Pass sanitaire : la poudre aux yeux du pseudonymat, des données médicales en clair

Un florilège de mauvaises idées

102 • 15

MOBILITÉ 8 MIN

Par Sébastien Gavois
Le lundi 7 juin 2021 à 10:36

Signaler une erreur

À compter de mercredi, « *un pass sanitaire sera mis en place de façon temporaire pour accompagner les Français au retour à une vie normale* », rappelle le Service-Public. Problème, on est loin de la promesse initiale pour ce qui est de préserver les données personnelles et médicales.

Depuis maintenant **plus d'un mois**, l'application TousAntiCovid dispose d'un carnet des tests et vaccinations, qui pourront servir dans le cadre des pass sanitaires. Mais « *cette application qui avait promis, craché, juré qu'elle ne contiendrait pas de données personnelles vient donc de revenir très discrètement sur ses promesses* », explique ainsi Christian Quest (porte-parole d'OpenStreetMap France, entre autres) dans un **billet** publié sur Médium.

Il relève que les QR-Code et 2D-DOC (**datamatrix**) « *contiennent des données personnelles et des données de santé* ». Pour ne rien arranger, elles sont en clair et donc lisibles par n'importe qui, sans aucune difficulté. Il suffit d'un lecteur basique QR-Code ou de datamatrix que l'on trouve dans les boutiques applicatives d'Android et iOS.

La CNIL avait pourtant alerté sur les risques dès le mois d'avril, en rappelant que les données doivent « *être limitées à ce qui est nécessaire (principe de minimisation)* ». De plus, « *les autorités qui*

vérifieront le Datamatrix ne doivent pas avoir accès aux données de santé qui ont permis sa délivrance et ne doivent, en aucun cas, générer la création d'une base centralisée de données ». Plusieurs experts relèvent des ratés sur ces deux points, ce qui pose la question de la réaction qu'auront la Commission et le gouvernement suite à leurs publications.

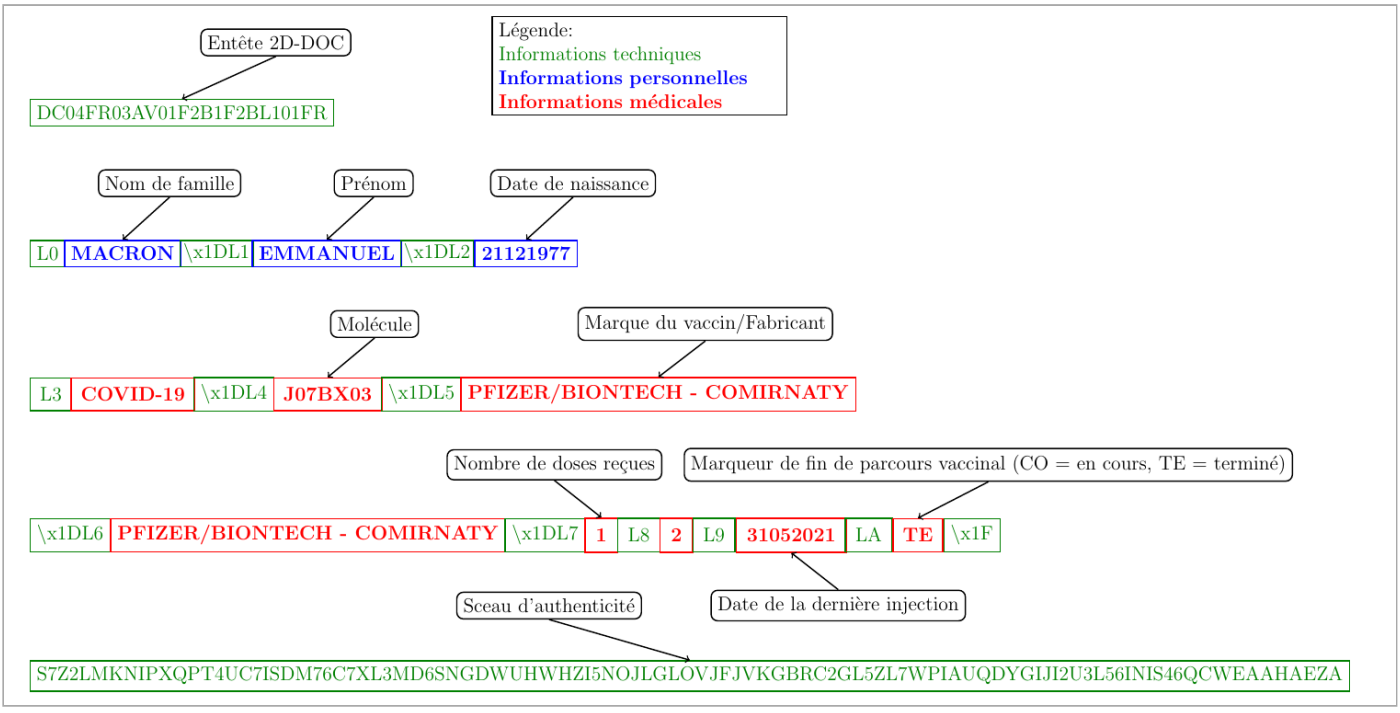
- **Carnet : la CNIL vigilante sur les ombres d'un pass sanitaire**

Des données personnelles et médicales en clair

Broken by Design a décomposé les informations contenues dans le 2D-DOC des certificats de vaccination. On y retrouve en clair les nom, prénom et date de naissance. Pour les données médicales, qui sont également lisibles par n'importe qui, on peut obtenir le type de vaccin et de molécule, le nombre de doses déjà reçues, la date de la dernière injection, le nombre de doses attendues et état du cycle de vaccination (en cours ou terminé).

De quoi permettre de déduire des informations médicales supplémentaires, pouvant être exploitées : « *ont-ils déjà été infectés par la COVID-19 (besoin que d'une seule dose) ? Sont-ils immunodéprimés (besoin de trois doses) ? Sont-ils parmi les citoyens prioritaires pour recevoir des injections tôt dans le calendrier vaccinal ?* ».

Bref, « *ces informations dépassent largement le cadre et la finalité du pass sanitaire* ».



Crédits : **Broken by Design**

2D-DOC, QR-Code : même combat

En plus du 2D-DOC, un QR-Code « classique » est présent sur les attestations de vaccination, que l'on peut **récupérer sur le site Ameli.fr**. Là encore, il est lisible par n'importe qui et contient un lien de la forme :

```
https://bonjour.tousanticovid.gouv.fr/app/wallet?v=Dxxxxxxx
```

Cette URL contient l'ensemble des informations du 2D-DOC (après le wallet?v=), sans protection particulière. Sur Twitter, le compte TousAntiCovid **se justifie** : « *L'ajout d'un QR Code sur le document permet notamment un scan simplifié avec de nombreux smartphones sans ouvrir immédiatement l'application TousAntiCovid. Le Deeplink qu'il contient offre également plus de liberté pour l'intégrer dans certains services web* ».

D'où l'importance de ne pas partager ces éléments en ligne ou avec n'importe qui.

Des promesses sur TousAntiCovid Verif… à la réalité

L'application TousAntiCovid Verif permet, dans les lieux concernés par le pass sanitaire, d'obtenir un feu « vert » ou « rouge » pour le passage d'une personne. « *Ils ne sauront que le nom, le prénom et la date de naissance de la personne concernée* », **affirmait Cédric O au Parisien** il y a quelques semaines.

Ce sont effectivement les seules informations affichées par TousAntiCovid Verif, mais uniquement, parce que l'application « cache » le reste. Cela n'empêche pas une personne utilisant une autre application d'y accéder sans mal. Quant au feu « vert » ou « rouge » il est déterminé en fonction des informations médicales du 2D-DOC.

« *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* », ajoutait Cédric O. Comme nous venons de le voir, une telle distinction n'a pas vraiment de sens puisque n'importe qui peut accéder au même niveau d'information.

Christian Quest propose une alternative pour protéger les données des utilisateurs : « *Plutôt que d'indiquer en clair nom, prénom et date de naissance, utiles pour vérifier quand c'est nécessaire la correspondance avec une pièce d'identité, on aurait pu stocker une empreinte de ces informations (un hash) dans le 2D-DOC* », comme c'est le cas avec les mots de passe par exemple.

De plus, « *la partie données de santé aurait pu être chiffrée, et donc accessible si besoin uniquement aux détenteurs d'une clé de déchiffrement dont l'accès aurait pu être sécurisé* », comme dans le cas des compagnies aériennes ainsi que l'indiquait le secrétaire d'État chargé de la Transition numérique.

Code 2D-Doc	 2D-DOC	
Date d'émission	1E6D - 29 avril 2021	
Date de signature	1E6D - 29 avril 2021	
Type de document	L1 - Attestation Vaccinale	
Périmètre	01 - Périmètre ANTS	
Pays émetteur	FR	
Champs obligatoires	L0	THEOULE SUR MER<GS>
	L1	JEAN PAUL<GS>
	L2	31051962
	L3	COVID-19<GS>
	L4	J07BX03<GS>
	L5	COMIRNATY PFIZER/BIONTECH<GS>
	L6	COMIRNATY PFIZER/BIONTECH<GS>
	L7	1
	L8	2
	L9	01032021
	LA	CO
Message complet	DC04FR0000011E6D1E6DL101FRL0THEOULE SUR MER<GS>L1JEAN PAUL<GS>L231051962L3COVID-19<GS>L4J07BX03<GS>L5COMIRNATY PFIZER/BIONTECH<GS>L6COMIRNATY PFIZER/BIONTECH<GS>L71L82L901032021LACO<US>32T2SI2RUMPDLBHAFSBDF2CUE7GI4NR5WC3NSBEU6AZ7QZJZCPMCTXTVIDZAKEYO7237SQ2ZPOCMZKG7U3Q2LIMPPVJMA7TQAAKC5DY	
Données signées	32T2SI2RUMPDLBHAFSBDF2CUE7GI4NR5WC3NSBEU6AZ7QZJZCPMCTXTVIDZAKEYO7237SQ2ZPOCMZKG7U3Q2LIMPPVJMA7TQAAKC5DY	
Signature (binaire)	DE A7 A9 23 51 A3 1E 35 84 E0 2C 82 32 E8 54 27 CC 8E 36 3D B0 B6 D9 04 94 F0 33 F8 65 39 13 D8 29 DE 75 40 F2 05 13 0E FE B7 F9 43 59 7B 84 CC A8 DF A6 E1 A5 A1 8F 7D 52 C0 7E 70 00 14 2E 8F	

Crédits : **Christian Quest**

Cédric O : n'a « pas d'inquiétude sur la protection de la vie privée »

Cédric O était ce matin **chez Franceinfo** pour défendre le pass sanitaire : « *Il y a un certain nombre d'informations comme le type de vaccin, la date de vaccination, le nom, le prénom, la date de naissance, le nombre de dose que vous avez reçues qui sont contenues dans le QR-Code, mais qui ne sont pas lisibles* », ce qui est faux. Elles ne sont simplement pas affichées par Tous Anti Covid Verif, mais sont parfaitement lisibles par n'importe qui.

« *La seule chose que la personne verra avec son application de lecture ce sera votre nom, votre prénom et votre date de naissance pour pouvoir vérifier votre identité. Pour le reste, elle saura soit que vous avez été malade et que vous êtes immunisé, soit que vous êtes vacciné, soit que vous avez un test PCR* », ajoute-t-il.

« *Si des personnes piratent ou demandent ces informations* [via l'attestation par exemple, ndlr] *qui sont illégales, elles sont passibles d'un an d'emprisonnement ou d'une amende extrêmement forte* ». Il conclut ainsi : « *Je n'ai pas d'inquiétude sur la protection de la vie privée des Français* » insiste-t-il.

TousAntiCovid Verif : quid du code source ?

Sur Twitter, **le compte Gilbsgilbs** s'est penché sur le fonctionnement de l'application TousAntiCovid Verif, qui a été développée par IN Groupe (anciennement Groupe Imprimerie Nationale), mais détenu à 100 % par l'État.

Premier problème identifié : « *on ne trouve le code source de cette application nulle part. Seul IN Groupe sait réellement ce que fait son app* ». TousAntiCovid est open source et Gilfsgilbs se demande donc pourquoi il n'y a « *pas la même transparence pour TousAntiCovid Verif ?* ».

En creusant un peu dans le fonctionnement de l'application, « *on s'aperçoit que l'application embarque des composants propriétaires de Google (Firebase et certains services Google Play)* ». Son rapport Exodus Privacy **est ici**. Il ajoute : « *pourquoi la totalité du contenu du 2D-DOC (à savoir le nom, prénom, date de naissance, numéro et marque de vaccin, date d'injection, signature, etc...) est envoyée sur un serveur d'IN Groupe ?* ».

On note d'ailleurs que l'application TousAntiCovid Verif ne fonctionne pas en mode avion. On obtient une « *Erreur de connexion* » lors d'une tentative précisant « *Aucun réseau disponible* ». Cela soulève plusieurs questions : « *Par exemple, comment garantir si ce pass est utilisé pour l'accès aux manifestations qu'il ne sera pas utilisé pour ficher les manifestants ? C'est quand même une sacrée dérive !* ».

Se posent aussi des questions vis-à-vis du RGPD : « *Est-ce que la finalité du traitement des données est vraiment légitime ? Comme on l'a vu, l'authenticité du certificat pouvait très bien être vérifiée localement et d'éventuelles révocations pourraient se vérifier en envoyant un simple hash du certificat* ».

« Aucun transfert ou partage »... vraiment ?

On est dans tous les cas loin de la **promesse du gouvernement** :

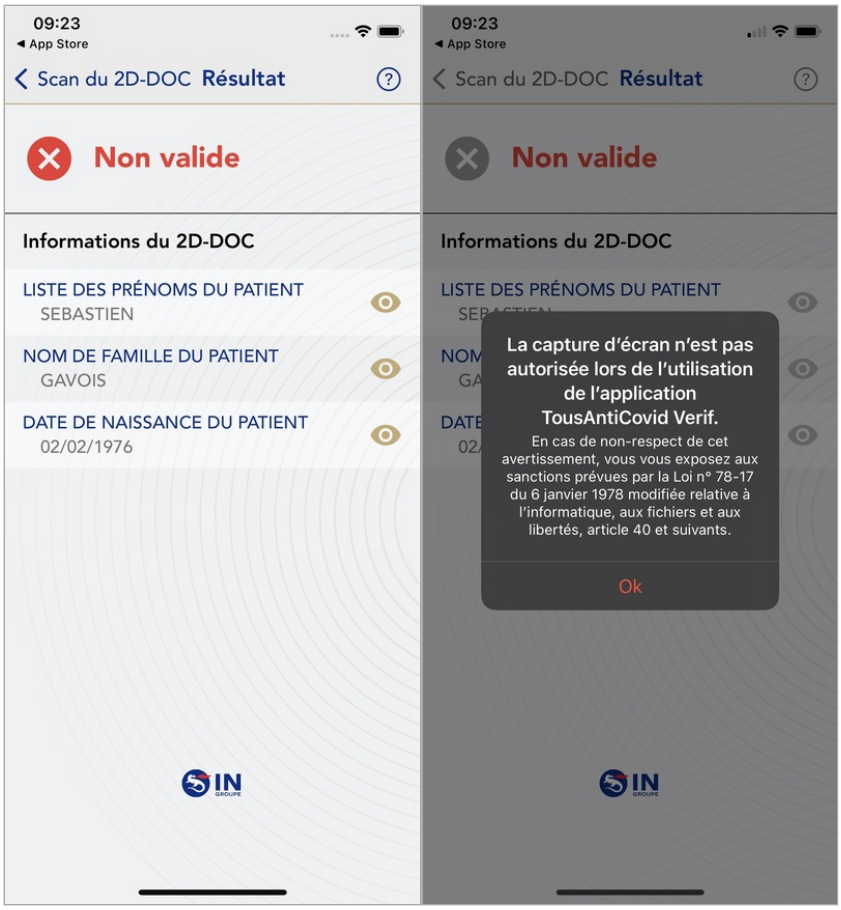
> « *Lors d'un contrôle de votre Pass sanitaire par une autorité ou une personne habilitée, l'opération de vérification/lecture se fait en local (grâce à l'application TAC-Verif), sans conservation de donnée, sans requête à un serveur central de données.*
>
> *Seule la signature de votre preuve sanitaire est vérifiée sur un serveur central avec l'application TousAntiCovid Verif pour s'assurer de son authenticité. TousAntiCovid Verif disposant des règles de gestion en local, seule la signature du certificat sera vérifiée par un serveur dédié d'IN Groupe respectant toutes les règles de sécurité des systèmes d'information afin de garantir au lecteur l'authenticité du certificat* ».

Dans **sa charte de protection des données personnelles**, IN Groupe donne une information différente, affirmant qu'« *aucun transfert ou partage n'est réalisé lors du contrôle* », alors que le gouvernement parle d'une vérification sur un serveur dédié. Dans tous les cas, TousAntiCovid Verif ne fonctionne pas en mode avion.

Il faudra donc attendre des clarifications ou la publication du code source pour en savoir plus.

Cerise sur le gâteau : la capture d'écran de Schrodinger

Dernier point problématique relevé : l'application TousAntiCovid sur Android, ne permet pas de réaliser une capture d'écran native : un message indique que ce n'est pas autorisé. Sur iOS par contre, la situation est cocasse, à l'image du reste de l'application diront certains : un message indiquant que « *la capture d'écran n'est pas autorisée lors de l'utilisation de l'application TousAntiCovid Verif* » est bien affiché… après que ladite capture est réalisée.



Nous avons effectué ce matin une capture d'écran via la dernière version en date de Tous Anti Covid Vérif

Signaler une erreur