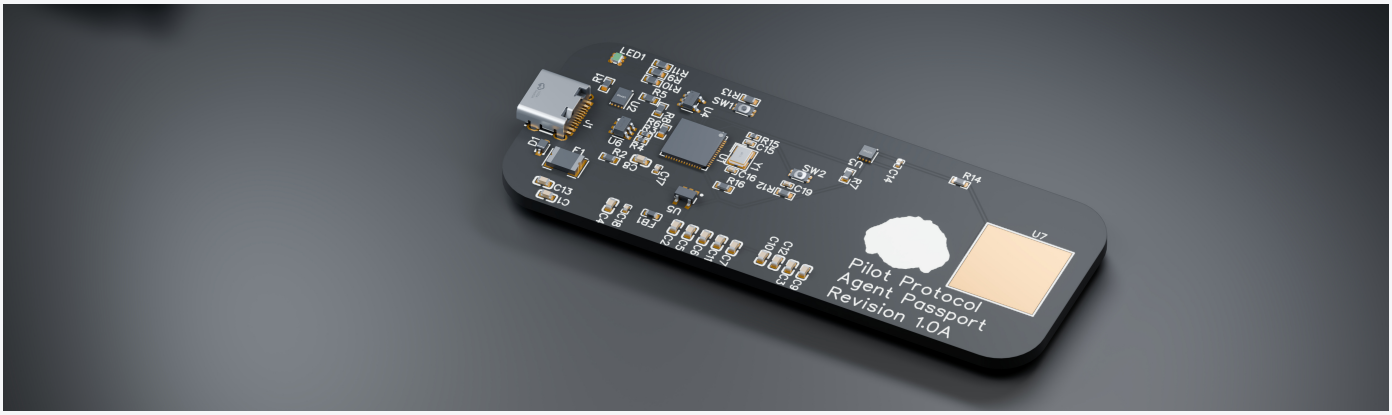
REVISION A / DEVELOPMENT PREVIEW

A physical key.
A verifiable request.

USB-connected hardware identity for agents. Designed to sign requests with a private key held in a secure element, so participating services can recognize a device and enforce its allowance.



01 / HARDWARE

Processor	ESP32-S3FN8 / 8 MB flash
Secure element	ATECC608B-MAHDA-S / ECDSA P-256
Presence sensor	AT42QT1010 capacitive touch
Power & connection	USB-C / 5 V input / 3.3 V logic
Controls & status	BOOT, RESET and RGB LED

02 / SIGNING INTERFACE

Transport	USB Serial/JTAG / newline ASCII
Digest	SHA-256 / 32 bytes
Public key	64 bytes / X || Y / 128 hex characters
Signature	64 bytes / r || s
SDK previews	TypeScript / JavaScript, Python, Go

DEVELOPMENT STATUS / READ BEFORE INTEGRATING

Current Revision A: touch directly powers the secure element. The bring-up firmware requires touch for each PUBKEY or SIGN operation.

Planned product: a periodic presence check with unattended signing between check-ins. This requires further hardware and firmware work.

A signature proves possession of a device key, not a unique person. Providers must verify the trusted issuer record, request binding, freshness, replay protection and device allowance. Electrical limits, mechanical dimensions and certifications remain unqualified.