Pass sanitaire et vie privée : quels sont les risques ?

Date [2021 Jun 03] Categories [privacy] Tags [privacy cryptography covid19]

Auteurs :

- Florian Maury
- Piotr Chmielnicki

Les auteurs de cet article peuvent être contactés :

- par email : florian.maury-pass-sanitaire VOUS-SAVEZ-QUOI broken-by-design.fr
- par chat, avec Matrix : #pass-sanitaire:matrix.piotr.paris

Il existe une vidéo compagnon, pour ceux qui préfèrent regarder que lire.

Sur Peertube :

En téléchargement : Haute qualité (1300MB) / Faible qualité (90MB)

Ce document porte sur le pass sanitaire, qui est en train d'être mis en place par le gouvernement français et qui entrera en vigueur le 9 juin 2021. Il vise à mettre au jour de fausses informations diffusées par certains membres du gouvernement, à expliquer et à illustrer pourquoi le pass sanitaire, tel qu'il est conçu, met en danger la vie privée, mais aussi des données médicales des citoyens. En outre, il accroit le risque de vol d'identité.

Le pass sanitaire est présenté sous la forme d'un code barre en deux dimensions, appelé datamatrix. Ce code barre, comme son nom l'indique, encode des informations. Il est en cela similaire aux codes barres des produits que vous achetez en grande surface, et que vous passez à la caisse. Il est juste en deux dimensions et contient plus d'information. Au lieu d'un numéro qui sert à indiquer à la caisse enregistreuse la nature du produit que vous achetez, ce qui lui sert à connaitre le prix à imputer, le code barre du pass sanitaire contient vos informations personnelles et des informations relatives à la vaccination. L'encodage de ces informations

ne constitue pas une mesure de protection des données puisque n'importe qui équipé d'un dispositif de lecture de code-barres peut acquérir les données qui ont été encodées. Le pass sanitaire ne fait pas exception.

D'après le site Service Public.fr, le pass sanitaire contient les informations suivantes :

> - nom, prénom ;
> - date de naissance ;
> - type de certificat et résultat éventuel (test PCR ou antigénique ou vaccination première et seconde dose) ;
> - type de vaccin le cas échéant ;
> - date et heure du certificat.

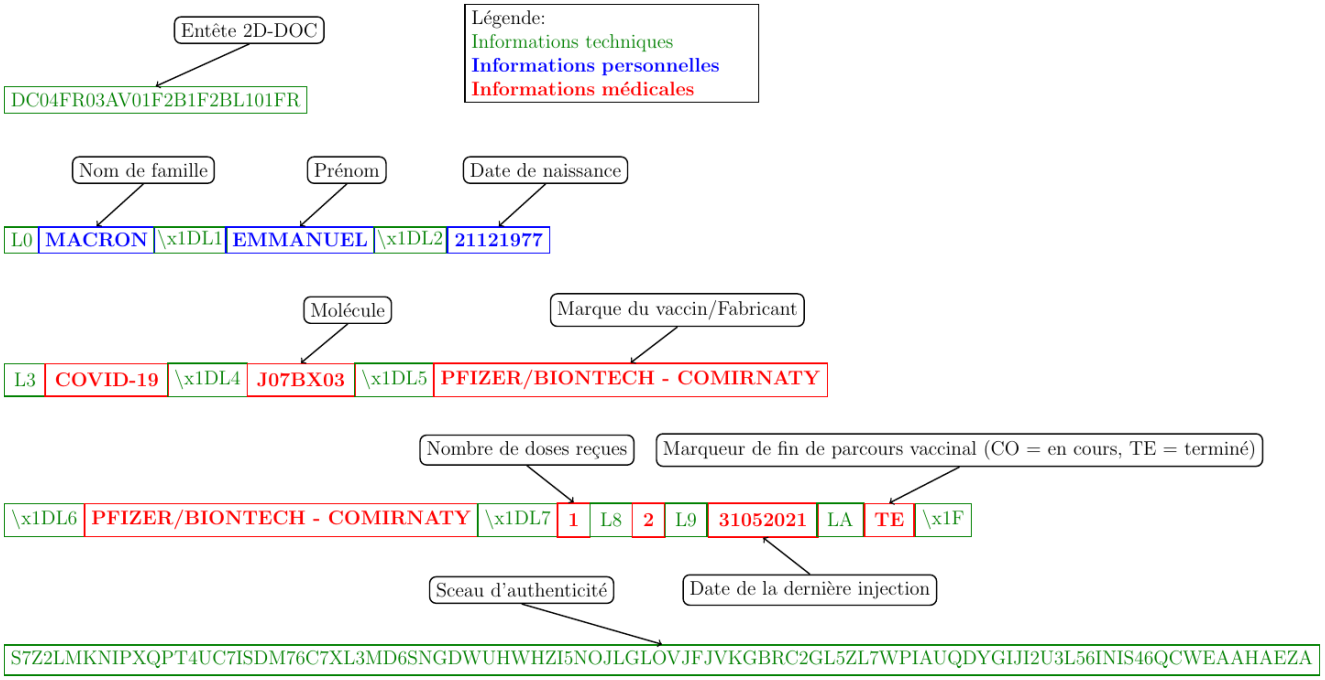
Le site gouvernement.fr indique la même liste.

Nous avons analysé le contenu du pass sanitaire, à l'aide d'outils grands publics, trouvables sur n'importe quel Store d'applications, comme le Google Play Store ou l'Apple Store. Par exemple, Barcode Scanner de ZXing Team sur le Google Play Store.

Nous affirmons que la liste dressée par les sites gouvernmentaux est incomplète.

Le pass est composé de 3 types d'informations :

- des informations techniques, qui permettent de vérifier l'authenticité du pass sanitaire ; on y retrouve des informations sur l'émetteur du pass sanitaire, ainsi que la date d'émission, et le sceau d'authenticité (une signature numérique) ;
- des informations personnelles : nom, prénom et date de naissance ;
- des informations de santé : le type de molécule injectée, le nom du vaccin reçu, le nombre de doses reçues, la date de vaccination et si ce nombre est suffisant pour être protégé de manière optimale pour la personne vaccinée.



Au-delà de ces informations de santé, il est également possible d'inférer des informations de santé encore plus privées sur certains citoyens : ont-il déjà été infectés par la COVID-19 (besoin que d'une seule dose) ? Sont-ils immunodéprimés (besoin de trois doses) ? Sont-ils parmis les citoyens prioritaires pour recevoir des injections tôt dans le calendrier vaccinal ?

Ces informations dépassent largement le cadre et la finalité du pass sanitaire.

Les sites gouvernementaux (comme gouvernement.fr et servic public.fr) se veulent cependant rassurants. Ils précisent :

> Pour accéder à un lieu, un établissement ou un événement, seuls les ouvreurs engagés par les organisateurs pourront lire :
>
> - nom et prénom ;
> - date de naissance ;
> - accès autorisé ou accès refusé, en fonction des règles sanitaires imposées pour accéder au lieu (les ouvreurs ne pourront pas connaître le détail du type de certificat sanitaire présenté).

De même, M. Cédric O, secrétaire d'État, chargé de la transition numérique, indique dans son interview exclusive donnée au journal Le Parisien :

> Comment les professionnels vérifieront-ils le pass sanitaire numérique ?
>
> D'ici le 9 juin, nous aurons déployé l'application de lecture appelée TousAntiCovid Verif. Pour les compagnies aériennes, il y aura une version spécifique car elles ont obligation d'avoir accès au contenu détaillé, avec la date de vaccination, le type de vaccination etc. Elles pourront la télécharger sur les stores, avec un contrôle d'accès par identifiant. En revanche, les organisateurs d'évènements ou les lieux concernés par le pass sanitaire en France, ne connaîtront pas ces informations. Ils ne sauront que le nom, le prénom et la date de naissance de la personne concernée et ne verront apparaître que « vert » ou « rouge » pour valider ou non l'accès. Pour eux, l'application sera en accès libre sur les stores.

Comme nous l'avons démontré plus tôt dans ce document, il n'existe aucune protection contre l'obtention de l'ensemble des données contenues dans le pass sanitaire. Tout lecteur de code barre grand public est suffisant. Il n'est nul besoin d'être membre d'une compagnie aérienne pour obtenir une application aux pouvoirs supérieurs permettant d'acquérir des informations de santé sensibles sur une personne qui exposerait volontairement ou par mégarde son pass sanitaire, sur Internet, dans une file d'attente, ou à un personnel de sécurité à l'entrée d'un événement.

Il existe également d'autres parties qui pourraient être mises au courant du contenu de votre pass sanitaire. D'après un tweet du compte TousAntiCovid du 20 mai 2021:

> #COVID19 | Les autorités compétentes peuvent lire vos certificats de tests avec l'application #TousAntiCovid Verif. Seule la signature du certificat est vérifiée par un serveur dédié d'@IN_Groupe respectant toutes les règles de sécurité des systèmes d'information.

Cette assertion est également corroborée par la demande de l'application TousAntiCovid Verif d'avoir un accès complet au réseau, lors de son installation. De même, on trouve dans les entrailles de l'application TousAntiCovid Verif, une URL (`https://portail.tacv.myservices-ingroupe.com`), et ainsi qu'un fichier comportant une fonction `call2dDoc`, qui fait une requête HTTP avec des paramètres `2ddoc`, `latitude` et `longitude`. Enfin, lorsque l'on scanne un pass sanitaire en mode avion, TousAntiCovid Verif affiche un message d'erreur "Erreur de connexion" et n'affiche pas de résultat.

Il n'est pas aisé de déterminer clairement ce que fait cette fonction, car l'application TousAntiCovid Verif, contrairement à l'application TousAntiCovid, n'est pas en sources ouvertes. Néanmoins, gilbsgilbs a su faire de l'ingénierie inverse et il confirme nos craintes et observations.

Il convient de noter qu'une telle communication réseau génère des meta-données de communication avec le serveur ; il y a notamment l'adresse IP de l'équipement faisant tourner l'application TousAntiCovid Verif. Cette adresse IP permet la géolocalisation de l'équipement faisant tourner TousAntiCovid Verif, par l'entremise des opérateurs de télécommunication, comme Orange.

En croisant ces données, l'État serait donc en mesure de dresser un listing des citoyens et de leurs lieux de fréquentation, grâce au pass sanitaire.

Il convient de noter que l'envoi des données (complètes ou sous la forme d'empreintes cryptographiques) n'est nullement nécessaire pour la vérification de la signature numérique du pass sanitaire. Toutes les informations nécessaires à cette vérification sont publiques. La validation du pass sanitaire peut donc être accomplie sans problème directement par l'application de lecture du code barre. Si un lecteur de code barre

est jugé par le gouvernement comme étant suffisamment de confiance pour lire les données médicales et afficher un verdict, il l'est aussi pour la vérification de la signature.

Nous ne sommes pas les seuls à dénoncer le pass sanitaire, et la quantité d'informations qu'il recèle. La CNIL, la Commission Nationale Informatique et Liberté, a été saisie et a rendu un avis le 12 mai 2021 :

> 36. La Commission considère qu'un dispositif visant à ne permettre la vérification que sur la base d'un résultat de conformité réduirait considérablement les données accessibles aux personnes habilitées à vérifier le statut des personnes concernées, et notamment de ne pas indiquer si elle a été vaccinée, a fait un test ou s'est rétablie d'une infection antérieure à la COVID-19, conformément au principe de minimisation des données
>
> 37. Un tel dispositif implique le téléchargement, du côté des vérificateurs, d'une application permettant de décoder les signaux, probablement sous forme de code-QR, qui contiendront l'information permettant de faire apparaître un résultat vert ou rouge et d'en vérifier l'authenticité. Dans l'hypothèse où ce code-QR correspondrait aux codes actuellement disponibles dans la fonctionnalité « TousAntiCovid Carnet », la Commission relève que celui-ci contient plus d'informations (nom, prénom, date de 8 naissance, date d'examen, type d'examen, résultat). Il est donc possible, dans ce cas, qu'un tel dispositif soit détourné de façon à ce que le lecteur (téléphone ou lecteur dédié) lisant le code-QR puisse accéder à davantage d'informations qu'un simple résultat de conformité (couleur verte ou rouge). Elle invite le Gouvernement à s'assurer de la mise en œuvre des mesures opérationnelles et à fournir, aux personnes gérant les lieux, événements et établissements toute documentation nécessaire (communication sur les lieux, établissements ou évènements soumis au dispositif, mise en place d'une signalétique visible sur place, etc.) permettant de se prémunir de ce risque.

Hélas, aucune "mesure opérationnelle" significative n'a été mise en place par le gouvernement. Il aurait, par exemple, été possible d'émettre plusieurs pass, contenant plus ou moins d'information, en fonction du type de lieu (e.g. salles de spectacle ou aéroports). Cela aurait été, de surcroit, conforme au principe de minimisation des données en regard de la finalité, comme indiqué par la CNIL ou par le Règlement Général de la Protection des Données (RGPD).

Nous affirmons donc, que la mise en oeuvre du pass sanitaire, en l'état, constitue un risque significatif pour la vie privée, pour les données personnelles (risque de vol d'identité accru) et pour les données médicales des citoyens.

Nous affirmons qu'il contient des informations sensibles sans aucun rapport avec la finalité énoncée.

Nous affirmons qu'il peut être détourné pour pister les citoyens.

Nous demandons le retrait du pass sanitaire dans sa forme actuelle.

Nous invitons les citoyens français à rejoindre cet appel et à déposer une plainte auprès de la CNIL et du défenseur des droits contre le pass sanitaire dans sa forme actuelle.

Nous invitons les citoyens européens et les responsables politiques à s'opposer au pass sanitaire européen qui est peu ou prou calqué sur le pass sanitaire français, avec les mêmes informations, les mêmes dérives et les mêmes risques.

Si un nouveau pass sanitaire français est créé, nous exigeons le retrait des informations qui sont sans rapport avec la finalité. Si certaines informations sensibles doivent figurer dans le pass sanitaire, plusieurs pass doivent être remis en fonction du besoin d'en connaitre des employés de sécurité filtrant l'accès à un lieu.

Finalement, nous exigeons que la vérification de l'authencité du pass sanitaire s'effectue localement par une application de vérification en source ouverte, sans avoir besoin de la permission d'accès au réseau.

M. Cédric O s'indigne, dans son interview au Parisien :

> Il y a une forme d'aberration dans la crispation sur ces sujets-là. Comme si nous avions si peur de la solidité de notre démocratie et de notre état de droit, qu'on ne puisse pas se doter de ces outils.

Nous affirmons que la confiance ne s'exige pas, mais qu'elle s'acquiert. Nous affirmons que son acquisition passe par la vérité, la transparence, et des actes en accord avec les paroles et les engagements. Sur ce point, le pass sanitaire est un échec.

De surcroit, les risques de détournement ou de mésusage évoquées dans ce document devraient au minimum avoir été considérés avec circonspection par les responsables politiques. S'ils l'avaient été, le pass sanitaire dans sa forme actuelle aurait été rejeté selon le principe de prudence, au nom de la protection des citoyens.

Autres documents :

- un excellent article de Christian Quest, sur ce même sujet, qui confirme nos observations ;
- un fil de tweets de Mathis Hammel, qui faisait une analyse similaire à la nôtre, au même moment où nous tournions les rushs de notre vidéo ;
- une application Android en preuve de concept, qui collecte et extrait les informations de pass sanitaires scannés, a été développée par Bastien Le Querrec ;
- une version alternative de TousAntiCovid maintenue par Olaf, qui contient notamment un lecteur/vérificateur du pass sanitaire au format 2D-DOC, prouvant la faisabilité d'une lecture et d'une vérification en local, sans avoir besoin des serveurs d'IN Groupe ;
- un fil de tweets de Pixel de Tracking, qui indique des trouvailles similaires à celles sur Android : le pass sanitaire est envoyé aux serveurs d'IN Groupe en totalité ;
- une application web qui vérifie les pass sanitaires de manière autonome ;
- l'article de presse de NextInpact
- l'article de press de Numerama
- l'article de Developpez
- l'article d'igen
- l'article de 01net
- l'article de lemondeinformatique.fr
- l'article de Mediapart
- l'article de Contrepoints
- l'article de NextInpact sur la réaction du gouvernement le 8 juin, en conférence de presse
- la délibération de la CNIL du 7 juin (PDF)

Remerciements : Aurélien Hugues, Émilie Gill, Stéphane Bortzmeyer

---

Historique d'édition :

- 5 juin 2021 à 13h55 : ajout des références aux travaux de gilbsgilbs et de Christian Quest
- 5 juin 2021 à 14h35 : ajout du fil de tweets de Mathis Hammel
- 5 juin 2021 à 16h20 : ajout des remerciements
- 6 juin 2021 à 8h45 : ajout de l'application en preuve de concept
- 6 juin 2021 à 11h50 : ajout de la version alternative de TousAntiCovid par Olaf

- 7 juin 2021 à 12h40 : corrections de coquilles, précisions sur les auteurs, rajout d'une réference à NextInpact, reformulation de la contribution d'Olaf
- 7 juin 2021 à 13h30 : ajout du fil de tweets de Pixel de Tracking
- 8 juin 2021 à 8h50 : ajout des articles de Numerama, de Developpez, et du code source de sanipasse
- 8 juin à 19h15 : ajout des articles d'igen, de 01net et de lemondeinformatique.fr
- 9 juin à 13h35 : ajout des articles de Mediapart, de Contrepoints, de Nextinpact, et la délibération de la CNIL du 7 juin ; remerciements à Stéphane Bortzmeyer sans lequel la diffusion de cet article n'aurait pas été celle qu'elle a connue

---

Fediverse Account RSS ⇧