FOUNDATION FOR AI-READY EMERGENCY SERVICES

911 Trust Ledger

Building the Trust Fabric for America’s 911 Data

Jon Whirledge, Founder

hello@911trustledger.org

www.911trustledger.org

“Trust is the invisible network behind every call for help. The moment that trust fails, everything else does too.”

240M+

911 calls placed in the US each year

6,000+

PSAPs with no unified trust layer

3

Architecture layers that change everything

0

Verifiable cross-system audit trails today

What 911 Needs — and Why It Doesn’t Exist Yet

Every day, across the United States, thousands of 911 calls are made — and each one is a test of trust. Trust that the call will route correctly. Trust that location data is accurate. Trust that systems will work together when seconds matter most.

Behind that trust lies an invisible digital ecosystem — dozens of independent systems and vendors, each passing critical pieces of information between them. Every event leaves behind digital fingerprints: timestamps, routing decisions, CAD updates, recordings, and responder logs. Together, these fragments tell the story of what happened when someone called for help.

And yet, there is no single verifiable record of that story. No shared proof of what happened, when, and who validated it. No foundation on which AI systems can build with confidence. No infrastructure that connects trust across every link in the emergency-response chain.

The 911 Trust Ledger Foundation (911TL) was created to close this gap — not by rebuilding 911, but by giving it a foundation of verifiable, structured, and economically self-sustaining trust.

> *“AI in public safety isn’t a question of if — it’s a question of whether the data it runs on can be trusted. 911TL makes that trust verifiable.”*
>
> **— Jon Whirledge · Founder, 911 Trust Ledger Foundation**

Fragmented Trust in Public-Safety Data

For most of its history, the 911 system has relied on cooperation rather than verification. Carriers, service providers, PSAPs, CAD vendors, and radio networks depend on one another — yet no mechanism exists to independently prove what happened once data moves between systems.

When 911 was local and analog, that was acceptable. As Next Generation 911 (NG911) moves call handling, location, and data exchange into digital networks, the old assumptions no longer hold. And as artificial intelligence enters public safety — predictive dispatch, real-time analytics, automated triage — the absence of verifiable data provenance becomes a systemic risk.

Four Structural Gaps

01

Fragmented records, no shared truth

Carriers, ESInets, PSAPs, and CAD vendors each maintain their own logs. None can prove their version matches another's. Every audit starts from scratch.

02

AI requires provenance

For AI to act reliably on 911 data — routing decisions, resource allocation, anomaly detection — it needs to know that data hasn't been altered, delayed, or corrupted in transit. Without provenance, AI outputs cannot be trusted or defended.

03

Liability grows with digitization

As NG911 fully digitizes, the inability to prove what happened — and when — becomes an operational, legal, and regulatory exposure for every vendor and agency in the chain.

04

No substrate for AI innovation

The 911 ecosystem generates extraordinary operational data. Today, that data is siloed, inconsistent, and inaccessible to the AI systems that could transform emergency response. The missing ingredient is not data volume — it is verified, normalized, AI-ready data infrastructure.

Why Existing Tools Fall Short

Public safety has made major strides in digitization and interoperability. None of the current approaches fully solve the trust problem.

Challenge	Existing Approach	911TL Advantage
Databases can be modified or owned by one entity	Centralized logging	**Distributed, tamper-evident records maintained by peers**
PKI is cumbersome across jurisdictions	Digital certificates	**Built-in, multi-party validation — no manual key exchange**
APIs exchange data but can't prove integrity	i3 / EIDO	**Each transaction notarized, producing verifiable proof**
Public blockchains lack privacy	Blockchain pilots	**Permissioned, private, and community-governed on Hyperledger Fabric**
No AI-ready data substrate exists	None	**Normalized data layer with verified provenance for AI systems**

Three Layers. One Pipeline. One Connection.

911TL provides the missing infrastructure through three integrated layers — each purpose-built, each building on the one beneath it. A vendor connects their i3 log stream to 911TL once. That single passive connection simultaneously powers all three layers with no additional integration required.

The three-layer architecture — Trust, Data, and Economic — each derived from the same i3 log stream.

Layer 1 — The Trust Layer

The Trust Layer is the foundation. Every critical event in the 911 workflow — call received, location resolved, call routed, PSAP answer, dispatch created, incident closed — generates a cryptographic proof. That proof stores only a hash (a cryptographic fingerprint) and digital signatures from the systems involved, never the underlying private data.

Built on Hyperledger Fabric — the open-source, enterprise-grade permissioned blockchain framework governed by the Linux Foundation — the Trust Layer creates an immutable, cross-agency audit trail. Participation is mandatory for all 911TL network members. It is the public good that the entire ecosystem depends on.

Layer 2 — The Data Layer

From the same i3 log connection, the 911TL pipeline simultaneously generates normalized, PII-free structured event records. These records capture the operational substance of each 911 event — event type, timestamps, routing path, resource dispatch, outcome classification — transformed so that no personally identifiable information is present. What remains is operationally rich and AI-ready.

Crucially, these records are stored locally in the participant's own infrastructure. The data never leaves their control. The Foundation never holds it. Participants decide independently how they want to participate:

> **Local use only** — The participant uses their local data store for their own operational analytics, quality improvement, and compliance — with no obligation to contribute to the shared commons.

Selective contribution — The participant chooses which data types or event categories to share with the commons — dispatch outcomes but not routing metadata, for example — and can adjust or withdraw at any time.

Full contribution — The participant contributes their full normalized event stream to the commons, maximizing their share of ecosystem rewards.

This optionality is not a compromise — it is the architecture. Sovereignty must be structural, not a policy promise. Because the data physically lives in the participant's infrastructure, “your data never leaves your control” is a verifiable technical fact.

Layer 3 — The Economic Layer

The Economic Layer is what makes 911TL self-sustaining and what aligns the interests of every participant toward growing the ecosystem. AI companies and analytics consumers pay licensing fees to access the data commons. Those fees flow into the Foundation, which distributes rewards back to contributors and validators proportional to their participation.

Contributors earn — Participants who contribute data to the commons earn rewards proportional to the volume, quality, and access frequency of their contributions.

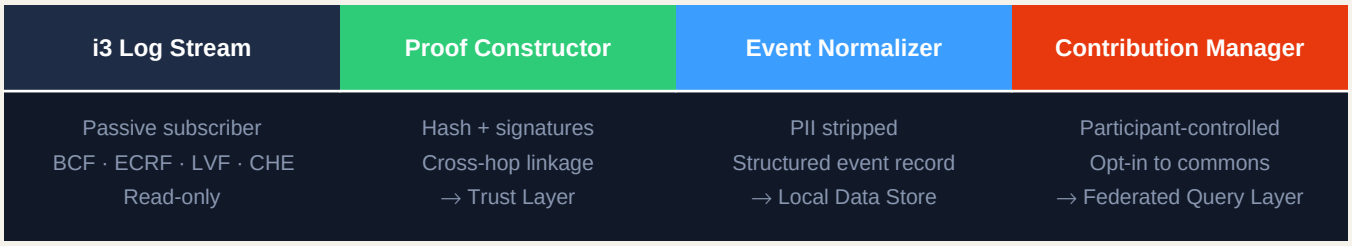
Validators earn — Nodes that maintain the Trust Layer ledger — ordering, endorsing, and archiving — earn for their role in sustaining the infrastructure.

Foundation operates — A portion of licensing fees funds Foundation operations: maintaining the open protocol, governing the network, and developing the ecosystem.

Protocol is open — The 911TL protocol is open-source. Any vendor can build on it. Access to the data commons is licensed. This distinction — open protocol, licensed data — is what makes the economic model durable.

One Connection. Three Outputs.

The elegance of 911TL's architecture is that the entire three-layer system is powered by a single passive connection to a vendor's existing i3 log stream. No new data sources. No bespoke integration per vendor. No modification to any ESInet component. 911TL observes and records — it never touches a 911 call.



The 911TL pipeline: one i3 log connection produces three outputs simultaneously.

Step 1 — Connect

A participating vendor connects their i3 log stream to 911TL's passive subscriber service. The subscriber attaches to existing NENA i3 log streams across BCF, ECRF, LVF, and CHE functional elements as a read-only downstream consumer. No upstream impact. No modification to the vendor's systems.

Step 2 — Generate Proof

From each i3 log record, the Proof Constructor generates a cryptographic fingerprint — a hash of the event data plus digital signatures from the originating components. Cross-hop linkage pointers chain each proof to the prior hop in the call's traversal path, forming a verifiable chain of custody from first ring to final dispatch.

Step 3 — Normalize Event Record

Simultaneously, the Event Normalizer processes the same i3 log record into a structured, PII-free event record. Identity-bearing and location-bearing fields are transformed at the point of processing — ANI becomes a call category, precise location becomes a jurisdiction code or census tract, caller identity becomes anonymized repeat-caller metadata. The normalized record carries operational meaning without carrying personal data.

Step 4 — Store Locally

Both outputs — the cryptographic proof and the normalized event record — are stored in the participant's local infrastructure. The proof is submitted to the Trust Layer ledger. The normalized event record is written to the participant's local data store. The participant has immediate access to both for their own operational use.

Step 5 — Contribute (Optional)

Through the Contribution Manager — a participant-facing interface for configuring data sharing — the participant chooses whether to contribute their normalized event records to the shared commons, which data types to include, and under what terms access is granted. Every query against their data is visible to them. They can adjust or withdraw their contribution at any time.

The AI Substrate for Emergency Services

When participants contribute their normalized event records to the shared commons, something extraordinary becomes possible: a verified, cross-jurisdictional, AI-ready dataset covering the full operational reality of emergency response in the United States.

This dataset doesn't exist anywhere today. Not in any government database. Not in any vendor's data lake. Not in any research archive. 911TL creates it as a byproduct of infrastructure that participants are already deploying for the Trust Layer.

What the Commons Contains

Event type and subtype — Call received, transfer, dispatch, incident closed — normalized across all vendors and jurisdictions.

Verified temporal sequences — What happened in what order, with cryptographic proof of timing anchored to the Trust Layer.

Routing paths — How calls traversed the ESInet — which components handled them, where handoffs occurred, where delays arose.

Resource dispatch records — What type and quantity of resources were dispatched, response time from dispatch to arrival.

Outcome classifications — How incidents resolved — anonymized, jurisdiction-coded, operationally meaningful.

Cross-jurisdictional patterns — The signal that makes AI powerful: aggregate behavior across thousands of incidents, hundreds of PSAPs, dozens of states.

What the Commons Does Not Contain

No caller identity. No precise location. No ANI or ALI. No recordings. No information that could identify any individual involved in any 911 call. This is not a policy choice — it is a structural guarantee enforced at the point of data generation, before any record enters the local data store.

How AI Companies Access It

The Foundation operates a federated query brokerage — an access layer that routes licensed queries to participant data stores and returns results, without the Foundation ever holding the data centrally. AI companies query through the Foundation's API. The API routes to contributing participants' local stores. Results are returned to the consumer. The participant sees every query against their data.

Access is licensed. Licensing fees are the economic engine that funds Foundation operations and distributes rewards to contributors and validators. The more the commons is used, the more participants earn. This flywheel — contribution drives value, value drives licensing revenue, revenue drives rewards, rewards drive contribution — is what makes 911TL self-sustaining.

Community-Governed. Foundation-Stewarded.

The 911 Trust Ledger Foundation is governed by its members, drawn from the 911 community — PSAPs, ESInet operators, carriers, vendors, and state authorities. The Foundation is the highest level of governance authority for the network, but that authority is community-held. No single vendor, carrier, or government entity controls it.

This model is not novel — it is the proven governance structure of the most durable technology commons ever built. The Linux Foundation. The Internet Engineering Task Force. The Apache Software Foundation. Each is governed by its community of participants, with a neutral steward ensuring the infrastructure serves the commons rather than any single interest.

Foundation Governance — Sets participation rules, privacy policy, consensus policy, and the economic framework. Governed by the membership. No single member has veto power.

Technology Stewardship — Maintains the open-source Hyperledger Fabric codebase, documentation, and independent security audits. The protocol belongs to the community.

Access Brokerage — Operates the federated query layer through which AI companies access the data commons. Enforces licensing terms and distributes rewards to contributors.

Ecosystem Development — Coordinates collaboration among 911 authorities, service providers, technology partners, and standards bodies including NENA and EIDO.

Relationship to NENA Standards

911TL is designed to extend NENA standards where they do not yet anticipate the NG911 future — not to compete with or replace them. Every integration point anchors to an existing NENA standard: i3 logging for proof generation, NENA PCA for node credentials. Every integration point is also built behind an abstraction layer so that as NENA standards evolve, 911TL evolves with them.

Where 911TL’s native specifications mature — the proof type registry, the normalized event schema, the federated access framework — they may inform future NENA standards rather than diverge from them. The goal is a 911TL that is deeply interoperable with the existing ecosystem on day one, and a contributor to that ecosystem’s evolution over time.

Built for Everyone in the NG911 Ecosystem.

NG911 Vendors & Integrators

Connect your i3 log stream once. Deliver verifiable data integrity to your customers. Reduce audit overhead and liability exposure. Earn rewards for validator participation. Build on open APIs and reference implementations.

AI & Technology Companies

Access a verified, normalized, cross-jurisdictional dataset that doesn’t exist anywhere else. Build models on data with cryptographic provenance. Meet regulatory and compliance expectations for AI in public safety.

PSAPs & State 911 Authorities

Deploy the Trust Layer as mandatory compliance infrastructure. Keep your data in your own infrastructure. Use your local data store for operational analytics. Earn rewards by contributing to the commons on your own terms.

Investors & Foundations

Fund the infrastructure AI can’t work without. A self-sustaining economic model with a clear path from pilot to national standard. Modeled after the most successful open infrastructure foundations ever built.

Standards Bodies & Regulators

A community-governed, open-protocol approach that extends NENA i3 and aligns with NG911 modernization objectives. A neutral infrastructure layer that no single vendor or agency controls.

Research & Academic Partners

A verified, longitudinal dataset of emergency response operations at national scale — available through licensed access. The foundation for evidence-based public safety policy and AI research.

From Infrastructure to Ecosystem.

Phase 1

Core Infrastructure

Launch the Trust Layer on Hyperledger Fabric. Demonstrate event notarization without operational disruption. Establish the Foundation governance framework. Deploy the local data store alongside the node software.

Phase 2

Data Layer & Commons

Activate the Event Normalizer and Contribution Manager. Onboard founding data contributors. Launch the federated query brokerage. Publish the normalized event schema as an open specification.

Phase 3

Economic Layer

Launch the licensing framework and reward distribution mechanism. Onboard initial AI and analytics consumers. Demonstrate the economic flywheel — contribution drives rewards, rewards drive contribution.

Phase 4

Scale & Standards

Expand participation nationally. Engage NENA and standards bodies with 911TL-native specifications for potential standardization. Grow the AI ecosystem built on the commons. Every new participant strengthens the network; every improvement contributes to the public good.

Trust as Infrastructure, Not Policy.

Public safety agencies and service providers face growing operational and legal exposure as public safety data becomes fully digital. The integrity of that data — and the ability to prove it — now defines both compliance and liability.

The 911 Trust Ledger introduces a verifiable chain of custody for public safety metadata. Each participating system generates a cryptographic proof and timestamp, creating an immutable, tamper-evident record that supports both auditability and legal defensibility.

Audit Readiness — Unified, verifiable records simplify incident reconstruction and oversight. A complete cross-agency audit trail is available on demand.

Regulatory Alignment — Supports NENA i3, EIDO, and state reporting requirements through verifiable provenance. Designed to complement, not compete with, existing compliance frameworks.

Data Integrity Assurance — Immutable hashes prevent undetected alteration or deletion. Entries cannot be modified without detection by every other participant on the network.

Liability Reduction — PSAPs reduce liability through provable logs. Service providers share accountability with neutral, validated records. Vendors enhance public confidence with verifiable evidence of system performance.

Privacy by Architecture — No PII is ever stored on the Trust Layer or Data Layer. This is a structural guarantee enforced at the point of data generation — not a policy that depends on administrative controls.

When Trust Becomes Infrastructure.

When public safety data becomes verifiable and AI-ready, everything built on top of it becomes stronger. The transformation is not incremental — it is structural.

Accountability

Every data handoff is provable. Disputes are resolved by the record, not by manual reconciliation between competing logs.

Resilience

Verified data can be reconstructed even if a local system fails. The distributed ledger survives the loss of any single node or participant.

AI Innovation

AI and analytics systems can safely rely on data with known provenance. The 911TL data commons is the substrate that makes AI in public safety trustworthy.

Transparency

Agencies can demonstrate integrity to regulators and the public without exposing sensitive information. Trust is proven, not asserted.

Economic Alignment

Participants are rewarded for contributing to the commons they depend on. The more the ecosystem grows, the more every participant benefits.

Foundational Infrastructure

Just as HTTPS became the foundation of secure communication online, 911TL can become the foundation of trustworthy communication in public safety.

“Public safety runs on trust. 911TL makes that trust verifiable, AI-ready, and economically self-sustaining.”

— Jon Whirledge · Founder, 911 Trust Ledger Foundation

The Proof Beneath the Promise.

Technology alone doesn’t build trust — people and institutions do. But technology can prove that trust was earned.

The 911 Trust Ledger Foundation ensures that every piece of public-safety data carries evidence of integrity. It gives responders, policymakers, and the public confidence that when help is needed most, the systems they rely on are transparent, resilient, and accountable.

And for the AI companies, analytics vendors, and technology innovators who will build the next generation of emergency services tools — 911TL provides the foundation they cannot build without: verified, normalized, provenance-anchored data at national scale, governed in the public interest, accessible under a framework that rewards every participant who makes it possible.

This isn’t blockchain for its own sake. It isn’t a data play. It’s the quiet architecture of confidence — the proof beneath the promise that when you call 911, someone will answer, the truth of that call will always be preserved, and the systems that served you will keep getting better because of it.

Get Involved

hello@911trustledger.org
www.911trustledger.org