ECOVENT AFRICA · VPAY GENESIS

Hardware & Oracle Bridge Architecture

Signing at the source — no trusted hand between the asset and the chain · Public edition

Version **1.0** (public) | Status: **pre-production hardware · design specification** | Scope: **capability-level (vendor part numbers withheld)** | Contact: Ano@ecoventafrica.com

> **Read this first — honest status.** The verification & anchoring software (§6) is **live on Polygon Mainnet today** and independently checkable. The measurement device (the GSU) is **engineered and in pre-production** — not yet field-deployed. This paper describes the *designed* signing mechanism and the security properties it is built to provide, not a claim of a shipped, third-party-audited product. Secure-element and sensor part numbers are withheld from this public edition and provided to partners under NDA. EcoVent is pre-revenue and claims no certifications, pilots, or endorsements.

1 · The trust gap every commodity rail still has

In the gold trade — and in carbon, agriculture, medicine and every physical market — the digital record is created by a human typing a number a human measured. Between the assay bench and the certificate, the certificate and the database, the database and the token, there are people, spreadsheets and editable fields. Each is a place the number can drift, by error or fraud, and nobody downstream can tell.

Blockchains do not fix this. Writing a forged number to a chain only makes the forgery permanent. The hard problem is the **first inch**: getting an honest reading from the physical world onto the chain with no trusted human in the path. That first inch is what this bridge is for.

2 · Principle: the reading signs itself

The device does not send a number to a server a person then approves. It **measures, serialises and signs the reading inside tamper-resistant hardware**, using a private key that never leaves that hardware and that no operator — including EcoVent — can read or export. What travels onward is the reading *plus a cryptographic signature* over it. Anyone can later check that signature against the device's public identity; if a single byte of the reading is altered downstream, the signature no longer verifies and the on-chain contract refuses it. This is the physical form of the protocol's founding rule: **no verification, no token.**

3 · End-to-end: from atom to anchor

```
Physical asset → Measurement device (sensors → serialise → secure element: SIGN) → Relayer
(untrusted) → AttestationBridge (verify signature, mint iff valid) → Public ledger — trust
          ends at the chip: everything to its right is verifiable, not trusted —
```

The crucial line is drawn at the chip. **Everything to the right of the secure element is untrusted by design** — the relayer, the network, even our own servers cannot alter the reading without invalidating the signature. The blockchain is the final, public arbiter: it re-checks the signature itself before it will mint.

4 · The signing device

The unit pairs industrial-grade physical sensors with a **hardware secure element** — a tamper-resistant chip of the class used in payment cards and passports, purpose-built to generate and hold private keys that cannot be read out, only used to sign.

Key provenance

- **Born on-chip.** Each device's key pair is generated inside the secure element at provisioning. The private key is never exported or transmitted, and is not known to EcoVent, the operator, or the manufacturer.
- **Public identity registered once.** Only the device's public key is published and registered on-chain against a device ID; the contract later accepts readings only from registered devices.
- **Tamper response.** The element detects physical intrusion and zeroises its key material if attacked — a compromised device stops being able to sign rather than signing fraudulently.

What it binds together

At capture the device records the physical reading (for gold: mass, spectroscopic purity, derived density and geometry), a multi-constellation satellite geolocation fix, and a trusted timestamp. These are serialised into one canonical byte string in a fixed, documented order, and that exact string is hashed and signed — binding the *what*, the *where* and the *when* into a single inseparable attestation.

5 · The attestation object

```
attestation = {
  deviceId      : registered public identity of the unit
  readingBytes  : canonical fixed-order serialisation of the measurement
  readingHash   : hash( readingBytes )         // integrity fingerprint
  geo           : satellite position fix at capture
  timestamp     : trusted time at capture
  signature     : sign( readingHash )          // produced inside the secure element
}
```

The canonical byte layout is fixed and documented so that anyone — partner, auditor, regulator — can independently re-serialise the same fields, re-hash and re-check the signature. There is no proprietary verification step: the math is the audit.

6 · On-chain enforcement — the part that is live today

The signed attestation is submitted to the **AttestationBridge** contract on Polygon, the enforcement point of "no verification, no token":

- **Recover & check the signer.** The contract recovers the signing key from the signature and confirms it matches a device registered on-chain; an unregistered or mismatched signer is rejected.
- **Re-bind the reading.** It confirms the signature is over the exact reading submitted; a reading altered in transit no longer matches and is refused.
- **Price the matter independently.** For value-bearing mints, conversion to token units is driven by a live on-chain market-price oracle (Chainlink XAU/USD on Polygon), not an admin-typed rate — so neither the operator nor EcoVent sets the number that mints.
- **Mint only on a clean pass.** Only if signer, reading and price all check out does the bridge mint; the attestation and outcome are written to the public ledger permanently.

This software is deployed and source-verified on Polygon Mainnet now. The companion Proof-of-Reasoning contract (AI/model outputs) and the Anchor Registry (forecast & metric snapshots) run on the same chain. Live registry: polygonscan.com/address/0x6a99Ac76fE9CcC6D5cF4d1c3fe865079f6a1C5c6

7 · Threat model — where a human could cheat, and why they can't

Attack	Without VPAY	How the bridge closes it
`Edit in transit`	Relayer/server changes mass or purity before recording.	Signed at the chip; any change breaks the signature, contract refuses. **closed**
`Replay`	A real past reading re-submitted to mint twice.	Trusted timestamp + single device session; chain rejects duplicates. **closed**
`Spoof device`	A fake device fabricates readings.	Only on-chain-registered public keys produce accepted signatures. **closed**
`Backdate / relocate`	Claim a reading happened elsewhere/earlier.	Geo + time signed inside the same attestation; cannot be detached. **closed**
`Admin rate-set`	Insider tweaks the mint conversion.	Value mints price off a live external oracle, not an admin field. **closed**
`Extract device key`	Clone a trusted device.	Key born & held in tamper-resistant element, zeroised on intrusion. **by design**
`True signature over a false physical input`	Fool the sensor itself (e.g. a salted sample).	**Residual / out of scope for crypto.** Signing proves the device produced the reading, not that the sample wasn't physically tampered pre-measurement. Mitigated by sampling protocol, multi-gate physical checks and chain-of-custody. See §8.

8 · Limits & honesty

- **It proves authorship and integrity, not virtue.** A signature proves *this device produced this reading, unaltered, here, then* — not that the underlying sample wasn't physically manipulated before the sensor. That is a sampling/custody problem, addressed by protocol and multi-gate checks, not by the signature.
- **The hardware is pre-production.** The mechanism above is the engineered design on which partners are invited to evaluate the architecture; it is not a claim of a field-deployed, third-party-certified unit. An independent hardware security evaluation is part of the path to production.
- **The software is real now.** On-chain enforcement (§6) and the public registries are live and verifiable on Polygon Mainnet today.
- **Vendor specifics under NDA.** The exact secure element, sensor suite and provisioning ceremony are documented for partners in the NDA edition.