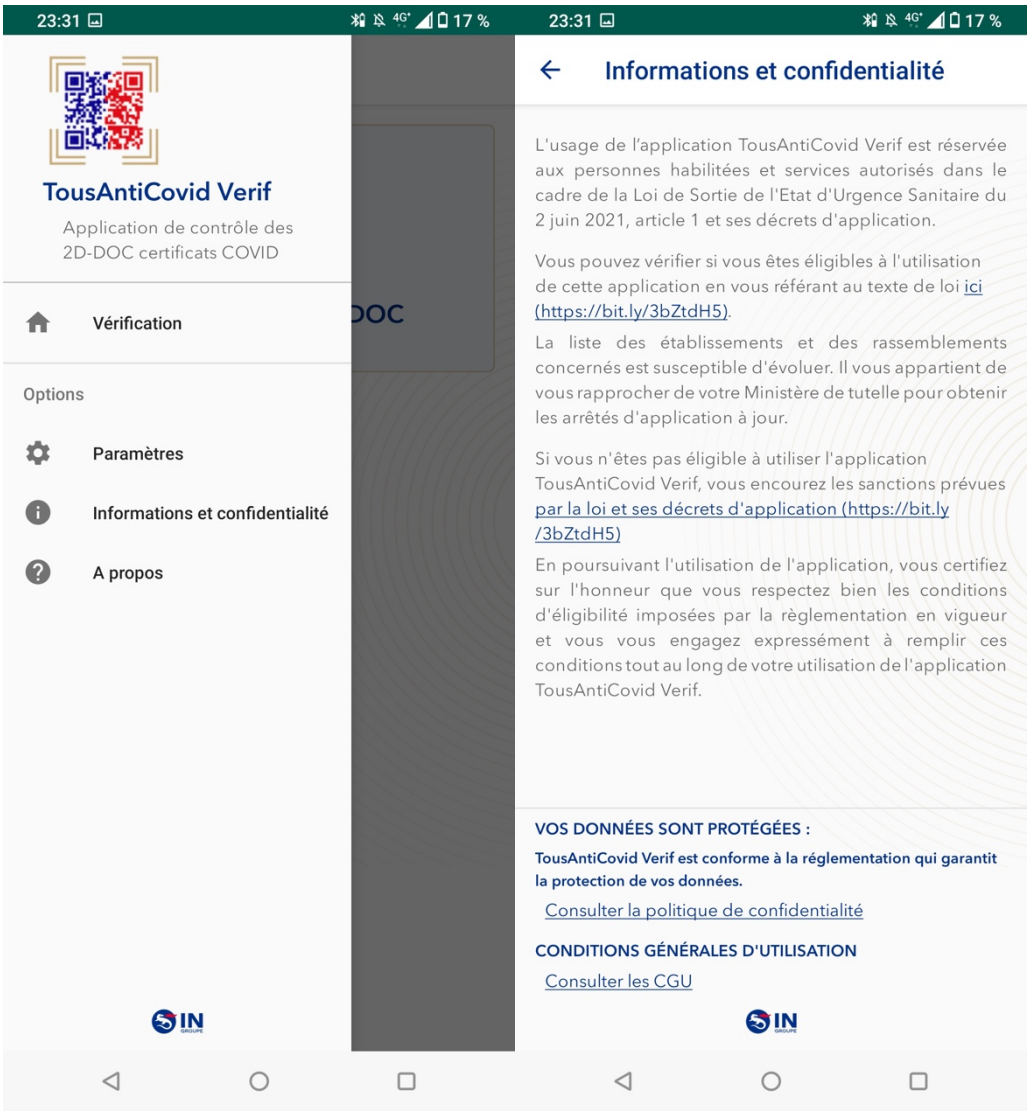




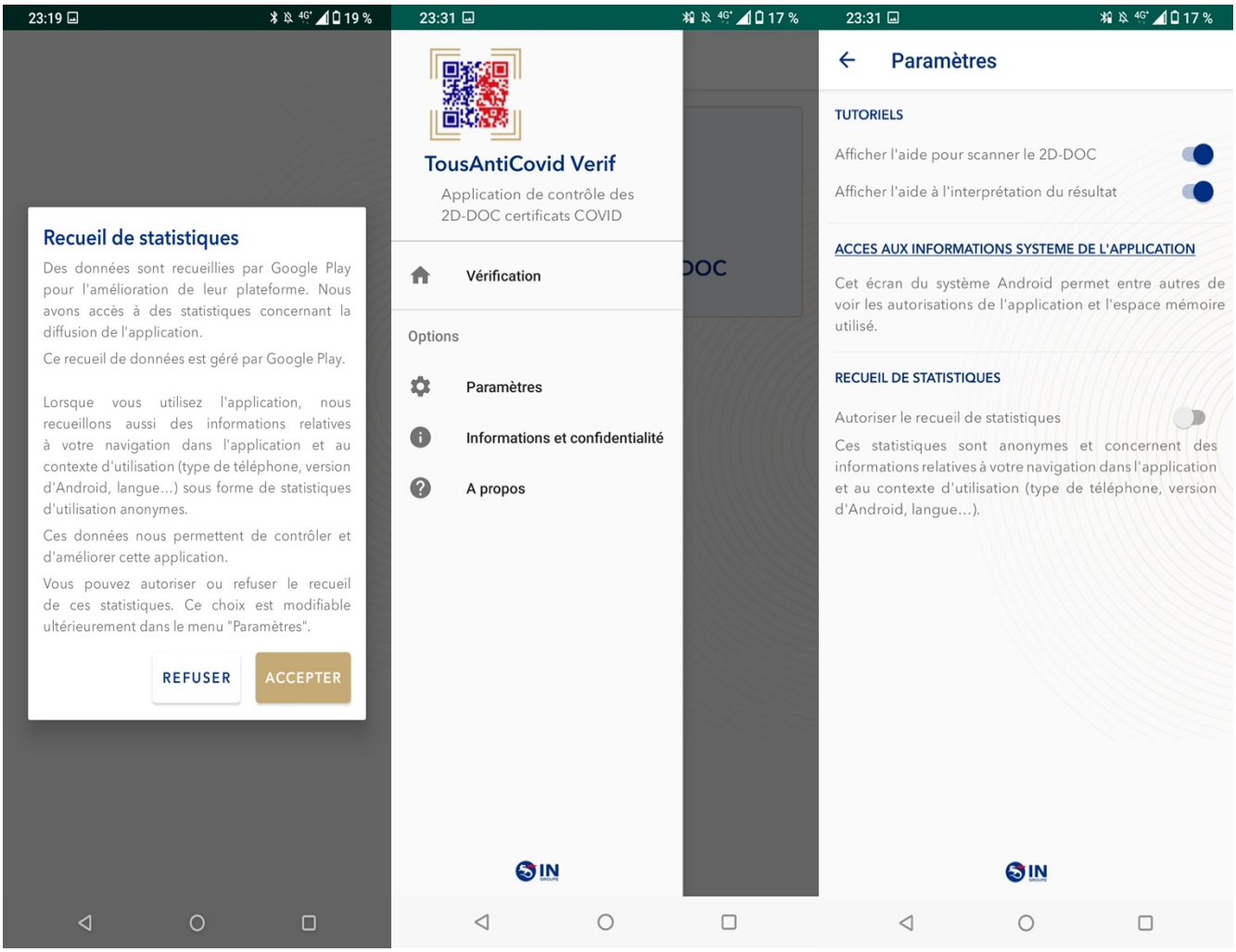
6.1.2 Écrans de travail de l'application TousAntiCovid Verif

Quand l'utilisateur télécharge l'application TousAntiCovid Verif, une page d'information s'affiche et rappelle les règles d'utilisation de l'application, et propose un accès vers les Conditions Générales d'Utilisation et la Politique de Confidentialité de l'application.

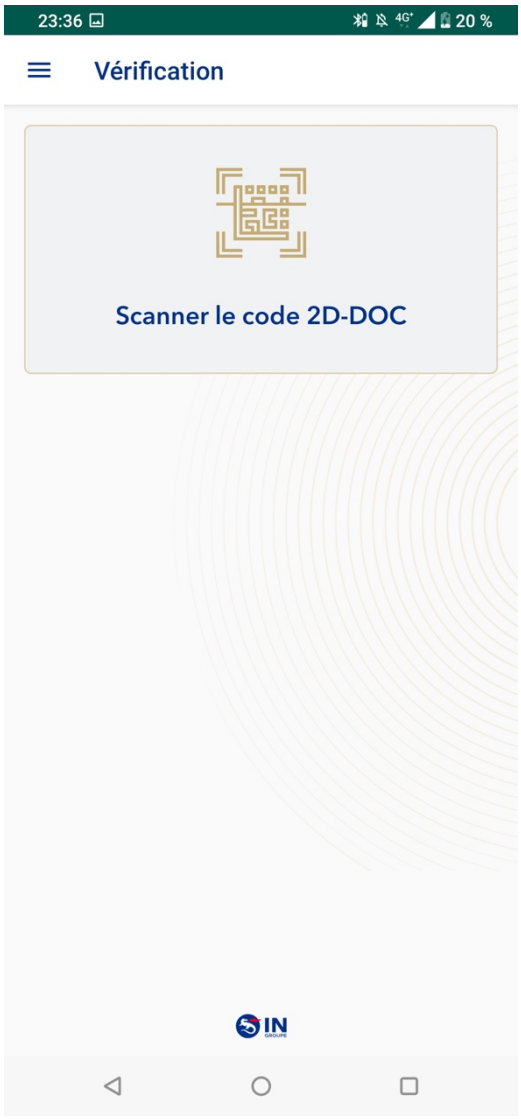
Ces documents sont accessibles à tout moment dans le menu « Informations » de l'application



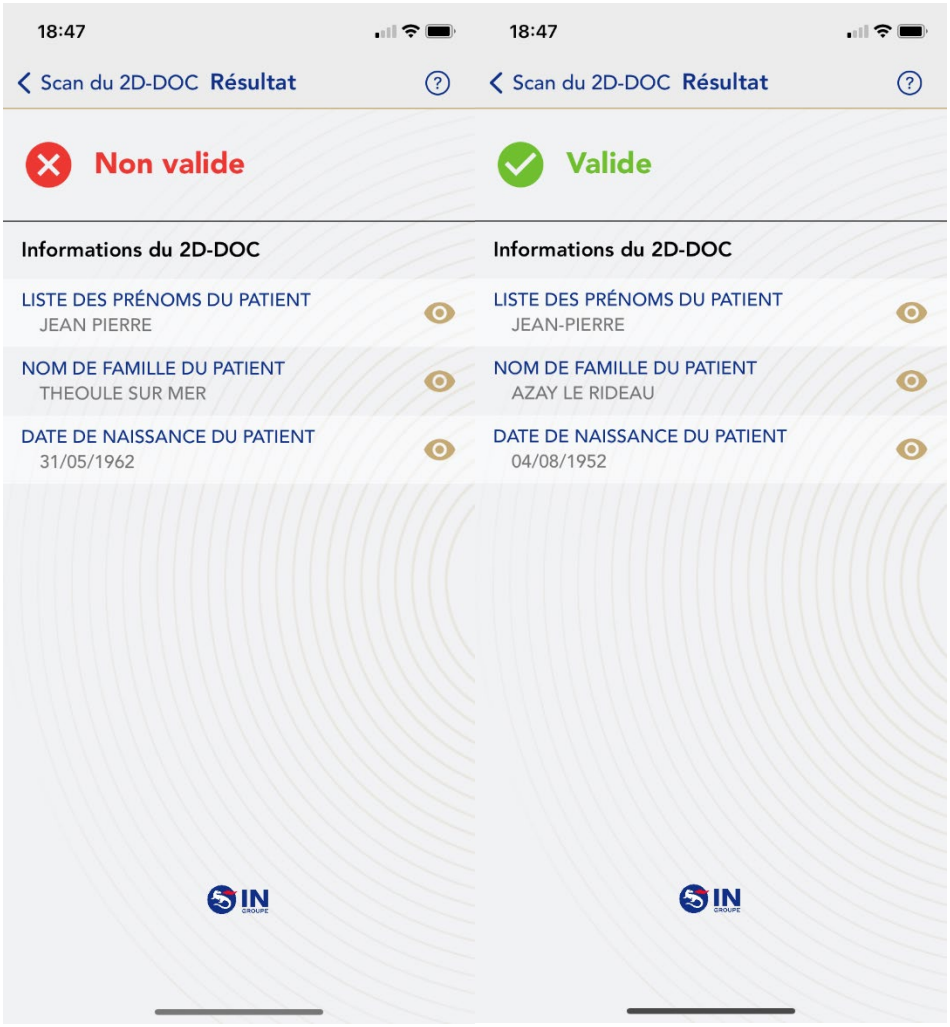
Ensuite l'application demande le consentement de l'utilisateur pour le recueil de statistiques anonymes. Le choix de l'utilisateur est modifiable à tout moment dans le menu « informations » de l'application.



L'utilisateur peut alors scanner un 2D-Doc, simplement en sélectionnant « Scanner le code 2D-Doc ».



En fonction de la validité du certificat scanné, deux réponses peuvent s'afficher :



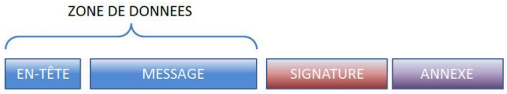
6.2 Certificats de vaccination ou de test ou de rétablissement à la Covid-19

6.2.1 Structure et format d'un 2D-Doc

STRUCTURE ET FORMAT D'UN 2D-DOC

Un code 2D-Doc est composé de deux zones principales et éventuellement une zone optionnelle positionnées dans cet ordre :

- La **zone des données** qui est elle-même composée de deux sous-parties :
  - Une **zone d'en-tête** de taille fixe qui fournit les informations nécessaires pour chaque code 2D-Doc.
  - La **zone de message**, qui contient des informations propres à chaque code 2D-Doc. Dans cette zone de taille variable et selon le type de document sont placées les données communes à tous les documents comme les données propres (obligatoires et facultatives) à chaque document. Chaque donnée doit être précédée d'un identifiant de données encodé sur deux caractères.
- La **zone de signature** de la zone des données dont le format dépend de la version du standard 2D-Doc.
- La **zone de données annexe** (introduite version '04') qui a la même structure que la zone de message mais qui se trouve après la zone de signature est une zone de données optionnelles dont le contenu n'est pas prise en compte dans la signature.

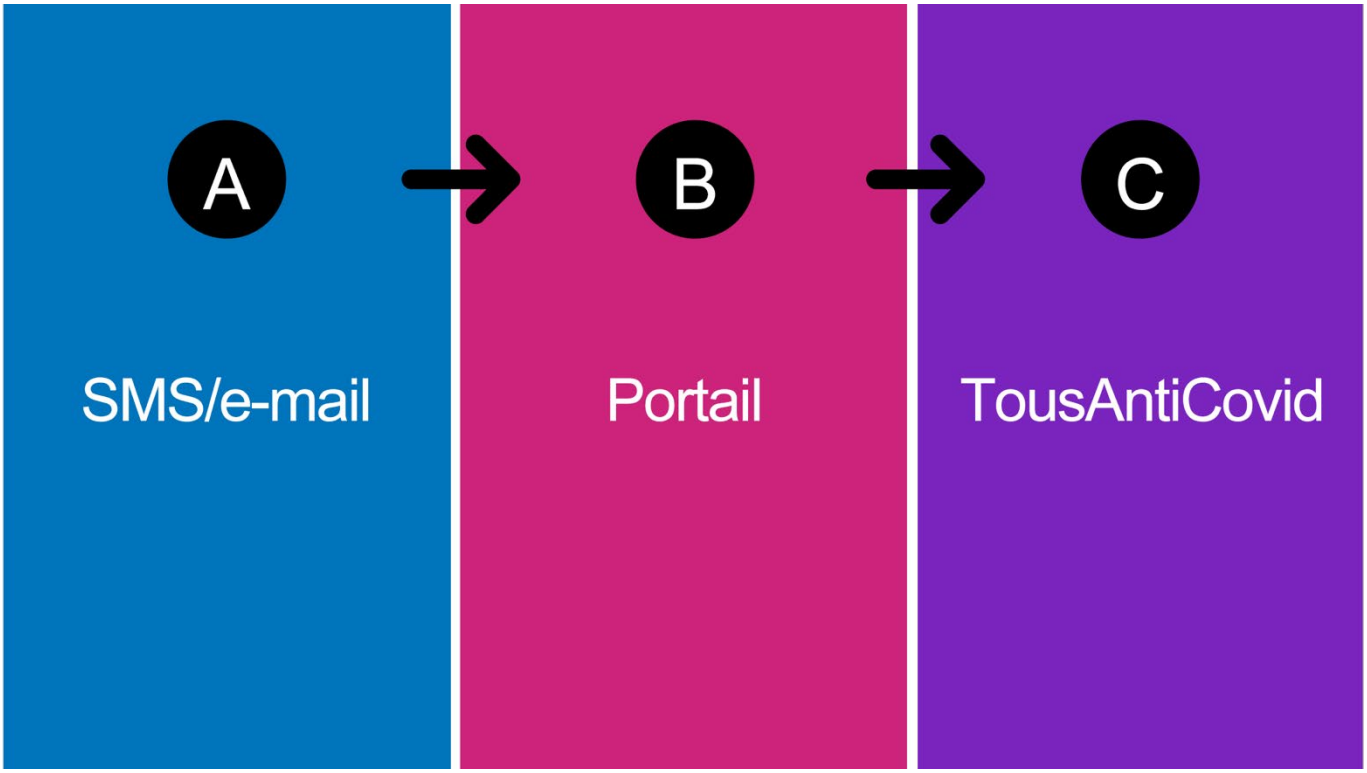


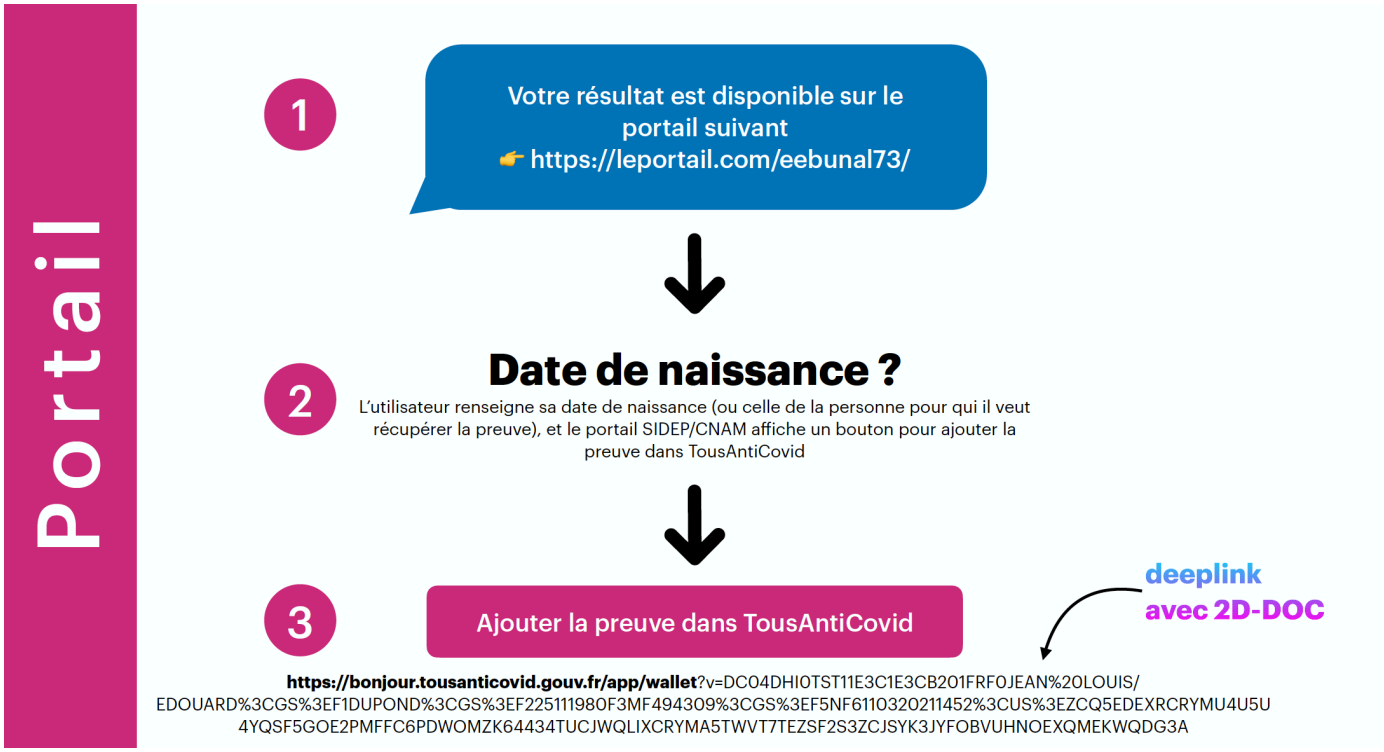
Il existe deux formats d'encodage pour un code 2D-Doc :

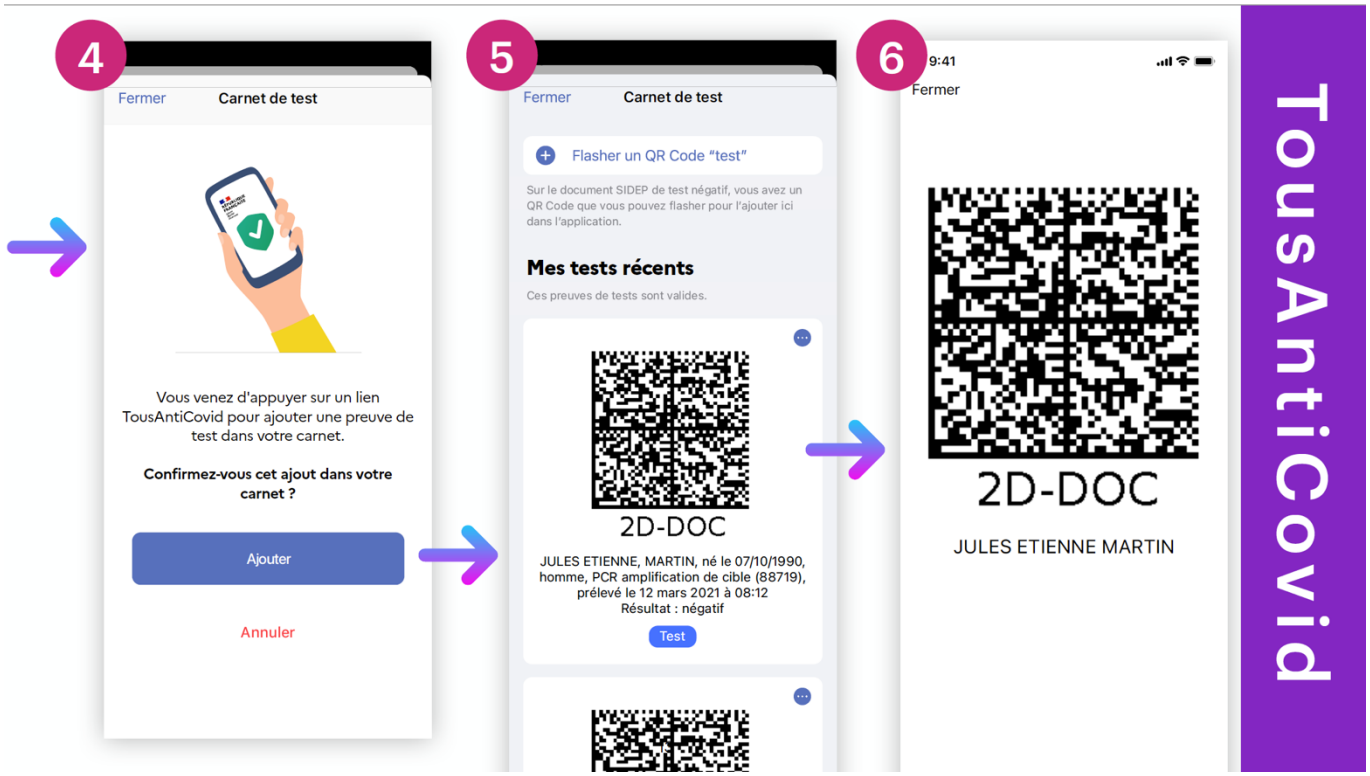
- Le format C40 exploitant un encodage en C40 des données utilisé depuis la version '01 (à l'exception de la signature de la version '01'
qui était au format binaire)
- Le format binaire introduit dans la version '04'

6.3 Ajout de certificat de test Covid-19 dans le module Carnet de TousAntiCovid

6.3.1 Après reception d'un SMS/e-mail

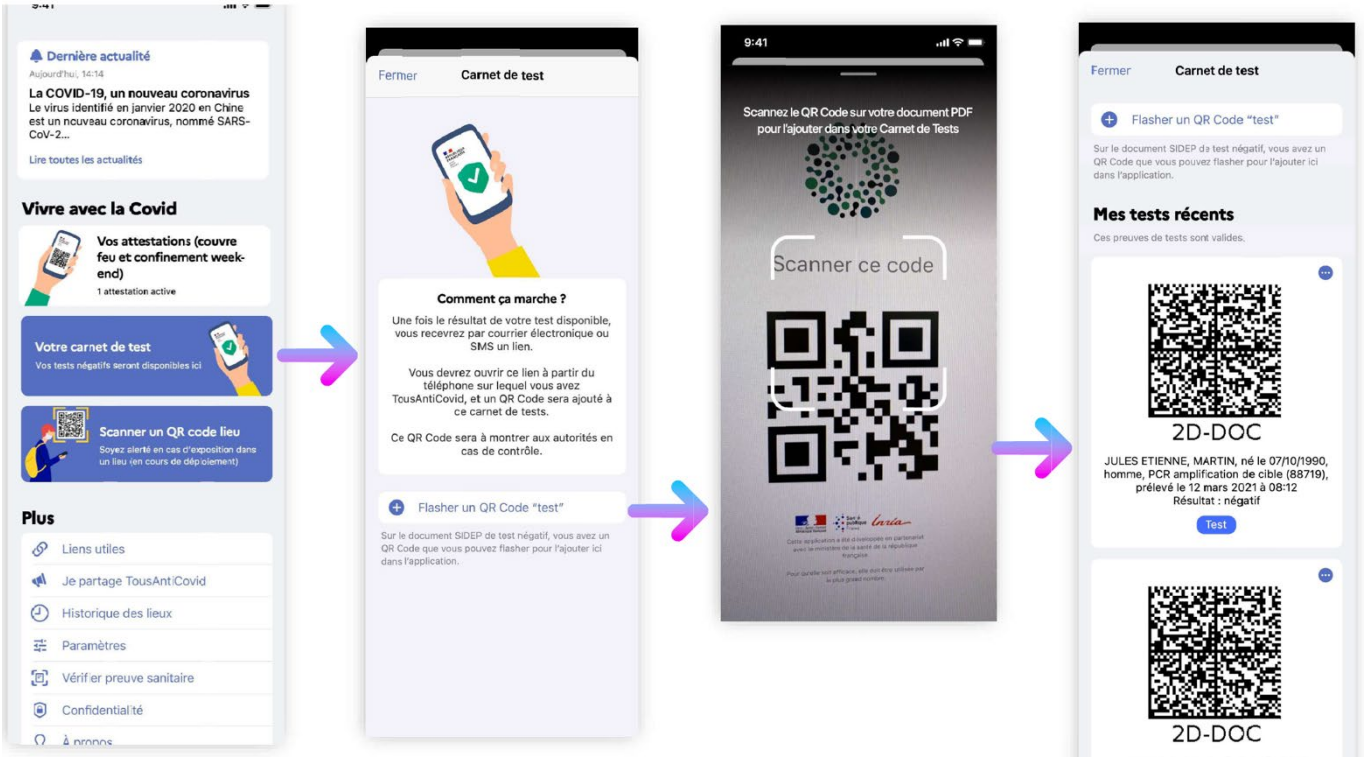






6.3.2 En scannant le QR Code sur le test SI-DEP

Le PDF de la certificat du Test Covid généré par SI-DEP présente un QR-Code qui contient également un deeplink pour l'ajout de ce certificat dans TousAntiCovid. L'utilisateur peut scanner ce QR Code avec TousAntiCovid.



6.4 Mesures de sécurité

Journalisation / Traçabilité

Le service TAC-V dispose de logs techniques permettant de réaliser des agrégats statistiques. Ces logs techniques ne sont accessibles qu'au service Exploitation d'IN Groupe et au Responsable de traitement (RT).

Pour chaque interrogation/ vérification, il est prévu de tracer :

- L'horodatage : date + heure + minutes du contrôle
- Résultat du contrôle
- Type d'équipement ayant réalisé le contrôle
- Type de 2D-Doc scanné

Ces traces sont anonymes et agrégées.

Archivage

Pas d'archivage dans le cadre de données de contrôles.

Sécurisation des documents papier (ACO)

Non applicable

Hébergement

L'ensemble des données ainsi que le portail d'interrogation seront hébergés dans les datacenters d'IN Groupe, sur le site de Flers-en-Escrebieux (59). Une infrastructure dédiée sera utilisée pour le projet TAC-V

Sécurisation de l'exploitation

Application de la « Procédure de gestion des vulnérabilités techniques et des correctifs de sécurité » IN Groupe pour les serveurs Linux.

- Veille en vulnérabilités basée sur l'outil de veille Argos d'Orange Cyberdefense animée par l'équipe SSI.
- Processus récurrent d'application des correctifs : sur la base des résultats d'un scan de vulnérabilité mensuel, application des correctifs permettant de corriger les vulnérabilités de niveau « critical » et « high », lors de la plage de maintenance mensuelle définie

- Processus d'application des correctifs en urgence : concerne la publication de vulnérabilités critiques ou majeures qui doivent être prises en compte avant la survenue de la prochaine campagne de patch périodique. Les alertes de ce type issues de la veille SSI doivent être traitées dans un délai d'1 mois maximum.

Lutte contre les logiciels malveillants

Application de la « Procédure de lutte contre les codes malveillants »

Stations d'administration :

Les stations d'administration sont positionnées sur un Vlan dédié ne disposant pas d'un accès direct à Internet. La protection contre les codes malveillants est réalisée via un antivirus basé sur des signatures.

Serveurs Linux :

Les serveurs Linux sont positionnés sur des vlan dédiés, sans accès direct à Internet. Ils ne sont pas couverts par un antivirus.

Gestion des postes de travail

Les postes de travail IN Groupe accédant à la plateforme sont des stations d'administration (sur un Vlan dédié sans accès à Internet)
Ces stations sont déployées selon le guide de durcissement Windows 10 défini par IN Groupe, qui contient notamment les règles suivantes :

- Durcissement de la configuration du BIOS (protection par mot de passe fort)
- Authentification forte par carte à puce
- Désactivation permanente de Cortana
- Désactivation de tous les paramètres concernant la confidentialité
- Activation du Pare-feu Windows
- Verrouillage automatique des comptes après 15 min d'inactivité
- Application d'une stratégie de mot de passe forte

Protection des sites web

Les développements, incluant les portails ouverts sur Internet, sont réalisés selon les standards de développement sécurisés IN Groupe qui intègrent notamment les recommandations de l'ANSSI et le Top10 de l'OWASP.
Des tests d'intrusion sont systématiquement réalisés avant mise en production et ouverture sur Internet.

Sauvegarde des données

Les sauvegardes des serveurs sont réalisées selon la « Procédure de sauvegarde et de restauration IN Groupe ».
Elles sont réalisées via l'outil Rubrik et sont de type « Incremental forever ». Une sauvegarde complète est donc assurée à l'initialisation d'une nouvelle sauvegarde, puis une sauvegarde incrémentale est réalisée en fonction de la politique appliquée.
Politique de sauvegarde appliquée :

- Un backup par jour pendant 7 jour – rétention des 7 derniers jours
- Un backup par semaine pendant 5 semaines – rétention des 5 dernières semaines
- Un backup par mois pendant 1an – rétention des 12 derniers mois
- Un backup par an pendant 2 ans– rétention des 2 dernières années

Ces sauvegardes sont stockées sur les boîtiers Rubrik chiffrés, hébergés dans les datacenters IN Groupe.

Maintenance

La maintenance physique des équipements est gérée par du personnel IN Groupe. Aucune maintenance à distance n'est autorisée.
Seuls les postes sur un réseau spécifique (administration) sont autorisés à se connecter aux serveurs.
Les disques défectueux sont conservés afin d'être détruits de manière sécurisée annuellement.

Sécurisation des canaux informatiques

Les réseaux sont dédiés au projets en s'appuyant sur une segmentation logiques d'équipements physiques mutualisés. En terme de sécurité logique, en accord avec la PSSI, généralement est mise en œuvre une approche 3 tiers.
L'architecture 3-tiers a pour objectif d'augmenter le niveau de sécurité de la bulle de production en mettant en œuvre le concept de la défense en profondeur et en distribuant les différentes briques applicatives sur trois niveaux différents :

- Les serveurs accessibles du web seront localisés en tiers 1 sécurisé par un cluster firewall dénommé FrontEnd qui lui-même sera connecté à un second cluster firewall localisé en tiers 2 et dénommé Middle-End,
- Les Serveurs d'Application (SA) seront localisés en tiers 2 sécurisé par un cluster firewall dénommé MiddleEnd qui lui-même sera connecté au cluster firewall localisé Front-End et à un troisième cluster firewall localisé en tiers 3 dénommé Back-End,

- Les serveurs de Base De Données (BDD) seront localisés en tiers 3 dans des zones distinctes et sécurisées par le cluster firewall Back-End qui lui-même sera connecté au cluster firewall Middle-End,

Chaque cluster firewall dispose de sa propre politique de sécurité qui autorise les flux selon les différents niveaux et les besoins applicatifs.
Une rupture technologique de firewall est implémentée au moins entre le cluster firewall Front-End et le cluster firewall Middle-End.
Les technologies utilisées sont Stormshield et Cisco.

Surveillance

Les firewalls utilisés disposent d'un système de prévention d'intrusion qui assure le filtrage des flux ainsi que leur analyse, dès les couches de transport jusqu'aux couches applicatives. Il applique des contrôles génériques de conformité, ainsi que des contrôles ciblés et comportementaux.
Des templates et des guides de configurations sont à disposition des équipes Réseau pour assurer une configuration homogène des équipements.
Un outil de la suite SolarWinds, Kiwi Cat Tools, permet de planifier des sauvegardes automatiques et d'appliquer des modifications globales aux configurations. Des comparaisons et analyse de la configuration peuvent être effectuées.
Des rapports sont générés pour surveiller d'éventuels anomalies.
Le SOC supervise notre système d'information et veille à la sécurité en surveillant les flux réseaux. Il collecte certaines informations, analyse et détecte des failles de sécurité.

Les équipements réseaux d'IN Groupe sont mis à jour dans plusieurs cas :

- La dernière version ou la version préconisée par le constructeur/éditeur est mise en place lors d'une nouvelle installation. L'équipe réseau regarde les « release note » et les contraintes à respecter.
- Lors d'un remplacement d'un équipement le service réseau installe le nouvel équipement avec l'une des dernières versions.
- Si un dysfonctionnement est constaté à cause d'un bug ou si un service n'est plus opérationnel, une intervention est prévue au plus vite pour remettre le service opérationnel. L'activation d'une gestion de crise est alors déclenchée.
- Lorsqu'il est possible d'intervenir sur les équipements réseaux en production, nous maintenons ceux-ci à jour pour corriger certaines failles de sécurité.

Quelques éléments sur la veille sécurité effectuée :
L'équipe réseau est alertée sur les vulnérabilités par plusieurs moyens et par plusieurs sources :

- Par la SSI qui nous transmet des versions conseillées sur les équipements, elle nous diffuse aussi les précautions à prendre en compte, alertes par le SOC.
- Par les éditeurs, constructeurs et revendeurs qui nous envoient les vulnérabilités détectées sur nos solutions.
- Nos solutions qui nous avertissent et préconisent une version plus à jour par rapport à celle installée.
- Communication intra et inter services.
- Réseaux sociaux, inscription sur des blogs techniques, webinars, etc…
- Recherches personnelles, veille technologique, etc..
- Formations annuelles.

Les mises à jour installées sur les équipements réseaux sont donc choisies soigneusement selon les besoins réels pour mener à bien l'activité de l'entreprise.

Sécurité physique contrôle des accès physiques

Les systèmes informatiques, les terminaux des opérateurs et les ressources d'information du site sont stockés dans des zones dédiées, physiquement protégées contre les accès non autorisés, la destruction ou la perturbation des activités.
Ces emplacements sont surveillés.
Chaque entrée et sortie est enregistrée dans le journal des événements (journaux système), une source d'électricité stable est fournie et la température est également surveillée et contrôlée.
L'accès physique au site est contrôlé et surveillé par un système intégré.
Une réception est ouverte 24h / 24 avec des agents de sécurité.
Un système de vidéosurveillance interne enregistre les actions dans tous les domaines critiques.
Le système est surveillé en permanence.
Si une alarme de sécurité se déclenche, une équipe d'intervention peut arriver sur place en quelques minutes.
Les systèmes de site disposent de systèmes de prévention des incendies, de systèmes de détection des intrusions et d'une alimentation électrique en cas d'urgence.
Les visiteurs du site doivent être accompagnés en permanence par des personnes autorisées.
L'accès au site n'est autorisé que par le personnel accrédité.
Les droits d'accès sont appliqués à l'aide de cartes et de lecteurs montés à côté du point d'accès.
Chaque entrée et sortie dans / depuis la zone est automatiquement enregistrée dans le journal des événements.

Gestion des accès sur le site IN Groupe :
Les services de génération des clés et des certificats sont hébergés dans une zone sécurisée, protégée par un périmètre de sécurité défini, avec des barrières de sécurité et des contrôles d'accès appropriés pour empêcher les accès non autorisés, les dommages et les interférences.

Les mesures de sécurité du site font l'objet de contrôles périodiques par les services de l'Etat français dédiés à la sécurité. Compte tenu de sa mission au profit de l'Etat français, IN Groupe bénéficie d'un appui institutionnel sécuritaire privilégié (réseaux de veille-alerte, soutien en situations de crise, réactions d'urgence, etc.). De ce fait, l'accès au site d'exploitation est hautement sécurisé (journalisation des accès, vidéo-protection).
Au sein de ce site, les activités sont cloisonnées dans différentes zones dont l'accès est soumis à habilitation/authentification.

Au niveau du site du site différents périmètres de sécurité sont constitués :

- Périmètre Niveau 0 : Zone Public
- Périmètre Niveau 1 : Zone Sécurisée
- Périmètre Niveau 2 : Zone de Haute Sécurité
- Périmètre Niveau 3 : Zone de Très Haute Sécurité

L'accès à ces différentes zones nécessite un badge (puce sans contact NXP Mifare Desfire 70pF EV1 v01.04 8k + puce contact morpho idealcityz version 1.6.0 Application IAS ECC) et des habilitations ad-hoc.
Les demandes d'accès des visiteurs s'effectuent au moins 48h à l'avance.
Tous les visiteurs sont criblés par la Préfecture.
Une vérification d'identité est effectuée sur présentation d'un justificatif d'identité (CNI ou passeport) en cours de validité.
Des sécurités spécifiques sont mises en place sur chacun des périmètres :

- Grillage périphérique + portails et portillons pour accéder dans la Zone Public (Périmètre Niveau 0)
- Vérification d'identité + signature d'une clause de confidentialité + attribution d'un badge qui doit être porté de manière visible avant de pouvoir se présenter à l'entrée de la Zone Sécurisée
- Dispositif anti-bélier + clôture électrique +Tourniquet pleine hauteur avec passage individuel par badge pour pouvoir pénétrer dans la Zone Sécurisée (Périmètre Niveau 1)
- Sas avec passage individuel des personnes contrôlées + correspondance biométrique pour accéder en Zone de Très Haute Sécurité (Périmètre Niveau 3)

Sécurité des matériels

La mise au rebut des matériels informatique est réalisée selon la « Procédure de mise au rebut des matériels informatiques IN Groupe ». Ce processus est sous contrôle du service sûreté du Groupe. La destruction est assurée sur site ou hors site par broyage ou incinération, en présence de 2 membres du service Sûreté du Groupe.

Eloignement des sources de risques

La zone d'implantation n'est pas exposée aux risques d'inondation (PPRN : non)
La zone d'implantation n'est pas impactée par les mouvements de terrain
Exposition faible au risque de séisme
1 site SEVESO à proximité de l'installation (périmètre : 1000m)
Source : https://www.georisques.gouv.fr/ (le détail du descriptif des risques est disponible auprès de la direction du site d'hébergement de la base de données de Flers-en-Escrebieux))

Protection contre les sources de risques non humaines

Présence 7/7 H24 équipe sureté formé SSIAP1 (Intervention Incendie).
Process Industriel / Stocks matières premières sur détection et extinction SPRINKLER (Certification APSAD)
Process Industriel Sensible / Coffres - Détection incendie par équipement VESDA (détection précoces) report alarme poste de sécurité
Datacenter – Détection et extinction Gaz (ARGON 55)
Zone Tertiaire – Détection fumée et extinction sprinkler
Suivi, contrôle et réglementation des extincteurs et RIA sur l'ensemble du site

Alimentation électrique du Site sur antenne par réseau ERDF.
1 poste de livraison 20000V sur le site, 2 câbles 20000 alimentant le site
3 postes de transformation HT – BT
Système de sureté, Datacenter, télécom sur secourus (Onduleur, Groupe électrogène) avec capacité autonomie de 96h

Organisation de la politique de protection des données – Supervision

IN Groupe a nommé un DPO depuis le 1er janvier 2017
Une gouvernance et des procédures ont été déployées afin d'encadrer la gestion de la protection des données au sein des activités

d'IN Groupe. Chaque nouveau projet fait l'objet d'une analyse de risques, identifiant notamment si un projet à vocation à traiter des données à caractère personnel et orientant – si c'est le cas – vers le DPO pour analyse et participation à la construction du projet.
Un programme de formation et de sensibilisation est dispensé aux personnels (au moins 1 fois par an et à chaque nouvel arrivant)

Gestion de la politique de protection de la vie privée et des libertés

IN Groupe a plusieurs chartes informatiques selon le profil des utilisateurs (intervenants internes, externes, administrateurs) qui traitent notamment de la protection de la vie privée et des libertés. Ces chartes font parties de la PGSSI et ne sont visibles que dans le cadre d'un audit sur site. IN Groupe a également une politique de protection des données à caractère personnel disponible sur son site internet (www.ingroupe.com)

Gestion des incidents de sécurité

Une procédure de gestion des incidents de sécurité / violation de données à caractère personnel est diffusée et appliquée (consultable sur site dans le cadre d'un audit)
Un registre des violations de données à caractère personnel est tenu à jour.

Gestion des personnels

Chaque nouvel arrivant au sein de IN Groupe suit un e-learning de sensibilisation au traitement de données.
Les fonctions qui sont amener à traiter / manipuler des données dans le cadre de leurs activités ont été formé au RGPD et aux obligations imposées par cette règlementation.
Les fonctions métiers qui traitent spécifiquement des données à caractère personnel (chefs de projet, service delivery managers, …) ont été formés à l'utilisation de l'outil de PIA de la CNIL.

Gestion des tiers accédant aux données – Contrats de sous-traitance

Toutes les relations de sous-traitance dans le cadre d'un traitement de données font l'objet d'une contractualisation (article 28.3 du RGPD), qui porte notamment sur :

- L'objet et la durée du traitement
- La nature et la finalité du traitement
- Le type de données et les catégories de personnes concernées
- Les obligations et droits du responsable de traitement
- Les obligations et missions d'assistance du sous-traitant
- Le sort des données à l'issue du traitement
- Les conditions de sous-traitance de 2nd rang
- Et le cas échéant, les conditions de transfert de données en dehors de l'UE