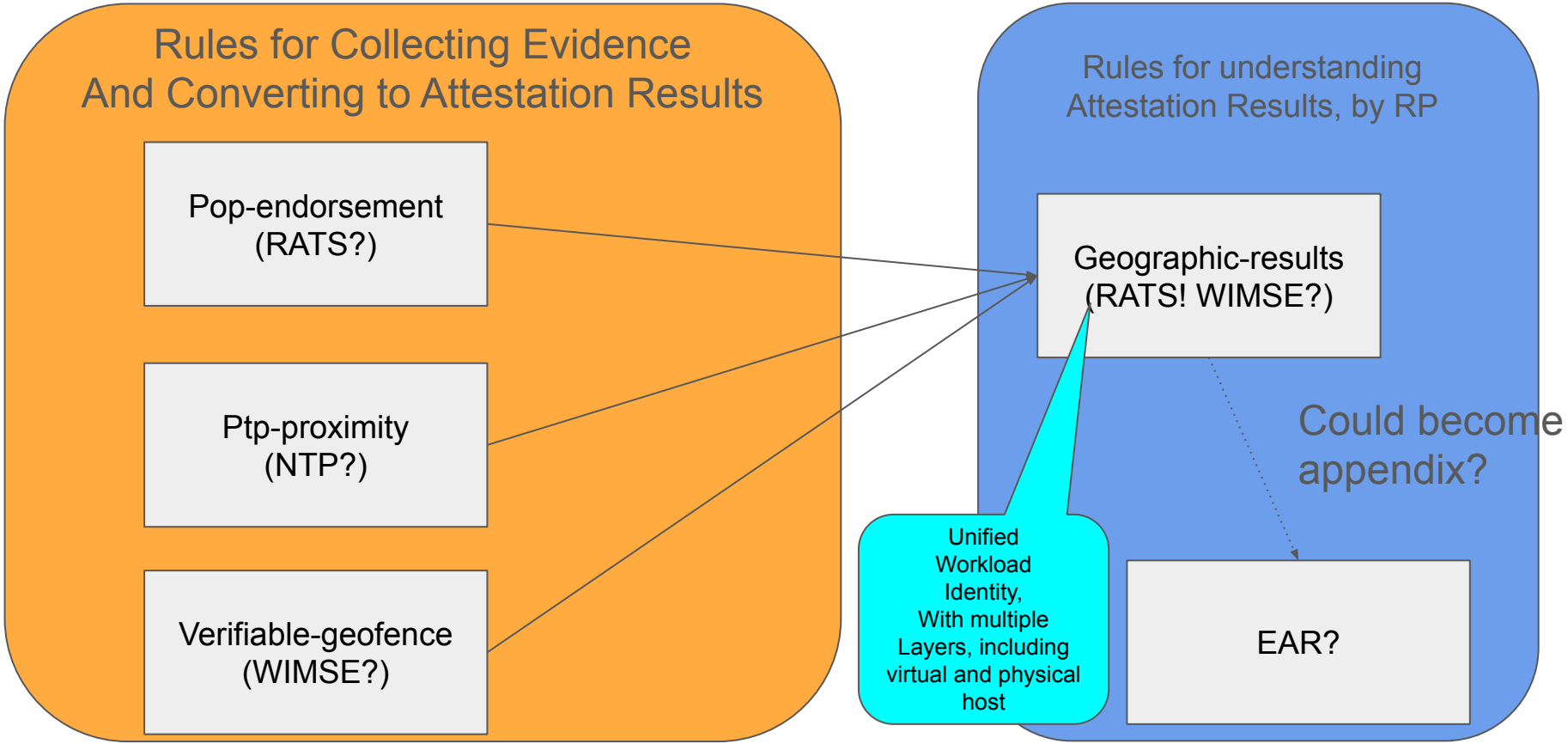
Remote Attestation And Geographic Evidence/Results

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

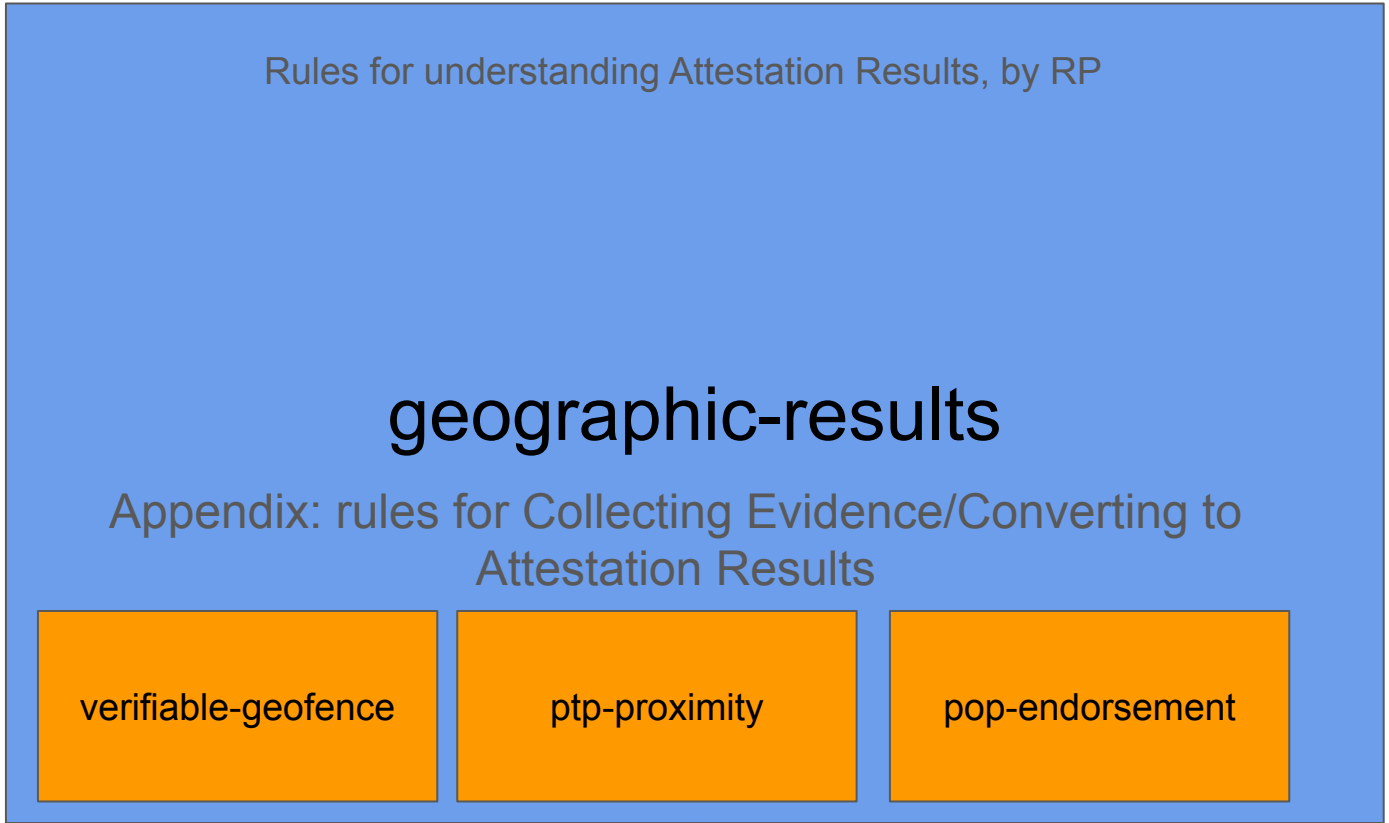
Relevant Document(s)

- 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 docs



Document Architecture/Combinations: fewer Documents, many appendix



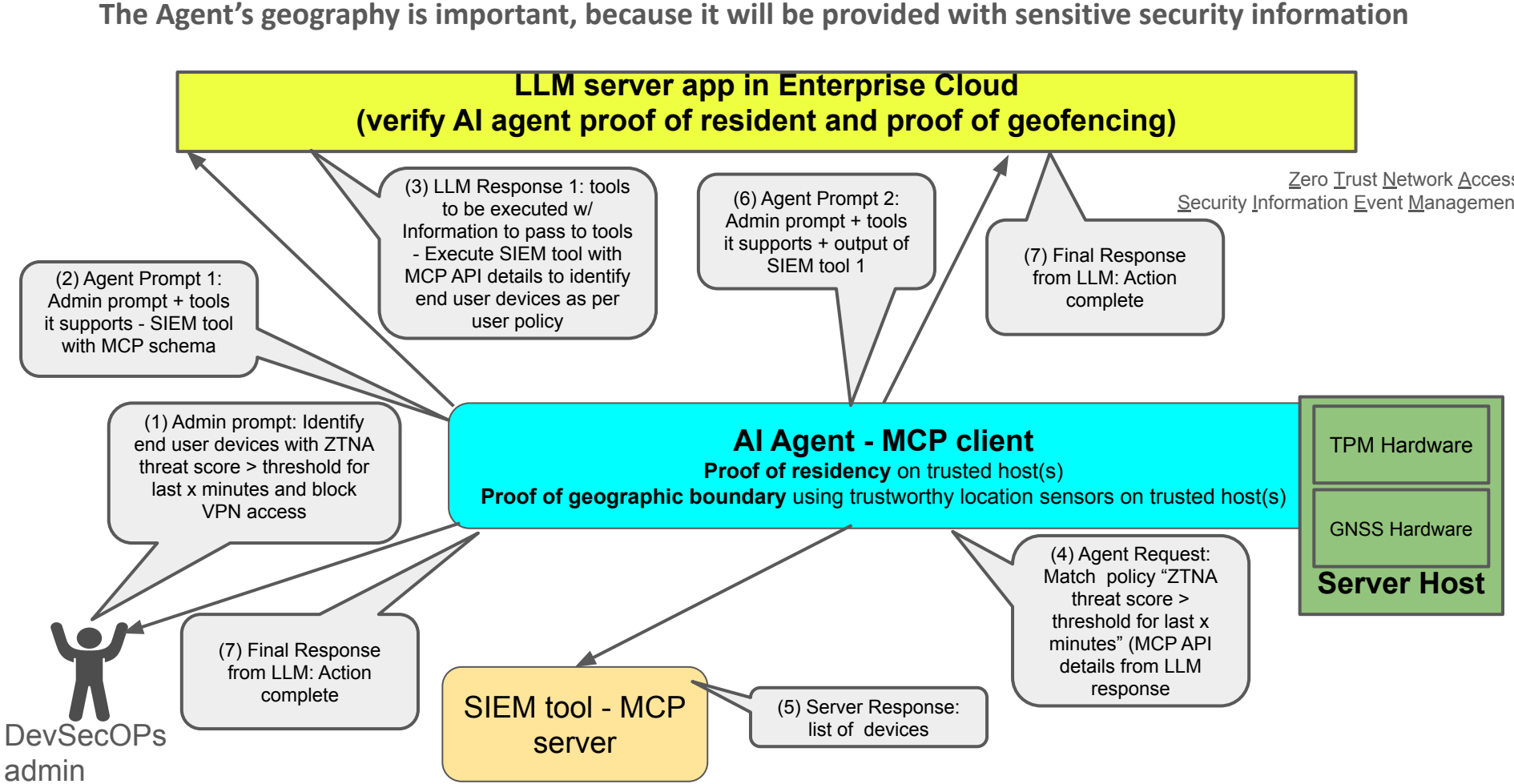
Geographic results (HW-rooted TPM attestation and Attested Geographic location): can be delivered in 3 formats --

Model 1: Single Identity JWT with all claims;

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

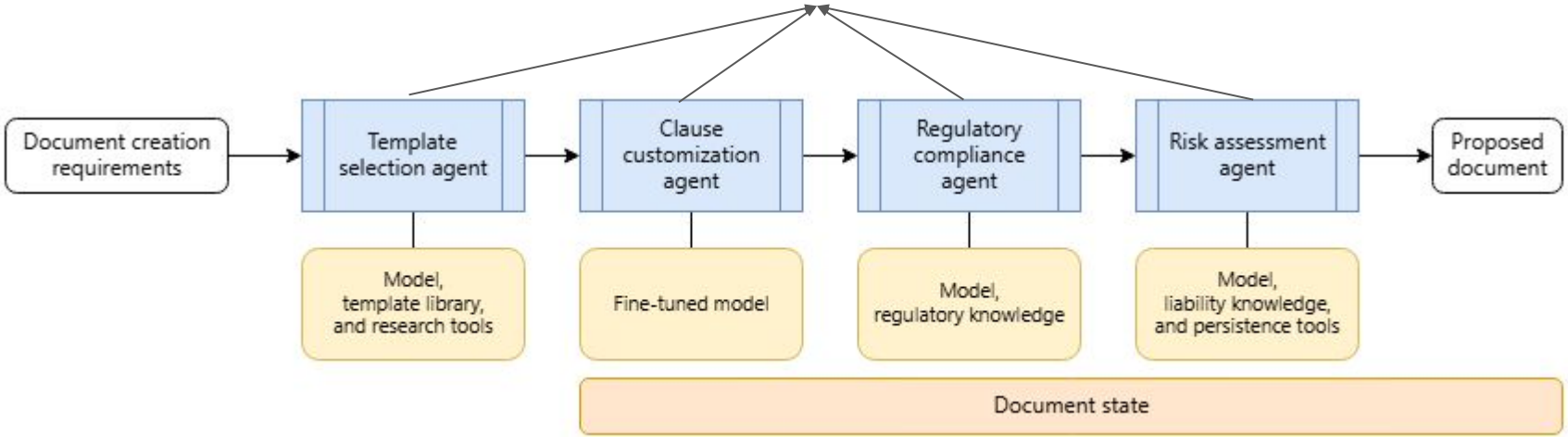
Model 3: New Claims with a short-lived X.509 Certificate (SVID)

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


Use Case: An AI Agent is assessing the trustworthiness of a VPN user. (DevSecOps)
The Agent's geography is important, because it will be provided with sensitive security information
LLM server app in Enterprise Cloud
(verify AI agent proof of resident and proof of geofencing)
Zero Trust Network Access
Security Information Event Managemen
(3) LLM Response 1: tools to be executed w/ Information to pass to tools - Execute SIEM tool with MCP API details to identify end user devices as per user policy
(6) Agent Prompt 2: Admin prompt + tools it supports + output of SIEM tool 1
(7) Final Response from LLM: Action complete
(2) Agent Prompt 1: Admin prompt + tools it supports - SIEM tool with MCP schema
(1) Admin prompt: Identify end user devices with ZTNA threat score > threshold for last x minutes and block VPN access
AI Agent - MCP client
Proof of residency on trusted host(s)
Proof of geographic boundary using trustworthy location sensors on trusted host(s)
TPM Hardware
GNSS Hardware
Server Host
(4) Agent Request: Match policy "ZTNA threat score > threshold for last x minutes" (MCP API details from LLM response
(7) Final Response from LLM: Action complete
SIEM tool - MCP server
(5) Server Response: list of devices
DevSecOPs admin

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

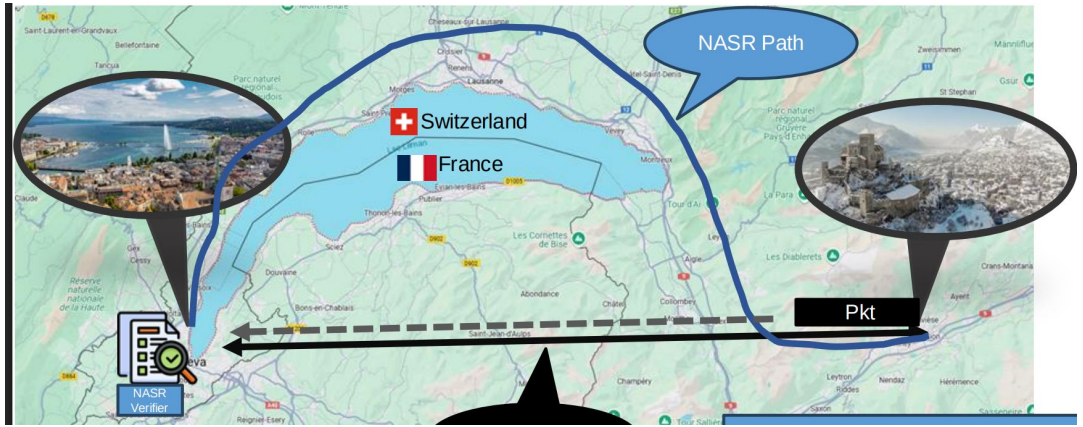
- Cryptographically verifiable proof of residency on trusted hosts
- Cryptographically verifiable proof of geofencing on trusted hosts with trusted sensors

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