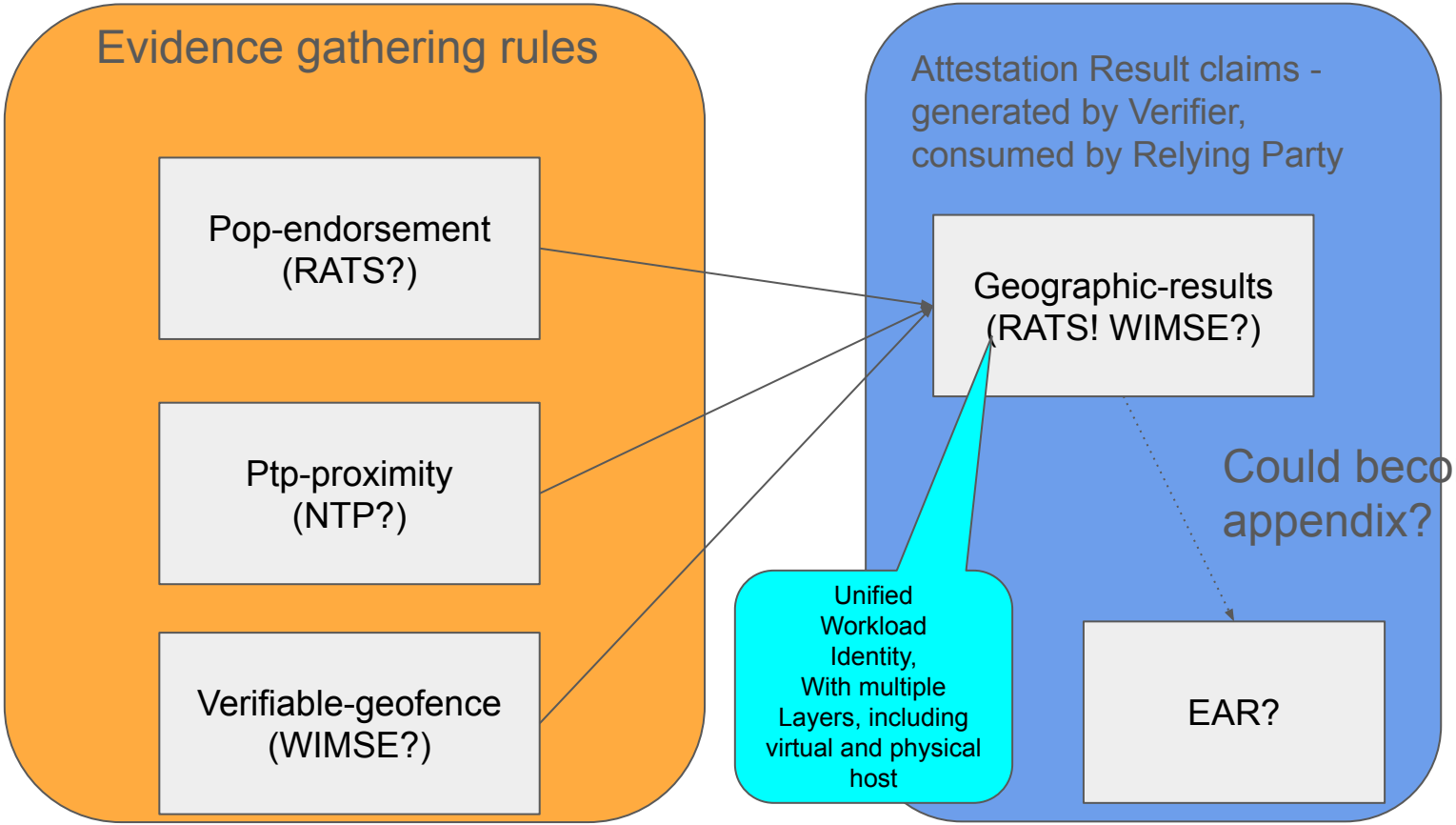
Remote Attestation And Geographic Evidence/Results

IETF 124 - Montreal
RATS and WIMSE WG
Ramki Krishnan (Vishanti Systems Inc.) and Michael Richardson
2025-11-06

Relevant Document(s)

- https://datatracker.ietf.org/doc/draft-richardson-rats-geographic-results/ (new)
- draft-lkspa-wimse-verifiable-geo-fence (discussed at IETF123: RATS+WIMSE)
- Using PTP to estimate proximity - https://github.com/ramkri123/ptp-asymmetric-authentication (new)
- https://datatracker.ietf.org/doc/draft-richardson-rats-pop-endorsement/ (discussed at IETF123: RATS)

Possible Document Architecture/Combinations: many IETF docs



Geographic results (HW-rooted TPM attestation and Attested Geographic location): can be delivered in 3 formats --

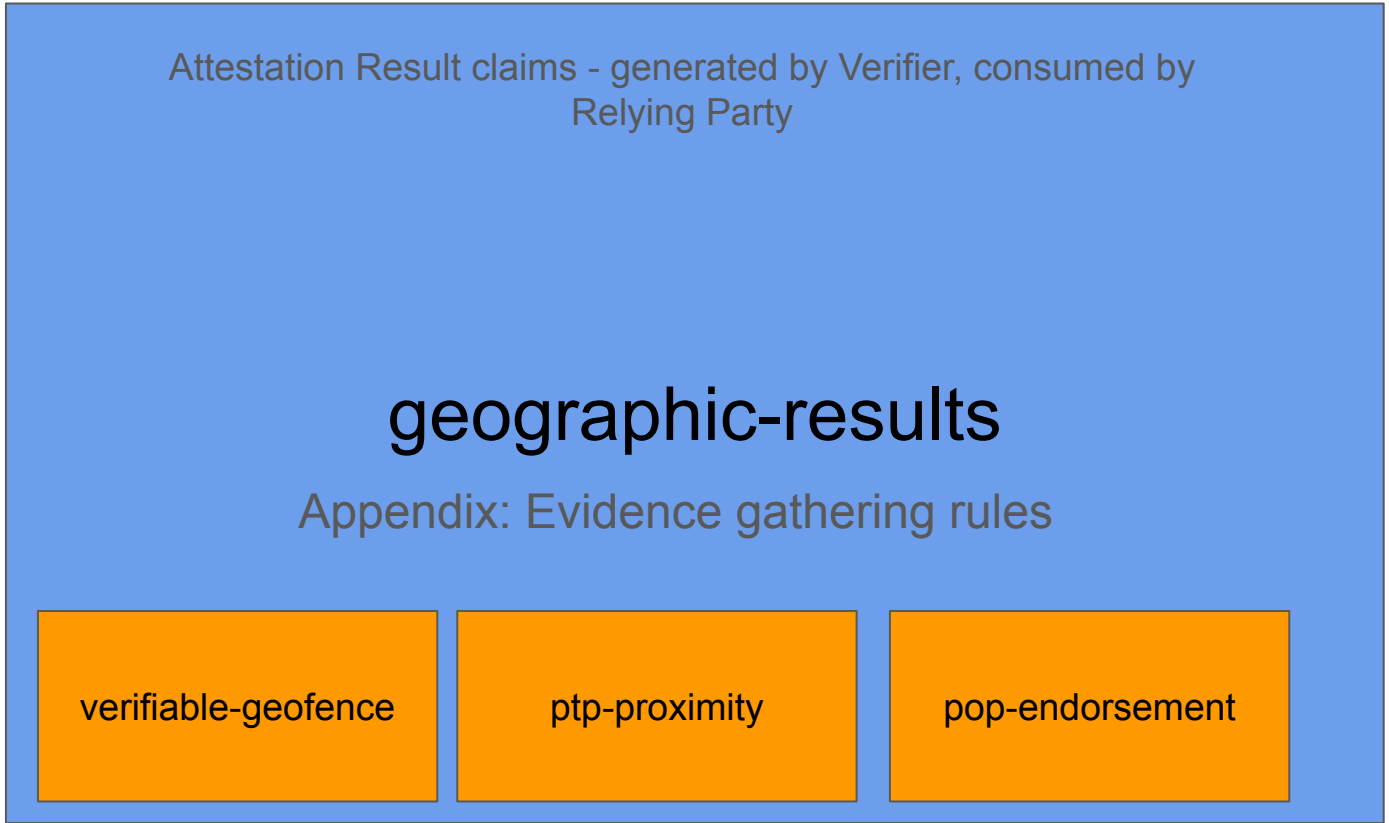
Model 1: Single Identity JWT with all claims;

Model 2: New Claims in a signed JWT within a HTTP header;

Model 3: New Claims with a short-lived X.509 Certificate (SVID)

Reference: https://github.com/lfedgeai/AegisEdgeAI/blob/main/docs/federated-jwt.md

Document Architecture/Combinations: fewer Documents, many appendix



Geographic results (HW-rooted TPM attestation and Attested Geographic location): can be delivered in 3 formats --

Model 1: Single Identity JWT with all claims;

Model 2: New Claims in a signed JWT within a HTTP header;

Model 3: New Claims with a short-lived X.509 Certificate (SVID)

Reference: https://github.com/lfedgeai/AegisEdgeAI/blob/main/docs/federated-jwt.md

Verifiable Geolocation in Tokens - current Gaps

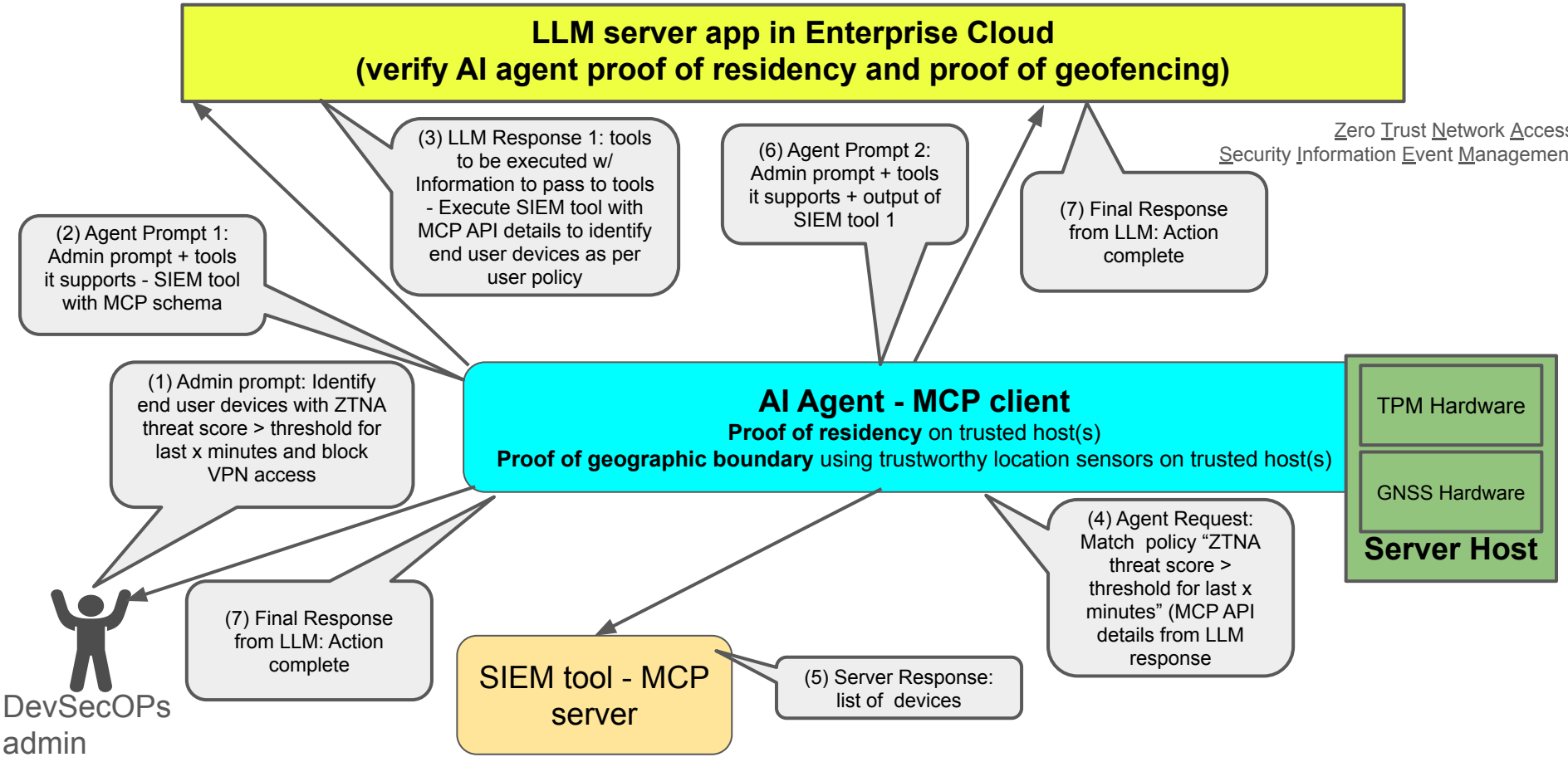
The Problem: The Authentication Method Reference (`AMR`): `"geo"` Claim (RFC 8176)

- A value in OIDC/OAuth tokens indicating geolocation was checked.
- **Critical Gap:** It's just an *unverifiable string*.
- It has **no defined semantics** (what does "geo" mean?).
- It has **no verifiability** (how can a Relying Party trust it?).

Our Proposal: A Standard for Verifiable Claims

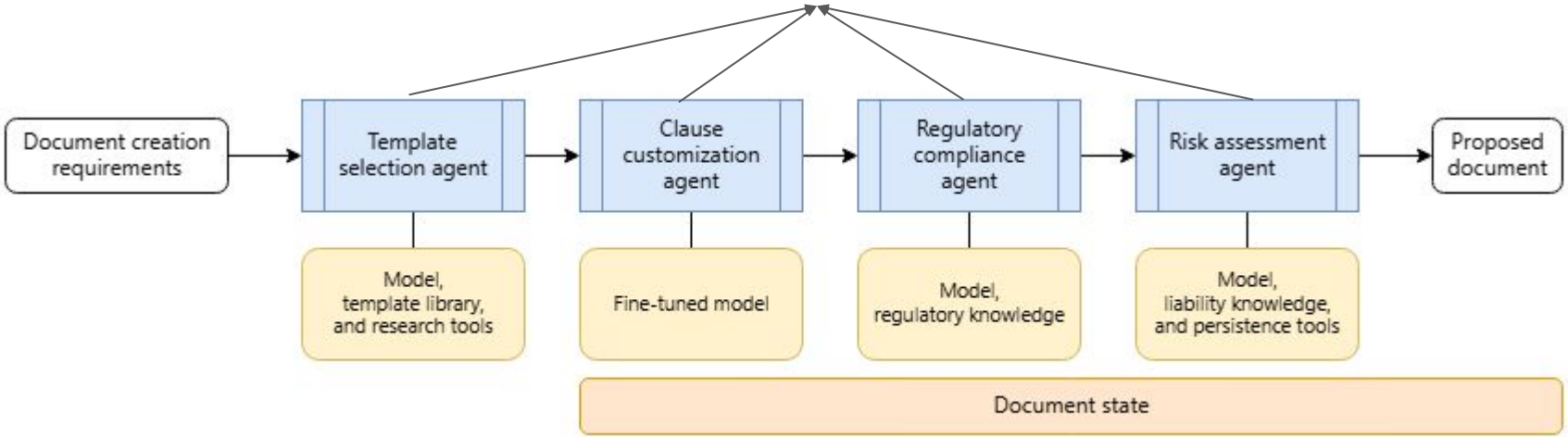
- Defines a **standard, interoperable JSON format** for rich location data.
- Provides **cryptographically verified** location results (e.g., via hardware attestation).
- Enables **drop-in use** in any JSON-based token (OIDC ID, OAuth Access) or SAML.

Use Case: An AI Agent (Devsecops admin persona) is assessing the trustworthiness of enterprise VPN users. The Agent's geography is important, because it will be provided with sensitive security information



Multi-agent **Use Case** - Verifiable host residency & geofencing

Trusted Agent Registry



Reference: https://learn.microsoft.com/en-us/azure/architecture/ai-ml/guide/ai-agent-design-patterns

Example contract use case: Ensure the contract processing matches the geolocation policy -- for instance, different consumer protection laws (GDPR, HIPPA, Local laws etc.) are geographic region specific.

Solution: Each agent in the Enterprise supply chain needs to provide to the trusted agent registry

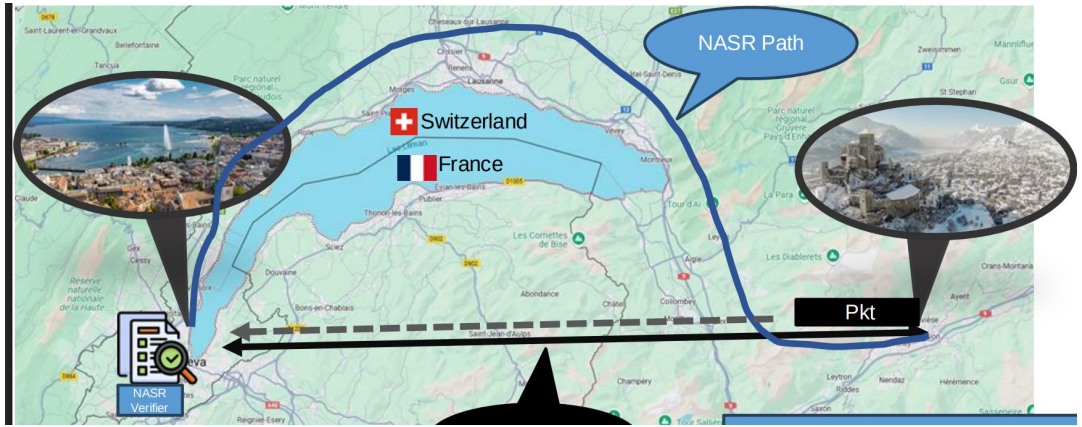
- Cryptographically verifiable proof of residency on trusted hosts
- Cryptographically verifiable proof of geofencing on trusted hosts with trusted sensors

Use Case: Network Attested Secure foRwarding (NASR)

Requires Evidence or Endorsement as to residency of forwarding elements:

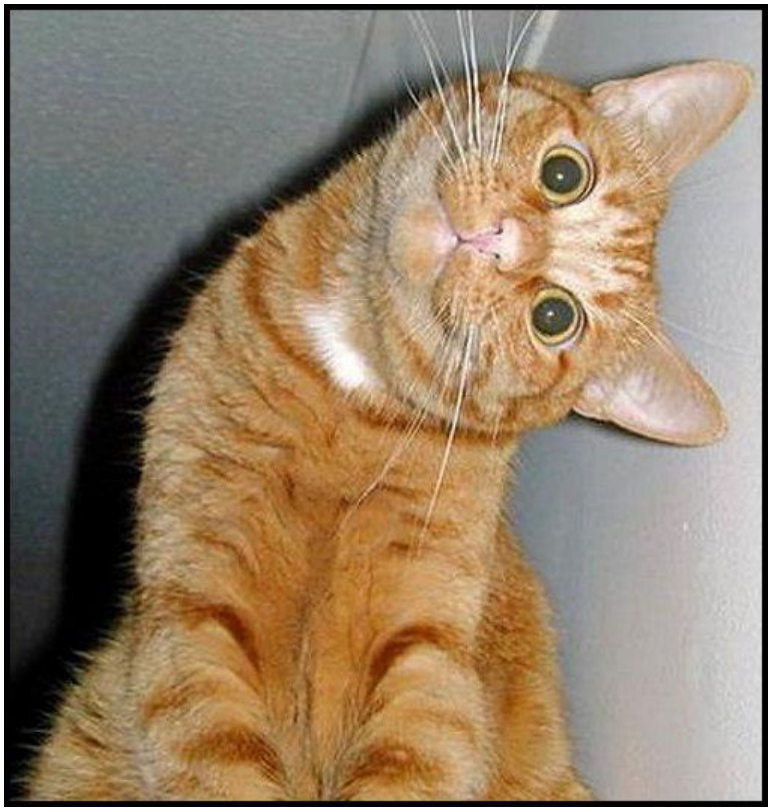
- Might be sovereignty
- Might be performance/latency
- Might be redundancy/resilience

Below is an example where
The shortest path would be via a different country.



Considerations

- Different groups will have different needs, and putting too much together may confuse and/or slow review process
- But, a goal is to simplify the effort by Relying Parties, to have common code
  - Thus a common Attestation Results, arrived at by many different procedures

Discussion

Before looking for adoption, We need to decide on structure.