Verified Provenance

The missing infrastructure of trusted trade.

TaaP

Traceability as a Platform | Anything · Anytime · Anywhere

Executive Summary

Almost every claim a government acts on at its border — where a good came from, what it's made of, whether it qualifies for a preference, whether it was made with forced labor or felled from a protected forest — is **self-attested.** Someone declares it; the system records the declaration; nobody verifies it until something goes wrong. That single weak point is why trade preferences leak, why forced labor and deforestation rules can't be enforced at scale, why illicit minerals launder into formal markets, why honest premium producers can't prove they're honest, and why customs revenue quietly bleeds.

The fix is not more paperwork, a bigger database, or a smarter guess. It's an **infrastructure layer that authenticates provenance at the source, against a published international standard, before goods move** — and that leaves each government governing its own data and owning its own enforcement. Verified data, not inferred intelligence.

This layer is dual-use by nature: the same authenticated record lets an **exporter** prove quality and access a market, lets an **importer** verify what it's bringing in is secure and compliant, and lets a **revenue authority** catch the fraud it's missing today. And it's interoperable — when two governments adopt it, their verifications recognize each other, so compliance work done once travels.

The team behind TaaP operates this layer in production today across roughly 29 independent state and territorial authorities, and TaaP itself runs an active polysilicon provenance pilot. This paper makes the case for it as public infrastructure.

1. The problem is structural, not operational

Every border runs on declarations. An exporter or its agent states a country of origin, a tariff classification, a value, and — increasingly — a set of compliance attestations: this timber wasn't felled from protected forest, this metal didn't come from a sanctioned mine, this product wasn't made with forced labour. The customs or revenue authority records the declaration and, in the overwhelming majority of cases, acts on it. Verification, where it happens at all, happens by exception: an audit sample, a physical inspection, an investigation opened after a tip or an anomaly — usually long after the goods have cleared and dispersed.

This is not a failure of any one agency's diligence. It is the design of the system. Global trade moves on self-attestation because nothing better has been available at scale. And **self-attestation** has a predictable set of failure modes that every trading nation now lives with:

- **Preferences leak.** Trade agreements grant duty-free or preferential access based on origin. But origin is declared, not proven, so goods are transshipped — routed through an intermediate country, lightly processed or simply relabelled — to capture a preference or dodge a duty they don't qualify for. The benefit meant for one country's producers is captured by another's.
- **Compliance rules outrun enforcement.** Forced labour import bans, deforestation regulations, conflict-mineral due-diligence rules, carbon-content requirements — the obligations have multiplied far faster than the means to verify them. A rule that depends on documentation that is easy to fabricate is a rule that is enforced against the honest and evaded by the rest.
- **Illicit material launders into the formal market.** Minerals mined illegally or extracted in sanctioned or conflict zones, fish caught outside quota — once it enters a formal supply chain without a verified origin record, it is indistinguishable from legitimate product. The formal economy becomes the laundromat for the informal one.
- **Honest premium producers can't prove it.** A producer of genuinely clean, ethically-sourced, sustainably-harvested goods has no durable way to prove that claim to a sceptical buyer or a foreign regulator. The premium that should reward good practice is competed away by cheaper product making the same claim with no basis.
- **Revenue bleeds.** Undervaluation, misclassification, and origin fraud are, in aggregate, an enormous and largely invisible drain on customs revenue — invisible precisely because the system has no way to test the declarations it collects.

These look like five different problems handled by five different parts of government. They are one problem wearing five hats. **The common root is that the claim is never verified at the point and moment it could be.**

2. Why the usual fixes don't fix it

Governments have tried to close this gap, and the standard approaches each run into a wall:

- **More documentation** raises the cost of compliance without raising its reliability. A thicker paper file is still a paper file — self-attested, easy to forge, and impossible to check at volume.
- **Bilateral data-sharing agreements** work between two willing, capable partners and stop there. They don't scale to the dozens of trading relationships a country actually has, and they founder on the question every government rightly asks: what happens to my data once it leaves my control?
- **Centralized databases** ask sovereign authorities to pool sensitive commercial and personal data in a system someone else runs. That is a non-starter for most governments, and correctly so.
- **Pure AI inference** — scoring risk by pattern-matching across third-party signals — is useful, but it infers; it does not verify. It produces a probability, not proof. A probability is a reason to look closer; it is not an audit-defensible record you can take to an enforcement proceeding or a trade dispute.

What's missing is not analysis. It's **ground truth** — an authenticated record of what actually happened, captured where and when it happened, that each government can rely on without surrendering its data into a system someone else runs.

3. The principle: verified data over inferred intelligence

The distinction that organises everything below is simple and it is the whole argument:

Most supply-chain systems aggregate signals and infer relationships through pattern-matching. The result is a probability. A verified-provenance system records authenticated, participant-attested events at the source and checks each later step against them. The result is a deterministic, audit-defensible record of where a good actually came from, who handled it, and what claims about it have been independently verified.

Concretely: origin is recorded against a registered entity at the moment of extraction or origination — stamped with location, time, and quantity, and cryptographically anchored before the goods move. Every subsequent step is a handshake against that original record. If product appears downstream without a matching upstream record, the system flags it automatically. The mechanism is deterministic and rules-based, not probabilistic — which means it is explainable, auditable, and defensible, the three properties an enforcement action or a trade dispute actually requires.

This is the difference between "we have reason to suspect" and "we have a record." For high-assurance decisions — revenue recovery, market-access determinations, forced labour or sanctions enforcement — only the second is worth much.

4. The Architecture

Underneath the principle is an architecture that has to be commodity-agnostic (a government's needs span minerals, food, timber, manufactured goods), jurisdiction-agnostic (it must work across borders without a common legal authority), and sovereignty-preserving (no government will adopt infrastructure that extracts its data). Four design choices make that possible.

A small set of event types. The data model is built around six event types that, between them, cover the full supply-chain lifecycle across commodity types: three origin events — mining (minerals, metals, fuels), harvesting (timber, coffee, cocoa, fisheries), and recycling (recovered and circular-economy inputs) — plus adjustment (an attribute changes — a weight correction, an assay, a grade — but custody and composition don't), transformation (smelting, refining, manufacturing — inputs are consumed and a new output identity is created, referencing its inputs so traceability survives physical change), and shipment (custody changes hands; the transfer is recorded as a handshake against the existing record). The same six describe a mine, a farm, a recycler, or a factory — which is what lets one model span very different commodities rather than a separate system per domain.

Four independent conformity layers. Following the structure codified in the international standard discussed in Section 5, the work is deliberately split among separate parties so no single actor can quietly corrupt the record:

1. **Tracking —** custody events, transfers, transformations, and rules-based checks on chain-of-custody completeness. (TaaP operates this layer.)
2. **Authentication** — tamper-evident, blockchain-anchored Certificates of Authenticity, issued by an independent authentication provider.
3. **Validation —** deterministic rules: documentation completeness, handshake verification, volume reconciliation, entity-history consistency. No black-box scoring.
4. **Oversight —** final adjudication and enforcement, which **stay with the government.** The platform supports the process; it never replaces the authority's decision.

The separation is the point. It assumes false or incomplete documents will be introduced somewhere along the chain and catches them through independent validation rather than trust.

Federated data, sovereign control. Each participating authority governs its owwn data, configures its own rules, and enforces its own access controls. How much of the stack sits inside the authority's own environment is a deployment choice — the same SaaS platform, hosted three ways: a TaaP-hosted multi-tenant service, a hybrid model, or a fully sovereign tenant in the authority's own cloud. In a hybrid or sovereign deployment, sensitive data (operator identities, coordinates, volumes, commercial terms) and the keys protecting it stay in the authority's environment; what crosses a boundary is the agreed signal — origin verified, conformity documented — never the underlying records that privacy and commercial-confidentiality law protect. This is what makes cross-border cooperation possible without anyone ceding control: the coordination problem is identical whether the participants are independent domestic regulators or sovereign customs administrations.

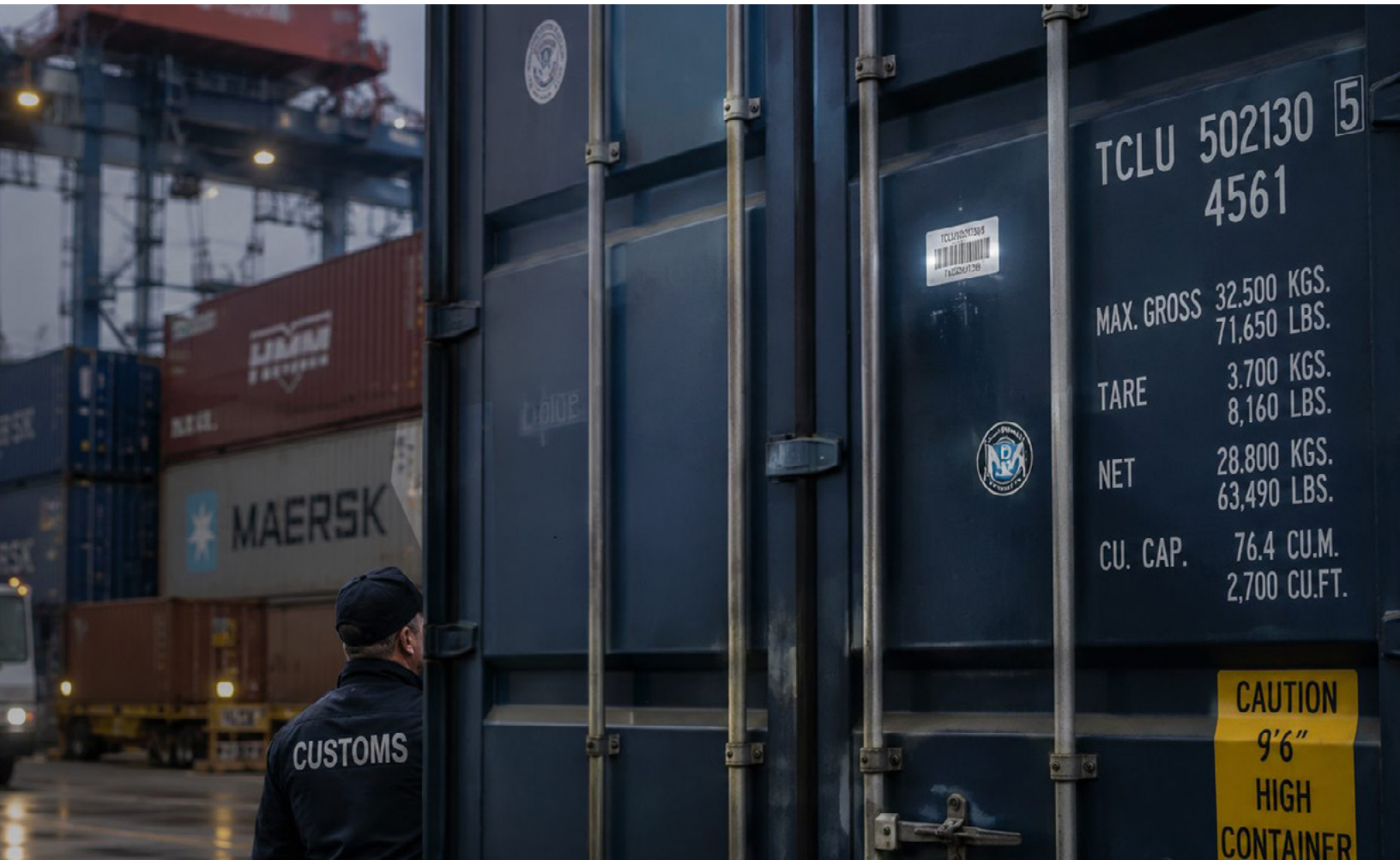
Configuration, not custom code. New commodities, new origin combinations, and new rules are added by configuration. New jurisdictions onboard through configuration rather than multi-year integration programs. And hardware is bring-your-own — QR, RFID, sensors, whatever fits the commodity and the budget — so the platform is a substrate, not a vendor lock-in.

5. Why a Published Standard Is the Linchpin

"Verified" is a marketing word until someone defines it. The element that turns this from a vendor's claim into public infrastructure is that the methodology implements a **published international consensus standard:** ASTM D8558-25, the first such standard for distributed-attestation supply-chain traceability. It specifies what data must be present at each step, what authentication is required, who validates it, and who retains oversight. With it, "verified" has a specification a government can point to — not a vendor's promise.

This matters for three reasons that compound:

- **It is neutral.** A consensus standard is authored by a standards body, not by the platform implementing it. The government adopts a standard, not a supplier. (TaaP implements D8558-25 under direct guidance from members of the technical subcommittee that authored it — but treats the standard as a guiding framework, not a dependency. The standard is the public good; the platform is one way to operationalize it.)
- **Accreditation travels.** The standard sits on top of the established ISO/IEC conformity-assessment system — the same architecture of accredited verification and validation bodies, certification bodies, and testing laboratories, overseen by accreditation bodies that recognize each other internationally through long-standing mutual-recognition arrangements. Verification work performed against the standard in one jurisdiction is recognizable in another. Compliance done once can be relied on more than once.
- **It is the path international trade law already prefers.** The WTO Agreement on Technical Barriers to Trade directs members to base measures on international standards where they exist, precisely to avoid each country inventing its own incompatible rules. Building enforcement and facilitation around a recognized consensus standard is the path the multilateral system points to — not an exception to it.



6. The Universal Hook: Comply Once, Sell Everywhere

Here is what makes this argument land the same way in a capital that mostly exports, one that mostly imports, and one wrestling with illicit extraction — the regulatory landscape every trading nation now faces is converging on provenance.

The customs world already runs on shared frameworks: the WCO Data Model and SAFE Framework of Standards, and the WTO Trade Facilitation Agreement, all push toward standardised, advance, electronic trade data. On top of that, a wave of market-access conditions now turns on verified provenance and supply-chain attributes:

- **Deforestation rules** require proof that commodities like timber, cattle, cocoa, coffee, soy, palm, and rubber were not produced on recently deforested land — with geolocation back to the plot.
- **Critical-raw-materials and battery rules** require provenance and recycled-content data and are introducing digital product passports that carry that data with the good.
- **Carbon border measures** require verified data on the embedded emissions of imported goods.
- **Forced labour import bans and corporate due-diligence duties** require importers to document that their supply chains are clean — and increasingly shift the burden onto the producer to prove it.

For a producing nation, these are not four problems; they are one capability. A single authenticated provenance record — origin, chain of custody, conformity to a recognized standard — is what each of these regimes is asking for, in different words. **Build the verification once, and your exporters can satisfy several markets' rules at the same time,** instead of running a separate, duplicative, fakeable paper exercise for each. That is a direct, quantifiable reduction in the cost of market access — and a competitive advantage a government can offer its own producers.

This is the dual-use payoff stated plainly: the same infrastructure that an exporting ministry wants for market access is the infrastructure an importing ministry wants for security and compliance, and the infrastructure a revenue authority wants for enforcement. They are the same system seen from three doors.

7. Sovereignty & Governance: The First Objection, Answered

Any government weighing infrastructure like this has three fair questions up front: who holds the data, is there lock-in, and who keeps control of enforcement. The architecture answers each one by design.

- **Deploy it to your sovereignty rules.** Hosting and key custody are a deployment choice — the same SaaS platform, hosted three ways: TaaP-hosted (multi-tenant), hybrid, or a fully sovereign tenant in your own cloud. Where your law requires it, sensitive data and the keys protecting it stay in your environment and only the agreed signal leaves your boundary. The design fits national data-protection law, not the other way around.
- **Oversight stays with you.** The platform structures and verifies; it never adjudicates. Enforcement decisions, penalties, and final determinations remain entirely with the responsible authority.
- **No lock-in.** Configuration over custom code, bring-your-own-tracker, and an open, published standard mean a government is adopting an interoperable capability, not a proprietary dependency. The standard is public; the data is yours; the hardware is your choice.
- **Self-sustaining.** The model proven at scale recovers its cost through participant and third-party scheme fees rather than ongoing government funding — the same way long-running conformity-assessment schemes (organic certification, product-safety testing) have funded themselves for decades.

8. This is Operating Today, Not a Concept

The architecture above is not a proposal on paper. The team behind TaaP built and operates **Metrc**, the largest multi-jurisdictional regulated-commodity track-and-trace system in the United States — the mandated infrastructure that tracks every unit of **legal cannabis** from seed to sale across roughly **29 independent state and territorial authorities.** That is one of the most demanding traceability mandates in existence: a high-value, diversion-prone commodity where every unit is legally accountable to a government regulator, in continuous production for **15 years:**

- ~29 independent authorities on shared infrastructure, each retaining control of its own data and rules
- 43 million transactions per day at sub-second response
- 13.9 billion event records to date; more than 500 third-party integrators across 165 API endpoints
- 500,000-plus users, from individual operators to multi-site enterprises
- 100% government contract retention over 15 years

That production architecture is now carried into commodity work beyond the regulated-goods base: an active polysilicon provenance pilot tracing roughly 6.5 billion dollars in annual downstream trade value across about 90,000 shipments from raw-material source to border arrival, with pallet-level authentication. The same architecture extends to any extractive or regulated commodity without a redesign.

The capability is delivered by a small, fit-for-purpose team rather than a fixed consortium. **TaaP** provides the platform — the founding team previously built and operates the system described above, and the underlying method is patented. An **independent authentication provider** supplies the layer behind the Certificates of Authenticity. When a use case genuinely needs machine-learning risk scoring on top of verified data, that comes from an **AI/ML analytics partner** with 25 years of government import-risk work — including the risk engine behind the US FDA's import-screening system (which the partner reports processes 130 million transactions a year at sub-tenth-of-a-second scoring) and customs risk systems for European anti-fraud and other national authorities. And standards and customs expertise comes from advisors including the chair and vice-chair of the subcommittee behind D8558-25 and a former senior customs leader with three decades across major ports.

9. What Adoption Looks Like

Adoption is phased and low risk by design:

1. **Scope and pilot.** Pick one commodity or one corridor where the pain is sharpest — illicit extraction, a leaking preference, a compliance exposure. Stand up the platform against it, ingesting the data formats source agencies already use, with nothing to reformat first.
2. **Prove and measure.** Run the pilot against real flows, measure what it surfaces (undocumented product, capacity mismatches, transshipment patterns, recoverable revenue), and validate the conformity record against the authority's own enforcement needs.
3. **Scale by configuration.** Extend to new commodities, corridors, and participating agencies by configuration, not rebuild. As neighboring or partner jurisdictions adopt the same standard, verifications begin to recognize each other and the value compounds.

10. The Argument, In One Line

Verified provenance is the missing infrastructure layer of the trading system — the layer that turns a self-attested declaration into ground truth. It serves the exporter, the importer, and the revenue authority at once; it preserves sovereignty by design; it rests on a published international standard rather than a vendor's promise; and it is operating in production today. Governments that build it first will help set the terms on which trusted trade flows through their borders and offer their producers a credential the rest of the world is already asking for.