AIPD - Passe sanitaire

Version mise à jour le 13 aout 2021

1 Contexte

1.1 Vue d'ensemble

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

Afin de permettre aux personnes concernées de prouver leur état sanitaire en présentant l'un des trois certificats autorisés (test PCR ou antigénique, certificat de rétablissement ou certificat vaccinal) face à la Covid-19, lors d'un contrôle par une personne physique habilitée, il a été décidé de développer cinq applications permettant de vérifier l'émetteur et l'authenticité des certificats présentés par les personnes souhaitant voyager ou participer à un événement intérieur ou extérieur regroupant plus de 1000 personnes.

L'application mobile TousAntiCovid Verif

Cette application a été développée à la demande de la DGS par la société IN Groupe pour permettre aux professionnels autorisés par les décrets d'application liés au passe sanitaire (ci-après les « Professionnels ») suivants : les exploitants de services de transport de voyageurs, les personnes chargées du contrôle sanitaire aux frontières, les responsables des lieux et établissements de loisirs et de culture ou les organisateurs des évènements, rassemblant plus de 50 personnes (salles de spectacles, les parcs d'attraction, les salles de concert, les festivals, les salles de sport, les cinémas, …) :

- d'identifier l'organisme émetteur et l'intégrité des données contenues dans le code à barres 2D-DOC ou DCC d'un certificat de vaccination, de rétablissement à la Covid 19 ou d'un résultat de test ;
- d'interpréter ces éléments aux regards des règles sanitaires applicables (dans l'hexagone ou en fonction de la destination de voyage envisagée) ;
- de réaliser des statistiques d'usage, sans aucune donnée à caractère personnel, par les opérateurs de transport dans le cadre de la facturation du sevrice à ces derniers. Ces éléments ont d'ailleurs été vérifié par la CNIL lors d'un audit.

Portail Web pour la Police aux Frontières et les douanes

La police aux Frontières n'étant pas équipées de smartphone, mais d'ordinateurs équipés de lecteurs laser (douchettes), il a été demandé à IN Groupe, par la Direction Générale de la santé et pour le compte du Ministère de l'Intérieur, de développer un portail web disposant des mêmes fonctionnalités que l'application mobile TousAntiCovid Verif OT. Ce portail sera également disponible pour les agents des douanes ne disposant pas d'un smartphone.

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

Ce service, développé par IN Groupe, permet à TousAntiCovid de demander la conversion d'un code à barre 2D-DOC vers le format certificat Covid numérique de l'Union Européenne (DCC) ou plus tard, vers un format international (IATA, OACI, WHO par exemple). Cette opération est réalisée par l'intermédiaire d'un appel à une API hébergée chez IN Groupe.

Côté SI-DEP et VACCIN-COVID, un mécanisme interne de conversion a été également mis en place pour permettre la conversion des 2D-DOC en certificat Covid numérique de l'UE.

La passerelle européenne (DCCG)

Cette passerelle permet aux pays membre de l'Union Européenne d'obtenir les certificats et les clés publiques émis par les autres pays afin de vérifier l'identité de l'organisme émetteur du certificat ainsi que l'intégrité des données contenues dans le code à barres du certificat de vaccination, de rétablissement à la Covid-19 ou du test de dépistage à la Covid-19 produit par un de ces pays. Sur celle-ci en vue du contrôle de la validité des certificats émis par les différents pays européens figure une liste s de révocation des certificats.

Le module Carnet de l'application TousAntiCovid

Le module Carnet entre dans le dispositif « Passe sanitaire » **au même titre** que les documents au format numérique ou papier. Le module permet à son utilisateur de conserver de façon sécurisée et dans un format numérique signé, ses certificats de vaccination ou résultats de tests ou de rétablissement à la Covid-19 ou résultats de tests. Il permettra également de convertir les certificats au format 2D-DOC en certificats Covid numérique de l'Union Européenne.

Dispositif pour les français à l'étranger

Dans le cadre de la demande de pass sanitaire pour les français de l'étranger et leurs ayants droit situés hors de l'EU), le ministère de l'Europe et des Affaires Etrangères à sollicité le ministère de la santé pour pouvoir réaliser la production de DCC relative aux preuves de vaccination ou de recouvrement transmises par les personnes selon les modalités indiquées sur « démarches simplifiées »

La présente **AIPD est dédiée aux applications ou portail utilisés dans le cadre du Passe sanitaire**

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 certificat Covid numérique de l'Union Européenne dit DCC dont l'objectif est de permettre, aux autorités de contrôle européennes de disposer d'un mécanisme commun pour contrôler, de manière fiable et sécurisée, tout document produit par les autorités d'un pays membre relatif à la Covid-19 qu'un citoyen européen circulant au sein de l'Union européenne, pourrait présenter.

La France s'inscrit pleinement dans cette démarche avec « le Passe sanitaire » et sa connexion avec la passerelle européenne (DCCG) afin d'identifier l'organisme émetteur, l'intégrité des données contenues dans le code à barres présentes dans les certificats de test de dépistage COVID-19 et de vaccination ainsi que l'application des règles sanitaires relatives à chaque Etat membre de l'Union Européenne.

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 numériques prouvant que la personne:

1. A été testée négative à la COVID-19,
2. S'est rétabli de la COVID-19,
3. A été vaccinée contre la COVID-19

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 (IATA, OACI, OMS etc.).

Il se traduit par la certification officielle des fiches de 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 signées de façon numérique, avec un code à barres 2D-DOC employé par l'Administration française pour certifier ses documents et notamment la nouvelle carte d'identité nationale.

Ceci permet de garantir l'intégrité du document électronique et d'en authentifier l'origine. 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, sera mise à disposition des entités autorisées de contrôle habilitées à vérifier les certificats de vaccination de rétablissement à la Covid-19 ou de tests négatifs (compagnies aériennes, police, douanes, etc.) contenus 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 de 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 était d'évaluer l'impact de ces contrôles sur la gestion des 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 Etats 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 code à barres 2D est de type QR code et non plus Datamatrix;
- L'organisation et le type des données diffèrent ;
- 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, doivent les convertir au format DCC s'ils veulent les voir reconnaitre sur le territoire européen. De manière générale 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 utilisé à partir de l'application TousAntiCovid Carnet pour convertir les certificats s'y trouvant.

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 sera interfacée avec un portail web accessible uniquement aux agents de la PAF qui ne sont pas dotés de smartphone, mais d'ordinateurs équipés avec des lecteurs de codes à barres. Cette application web devrait être disponible d'ici courant juillet 2021.

Les principaux enjeux du module du Passe 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 réduire l'erreur humaine et d'uniformiser l'interprétation des règles sanitaires ;

Les finalités du traitement sont

- permettre la reprise de diverses activités interrompues et la réouverture des lieux fermés en minimisant, dans la mesure du possible, les risques associés de contamination.
- de proposer un service simple et gratuit pour tous ;
- de garantir un accès égalitaire avec la possibilité d'obtenir son certificat en version papier comme 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 au sein du module Carnet de l'application TousAntiCovid.

1.1.2 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.
  - OVH : hébergement d'une copie des règles sanitaires afin de permettre une répartition de charge avec le datacenter d'IN Groupe.
  - Lunabee : développement de l'application TousAntiCovid et du Module Carnet ;
  - Akamai : fourniture d'une solution anti-DDOS et pare-feu applicatif (WAF) => ce dernier sera remplacé par Orange d'ici quelques semaines.
- **Destinataires**
  - Les utilisateurs du module TousAntiCovid Carnet qui enregistrent leur certificat numérique de vaccination ou de test ou de rétablissement à la Covid-19 ;
  - Les utilisateurs de l'application TousAntiCovid Verif qui scanneront les certificats numériques 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.

1.1.3 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

1.1.4 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 la mise en production.
- Référentiel SecNumCloud de l'ANSSI pour la partie infra
- Hébergement de Données de Santé (HdS)

1.2 Composants du Passe sanitaire

1.2.1 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[1]/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 du 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.

1.2.2 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, dans deux situations de contrôle :

- le passe sanitaire « activités » d'une part, s'agissant de l'accès à des évènements, lieux de loisirs ou culturels,
- Le passe sanitaire « voyage » d'autre part, s'agissant de la circulation au sein des pays membres de l'Union européenne (et à terme, à l'international).

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.

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

L'application fonctionne selon deux modes

- le mode « LITE », dans le cadre du passe sanitaire « activités » affichant le minimum d'information aux Professionnels (nom, prénom(s), date de naissance, résultat valide/non valide)
- le mode « OT » (opérateur de transport), dans le cadre du passe sanitaire « voyage » permettant l'affichage de plus d'information nécessaires afin de procéder à la validation du passe en fonction des règles qui peuvent être fluctuante dans les différents pays de destination.

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 seuls Professionnels limitativement prévues au décret n° 2021-724 du 7 juin 2021 (article 2, II, 1° et suivants). Chaque Professionnel s'engage à respecter les règles d'utilisation de l'application.
- Le Professionnel scanne un certificat au format 2D-DOC/DCC grâce au lecteur dans l'application ;
- Le certificat est traité en local dans le téléphone du Professionnel pour 3 opérations :
    - Vérification de la signature du certificat (une synchronisation quotidienne avec le serveur central permet la récupération de nouvelles clés publiques de signature) ;
    - Décodage du certificat ;
    - 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
- En mode « LITE », 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 affiché sur l'équipement du Professionnel;
- En mode « OT », le résultat du contrôle, sous la forme d'un statut bleu ou rouge, le nom, prénom et date de naissance du détenteur du certificat ainsi que le contenu du 2D-Doc ou DCC relatif à la preuve présentée, est affiché sur l'équipement du Professionnel;
- Aucun log identifiant le Professionnel ou son équipement n'est collecté ou généré : l'application fonctionne en local. A ce stade, aucune statistique n'est sont réalisée. La collecte de données statistique fait partie de la feuille de route des évolutions à venir au sein de l'application TousAntiCovid Verif;
- Aucune donnée personnelle n'est conservée 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)

1.2.3 Le portail web pour la Police aux Frontières et les douanes

Le portail web Tous AntiCovid Verif permet aux agents de la Police aux Frontières et les douanes 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 et les douanes n'étant pas équipées de smartphone, mais d'ordinateurs de bureau auxquels sont connectés des lecteurs de code à barres (douchettes).

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

- L'utilisation du portail web TousAntiCovid Verif est réservée aux seuls personnels de la Police aux Frontières et des douanes.
- Le Professionnel scanne un certificat au format 2D-DOC ou DCC grâce à un lecteur laser, et l'application Web fait usage d'une API à travers un canal sécurisé, après identification et identification de l'adresse IP appelant sur le serveur central d'IN Groupe. Seuls les équipements figurant sur le réseau du Ministère de l'Intérieur sont autorisés à accéder à la page d'authentification du portail Web.
- Le certificat est transmis au serveur central d'IN Groupe pour 3 opérations :
    - Vérification de la signature du certificat grâce à la clé publique qui est conservée chez IN Groupe,
    - Décodage du certificat,
    - Application des règles de gestion sanitaire spécifique au contexte « voyage ». Ce traitement est fait alternativement, pour des raisons de répartition de charge, chez IN Groupe ou OVH.
- 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 du Professionnel.

- Aucun log identifiant le Professionnel ou son équipement n'est collecté ou généré : l'application fonctionne en canal sécurisé par identification et reconnaissance d'adresse IP. Seuls des logs d'utilisation de l'API sont conservés (date/heure/minute/seconde, résultat du contrôle – motif, canal d'appel (API « Border-Portal »), type de preuve vérifiée)
- Aucune donnée personnelle n'est conservée ni dans l'équipement du Professionnel ni au niveau du serveur central.

1.2.4 Convertisseur de certificat 2D-DOC / DCC

Ce service, développé par IN Groupe, permet à l'application TousAntiCovid 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.

1.2.5 SI-DEP et VACCIN-COVID

Les personnes concernées peuvent se connecter au portail SI-DEP[2] et VACCIN-COVID[3] afin de récupérer les certificats de vaccination ou de test ou de rétablissement à la Covid-19 au format 2D-DOC/DCC.

1.2.6 Le 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 à caractère personnelle n'est transmise à ce portail

1.3 Données, processus et supports

1.3.1 Quelles sont les données traitées ?

Les données contenues dans le code à barres

1. Données dans un 2D-DOC

Données d'identification
- Prénom
- Nom
- Date de naissance

Certificat de vaccination
- Producteur du vaccin
- Type de vaccin
- Date d'injection
- Dose courante
- Dose totale attendue
- Statut du vaccin (en cours, fini)

Certificat de test
- Code du test (LOINC)
- Résultat du test
- Date du test

Données relatives au certificat de signature numérique
- Identifiant de l'autorité de certification
- Identifiant du certificat
- Date d'émission du document
- Date de création de la signature

2. **Dans un certificat covid numérique de l'UE (DCC)**

Données d'identification (commun aux preuves vaccinales et tests)
- Liste des prénoms
- Nom de famille
- Date de naissance

Certificat de vaccination

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

- Date du dernier état du cycle de vaccination (date de vaccination)
- Rang du dernier état de vaccination effectué
- Nombre de doses attendues pour un cycle complet
- Nom de la maladie couverte => (code SNOMED 840539006)
- Agent prophylactique => Il s'agit du type de vaccin, ce champ contient une valeur du code SNOMED représentant la technique du vaccin utilisé (Ex. SARS-CoV-2 mRNA vaccine, SARS-CoV-2 antigen vaccine)
- Nom du vaccin (COMINARTY/MODERNA/VAXZEVRIA/JANSSEN)
- Fabriquant (BIONTECH/MODERNA/ASTRAZENECAS/JANSSEN)

Test de dépistage

- Date et heure du prélèvement
- Résultat du test (Négatif/Positif)
- Type de test (Test Antigénique COVID)
- Nom de la maladie couverte
- Nom du test
- Appareil de test & Fabriquant
- Centre de test

Guérison

- Date du premier prélèvement positif
- Date de début de validité
- Date de fin de validité
- Nom de la maladie couverte (code SNOMED 840539006)

Données relatives au certificat de signature numérique (commun aux preuves vaccinales et tests)

- Pays
- Autorité de certification
- Identifiant du certificat

Les données affichées dans le module Carnet de TousAntiCovid

Les données contenues dans le module Carnet de l'application TousAntiCovid suite au scan d'un certificat de vaccination ou de test ou de rétablissement à la Covid-19 d'une personne concernée sont les suivantes :

- Liste des prénoms
- Nom de famille du patient
- Date de naissance du patient
- Certificat de vaccination
  - Producteur du vaccin ;
  - Type de vaccin ;
  - Date d'injection ;
  - Dose courante ;
  - Dose totale attendue ;
  - Statut du vaccin (en cours, fini).
- Certificat de test
  - Code du test (LOINC) ;
  - Résultat du test ;
  - Date du test.
  - Date de prélèvement
  - Information expiration
  - Résultat du traitement : test non PCR/Valide/Non Valide

Les données affichées dans l'application TousAntiCovid Verif

- **TousAntiCovid Verif Lite (dans le cadre des lieux et établissement de loisirs ou culturels ou événements rassemblant plus de 50 personnes)**
    - Liste des prénoms
    - Nom de famille du patient
    - Date de naissance du patient
    - Résultat du traitement : test non PCR/Valide/Non Valide
- **TousAntiCovid Verif OT (utilisée par les opérateurs de transports, la PAF et les douanes)**
    - Liste des prénoms
    - Nom de famille du patient
    - Date de naissance du patient
    - Certificat de vaccination
        - Producteur du vaccin ;
        - Type de vaccin ;
        - Date d'injection ;
        - Dose courante ;
        - Dose totale attendue ;
        - Statut du vaccin (en cours, fini).
    - Certificat de test
        - 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 ;

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 contenues dans le code à barres 2D-DOC.

Données traitées par la passerelle européenne DCCG

La passerelle européenne DCCG ne traite que les certificats et les clefs publiques produites par les Etats membre.

1.3.2 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, 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 du Professionnel 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 du Professionnel et aucune capture d'écran n'est possible lorsque l'application mobile est en fonction. L'application se contente de lire les informations contenues dans le code à barres 2D-DOC/DCC et de les afficher sur l'écran du Professionnel. 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.
- Deux cas se présente selon la version de l'application
  - Version Lite et OT
    - La règle sanitaire est traitée localement
  - Version plateforme Web (PAF et douane)
    - La règle sanitaire est traitée côté serveur IN GROUPE ou OVH après vérification de l'émetteur et de l'intégrité des données transmises.
    - Le résultat est ensuite renvoyé à l'application TousAntiCovid Verif

- **Conversion du certificat au format DCC** uniquement si le certificat d'origine est au format 2D-DOC et signé par l'Etat Français.

  L'utilisateur de l'application TousAntiCovid peut demander la génération d'un certificat au format DCC, depuis le module Carnet de TousAntiCovid.

  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[4] (format utilisé par le DCC), signature de ce format par IN Groupe, et envoi de la chaine à TousAntiCovid Carnet.

  Aucune donnée n'est stockée par l'outil de conversion, l'appel et la réponse se font dans un temps système. Aucun log applicatif ou relatif au contenu des requêtes au serveur de conversion n'est conservé

1.3.3 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.
- **Serveur antiDDOS**
  Serveur WAF

2 Principes fondamentaux

2.1 Proportionnalité et nécessité

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

La finalité du traitement déterminée et explicite est de permettre aux personnes concernées de donner une information sur son état de santé en présentant un certificat de vaccination ou résultats de tests ou de rétablissement à la Covid-19, lors d'un contrôle par une personne habilitée à réaliser ces contrôles.

Ce contrôle peut se faire par la présentation d'un certificat apposé sur un document papier, numérique ou enregistré dans le module Carnet de l'application TousAntiCovid.

[4] Concise Binary Object Representation

Cette finalité est légitime, elle est décrites dans le décret n° 2021-724 du 7 juin 2021.

2.1.2 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.

2.1.3 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) ?

Depuis le 8 juin au soir pour la version Android et du 10 juin soir pour la version iOS, TousAntiCovid Verif Lite fonctionne en mode hors-ligne sans transmettre de données personnelles aux serveurs d'IN Groupe.

En raison du risque potentiel de corruption du code source (disponible sur le Gitlab Inria), il a été jugé opportun de ne pas mettre en œuvre une interconnexion entre l'application TousAntiCovid avec les SI SI-DEP et VACCIN-COVID.
En revanche, dans le cadre d'un appel à la règle sanitaire (TousAntiCovid Verif LITE / OT/ Plateforme web pour la PAF) ou à la conversion (module Carnet de l'application TousAntiCovid), ce risque est nul car aucune donnée de santé n'est hébergée sur les serveurs d'IN Groupe ou OVH.

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

L'exactitude des données repose sur le fait que le certificat d'un certificat de vaccination ou de test ou de rétablissement à la Covid-19 a été produit et signé par SI-DEP et VACCIN-COVID afin de permettre aux personnes habilitées de vérifier l'émetteur du certificat et l'intégrité des données transmises.
Concernant l'actualisation des données, il est de la responsabilité de l'utilisateur de reprendre contact avec le centre de vaccination ou de dépistage afin de récupérer ensuite et auprès de SI-DEP ou VACCIN-COVID, une version actualisée de son certificat papier, numérique qu'il lui appartient de ré-enregistrer dans le module Carnet de l'application TousAntiCovid.

2.1.5 Quelle est la durée de conservation des données ?

L'utilisation du passe sanitaire est aujourd'hui autorisée au plan juridique jusqu'au 30 septembre 2021 par la loi de gestion de la sortie de crise sanitaire

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 le Professionnel 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 du Professionnel pendant 20 secondes.
Elle et ne permet pas le stockage des informations sur le téléphone mobile du Professionnel utilisant TousAntiCovid Verif.

2.2 Mesures protectrices des droits

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

Sur le site web du Ministère et des campagnes de communication

Une description du traitement figurera sur la page https://solidarites-sante.gouv.fr/ministere/article/donnees-personnelles-et-cookies du Ministère de la santé et des solidarités et sur https://www.gouvernement.fr/info-coronavirus/pass-sanitaire

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. Un kit de communication est disponible et est diffusé auprès de l'ensemble des Professionnels utilisant l'application de contrôle TousAntiCovid Verif, afin de les aider à informer les personnes concernées.

2.2.2 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 au Professionnel un document papier, un document numérique ou sa représentation dans le Carnet TousAntiCovid mais toujours en accord avec elle.

2.2.3 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.

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

Durant les 3 mois suivant son enregistrement dans le SI-DEP et VACCIN-COVID, la personne concernée ne peut exercer son doit à l'effacement en raison de l'obligation légale de conservation liée aux décrets respectifs des SI précédemment mentionnés. En revanche, il lui est possible de supprimer à tout moment l'ensemble de ses certificats en sa possession (papier, numérique ou Carnet dans l'application TousAntiCovid

En ce qui concerne l'application TousAntiCovid Verif, et étant donné qu'aucune information n'est stockée, ce droit de rectification et d'effacement n'a pas de mise en œuvre pratique.

2.2.5 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 exercer son droit d'opposition ou de limitation en effaçant ses certificats enregistrés dans le module Carnet de l'application TousAntiCovid ou en ne demandant pas leurs conversions.

Pour l'application TousAntiCovid Verif

La personne concernée peut s'opposer à ce que ces certificats soient vérifiés ou convertis, avec le risque qu'elle ne puisse alors pas accéder à un lieu ou un établissement de loisir ou culturel, participer à un événement ou voyager.
De plus, ces droits peuvent difficilement s'appliquer du fait que le traitement se termine dès que le résultat disparaît de l'écran de l'utilisateur de TousAntiCovid Verif.

2.2.6 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 a été signé entre Inria et IN GROUPE

2.2.7 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

- **Pour le module Lite et OT**
    - Aucun transfert de données à caractère personnel.

- **Pour la plateforme Web (PAF et douane)**

  Un transfert de données hors UE peut avoir lieu lors de l'utilisation d'Akamai (en cours de portage vers la solution équivalente d'Orange)
    - Pour toutes les requêtes effectuées en métropole, ce seront les serveurs français ou UE qui répondront
    - Si la requête est réalisée depuis un territoire outre-mer, c'est un serveur hors UE qui pourra répondre.

  Actuellement, les contremesures mises en place sont les suivantes
    - Rédaction d'un accord RGPD entre IN Groupe et Akamai conforme suite à l'invalidation Privacy Shield 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.

3 Risques

3.1 Mesures existantes ou prévues

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

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

3.2 Analyse de risque

Cette analyse porte sur l'utilisation du module Carnet de l'application TousAntiCovid, l'application TousAntiCovid Verif, la plateforme Web (PAF et douane) et le convertisseur 2D-DOC / DCC

.

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
        - Interception des données en transit
        - Vol des documents contenant les 2D-DOC ou DCC sous sa forme numérique ou papier
        - Intrusion dans les serveurs d'IN Groupe ou OVH
        - Altération du code des applications
        - Diffusion d'une application TousAntiCovid Verif 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
        - Personnels interne au projet et ayant accès au système
        - Personnels en charge du contrôle
        - Cybercriminel
        - Hackeur amateur
    - Mesures contribuant à traiter ou limiter le risque
        - Cloisonnement
        - Sécurisation des canaux informatiques
        - Sécurisation matérielle
        - Contrôle des accès logiques
        - 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 / limité / Important / Maximale)
        - Importante
    - Vraisemblance du risque
        - Importante
    - Plan d'action
        - Passage de l'application en mode « hors-ligne »
        - Communication auprès des autorités de contrôle
    - Révision des échelles de gravité et vraisemblance
        - Gravité: importante
        - La vraisemblance du risque devient limitée
- **Modification non désirée des données**
    - Impact sur les personnes concernées
        - Atteinte à liberté de mouvement en ne permettant pas l'accès à un évènement, à un moyen de transport.
        - Sentiment d'intrusion dans la vie privée
        - Affectation psychologique mineure de type diffamation/réputation.
        - Difficultés relationnelles avec l'entourage personnel comme professionnel
        - Atteinte à la vie privée
        - 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
        - Interception des données en transit avec altération à la volée
        - Altération malveillante du 2D-DOC ou DCC sous sa forme numérique ou papier
        - Altération malveillante des règles sanitaires
        - Altération du code des applications
        - Vol des éléments cryptographiques
    - Sources de risque
        - Personnels interne au projet et ayant accès au système
        - Personnels en charge du contrôle
        - Cybercriminel
    - Mesures contribuant à traiter ou limiter le risque
        - Cloisonnement
        - Sécurisation des canaux informatiques
        - Sécurisation matérielle
        - Contrôle des accès logiques
        - Audits de code
        - Tests d'intrusion
        - Journalisation
        - Gestion des postes de travail d'IN Groupe
        - 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 / limité / Important / Maximale)
        - Importante
    - Vraisemblance du risque
        - Limitée
    - Plan d'action
        - Passage de l'application en mode offline
    - Révision des échelles de gravité et vraisemblance
        - Gravité reste: importante
        - La vraisemblance reste Limitée
- **Disparition des données**
    - Impact sur les personnes concernées
        - Impossibilité de participer à un événement rassemblant plus de 1000 personnes ou de voyager
        - Démarches pour obtenir un duplicata de son certificat (si perte locale)
        - Réalisation d'un test RT-PCR pour les personnes non vaccinées
    - Menaces permettant réalisation du risque
        - Suppression des données figurant dans SI-DEP et VACCIN-COVID
        - Incendie dans les datacenters
        - Vol des serveurs

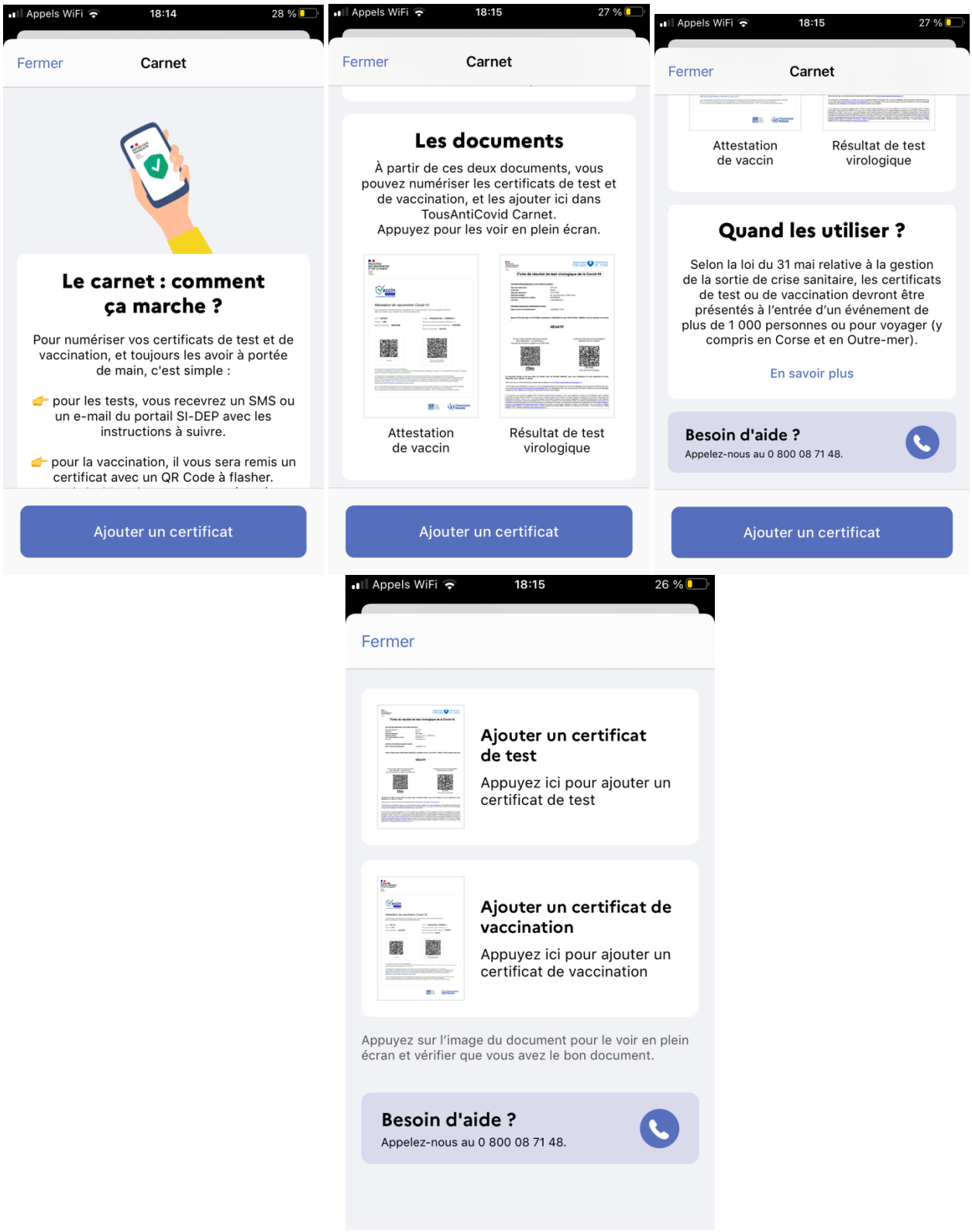
      Mesures contribuant à traiter ou limiter le risque
        - Cloisonnement
        - Sécurisation des canaux informatiques
        - Sécurisation matérielle
        - Contrôle des accès logiques
        - Audits de code
        - Tests d'intrusion
        - Journalisation
        - Gestion des postes de travail d'IN Groupe
        - 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)
        - Importante
    - Vraisemblance du risque
        - Limitée
    - Plan d'action
        - Du fait que le certificat est transmis, via SI-DEP et VACCIN-COVID, sous une forme papier ou numérique, la seule mesure que nous pouvons indiquer et de demander aux patients de les conserver précieusement même si nous serions en capacité d'en transmettre une copie dans la limite des 3 mois pour les tests de dépistage. La personne devra alors réaliser un nouveau test RT-PCR.

4 Annexes

4.1 Information des personnes concernées

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

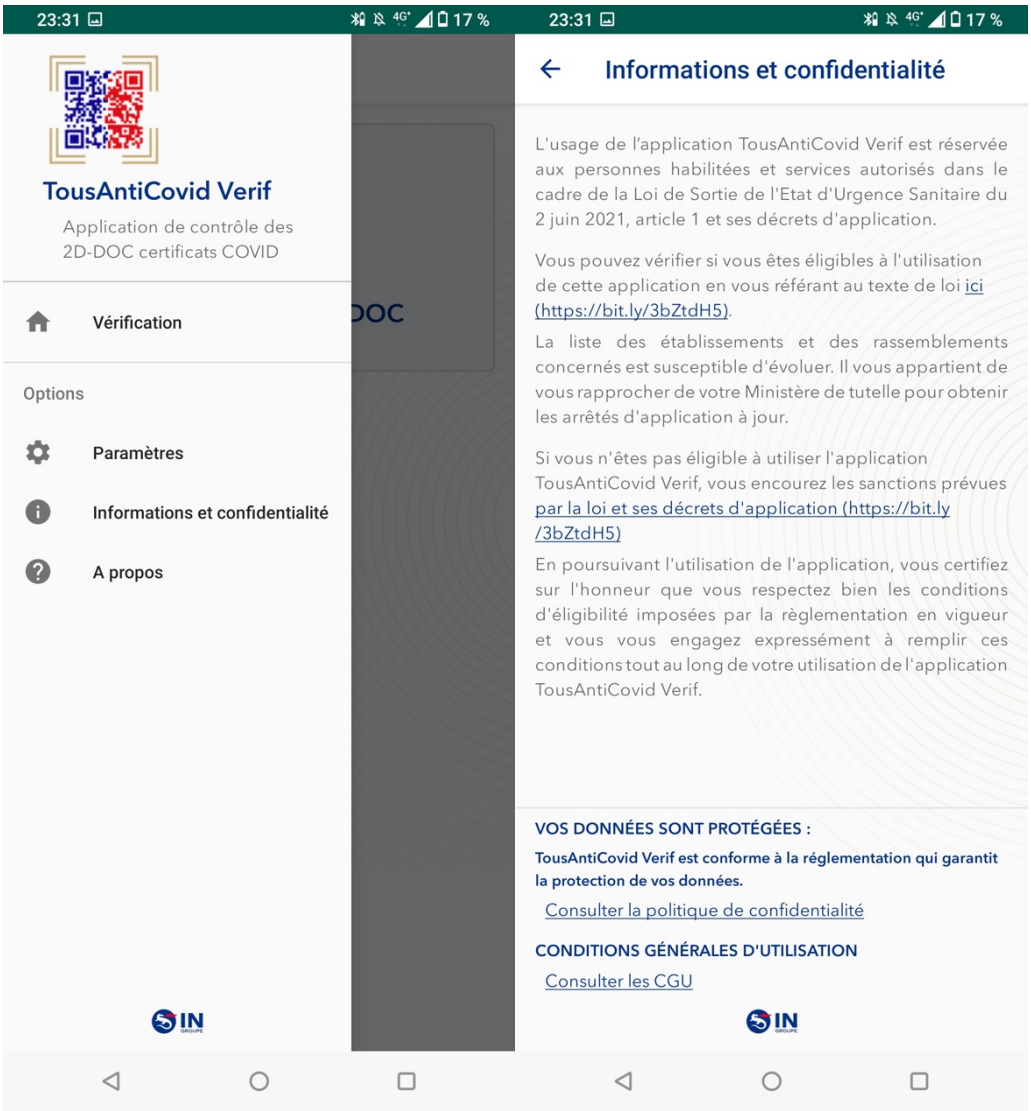
NB : Ces écrans de travail sont donnés à titre indicatif car ils sont amenés à évoluer



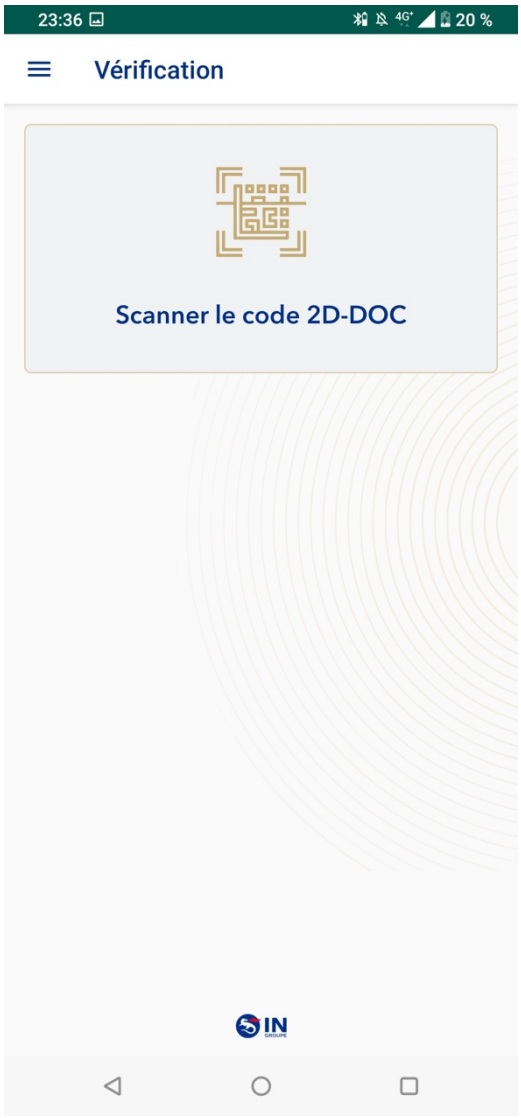
4.1.2 Écrans de travail de l'application TousAntiCovid Verif

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



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



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


18:47
Scan du 2D-DOC Résultat
Non valide
Informations du 2D-DOC
LISTE DES PRÉNOMS DU PATIENT
JEAN PIERRE
NOM DE FAMILLE DU PATIENT
THEOULE SUR MER
DATE DE NAISSANCE DU PATIENT
31/05/1962
18:47
Scan du 2D-DOC Résultat
Valide
Informations du 2D-DOC
LISTE DES PRÉNOMS DU PATIENT
JEAN-PIERRE
NOM DE FAMILLE DU PATIENT
AZAY LE RIDEAU
DATE DE NAISSANCE DU PATIENT
04/08/1952

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

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

4.2.1 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 :

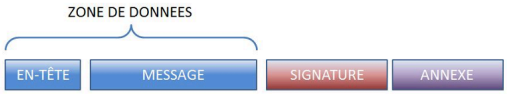
•La **zone des données** qui est elle-même composée de deux sous-parties :

-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.



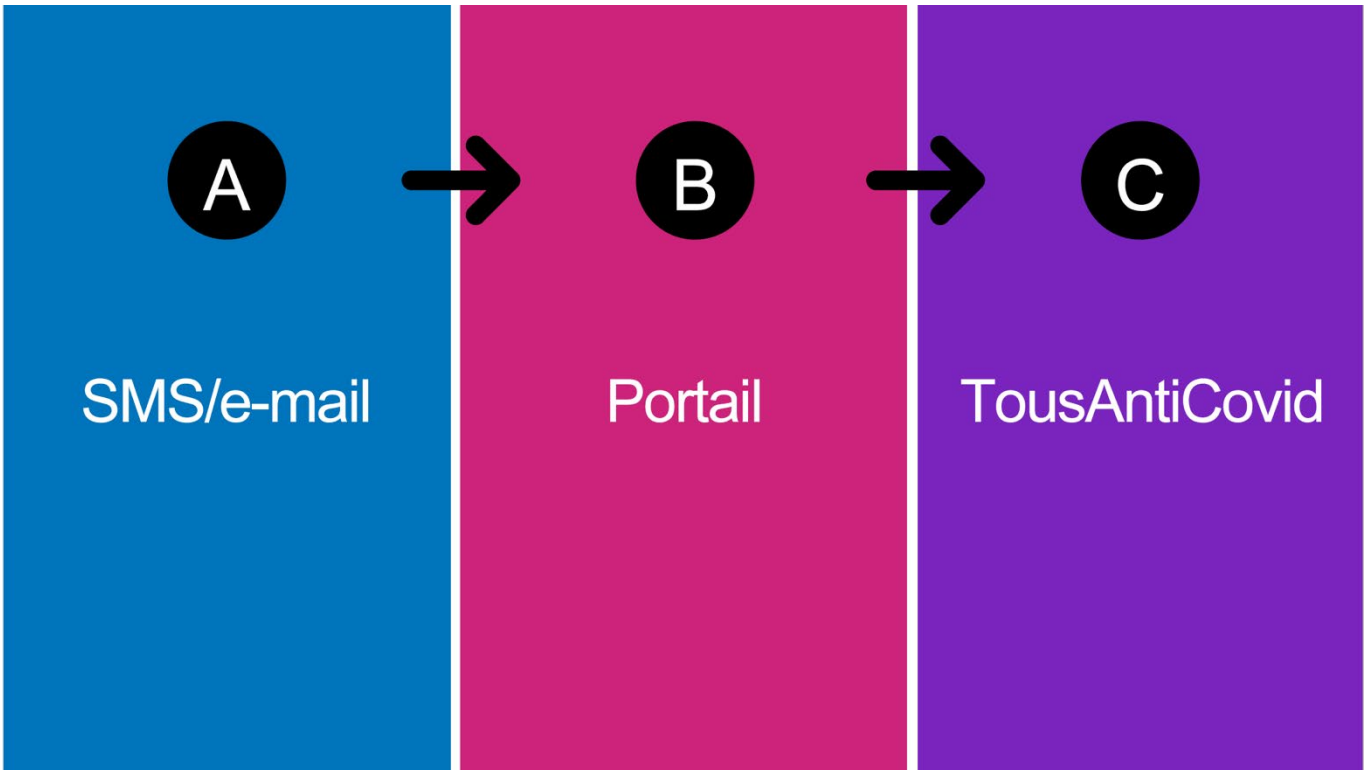
Il existe deux formats d'encodage pour un code 2D-Doc :

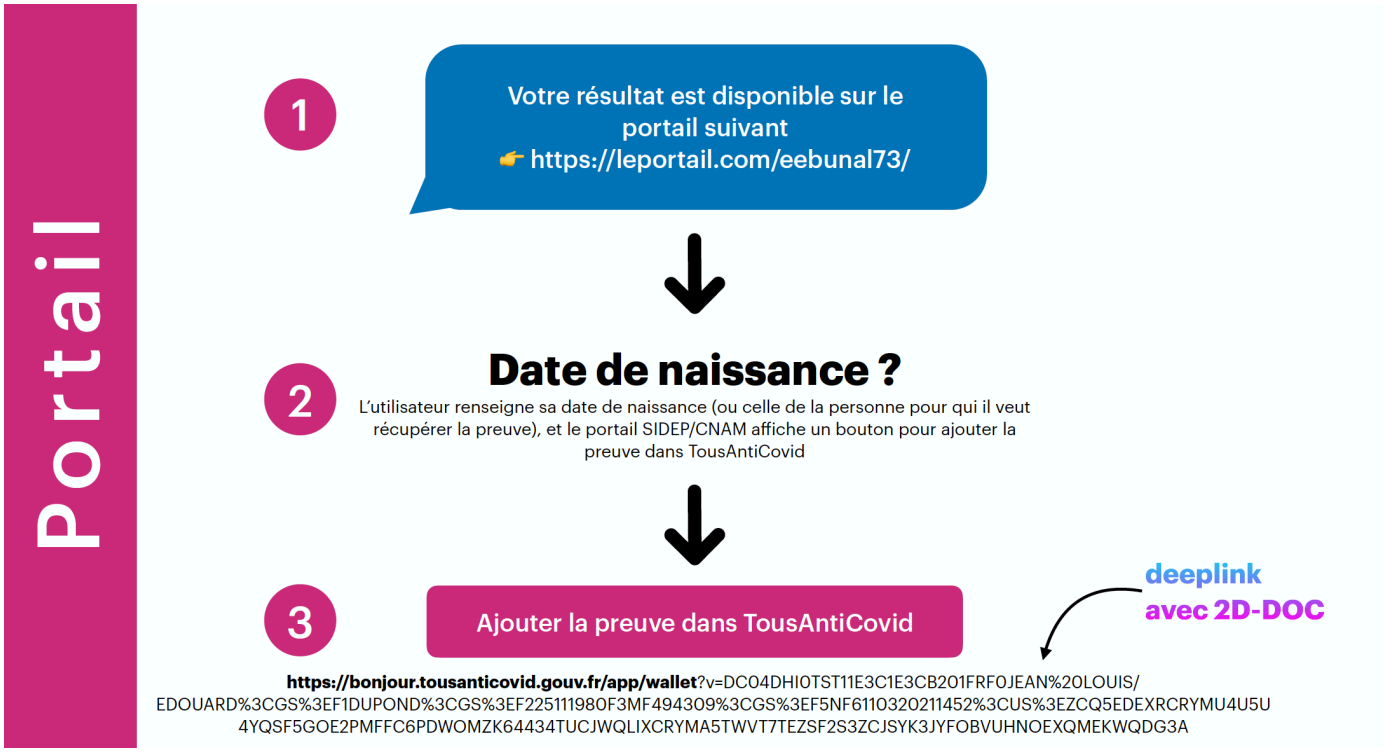
• Le format C40 exploitant un encodage en C40 des données utilisé depuis la version '01 (à l'exception de la signature de la version '01'
qui était au format binaire)

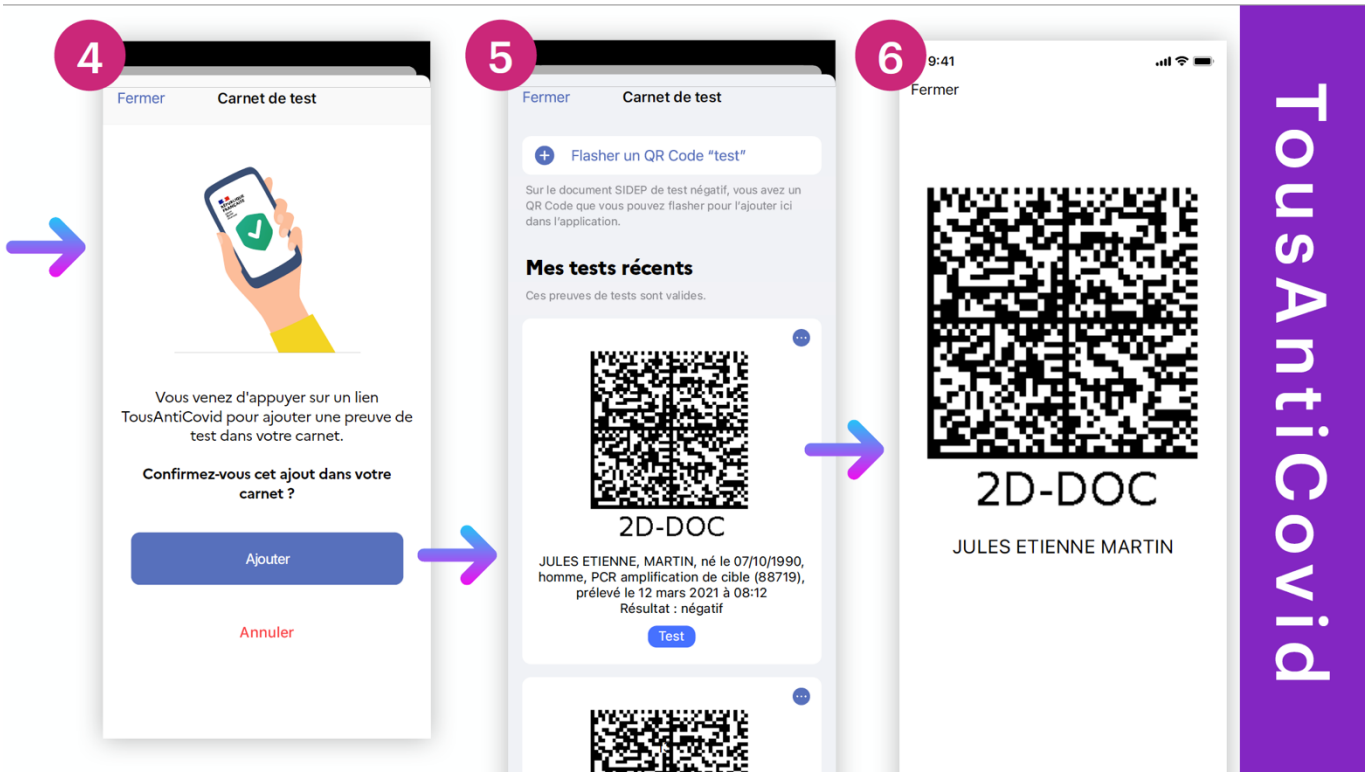
• Le format binaire introduit dans la version '04'

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

4.3.1 Après reception d'un SMS/e-mail

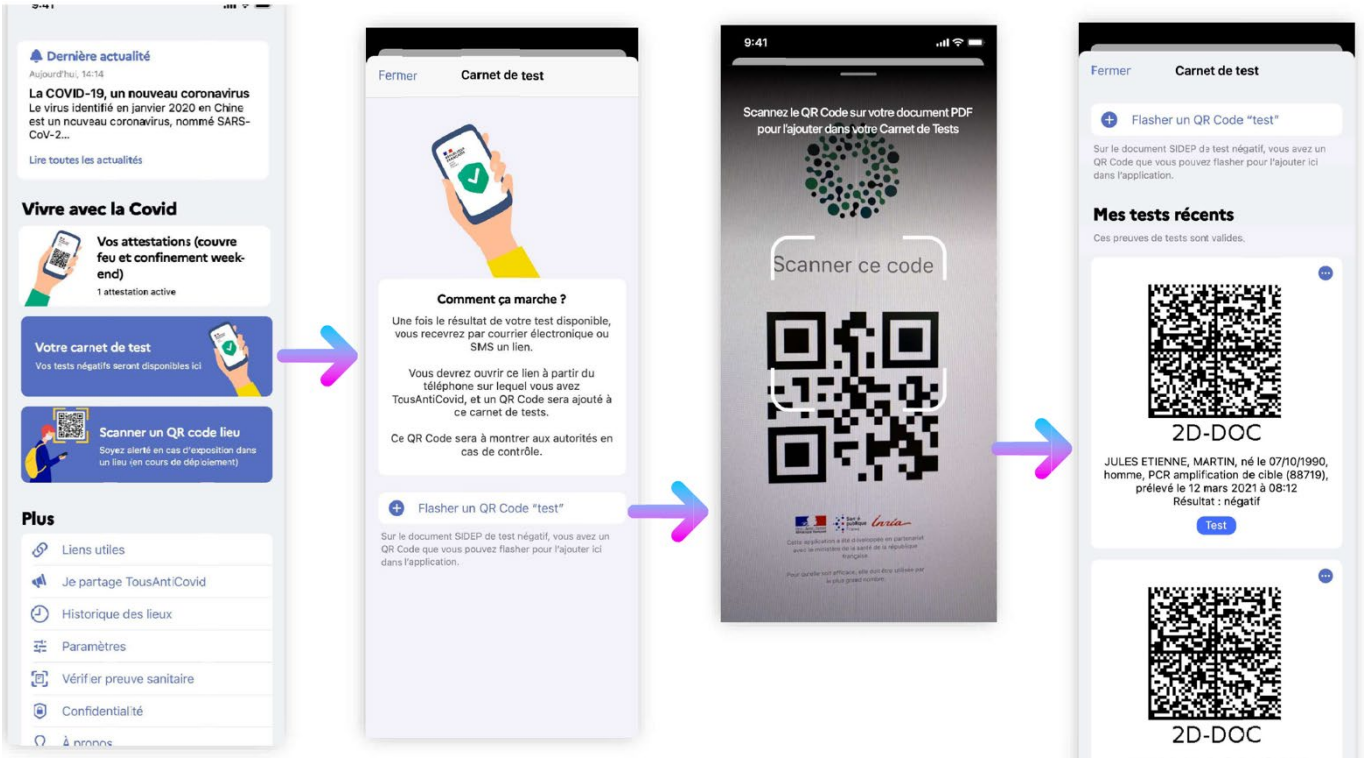






4.3.2 En scannant le QR Code sur le test SI-DEP

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.



4.4 Mesures de sécurité

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). Des serveurs ont été également mis en œuvre par IN GROUPE chez OVH afin de permettre le mécanisme de répartition de charge dans le cadre de l'analyse des règles sanitaires

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 les plus brefs.

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 disposant d'un accès à Internet dont l'usage est strictement encadré. La protection contre les codes malveillants est réalisée via un antivirus basé sur des signatures.

Serveurs:

Les serveurs sont positionnés sur des vlan dédiés, avec un accès à Internet limité aux stricts besoins des prestations. 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 Ces stations sont déployées selon le guide de durcissement 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 Top 10 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.
Une rupture technologique de firewall est implémentée au moins entre le cluster firewall Front-End et le cluster firewall Middle-End.

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 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.

L'accès à ces différentes zones nécessite un badge 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 parmi :

- Grillage périphérique + portails et portillons
- Vérification d'identité + signature d'une clause de confidentialité + attribution d'un badge qui doit être porté de manière visible
- Dispositif anti-bélier + clôture électrique + Tourniquet pleine hauteur avec passage individuel par badge
- Sas avec passage individuel des personnes contrôlées + correspondance biométrique

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, télécoms 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 amenées 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 formées 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