

Lettre Informatique du CGA

Septembre 2021



Voici la rentrée ... Il est temps de reprendre nos activités et une vie « presque » normale. Voici quelques informations de rentrée.

Les permanences du CGA ont repris les mercredi matin à l'orangerie (place de la mairie) de 10h00 à 12h00.

Le forum des associations aura lieu le 11 septembre à Belleville de 10h00 à 18h00.

Pensez à vous inscrire à l'entraide informatique et/ou Contactez-nous : informatique@clubgiffois.fr pour toute demande d'information.

En attendant les sujets du mois :

Sommaire

- **L'authentification forte pour les paiements en ligne**

Depuis le 15 mai 2021 une directive européenne a imposé aux banques une authentification renforcée pour les paiements en ligne par carte

bancaire... celle-ci rentre en vigueur au 15 septembre 2021 : de quoi s'agit-il ? Et les arnaques apparaissent également attention !

- **Windows 11 arrive le 5 octobre**

Petit tour visuel de cette nouvelle version. Plus sobre, plus simple, plus épurée... Mais inutile de se précipiter, il faudra s'assurer au préalable de la compatibilité de votre machine surtout si elle a plus de 3 ou 4 ans.

- **Les « QRcodes » ?**

On en parle beaucoup avec le Pass sanitaire, voici quelques précisions.

L'authentification forte pour les paiements en ligne

Depuis le 15 mai une directive européenne impose aux banques une authentification renforcée pour les paiements en ligne (internet) par carte bancaire afin de renforcer la sécurité des opérations. Qu'est ce qui va changer ?

- Actuellement lorsque vous effectuez un achat sur internet une simple authentification pouvait suffire. Par exemple vous rentriez votre n° de carte bancaire et la clé située au dos de la carte puis vous receviez un SMS avec un code que vous deviez renseigner sur la page de paiement en ligne (un code -> une authentification).

Or ce dispositif n'est plus assez sécurisé car des pirates arrivent à récupérer les informations qui transitent chez certains commerçants ou fournisseurs en ligne.

- Une authentification plus sécurisée va devenir obligatoire et se mettre en place progressivement à partir du 15 mai pour être obligatoire le 15 septembre 2021. Ce sont les banques qui sont tenues d'imposer le dispositif (et non pas les commerçants). En quoi cela consiste-t-il ?

Pour valider un achat sur internet ou une opération bancaire, il faudra désormais **2 éléments d'authentification** parmi les 3 suivants (et non plus un seul) liés à votre compte bancaire :

- **un élément que vous seul connaissez** (un mot de passe, un code secret, etc.)
- **un élément que vous seul possédez** (votre téléphone mobile via l'application de votre banque, une carte bancaire, etc.)
- **une caractéristique biométrique** (votre empreinte digitale, la reconnaissance vocale, etc.)



- Conséquence, il devient presque indispensable de télécharger sur son smartphone l'application de sa banque. Cette opération va permettre **l'identification de votre téléphone par votre banque** comme appareil de confiance. Par la suite lorsque vous vous connecterez (au cours d'une transaction bancaire comme un achat) à l'application de votre banque avec votre mot de passe et êtes ainsi « authentifié ». Tous les 90 jours vous serez obligé de ressaisir votre code personnel (le mot de passe permettant d'accéder à votre compte client).
- Si **vous n'avez pas de smartphone** ? Votre banque vous proposera un système de SMS unique (avec un code temporaire : mot de passe à usage unique) couplé avec un mot de passe que vous seul connaissez (le mot de passe permettant d'accéder à votre compte client à la banque par exemple). Certaines banques proposent des solutions alternatives (le CIC par exemple propose un appareil lecteur de code le Digipass)

A noter que ce dispositif sera également obligatoire pour toute opération sur votre compte bancaire « en ligne » comme l'accès à votre espace client, une transaction en ligne, une action en ligne comportant un risque de fraude (tel qu'un changement d'adresse).

Exemple : Avec la BNP il faudra valider l'opération avec son téléphone et l'application « clé digitale » et saisir son code secret de connexion

POUR VALIDER UN PAIEMENT SUR INTERNET
la saisie de ce code reçu par SMS ne suffira plus : une authentification forte sera nécessaire avec votre Clé Digitale⁽²⁾ ou, à défaut, vous devrez :

01
Saisir votre code secret de connexion⁽³⁾

02
Saisir le code reçu par SMS

Chaque banque a une solution équivalente, ci-dessous la Banque Postale :

Changer de site
Particuliers

Solutions citoyennes Je deviens client

Comptes et cartes Epargner Emprunter Assurer Accompagner

La Banque Postale > Particulier > Comptes et cartes > Services digitaux > Sécurité > Certicode Plus

SÉCURITÉ
Certicode Plus
Pratique et simple d'utilisation, Certicode Plus vous offre une expérience digitale nouvelle

Qu'est ce que Certicode Plus ?

Certicode Plus est un service gratuit d'authentification forte permettant de réaliser vos opérations bancaires sensibles en toute sécurité tout en étant conforme avec la directive européenne sur les services de paiement (DSP2).

Simplicité
Un service gratuit, accessible 24/7 sur la banque en ligne et l'application mobile La Banque Postale

Autonomie
Des opérations engageantes réalisées directement en ligne

Sérénité
Une notification sur votre appareil enregistré Certicode Plus vous permet de valider chaque opération

Comment activer Certicode Plus ? Comment valider une opération ?

Attention aux arnaques !

Dans la foulée de cette exigence réglementaire supplémentaire, fleurissent de faux mails qui cherchent à récupérer vos données de connexion !!

Exemple mail au nom de la société générale,

Espace Client <support@denverfineartfair.com>  

Ce qui change pour vous
À : pass@securekey.com,
Répondre à : support@denverfineartfair.com

Tout a l'air vrai sauf :

- Les adresses Mail
- Quand on place sa souris sur le bouton « Me connecter » on voit apparaître : <https://hotelroyalkirchen.com>

Donc à mettre à la poubelle !!

SOCIETE GENERALE NEWSLETTER

VOUS PROTÉGER, C'EST AUSSI NOTRE MÉTIER

Cher client ,
Société Générale renforce votre sécurité en ligne en généralisant l'authentification forte lors de vos achats sur Internet, en accord avec la Directive européenne sur les Services de Paiement 2.
En effet, afin de lutter contre la fraude, l'acheteur doit pouvoir prouver son identité à travers plusieurs actions (on parle d'authentification « forte »). Cette authentification renforcée est à renouveler tous les 90 jours.
Ainsi, à partir de septembre 2021, la saisie du code reçu par SMS ne suffit plus pour valider vos achats Internet et doit être complétée par une connexion sur votre Espace Client en ligne ou via l'Appli. Cela implique la nécessité pour vous de déclarer votre numéro de téléphone.

[Me connecter](#)

Sans déclaration de votre numéro de téléphone, vous ne pourrez plus accéder à vos services de banque à distance, depuis votre Appli mobile ou votre espace client. Toutes les banques sont concernées par cette réglementation.
Prenez soin de vous et de vos proches !

 **INFORMATIONS SÉCURITÉ**

Société Générale ne vous demandera jamais de transmettre ou de saisir par e-mail :

- Les données de votre carte bancaire et votre code confidentiel (cryptogramme)
- Toute autre information personnelle

Pour toutes questions concernant la sécurité informatique et pour contacter notre service dédié, rendez-vous dans la rubrique Sécurité du site internet particuliers.societegenerale.fr.

Certaines de vos informations personnelles ne sont pas à jour ?
Vous avez la possibilité de consulter et modifier si besoin vos informations d'identité et vos coordonnées dans la rubrique « Mon profil » de votre espace client.

Pour toute information concernant la protection de vos données à caractère personnel et l'exercice de vos droits en la matière, veuillez prendre connaissance de notre Politique Données Personnelles disponible sur l'espace internet particuliers dans la rubrique – nos engagements / informations réglementaires – ou la consulter directement en cliquant ici.

Société Générale – Tour Granite – 75886 Paris Cedex 18 – SA au capital de 1 066 714 367,50 EUR – 552 120 222 RCS Paris – Siège social : 29, Bd Haussmann – 75009 Paris – Crédit photo : Getty Images – mai 2020.

Merci de ne pas répondre à ce message, il ne pourra pas être lu.

[Se désabonner](#)

Autre exemple de faux mail ! Surtout ne rien faire et mettre à la poubelle.

Centre de Relation Client C--A <bernardmichel@akeonet.com>

Boîte de réc...nblitz@orange

Alerte : Authentification Renforcée "AG" ✓

À : notificationsg.service@mail.fr,

Répondre à : Centre de Relation Client C--A <bernardmichel@akeonet.com>

Message(s) important(s) disponible(s)

Madame, Monsieur,

Veillez sécuriser votre compte en authentifiant avec les nouvelles techniques de réglementation relatives à des consignes qui sont également entrées en application.

Pour sa mise en œuvre. Nous vous invitons à vous authentifier au plus vite.

- [M'authentifier à ma Banque](#)

Cordialement,

Votre Conseiller CA

Informations sécurité

- **En ignorant cet avis vous vous exposez à une interdiction temporaire de toute opération de débit.**

- 1 - Saisissez le code à usage unique (5 chiffres et une lettre) reçu par SMS.
- 2 - Patienter pour recevoir un autre code par SMS à 6 chiffres.
- 3 - Vérifier votre Boîte e-mail associée à votre compte pour récupérer le code.
- 4 - Réactivez votre carte bancaire.

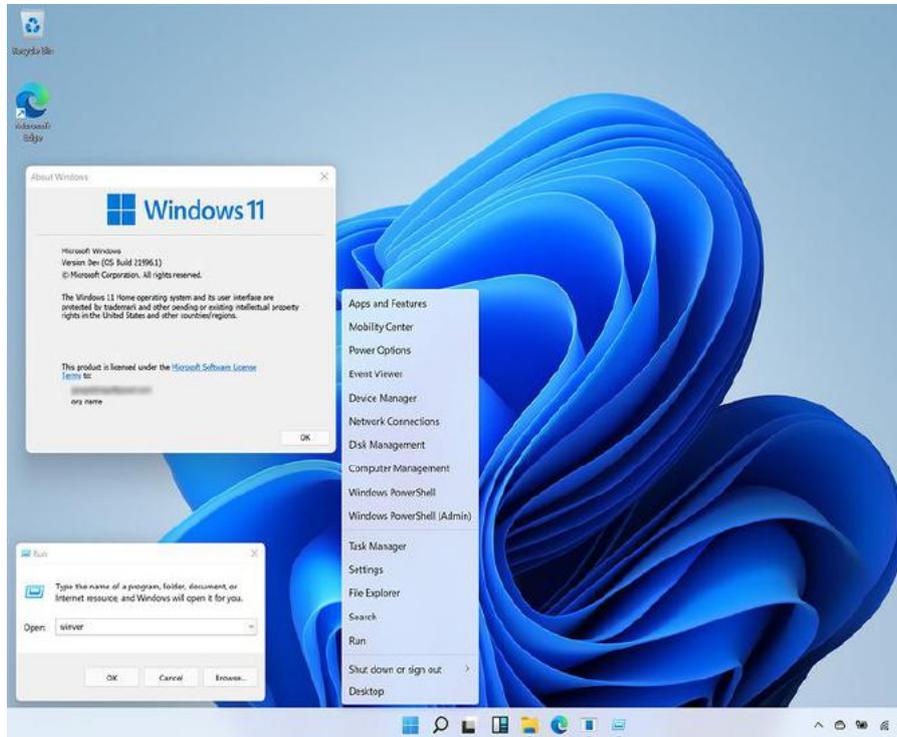
NB : Veuillez respecter le temps de 3 minutes après réception des SMS et par e-mail

- Afin de contribuer au respect de l'environnement, merci de n'imprimer ce message qu'en cas de nécessité.

- **Pour une meilleure protection de vos données personnelles,** consultez le guide internet et sécurité bancaire sur notre site internet

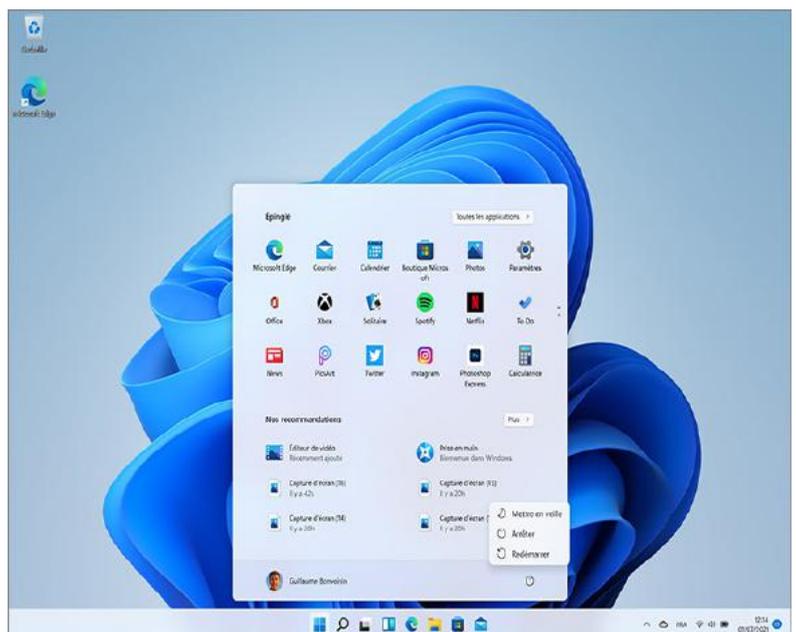
Windows 11 arrive Le 5 octobre !

Une nouvelle version de Windows est en approche chez Microsoft, qui devrait arriver au mois d'octobre.

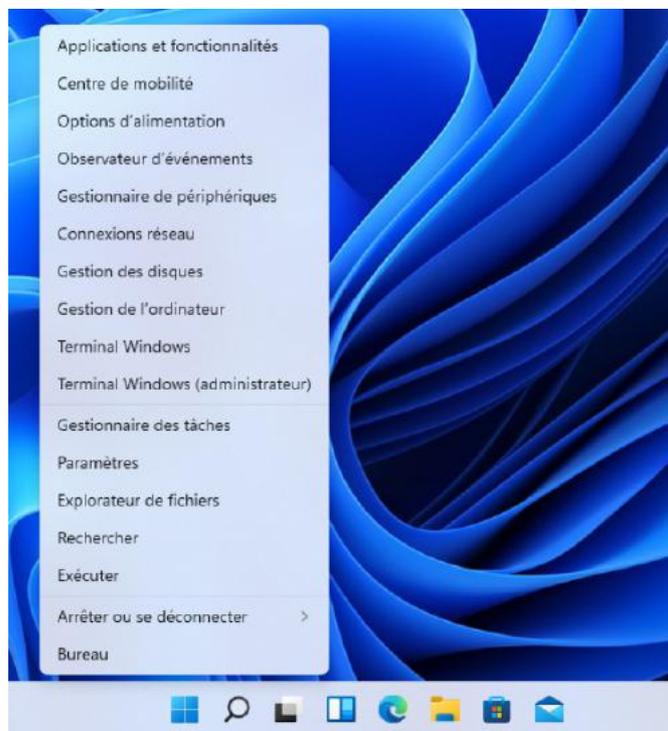
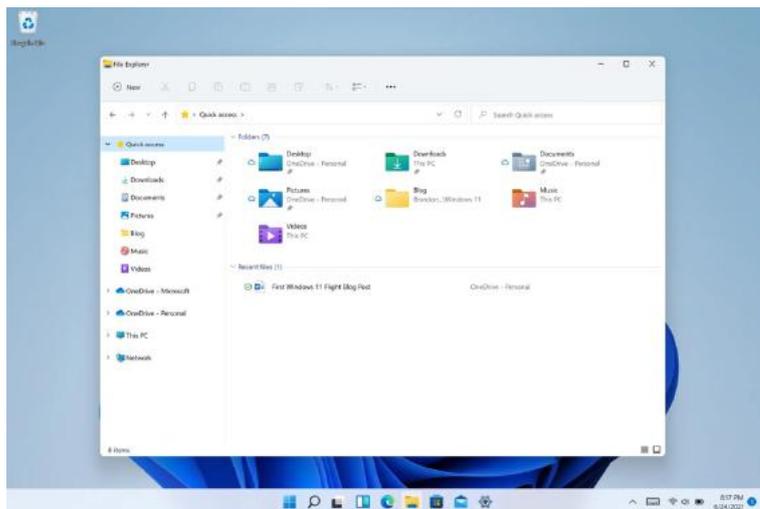


Petit tour d'horizon de cette nouvelle version :

1. Une **refonte de l'interface graphique** : les coins des différentes fenêtres sont arrondis pour plus de « douceur »,
2. Le « **menu démarrer** » a été **profondément modifié** et se trouve maintenant dans la barre des tâches au milieu du bas de l'écran sous forme d'une icône à 4 fenêtres. Un clic dessus ouvre la fenêtre principale. Elle comporte quatre parties distinctes : un champ de recherche, les applications épinglées, les applications et fichiers récents suggérés par Windows, et deux boutons permettant pour le premier de changer de compte ou de verrouiller sa session, et pour le second de mettre en veille, arrêter ou redémarrer l'ordinateur. Un clic sur l'icône du compte en bas à gauche permet d'accéder directement à la fenêtre des paramètres du compte. (Voir l'image ci-contre ----->)

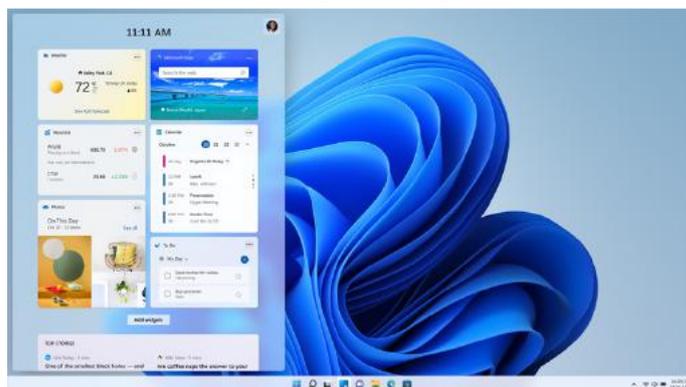
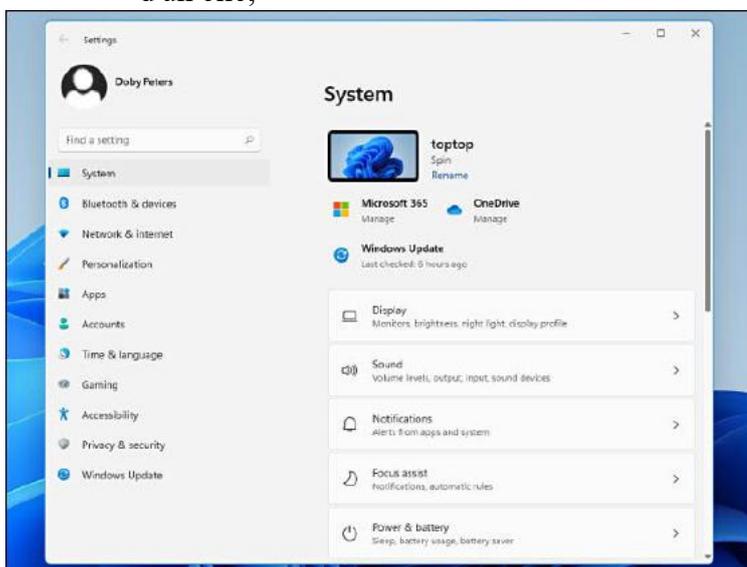


- Un clic droit sur le menu Démarrer permet d'accéder à des options avancées ou certaines actions rapides (comme les paramètres) ---->



- Le look de « l'explorateur de fichier » a été revu également. Simplification et modernisation de la fenêtre. Le bouton New permet de créer un nouvel élément (sous dossier par exemple)

- Un **nouveau Panneau de widgets** : dans un panneau séparé tout en transparence qui s'ouvre d'un clic,



- Un nouveau design également du panneau de paramètres,

- L'intégration de Teams (à la place de Skype) pour chatter, passer des appels vocaux et vidéos simplement (Microsoft pousse à son utilisation)

- Un nouveau « Microsoft Store » au design revu également avec l'intégration des applications **Android** des téléphones. En effet Windows 11 devrait être capable d'exécuter les applications Android dans une fenêtre dédiée.
- De nouveaux « sons » comme au démarrage du système, plus discrets et de nombreuses autres nouveautés...

Au final une belle évolution surtout graphique, mais hélas comme à chaque évolution, tous les ordinateurs ne seront pas forcément compatibles, surtout les plus anciens.

A suivre...

Les QR codes ??

En anglais « *quick response code* ou code à réponse rapide ». C'est comme une sorte de code-barres à deux dimensions (ou code matriciel) qui consiste en un format optique lisible par une machine pouvant être visualisé sur l'écran d'un appareil mobile ou imprimé sur papier et constitué de modules-carrés noirs disposés dans un carré à fond blanc. Ces points définissent l'information que contient le code.



On peut y stocker plus d'informations que sur le code-barres classique.

Il est apparu au Japon en 1999, à l'origine pour suivre des pièces détachées dans l'usine de Toyota.

Sa définition est libre (sous licence libre). C'est avec l'arrivée des smartphones qu'il se généralise. En effet les smartphones peuvent nativement lire les QR codes. Il en existe des versions différentes en fonction du nombre de caractères codés : de 25 à 4296.

Voici un QR code donnant l'adresse du site internet du CGA.

Faites l'expérience avec votre smartphone et vous vous retrouverez sur notre site !!

Scannez le →



Il existe en effet des générateurs gratuits de QR code, pour coder des informations diverses.

Il existe de nombreuses applications Apple ou Android pour scanner les QR codes (mais l'appli photo de base marche)

Les QR codes permettent donc de renvoyer vers une adresse internet, envoyer un sms, transmettre une carte de visite électronique, fournir un rendez-vous sur un agenda le tout souvent pour un usage publicitaire.

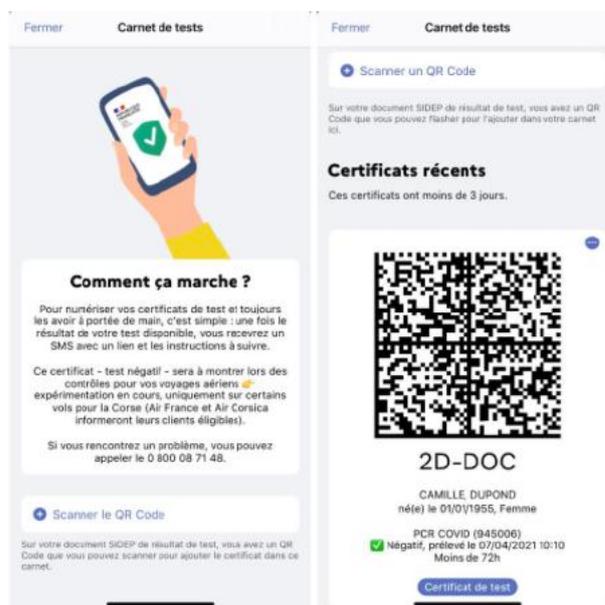
Il peut aussi être utilisé pour se raccorder à un site wifi en donnant les données de connexion (SSID et mot de passe)

Vous l'avez compris c'est un système de codage de l'information sous une forme particulière.

L'utilisation très en vogue actuellement c'est le **QR Code du pass sanitaire !!**

Le QR Code est généré par AMELIE à partir d'informations personnelles que possède l'assurance Maladie. C'est un cryptage connu à priori seulement d'AMELIE. Il est intégré à un document papier ou numérique. Qui constitue le Pass sanitaire.

Il peut être lu par l'application « TAC vérif » qui n'indique que la validité du Pass (aucune autre information).



Autre QR code, celui présent dans les restaurants, salles de sports etc... Il peut être généré par tous les gérants de ces commerces.

Vous le scannez en allant dans ces lieux ce qui permet d'assurer une traçabilité via l'application Tous Anti Covid en cas de suspicion de cas contact.

En effet ce QR Code contient de manière cryptée, le lieu où vous êtes allés. Si un usager se déclare positif en ayant scanné le même QR Code de lieu que vous dans un délai propice à la contagion, vous serez averti de manière anonyme, par l'application, d'un risque de contamination vous concernant.

#TousAntiCovidSignal,
le cahier de rappel numérique
Entrer. Scanner. Profiter.
Simple comme bonjour.



Rappel : le Pass sanitaire se retire à l'adresse suivante : <https://attestation-vaccin.ameli.fr/>

Explications ici : <https://www.ameli.fr/essonne/assure/actualites/covid-19-comment-telecharger-son-attestation-de-vaccination-utile-pour-les-grands-rassemblements>

« Les personnes ne maîtrisant pas les outils numériques ou n'y ayant pas accès peuvent demander leur attestation au professionnel les ayant vaccinées ou, à défaut, il est aussi possible de demander à un professionnel de santé (médecin, pharmacien, infirmier, sage-femme) s'il peut fournir l'attestation »