Guide d'installation de la Passerelle

Version 1.0 — 20 août 2026

Ce guide s'adresse au professionnel de santé et à la personne qui installe la Passerelle sur son poste — le praticien lui-même, son assistant, ou son prestataire informatique.

Certaines exigences de sécurité ne peuvent pas être tenues par Askara : le poste, son système d'exploitation et le réseau du cabinet appartiennent au praticien, pas à nous. Ce guide indique donc, à chaque étape, qui est responsable de quoi — c'est ce qui rend chaque recommandation applicable.

1. Prérequis

1.1 Poste de travail

La Passerelle fonctionne sur Windows et sur macOS.

	Windows	macOS
Système d'exploitation	Windows 10 64 bits ou plus récent	macOS 12 (Monterey) ou plus récent — Intel et Apple Silicon
Lecteur de cartes	Lecteur PC/SC bi-fente (un emplacement pour la carte CPS, un pour la carte Vitale)	
Carte	La CPS du professionnel de santé, en cours de validité	

Le plancher Windows 10 est délibérément plus élevé que celui accepté par les Fournitures SESAM-Vitale elles-mêmes : un système qui ne reçoit plus de correctifs de sécurité ne doit pas héberger un logiciel qui manipule des données de santé. Même logique pour macOS, avec Monterey comme plancher.

Le gestionnaire de cartes à puce fait partie du système d'exploitation, sur Windows comme sur macOS : il n'y a rien à installer pour lui.

1.2 Composants fournis par les organismes

Ces deux composants ne sont pas fournis par Askara. Ils sont édités par l'Agence du Numérique en Santé (ANS) et par le GIE SESAM-Vitale, et se téléchargent directement chez eux.

Composant	Windows	macOS
Cryptolib CPS	édition 64 bits	disponible auprès de l'ANS
Fournitures SESAM-Vitale (FSV)	`.msi` — version d'exploitation, signée	`.pkg` — même version, livrée sous le même bulletin

Sur un poste 64 bits, installez la Cryptolib 64 bits : elle embarque également les bibliothèques 32 bits dont d'autres logiciels peuvent avoir besoin. Installer la version 32 bits sur un poste 64 bits produit une installation qui semble fonctionner et qui échoue à la première lecture de carte.

Installez la version d'exploitation des FSV, jamais une version de bêta-test : les versions de bêta-test circulent, portent des numéros proches, et leur installeur n'est pas signé avec un certificat de production.

1.3 Ce qui est fourni par Askara

La Passerelle Askara, et elle seule. Elle est distribuée sous forme d'un exécutable signé, et le système vérifie cette signature avant de l'exécuter — signature Authenticode sur Windows, signature Developer ID et notarisation Apple sur macOS, contrôlées par Gatekeeper au premier lancement. Dans les deux cas, un exécutable altéré est refusé avant de démarrer : vous n'avez aucune vérification manuelle à faire.

2. Installation

2.1 L'ordre compte

Installez dans cet ordre. Chaque étape suppose la précédente réussie.

1. La Cryptolib CPS — elle installe aussi les autorités de certification de l'IGC-Santé dans le magasin de la machine. Sans elle, les téléservices ne peuvent pas être appelés, même si tout le reste est correct.
2. Les Fournitures SESAM-Vitale — elles apportent les bibliothèques de lecture de carte et de facturation.
3. Le lecteur de cartes — branchez-le et laissez le système installer son pilote.
4. La Passerelle Askara.

2.2 Vérifiez après chaque étape, pas à la fin

Une installation qui échoue en bout de chaîne ne dit presque jamais où elle a échoué. Vérifier au fur et à mesure fait gagner beaucoup plus de temps que ça n'en coûte.

Après	Ce qui doit être vrai
la Cryptolib	l'utilitaire de gestion des cartes fourni avec elle lit votre CPS et affiche votre identité
les FSV	leur utilitaire de configuration démarre et voit le lecteur
le lecteur	les deux emplacements sont reconnus, l'un pour la CPS, l'autre pour la carte Vitale
la Passerelle	l'application signale un lecteur détecté et vous demande votre code porteur à l'insertion de la carte

Si une étape échoue, n'installez pas la suivante : vous ajouteriez une cause possible à un problème qui en a déjà une.

3. Renforcement du poste de travail

Le poste appartient au praticien : Askara ne peut ni le configurer, ni vérifier qu'il l'est. Ces mesures relèvent donc de vous.

3.1 Ce qui protège le poste lui-même

- **Protégez l'accès au firmware par un mot de passe** (BIOS/UEFI sous Windows, mot de passe du programme interne sous macOS Intel — sur Apple Silicon, la puce de sécurité et FileVault assurent cette protection). Sans cela, un poste démarré sur une clé USB s'ouvre comme un livre.
- **Chiffrez le disque** — BitLocker sous Windows, FileVault sous macOS. C'est la mesure la plus efficace de cette liste : un poste volé ou revendu emporte tout ce qu'il contient.
- **Verrouillez la session en cas d'absence.** Un poste de cabinet est dans une pièce où passent des gens.
- **Laissez actives les protections du système** — contrôle de compte d'utilisateur et protections mémoire sous Windows, Gatekeeper et protection de l'intégrité du système sous macOS. Elles sont parfois désactivées pour « faire marcher » un logiciel récalcitrant : ne les désactivez pas.

3.2 Ce qui limite la surface d'attaque

- N'installez que les applications nécessaires à votre activité.
- Désactivez les services réseau inutiles, notamment le partage de fichiers s'il ne sert pas.
- Supprimez les comptes inutilisés, un compte par personne — un compte partagé rend impossible de savoir qui a fait quoi.
- Ne travaillez pas en administrateur au quotidien.
- Désactivez les fonctions de débogage.

Cette dernière mesure, Askara se l'applique aussi : les fonctions de débogage de la Passerelle n'existent pas dans la version qui vous est distribuée, et aucun réglage ne permet de les réactiver.

3.3 Mises à jour de sécurité

Composant	Responsabilité
Windows / macOS	vous — mises à jour automatiques activées
Antivirus	vous — installé, actif, base de signatures à jour
Cryptolib CPS et FSV	vous — suivre les publications de l'ANS et du GIE
Passerelle Askara	Askara publie, vous décidez d'installer

La Passerelle vérifie l'existence d'une nouvelle version et la télécharge, mais ne s'installe jamais sans votre accord : une fenêtre vous propose l'installation, et rien ne se produit tant que vous ne l'avez pas acceptée. La mise à jour est signée, et une mise à jour dont la signature ne serait pas valide est refusée par le système avant même de démarrer.

N'ignorez pas indéfiniment les propositions de mise à jour : elles portent des correctifs de sécurité, et une version ancienne peut cesser d'être acceptée par les téléservices.

4. Réseau du cabinet

Askara ne fournit ni équipement réseau, ni connexion. La mise en œuvre du réseau du cabinet relève entièrement du professionnel de santé.

Si le poste est connecté en Wi-Fi, deux exigences minimales : chiffrement et intégrité en WPA2-AES (CCMP) au minimum — WPA2-TKIP, WEP et un réseau ouvert sont exclus — et authentification des postes en 802.1x (EAP-TLS).

- Changez les mots de passe par défaut de la box et des équipements réseau : c'est la première chose que cherche un attaquant, et elle est souvent trouvable dans une notice publique.
- Séparez le réseau des patients de celui des soins. Si le cabinet offre un Wi-Fi en salle d'attente, il doit être distinct de celui où vit le poste de facturation — un réseau « invité », pas le même.

5. Usage quotidien

5.1 La carte CPS et le code porteur

- Le code porteur ne se communique à personne, et ne se note nulle part : il vaut votre signature de professionnel de santé.
- Retirez la carte en fin de session, et ne la laissez pas dans le lecteur en quittant le cabinet.
- Trois codes faux bloquent la carte. Ce n'est pas une pénalité mais une protection : en cas de doute, arrêtez-vous plutôt que de tenter une troisième fois.

Ce qu'Askara garantit de son côté : le code porteur vous est demandé à l'insertion de la carte et n'est jamais mémorisé, le retrait de la carte est détecté et déclenche l'effacement des données encore présentes en mémoire, et aucune donnée de carte n'est écrite sur le disque de votre poste.

5.2 La boîte de télétransmission

La boîte utilisée pour émettre vos lots et recevoir les retours de l'Assurance Maladie est créée et administrée par Askara. Vous n'avez rien à configurer.

Elle est réservée exclusivement à la facturation, et ne doit jamais servir de messagerie. Ce n'est pas une préconisation de confort : un message étranger déposé dans cette boîte perturbe le traitement des retours.

5.3 Les numéros de lot

Chaque émission consomme un numéro de lot, qui est immuable et jamais réattribué. Conséquence pratique : un lot déjà transmis ne se retransmet pas. Si vous avez un doute sur le sort d'un lot, regardez son état dans le logiciel ou contactez le support — ne le réémettez pas « pour être sûr ». Une double émission produit un rejet côté caisse et un travail de correction qui n'était pas nécessaire.

5.4 En cas d'incident

Signalez sans attendre, à l'adresse de support figurant dans l'application :

- une carte CPS perdue ou volée — prévenez aussi l'ANS, qui seule peut la révoquer ;
- un poste compromis ou soupçonné de l'être ;
- un comportement anormal du logiciel touchant la facturation ;
- la réception, dans la boîte de télétransmission, de messages qui n'ont rien à y faire.

En attendant une réponse, n'effacez rien — ni journaux, ni messages, ni fichiers : ce sont eux qui permettent de comprendre ce qui s'est passé. Déconnecter le poste du réseau est en revanche une bonne réaction si vous suspectez une compromission.

6. Ce que la Passerelle ne fait pas

La Passerelle Askara ne comporte aucune fonction de prise de contrôle à distance de votre poste de travail. Aucune connexion entrante vers ce poste n'est établie par Askara, à aucun moment, pour aucun motif — support compris.

- Le support ne vous demandera jamais de lui ouvrir un accès à votre poste au titre de la Passerelle. Une sollicitation en ce sens, prétendument de notre part, doit être traitée comme une tentative de fraude et signalée.
- Toutes les connexions sont établies depuis votre poste, à votre initiative. Lancer l'application est cette initiative : aucune connexion ne s'établit avant que vous l'ayez ouverte, et fermer l'application les ferme.

7. Traçabilité

La Passerelle enregistre les événements nécessaires à la sécurité et au diagnostic : initialisation du lecteur, lecture de carte, appel de téléservice, émission de flux, refus d'émission et son motif, ainsi que les événements touchant les certificats et les mises à jour de l'application.

Ces traces ne contiennent aucune donnée de santé. Elles portent des tailles, des codes retour et des identifiants techniques. Le numéro de sécurité sociale y est tronqué et le code porteur n'y figure jamais. Elles sont conservées douze mois.

8. Récapitulatif de vos engagements

Ces engagements sont contractuels et repris dans les Conditions Générales d'Utilisation d'Askara.

#	Vous vous engagez à
1	Installer et maintenir un système d'exploitation encore supporté, avec ses mises à jour de sécurité automatiques
2	Maintenir un antivirus actif et à jour
3	Chiffrer le disque du poste et protéger l'accès au firmware
4	Ne pas désactiver les protections du système
5	Ne pas travailler en administrateur, un compte par personne
6	Sécuriser le réseau du cabinet, filaire et Wi-Fi, et séparer le réseau des patients
7	Ne jamais communiquer votre code porteur et retirer votre carte en fin de session
8	N'utiliser la boîte de télétransmission que pour la facturation
9	Ne pas réémettre un lot déjà transmis
10	Signaler sans délai tout incident, et ne rien effacer en attendant
11	Installer les mises à jour de la Passerelle qui vous sont proposées

Versions de ce guide

Ce guide évolue avec la Passerelle. Les versions antérieures restent consultables ci-dessous, afin que chaque client puisse retrouver celle en vigueur au jour de sa souscription.

Version	Date
1.0	20 août 2026