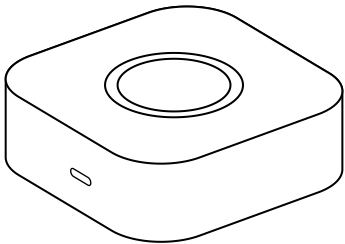


Wireless Fingerprint Key



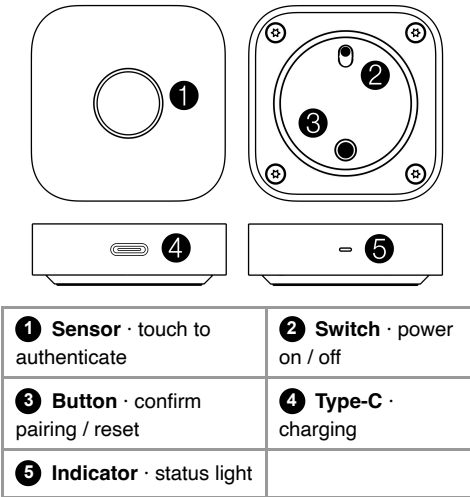
User Manual & Quick Start Guide

immurok IK-1 · EN



<https://immurok.com>

■ Hardware



1 Sensor · touch to authenticate	2 Switch · power on / off
3 Button · confirm pairing / reset	4 Type-C · charging
5 Indicator · status light	

■ Specifications

Processor	RISC-V @ 60 MHz max
Connectivity	Bluetooth LE
Fingerprint sensor	Capacitive
Standby current	~50 µA
Recognition time	<500 ms
Battery	LiPo 110 mAh (USB-C)
Battery life	1+ month typical use
Dimensions	44 × 44 × 14.2 mm
Weight	~40 g

■ Install the App

Download from
<https://immurok.com/download>:

- macOS 13.0+
- Windows 10 / 11
- Linux major distributions

■ Pair: First Computer

1. Slide the **Switch** on. (B) blue blinking
2. First, connect the key in your **system's Bluetooth settings**, like a wireless keyboard. (B) blue = connected
3. Then open the app → **Pair**. This is a second, encrypted pairing step.
4. When the indicator blinks white, press the **Button** once within 30 s. (W) white blinking
5. Key exchange runs a few seconds. (B) blue Done.

To cancel pairing, hold the Button and release while the indicator is yellow (1 to 3 s). Do not hold past 3 s: that starts a factory reset.

■ Pair: Second Computer

1. On computer 1: app → **Dual Host** → enroll a **switch fingerprint**.
2. Touch the switch fingerprint. (W) white flash The device restarts as Computer 2. (W) white blinking
3. On computer 2: connect the key in **Bluetooth settings** first, then open the app → **Pair**.
4. Touch an enrolled fingerprint when asked. (G) green → (B) blue
5. Press the **Button** once during the white blink. Done.

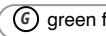
Touch the switch fingerprint anytime to jump between computers. The flash color shows the destination: (B) Computer 1, (W) Computer 2.

■ Indicator Reference

The indicator is the device's only display.

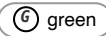
LIGHT	MEANING
(B) Blue blinking	Waiting to connect as Computer 1 . Slows to a flash every 10 s, then sleeps. Press the Button to wake.
(W) White blinking	Waiting to connect as Computer 2 .
(B) Blue solid 2 s	Connected.
(G) Green	Reading your finger.
(B) Blue after green	Matched / computing.
(R) Red	No match or failed. Try again.
(W) White quick blink	Pairing: press the Button (30 s window).
(G) Green fast blink	Enrollment: capturing.
(B) Blue rapid flicker	Firmware updating. Then (G) = success, (R) = failed.
(Y) Yellow	Battery low (shown instead of green). Also: Button held 1–3 s (reset warning), or touch while not connected.
(R) Red, Button held	Factory reset engaged (3 s).

■ Enroll Fingerprints

1. App → **Device** → **Add Fingerprint**.
2. **First fingerprint:** starts immediately. **Later ones:** verify an enrolled finger first.
 green →  blue
3. Touch and lift 6 times, following the app's on-screen guide. Each capture:
 green fast blink
4. Saved:  blue flash . Error:
 red flash , simply retry.

Up to 6 fingerprints: 5 for authentication, plus 1 switch fingerprint.

■ Unlock Password

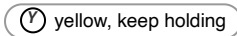
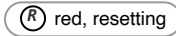
1. App → **Configure unlock password** → enter your computer login password (stored encrypted, on this computer only).
2. Lock the screen, touch the sensor:
 green →  blue , unlocked.

Re-save it whenever you change your login password.

Lock the screen

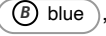
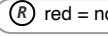
Hold a matched finger ~2 s:  white flash and the computer locks.

■ Factory Reset

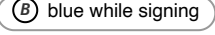
Hold the **Button**: at 1 s
 yellow, keep holding , at 3 s
 red, resetting . Release before 3 s to cancel.

Erases **all fingerprints, SSH keys, and both pairings**. SSH keys cannot be recovered.

■ Authentication

When a password prompt appears (screen unlock, sudo, system settings, installers), touch the sensor instead of typing.  green →  blue ,  red = no match
macOS: 1Password and Bitwarden unlock prompts can also be filled. Enable in Settings → Automation, each with its own stored password.

■ SSH Keys

App → **Keys**: generate or import SSH keys that live inside the device; private keys never leave it. Every `git push / ssh` signature asks for a touch.  green blink →  blue while signing

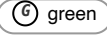
■ AI Agents (imk)

The imk CLI (installed with the app) puts a fingerprint gate in front of commands AI agents run for you:

```
imk run --agent -- git push origin main
```

An on-screen overlay shows the command; one touch approves the whole session, including sudo and SSH inside it. Agent setup:
<https://github.com/immurok/imk-skill>

■ Firmware Updates

1. The app offers updates automatically: **Settings** → **Firmware Update**.
2. Keep the device nearby; transfer takes about a minute.  blue rapid flicker
3.  green = verified, reboots and reconnects.  red = failed. Current firmware is kept, just retry.

■ Settings & Shortcuts

Menu-bar / tray icon → **Open Settings**. Tabs: Device (fingerprints, dual host, battery), Keys, Automation, About. A global hotkey for Quick Fill can be assigned in Settings.

Unpair one computer

App → Device → **Unpair**. Removes only this computer; the other pairing and all fingerprints stay.

■ Tamper Protection

Opening the case triggers an immediate security wipe: all fingerprints, SSH keys, and both pairings are erased, then the indicator blinks red until you power-cycle the Switch. The wipe cannot be undone. Never open the device; contact support instead.

■ Troubleshooting

Indicator off	Asleep. Press the Button. Still off: charge, check the Switch.
 on touch	Not connected / app not running. Open the app, check Bluetooth.
Touch does nothing	Short-press the Button (sensor reset), retry.
Won't reconnect	Press the Button; verify the computer identity, touch the switch fingerprint if wrong.
Unlock doesn't type	macOS: enable immurok under Privacy & Security → Accessibility. Re-save the password after changing it.
 every touch	Finger not enrolled, or wet/dirty sensor. Wipe it.

■ Open Source

The desktop apps for macOS and Linux (including the PAM module) are open source under **Apache 2.0**. Firmware and other components are source-available under the **Business Source License 1.1**, converting to Apache 2.0 over time.

Source code: <https://github.com/immurok>

■ Custom Development

The hardware design is published as well. To flash your own firmware, use WCH-Link serial download: short **BOOT** to **GND** while powering on.

Custom firmware voids the warranty and permanently disables official firmware updates.

■ Regulatory & Safety

FCC CE  

FCC ID: 2BW5FIK1 · Model IK-1 (IK-1-W/-B/-G) · BLE 2402–2480 MHz, max output <1 mW.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Tested to comply with the limits for a Class B digital device (Part 15); if interference to radio or TV reception occurs, try reorienting the antenna, increasing separation, or a different circuit. **Warning:** changes or modifications not expressly approved by Nervina Next Pte. Ltd. could void the user's authority to operate the equipment. This device meets FCC RF exposure requirements; its low output power (<1 mW) exempts it from SAR evaluation.

Hereby, Nervina Next Pte. Ltd. declares that radio equipment type IK-1 complies with Directive 2014/53/EU (RED; EN IEC 62368-1, EN 301 489, EN 55032/35, EN 300 328, EN 62479) and RoHS 2011/65/EU. The full text of the EU declaration of conformity is available at <https://immurok.com/doc>. The crossed-out wheeled bin means: do not dispose of this product or its built-in battery with household waste. Use electronics recycling (WEEE).

Battery: non-removable LiPo, 110 mAh. Do not disassemble, crush, puncture, incinerate, or expose above 60 °C. Charge via USB-C at 5 V only; charging pauses automatically in high ambient temperature. Do not use if the enclosure is damaged. Keep away from small children.

Nervina Next Pte. Ltd. (UEN 202128549C)
24 Sin Ming Lane, #06-97 Midview City, Singapore 573970
Web <https://immurok.com> · Support
support@immurok.com