

IETF 125 — RATS WG Presentation

draft-ikspa-rats-verifiable-geo-fence-00

Draft co-authors: R. Krishnan, N. Smith, D. R. Lopez, A. Prasad, S. Addepalli

Slide 1: Problem Statement

Title: Why Workload Geofencing Needs Hardware Roots

- Software-only identities (bearer tokens, SVIDs) are **stolen, replayed, or proxied** — no binding to physical hardware
- IP-based geolocation is **trivially spoofed** — VPNs, proxies, cloud region labels provide zero cryptographic assurance
- Regulations (RBI India, South Korea Spatial Data Act etc.) **require provable data residency** — but today's tooling can't prove it
- Location metadata is **unsigned** — no integrity, no audit trail, no verifiable provenance
- Result: **no cryptographic link** between a workload's identity, its platform integrity, and its physical location

Slide 2: Solution — V-GAP

Title: Verifiable Geofencing Attestation Profile (V-GAP)

- **RATS Architecture profile** (RFC 9334) — not a new framework, builds on existing RATS plumbing
- Binds workload identity issuance to two hardware-rooted proofs:
- **Platform integrity** — TPM quote seals all evidence fields into a single hardware statement
- **Geographic residency** — "in-zone" proof, optionally privacy-preserving via transparent ZKPs
- **Three-layer trust chain** (silicon → agent → workload):

Layer	What	How
Layer 1	Workload ↔ Agent binding	Transitive Attestation (draft-mw-wimse)
Layer 2	Platform integrity	TPM quote + PCR validation (this document)
	Residency verification	

Layer	What	How
Layer 3		Geolocation proof + location endorsement (this document)

- Credential issued **only when both layers pass** — fail-closed via X.509 CRITICAL extension

Slide 3: V-GAP Profile — RATS Mapping

Title: How V-GAP Maps to RATS Roles

RATS Role	V-GAP Entity	What It Does
Attester	Location Anchor Host (LAH)	Produces lah-bundle — TPM quote + geo proof
Verifier	Host Identity Mgmt Plane	Validates TPM, PCRs, geo proofs → Attestation Result
Endorser	Location Endorser (e.g., MNO)	Signs location claim; MAY be an MNO, satellite operator, or other trusted location authority
Relying Party + CA	Workload Identity Mgmt Plane	Issues X.509-SVID only if attestation passes
Downstream RP	mTLS peer	Trusts CA signature as proxy for verified residency

Evidence flow (background-check model, RFC 9334 §3.2):

LAH (Attester) → lah-bundle → Verifier ← Location Endorsement

↓

Attestation Result

↓

RP + CA → X.509-SVID (CRITICAL ext)

↓

Downstream RP (mTLS)

Key design choice: RP acts as "trust translator" — embeds attestation result into standard X.509, so downstream consumers don't need to understand RATS or V-GAP.

Slide 4: Next Steps

Title: Path to WG Adoption

1. **Merge opportunity** with [draft-richardson-rats-geographic-results-01](#)
2. Richardson defines **geographic claim encoding** in EAR (Attestation Results)
3. V-GAP defines the **Evidence profile and verification flow** that produces those results
4. Complementary scope — V-GAP is "how you get the evidence," Richardson is "how you encode the result"
5. **Seeking WG adoption** as a Standards Track document
6. Draft restructured to normative (category: std)
7. Core V-GAP profile is normative; operational/deployment guidance in informative appendices
8. Reference implementation: github.com/lfedgeai/AegisSovereignAI
9. **Feedback requested on:**

10. RATS role mapping — is the "trust translator" (RP + CA) pattern the right fit?
11. Privacy technique extensibility — currently `none` and `zkp`, should we define a registry?
12. Proximity profiles — deferred to future docs, any interest in co-authoring?