PROTOCOL OVERVIEW · 911 TRUST LEDGER FOUNDATION

911 Trust Ledger

Protocol Overview

Jon Whirledge, Founder
hello@911trustledger.org
www.911trustledger.org

“Three layers. One passive connection.
An immutable trust fabric for the NG911 ecosystem.”

PROTOCOL	INTEGRATION	DATA ON LEDGER	PII ON LEDGER
Hyperledger Fabric	**NENA i3 log stream**	**Cryptographic proofs only**	**Never**

PROTOCOL OVERVIEW

What 911TL Does

The 911 Trust Ledger (911TL) is an open, permissioned protocol that records cryptographic proofs of key events across the 911 workflow — not the data itself, but verifiable proof that the data existed, was accurate, and was properly handled. The result is an **immutable, cross-agency audit trail** that any participant can verify and no single party can alter.

911TL connects to existing systems through a single passive integration point — the NENA i3 log stream already present on every ESInet functional element. That one connection simultaneously powers three independent layers. Existing 911 operations are never touched, blocked, or altered.

THE THREE-LAYER ARCHITECTURE

Three Layers. One Pipeline. One Connection.

A vendor connects their i3 log stream to 911TL once. That single passive connection simultaneously powers all three layers with no additional integration required.

Economic Layer	Licensing & Rewards
Data Layer	Normalization & AI Commons
Trust Layer	Cryptographic Proof & Audit Trail

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 and digital signatures from the systems involved, never the underlying private data. Built on Hyperledger Fabric. Immutable. Tamper-evident. Community-governed. Participation is mandatory for all 911TL network members.

Layer 2 — The Data Layer

From the same i3 log connection, 911TL simultaneously generates normalized, PII-free structured event records stored locally in the participant's own infrastructure — the Foundation never holds them. Participants choose: local analytics only, selective contribution to the shared AI commons, or full contribution maximizing their ecosystem rewards. Local sovereignty is structural, not a policy promise.

Layer 3 — The Economic Layer

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. The more the commons is used, the more participants earn. Contribution drives value, value drives revenue, revenue drives rewards, rewards drive contribution.

HOW IT WORKS

One Connection. Three Outputs.

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.

i3 Log Stream	Proof Constructor	Event Normalizer	Contribution Manager
Passive subscriber BCF · ECRF · LVF · CHE Read-only	Hash + signatures Cross-hop linkage → Trust Layer	PII stripped Structured event record → Local Data Store	Participant-controlled Opt-in to commons → Federated Query Layer

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

Step 1 — Connect

A vendor connects their ESInet functional element's i3 log stream to 911TL once. The integration is passive — 911TL subscribes as a downstream observer. No call traffic is touched, delayed, or rerouted.

Step 2 — Generate Proof

For each relevant event, the Proof Constructor creates a cryptographic proof: a hash of the event data plus digital signatures from the contributing system. PII fields are hashed before they reach this stage.

Step 3 — Sign & Submit

The proof is signed using the participant's NENA PCA-grounded key and placed in an async submission queue. Ledger latency has zero impact on 911 operations.

Step 4 — Consensus & Record

Validator nodes reach consensus and the proof is written to the distributed ledger. Once committed, entries cannot be modified or deleted by any party. Cross-hop hash pointers link proofs into a verifiable chain of custody.

Step 5 — Query & Verify

Any authorized participant — PSAP supervisors, state authorities, legal teams, AI systems — can query the ledger via REST, WebSocket, or gRPC to reconstruct the complete verified history of any call.

DESIGN PRINCIPLES

Key Design Principles

Passive by design
Observes and records. Never touches a 911 call, never sits in the signaling path, zero impact on call routing, latency, or availability.

PII never on ledger
PII fields are hashed at proof generation. Raw PII never appears in a proof, never reaches the ledger, never leaves the participant's system boundary.

Immutable by default
Committed proofs cannot be modified, deleted, or reordered. No administrative override exists. The record is permanent.

Local data sovereignty
Data Layer records stay in the participant's own infrastructure. The Foundation never holds participant data. Commons contribution is opt-in.

Standards-anchored
Every integration point anchors to an existing NENA standard — i3 for proof generation, NENA PCA for node credentials. 911TL extends, not replaces.

Open, neutral governance
No single vendor controls the protocol. Governed by PSAPs, ESInet operators, vendors, and state authorities via the Technical Advisory Committee.

STANDARDS ALIGNMENT

Standards Alignment

911TL extends 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.

Integration Point	Standard	Role
Proof generation	NENA i3 (NENA-STA-010)	i3 log stream subscriber — passive, read-only
Node credentials	NENA PCA / PKI	Certificate-grounded identity for all participants
Event schema	NENA i3 / EIDO	Proof types anchored to standardized event taxonomy
Data normalization	911TL Proof Type Registry	Community-governed; designed to inform future NENA specs

“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