Passerelle Installation Guide

Version 1.0 — 20 August 2026

This guide is for the health professional and for whoever installs the Passerelle on their workstation — the practitioner themselves, an assistant, or an IT provider.

Some security requirements cannot be met by Askara: the workstation, its operating system and the practice's network belong to the practitioner, not to us. This guide therefore states, at each step, who is responsible for what — that is what makes each recommendation actionable.

1. Requirements

1.1 Workstation

The Passerelle runs on Windows and on macOS.

	Windows	macOS
Operating system	Windows 10 64-bit or later	macOS 12 (Monterey) or later — Intel and Apple Silicon
Card reader	Dual-slot PC/SC reader (one slot for the CPS card, one for the Vitale card)	
Card	The health professional's valid CPS card	

The Windows 10 floor is deliberately higher than the one accepted by the SESAM-Vitale software supplies themselves: a system that no longer receives security patches should not host software that handles health data. The same logic sets Monterey as the macOS floor.

The smart-card manager is part of the operating system, on both Windows and macOS: there is nothing to install for it.

1.2 Components supplied by the agencies

These two components are not supplied by Askara. They are published by the Agence du Numérique en Santé (ANS) and by the GIE SESAM-Vitale, and are downloaded directly from them.

Component	Windows	macOS
Cryptolib CPS	64-bit edition	available from the ANS
SESAM-Vitale software supplies (FSV)	`.msi` — production release, signed	`.pkg` — same version, shipped under the same bulletin

On a 64-bit workstation, install the 64-bit Cryptolib: it also bundles the 32-bit libraries other software may need. Installing the 32-bit edition on a 64-bit workstation produces an install that appears to work and then fails on the first card read.

Install the production release of the FSV, never a beta version: beta versions circulate under nearby version numbers, and their installer is not signed with a production certificate.

1.3 What Askara supplies

The Askara Passerelle, and only that. It is distributed as a signed executable, and the system verifies that signature before running it — Authenticode signature on Windows, Developer ID signature and Apple notarization on macOS, checked by Gatekeeper on first launch. Either way, a tampered executable is rejected before it starts: you have no manual check to perform.

2. Installation

2.1 Order matters

Install in this order. Each step assumes the previous one succeeded.

1. Cryptolib CPS — it also installs the IGC-Santé certificate authorities into the machine's certificate store. Without it, teleservices cannot be called, even if everything else is correct.
2. SESAM-Vitale software supplies — they provide the card-reading and billing libraries.
3. The card reader — plug it in and let the system install its driver.
4. The Askara Passerelle.

2.2 Check after each step, not at the end

An installation that fails at the very end almost never tells you where it failed. Checking as you go saves far more time than it costs.

After	What should be true
Cryptolib	its card-management utility reads your CPS and displays your identity
FSV	their configuration utility starts and sees the reader
the reader	both slots are recognised, one for the CPS card, one for the Vitale card
the Passerelle	the app reports a detected reader and asks for your cardholder code when the card is inserted

If a step fails, do not install the next one: you would be adding a possible cause to a problem that already has one.

3. Hardening the workstation

The workstation belongs to the practitioner: Askara can neither configure it nor verify that it is configured. These measures are therefore yours to apply.

3.1 What protects the workstation itself

- **Protect firmware access with a password** (BIOS/UEFI on Windows, firmware password on Intel Mac — on Apple Silicon, the security chip and FileVault provide this protection). Without it, a workstation booted from a USB drive opens like a book.
- **Encrypt the disk** — BitLocker on Windows, FileVault on macOS. This is the single most effective measure on this list: a stolen or resold workstation carries everything it holds.
- **Lock the session when away.** A practice's workstation sits in a room people walk through.
- **Leave system protections enabled** — User Account Control and memory protections on Windows, Gatekeeper and System Integrity Protection on macOS. They are sometimes disabled to "make a stubborn piece of software work": do not disable them.

3.2 What limits the attack surface

- Install only the applications your activity requires.
- Disable unneeded network services, in particular file sharing if it is not used.
- Remove unused accounts, one account per person — a shared account makes it impossible to know who did what.
- Do not work as administrator day to day.
- Disable debugging functions.

Askara applies this last measure to itself as well: the Passerelle's debugging functions do not exist in the version distributed to you, and no setting re-enables them.

3.3 Security updates

Component	Responsibility
Windows / macOS	you — automatic updates enabled
Antivirus	you — installed, active, signatures kept up to date
Cryptolib CPS and FSV	you — follow ANS and GIE publications
Askara Passerelle	Askara publishes, you decide when to install

The Passerelle checks for a new version and downloads it, but never installs without your consent: a window prompts you to install, and nothing happens until you accept. The update is signed, and an update whose signature is not valid is rejected by the system before it even starts.

Do not indefinitely ignore update prompts: they carry security fixes, and an old version may stop being accepted by the teleservices.

4. Practice network

Askara supplies no network equipment or connectivity. Setting up the practice's network is entirely the health professional's responsibility.

If the workstation connects over Wi-Fi, two minimum requirements apply: encryption and integrity via WPA2-AES (CCMP) at minimum — WPA2-TKIP, WEP and an open network are excluded — and device authentication via 802.1x (EAP-TLS).

- Change the default passwords of the router and network equipment: it is the first thing an attacker looks for, and it is often found in a publicly available manual.
- Keep the patient network separate from the care network. If the practice offers Wi-Fi in the waiting room, it must be distinct from the network the billing workstation lives on — a "guest" network, not the same one.

5. Day-to-day use

5.1 The CPS card and the cardholder code

- The cardholder code is never shared with anyone, and never written down anywhere: it stands in for your signature as a health professional.
- Remove the card at the end of a session, and do not leave it in the reader when leaving the practice.
- Three wrong codes lock the card. This is not a penalty but a protection: if you are unsure of the code, stop rather than risk a third attempt.

What Askara guarantees on its side: the cardholder code is requested when the card is inserted and is never stored, card removal is detected and triggers erasure of any card data still held in memory, and no card data is ever written to your workstation's disk.

5.2 The transmission mailbox

The mailbox used to send your batches and receive returns from health insurance is created and administered by Askara. There is nothing for you to configure.

It is reserved exclusively for billing, and must never be used as a mailbox for messages. This is not a matter of convenience: a stray message deposited in this mailbox disrupts the processing of returns.

5.3 Batch numbers

Each transmission consumes a batch number, which is immutable and never reassigned. The practical consequence: a batch that has already been sent cannot be re-sent. If you are unsure what happened to a batch, check its status in the software or contact support — do not re-send it "to be safe". A duplicate submission produces a rejection on the insurer's side and correction work that was not necessary.

5.4 In the event of an incident

Report without delay, to the support address shown in the app:

- a lost or stolen CPS card — also notify the ANS, who alone can revoke it;
- a compromised workstation, or one you suspect is compromised;
- abnormal software behaviour affecting billing;
- messages received in the transmission mailbox that have no business being there.

While waiting for a response, do not delete anything — no logs, no messages, no files: they are what allows the incident to be understood. Disconnecting the workstation from the network is, on the other hand, a good reaction if you suspect a compromise.

6. What the Passerelle does not do

The Askara Passerelle includes no function that takes remote control of your workstation. No inbound connection to this workstation is ever established by Askara, for any reason — support included.

- Support will never ask you to open access to your workstation on behalf of the Passerelle. A request to that effect, purportedly from us, should be treated as a fraud attempt and reported.
- All connections are established from your workstation, at your initiative. Launching the app is that initiative: no connection is established before you open it, and closing the app closes them.

7. Traceability

The Passerelle logs the events needed for security and diagnostics: reader initialisation, card reads, teleservice calls, flow submissions, submission refusals and their reason, and events affecting certificates and app updates.

These logs contain no health data. They carry sizes, return codes and technical identifiers. The social security number is truncated in them, and the cardholder code never appears. They are kept for twelve months.

8. Summary of your commitments

These commitments are contractual and are carried in Askara's General Terms of Use.

#	You commit to
1	Install and maintain a still-supported operating system, with automatic security updates
2	Keep an antivirus active and up to date
3	Encrypt the workstation's disk and protect firmware access
4	Not disable system protections
5	Not work as administrator, one account per person
6	Secure the practice's network, wired and wireless, and separate the patient network
7	Never share your cardholder code and remove your card at the end of a session
8	Use the transmission mailbox only for billing
9	Not re-send a batch that has already been transmitted
10	Report any incident without delay, and delete nothing in the meantime
11	Install the Passerelle updates offered to you

Versions of this guide

This guide evolves alongside the Passerelle. Earlier versions remain available below, so that every customer can find the one in force on the date they subscribed.

Version	Date
1.0	20 August 2026