

SECURITY ARCHITECTURE · 2026

THE ROOT OF TRUST

On-device AI you can prove.

Signed weights. Fused silicon. Nothing leaves the room.

01

SILICON ROOT

A one-time-programmable fuse in every SoC anchors secure boot. The key is burned at our factory and can never be rewritten.

02

SIGNED DELIVERY

Every model we ship is cryptographically signed. The puck verifies our signature itself — the courier is never trusted.

03

ZERO EGRESS

Inference runs entirely on the device. No prompt, no audio, no embedding ever leaves the room. Privacy by construction.

THE THESIS

Cloud AI asks you to trust a promise — that data sent away is handled well. Aura replaces the promise with proof: a chain of verification that begins in silicon you can't rewrite and ends at a model that only runs if we signed it. Trust becomes a property of the hardware, not a policy.

SIGNED · FUSED · SILENT

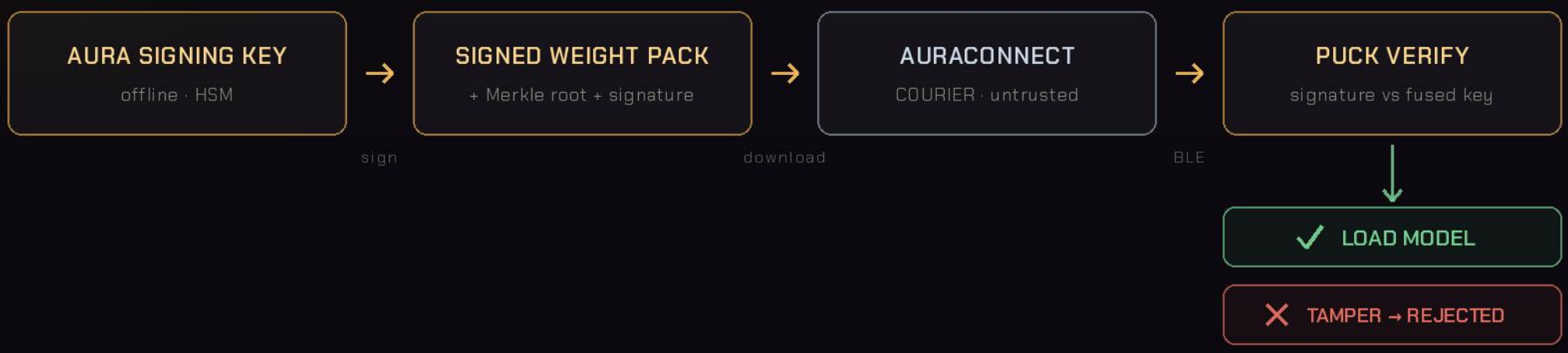
01 – SIGNED MODEL DELIVERY

The courier is never trusted.

Aura's capability compounds over time: the architecture monitors the open-weight ecosystem and swaps in newer, stronger models — the same device gets smarter without new silicon. Every one of those models is delivered through a single hardened path.

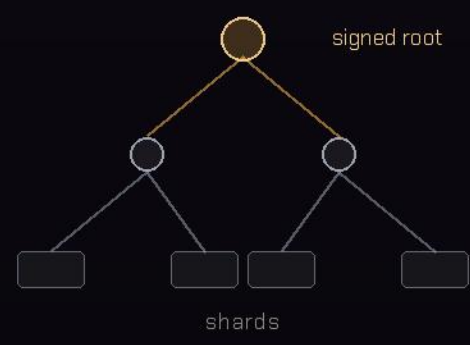
The AuraConnect app (Mac / Windows) downloads the signed weight pack and carries it to the puck over Bluetooth. But AuraConnect, the host computer, and the Bluetooth link are all treated as hostile. The puck trusts exactly one thing: bytes that verify against our public key, which it already holds in fused silicon. A tampered or unsigned model is simply refused.

DELIVERY CHAIN



WHY A MERKLE TREE

Weight packs are large and Bluetooth is slow, so we never buffer the whole file to check one signature. We build a Merkle tree over the shards and sign only the root. Each shard then arrives with its proof and is authenticated incrementally — resumable, streaming, and a single flipped bit fails just its own branch.



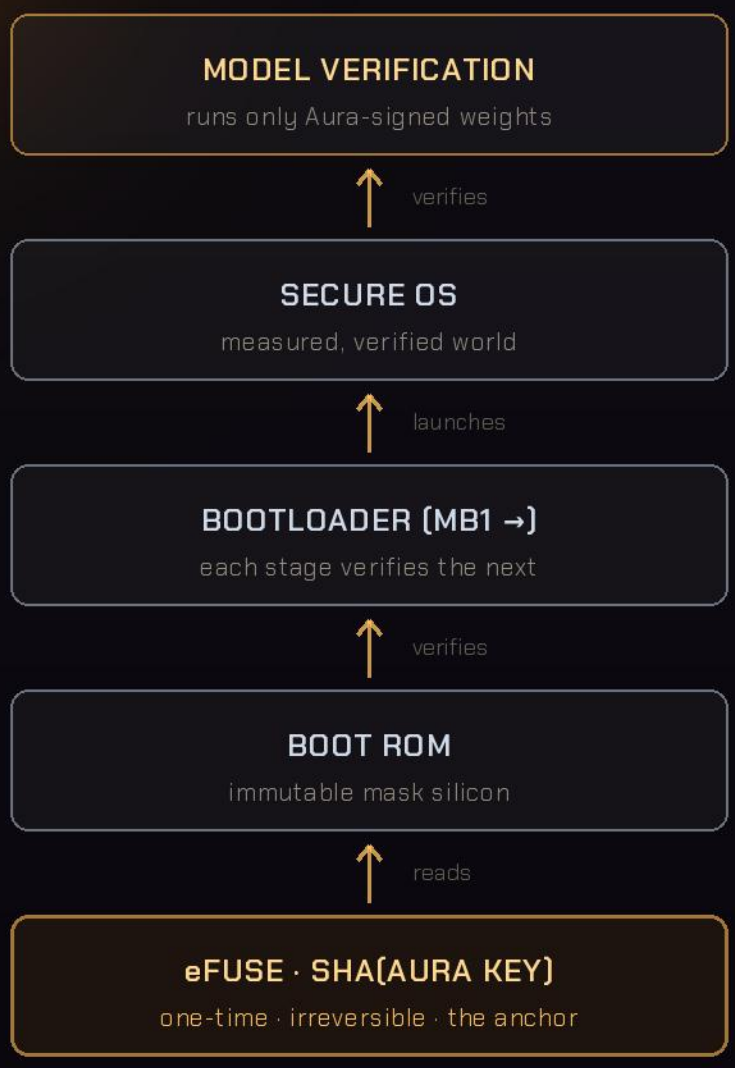
◆ ENGINEERING NOTE — BANDWIDTH

Raw Bluetooth-LE throughput is low. It is ideal for the control channel and the signed manifest, and for small model-swap deltas. For a full base-model refresh we use BLE to orchestrate and a fatter local pipe for the bulk bytes — the on-device signature check is identical either way. The trust lives in the key, not the wire.

02 – THE SILICON ROOT

Burned once. Enforced every boot.

eFUSEs are one-time-programmable fuses physically inside the processor. Writing one blows a microscopic link — irreversible, per-bit, and impossible to fake in software. At our factory we burn the hash of our signing public key. From then on the chip's immutable boot ROM will only run firmware we signed — a root of trust anchored in physics, not policy.



WHAT WE BURN

- **Public-key hash**
  the chip only runs bootloaders we signed
- **Secure-boot key**
  firmware can be encrypted, not just signed
- **Production latch**
  no fallback to unsigned boot; debug locked

ONE ROOT, MANY IDENTITIES

FLEET ROOT · fused

Same across every puck. Proves the firmware and the weights are genuinely ours.

PER-DEVICE KEY · issued

Unique to each unit, signed under the fleet root. Gives every puck an attestable identity of its own.

Silicon you can't rewrite, a boot chain that checks itself, and a model that only loads if we signed it — one unbroken chain from the fuse to the first token. That is what it means to prove, not promise.

AURAVISION · THE ROOT OF TRUST