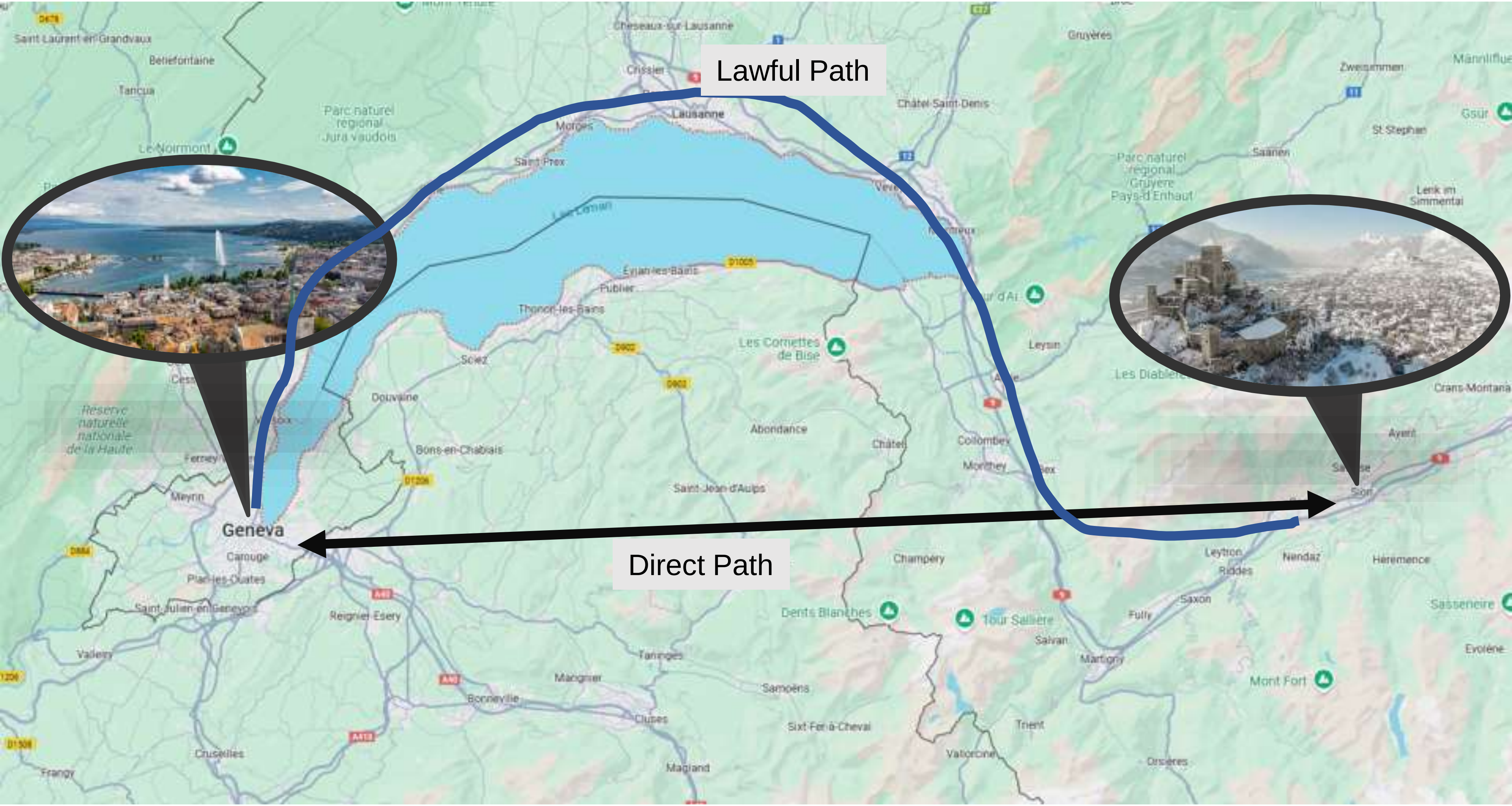
NASR

Network Attestation for Secured foRwarding

IETF 122 – Bangkok

Use Cases


Lawful Path
Direct Path
Geneva
Lausanne
Morges
Saint-Prex
Cheseaux-sur-Lausanne
Crissier
Châtel-Saint-Denis
Gruyères
Zweisimmen
St Stephan
Saanen
Parc naturel régional Gruyère Pays-d'Enhaut
Lenk im Simmental
Parc naturel régional Jura vaudois
Le Noirmont
Saint-Laurent-en-Grandvaux
Bellefontaine
Évian-les-Bains
Publier
Thonon-les-Bains
Sciez
Douvaine
Les Cornettes de Bise
Abondance
Bons-en-Chablais
Saint-Jean-d'Aulps
Châtel
Collombey
Monthey
Leysin
Champéry
Crans-Montana
Ayent
Sion
Leytron
Riddes
Nendaz
Hérémence
Saxon
Fully
Martigny
Salvan
Tour Sallière
Dents Blanches
Meyrin
Carouge
Plan-les-Ouates
Saint-Julien-en-Genevois
Reignier-Esery
Taninges
Marignier
Bonneville
Cluses
Samoëns
Sixt-Fer-à-Cheval
Trient
Vallorcine
Orsières
Mont Fort
Évolène
Magland
Cruseilles
Frangy
Valleiry

Policy Drivers

From RATS to NASR – Extending attestation from single device to network deployments

RATS WG

Goals: Establish a level of confidence in the trustworthiness of remote peers.

Effect: The (network) device functions correctly as expected.

NASR WG

Goals: Proving state and characteristics of a network path are compliant to a set of claims

Effect: Achieve predictable and verifiable forwarding behavior of a network deployment.

Why NASR now?
RATS fundamentally changed security assumptions to routing/forwarding securit

Deployment of RATS technology allows **stricter security assumptions** to network devices, permitting **higher network forwarding security goals**.

Before RATS

- Device is either fully trusted or fully distrusted, according to deployment location.
- No integrity check, no deterministic behavior → **correctly propagated routing information does NOT guarantee correct forwarding**

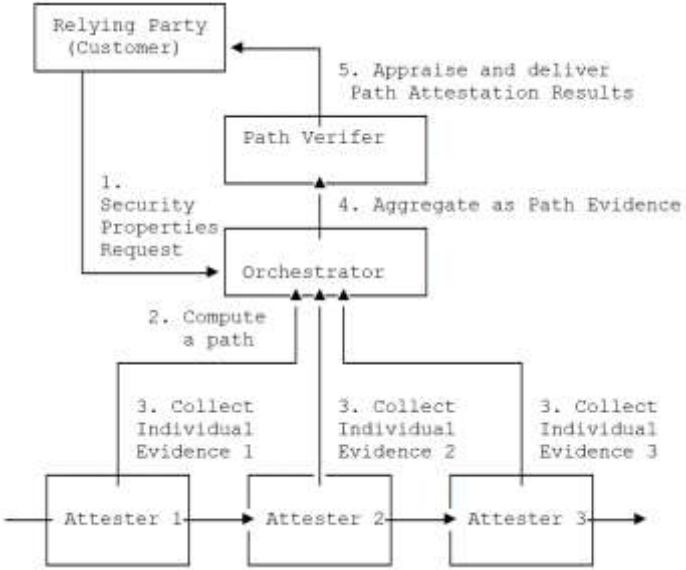
After RATS

- Finer granularity of security visibility down to each security claim – allows **differentiated services.**
- Deterministic forwarding behavior. Picking RATS-deployed devices allows **high-security connectivity services.**

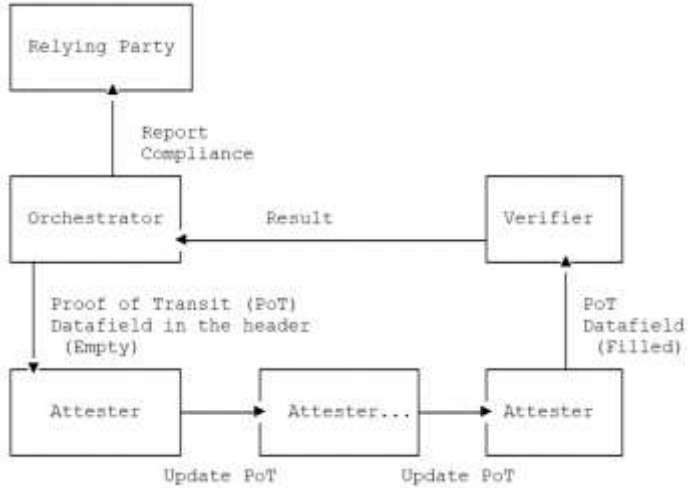
Architecture at-a-glimpse

Solution Steps

1. **[Prepare] Clients choose a set of security properties he desires for a network deployment,**
2. **[Before Use] these properties are collected (YANG/BGP-LS), verified on a path through attestation**
3. **[During Use] the behavior can be audited and (continuously) verified (e.g., Proof of Transit).**



Step 1 and 2



Step 3

Next Steps

THANKS!