InfraVeritas — Witnessed Generation

A hardware root of trust for renewable energy attestation

Technical whitepaper · Version 1.0 · July 2026
InfraVeritas LLC · Sniatyn, Ukraine

Summary

Every renewable energy certificate in circulation today rests on a number that the seller reported about themselves. The meter belongs to the generator, the inverter firmware belongs to the manufacturer, and the data path from the panel to the registry is a chain of self-declarations that nobody outside the chain can independently check.

Granularity reforms — hourly certificates, 24/7 matching, EnergyTag — make that number more precise in time. They do not make it more trustworthy. An hourly certificate answers **when** electricity was allegedly produced. It does not answer **whether** it was.

InfraVeritas addresses the second question. A measuring device signs each measurement window inside a secure element whose private key was generated there and cannot be extracted — not by the owner, not by us, not by the manufacturer. An Ethereum contract verifies that signature against a key held in a device registry and records the statement permanently. A separate service, which is not the witness, cross-checks the statement against independent weather data and publishes its conclusions alongside — never inside — the record.

The result is a kilowatt-hour that a counterparty can verify without trusting the generator, the auditor, or us.

---

1. The problem: generation is reported, not witnessed

A guarantee of origin is issued on the basis of metered data submitted by the generator. The submission chain has three properties that would be unacceptable in any other measurement-based market:

The instrument is controlled by the party it measures. Inverter firmware is updatable by the manufacturer and, on many models, by the site owner. A measurement produced by software under the control of the beneficiary is a claim, not evidence.

The data path has no integrity guarantee. Values travel from inverter to portal to registry through interfaces where nothing is signed at origin. Any step can alter a number without leaving a trace that survives the next step.

Absence is invisible. When a monitoring system is offline, the gap is typically backfilled or interpolated. Nothing distinguishes “the plant produced nothing” from “nobody was watching.”

The market prices this. Guarantees of origin from jurisdictions with weaker verification regimes — Ukraine’s among them — trade at a substantial discount to their western European equivalents for electricity that is physically identical. That spread is distrust, denominated in euros. It is also the clearest available measure of what verifiable origin would be worth.

---

2. Why now: the regulatory clock

Three developments turn a long-standing weakness into a near-term compliance problem.

CBAM's definitive period. From 1 January 2026 the EU carbon border mechanism moves from reporting to payment. Electricity is in scope, and the default values that importers may use are punitive by design: the alternative is verified, granular data about the electricity actually consumed. The first enforcement of payment obligations, expected in 2027, is when a European importer's cost becomes directly sensitive to whether their supplier's generation data can withstand scrutiny.

RED III and 24/7 matching. Hourly matching of consumption to generation is moving from voluntary best practice into procurement requirements, particularly for hydrogen and for data centres with corporate clean-energy commitments. The finer the time resolution, the more the underlying measurement matters: an error that averages out over a year does not average out over an hour.

Ukraine's integration into the European certificate market. The national regulator joined the Association of Issuing Bodies in 2024, and market coupling legislation took effect in April 2026. Ukrainian generators gain access to a market that prices their certificates below equivalents — and gain, for the first time, a commercial reason to prove rather than assert.

Hourly certification makes fraud more precisely documented. It does not make it less possible. If the underlying measurement is unverified, finer granularity records the false number four times an hour instead of once.

---

3. The chain of custody

The system is built so that trust originates at the point of measurement and survives every subsequent step without requiring any of them to be trusted.

Measurement. A device measures voltage and current directly at the generation source — not through the inverter's reporting interface. Samples are taken evenly across the whole measurement window, so the energy figure is an integration over real time rather than an instantaneous snapshot extrapolated across an interval. The window length is measured by the device and carried inside the signed statement.

Signature in silicon. The private key is generated inside an ATECC608B secure element during provisioning and is never present in the device's memory, its firmware, or any file. The device cannot disclose it, and neither can its owner. Each epoch is serialised into a typed EIP-712 statement — seventeen fields, fixed order, frozen schema — and the resulting digest is signed by the chip itself. What travels over the network is a signature, not a secret.

Verification on chain. An Ethereum contract recomputes the digest from the submitted fields, retrieves the device's public key from a registry keyed by the hash of its certificate, and verifies the P-256 signature. The submitted statement carries no public key: substituting a different key is not prevented by policy, it is structurally impossible. A used epoch index cannot be submitted twice, whatever signature accompanies it.

Independent cross-check. A validator service compares each attestation against irradiance data from three independent weather services and against the device's own history, and publishes its conclusions.

Permanent, checkable record. Every field, the digest and the signature are in public transaction data. A third party can reconstruct the entire verification without asking us for anything — a two-hundred-line script in the public repository does exactly that.

The physical constraints the record must satisfy

Signatures establish authorship, not truth. A device with a valid key can still sign a false number. Three constraints bound what a signed statement can plausibly claim:

- **Energy, mean power and window length are locked together.** The contract enforces the arithmetic relationship between them, so claimed energy cannot be inflated without a correspondingly inflated measurement window.
- **Location is sealed at registration and proved by GPS at measurement.** An attestation whose coordinates drift beyond tolerance from the sealed position is rejected on chain, which is what makes cross-checking against weather at that location meaningful.
- **Generation is compared against irradiance.** Power reported during darkness is physically impossible for a photovoltaic array, and a device that reports it is either connected to something other than a panel or measuring incorrectly. Either way, the discrepancy is recorded.

---

4. The separation that matters

A witness with an interest in the verdict is not a witness.

This principle determines an architectural boundary that most comparable systems do not draw. The chain record contains only what the device measured and signed. The validator's conclusions — irradiance comparisons, statistical outliers, anomaly flags — are published separately and never enter the signed record.

The reason is practical, not philosophical. If the party operating the measurement network could also alter the immutable record of what was measured, the immutability would be decorative. By keeping the verdict outside the record, a dispute has something fixed to be about: the device's statement stands unchanged, and the validator's judgement of it can be challenged, overturned, or replaced by a third party's judgement without touching the underlying evidence.

The same reasoning excludes a design that several projects in this space adopt: issuing a token whose value depends on the measurement, to the same party that performs the measurement. A system that profits from the number it certifies has re-created, with additional steps, the conflict of interest it was built to remove.

---

5. Evidence: what is proven today

The following is running on real hardware — a bench device on the Sepolia test network, measuring a controlled direct-current load — and can be verified by any reader. Nothing in this section is a projection.

Cryptographic core on the chip. A secure element was irreversibly provisioned in July 2026; its key has never existed outside the chip. The device computes the EIP-712 digest on-chip and signs it there. The encoder is verified against reference vectors at every start-up, on the device itself: if the encoding ever drifted, the device would refuse to sign rather than sign something unintended.

End-to-end epochs on Ethereum. The device measures, signs and submits autonomously on a fifteen-minute grid. A representative attestation — transaction `0xcf1de65f…65720` — records 0.567 Wh integrated over a measured window of 791.996 seconds across 100 samples, with mean power 2.577 W. Anyone can check it:

```
node tools/verify-attestation.mjs 0xcf1de65f...
```

The tool pulls the transaction from a public node, decodes the attestation and signature from its calldata, recomputes the digest independently, reads the device key from the registry, and verifies the signature. It reports four independent checks and does not contact any InfraVeritas service.

Anomaly detection, demonstrated rather than described. On the night of 25 July 2026 a 2.6 W lamp was connected to the measurement channel. The device witnessed and signed the power honestly. The validator compared it against irradiance data showing darkness and flagged the discrepancy. The attestation remains on chain, unaltered, transaction `0x4a55071d…172b` — the record of what the device said, and separately the record of why it should not be believed.

Formal properties under adversarial search. Twelve invariants of the contract were held over ten million randomised call sequences: no epoch replay, no acceptance against a key outside the registry, no violation of the energy-power relationship, no acceptance outside the location tolerance, no role escalation. The previous architecture failed one of these — an attestation could be accepted against a substituted key — and the fix was structural rather than a patch.

Independent indexing. Chain events are indexed by a public subgraph on The Graph. The public register reads the chain layer from that indexer, not from our own database, so a visitor is not depending on our word for what the chain contains. The register also shows which measurement channels are installed on a given unit and which are specified but not yet fitted, so a reader never has to guess whether an empty column means zero or means absent.

---

6. Where this fits

Guarantees of origin. Attestations are not certificates and do not substitute for them. They are the evidentiary layer beneath a certificate: an issuing body or auditor can, for the first time, check the measurement rather than accept the submission. The natural path is a verified attribute attached to existing instruments, not a competing registry.

24/7 carbon-free energy. Hourly matching requires hourly data whose provenance can withstand a buyer’s due diligence. Corporate buyers with credible commitments — data centres in particular — are the first counterparties for whom the difference between reported and witnessed is a procurement criterion rather than a technicality.

CBAM. Importers who can substitute verified data for default values reduce their obligation. The verification quality of that data determines whether the substitution survives review.

Adjacent application. The same measurement, applied to performance rather than origin, addresses warranty disputes, lender covenants and parametric insurance — situations where the disagreement is about what a plant actually produced, and where an instrument controlled by one of the parties is unsatisfactory to the other.

Positioning. Platforms building hourly matching and granular certificate infrastructure improve the resolution and logistics of the existing data. They consume the number; they do not verify it. This is

a complementary layer, and the natural relationship with those platforms is supply rather than competition.

Company

InfraVeritas LLC — EDRPOU 46373384, Sniatyn, Ivano-Frankivsk region, Ukraine.

United States provisional patent application **63/876,031** covering the verification architecture.

Contracts, normative specifications, the indexer and the verification tool are published under a source-available licence. Device firmware, the validation service and the internal architecture and threat models are not published: everything required to *verify* is public, everything required to *produce* is not.

Public register: **verify.infraveritas.pro**
Repository: **github.com/sidliarchukpetro/infraveritas-verify**
Contact: **petro@infraveritas.pro**

This document describes a system under active development. Every statement about what has been demonstrated is limited to what can be independently verified from public data as of July 2026 — the transactions cited above are the whole of the claim, and the tool that checks them is public. Nothing here is an offer of securities or an investment recommendation.