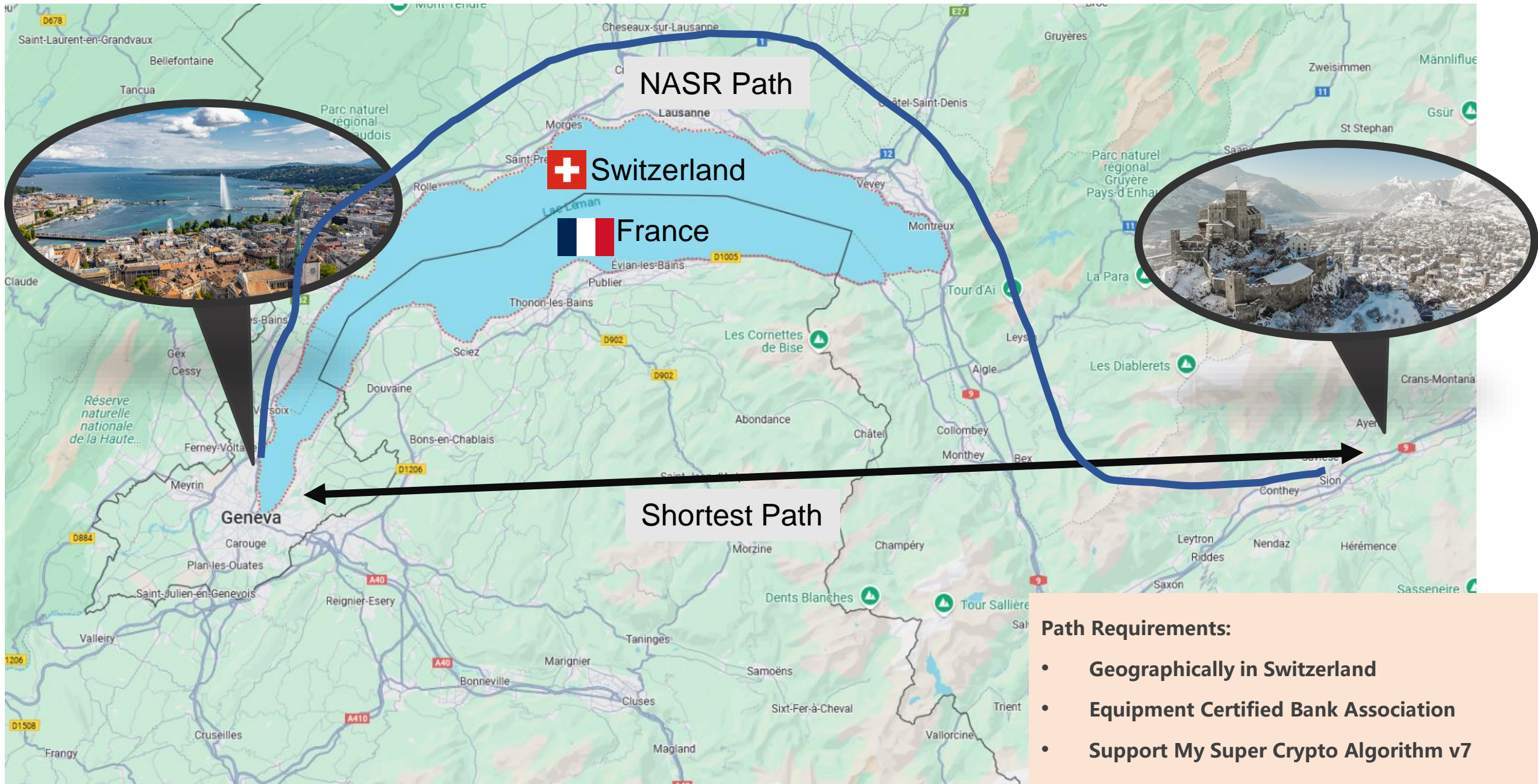


Network Attestation for Secured forwarding (NASR) Use Case for ANIMA

Feb, 2025

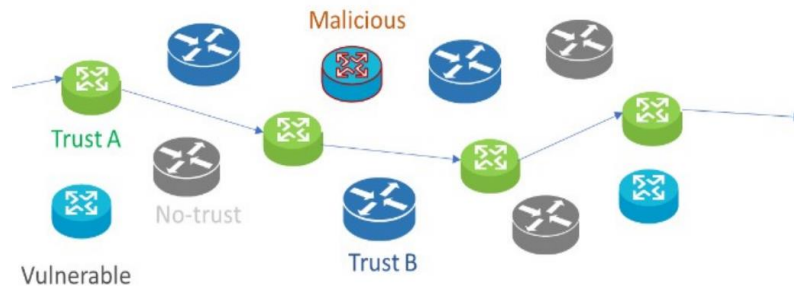
Peter Chunchi Liu

Swiss Bank Use Case: SION-GENEVA Transaction

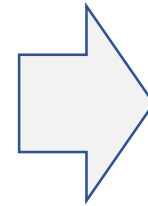


Distributed Operations in NASR

NASR Scenario/Requirements



Currently centralized
computed path



NASR Goals

- prove that data is traversed through network elements (devices, links and services—trusted path) that satisfy client security requirement claims,
- avoid exposure of unqualified elements, thus leakage.

Major Use Cases

- Enterprise Trusted Connection service • Data sovereignty

(More details: <https://datatracker.ietf.org/wg/nasr/about/>)

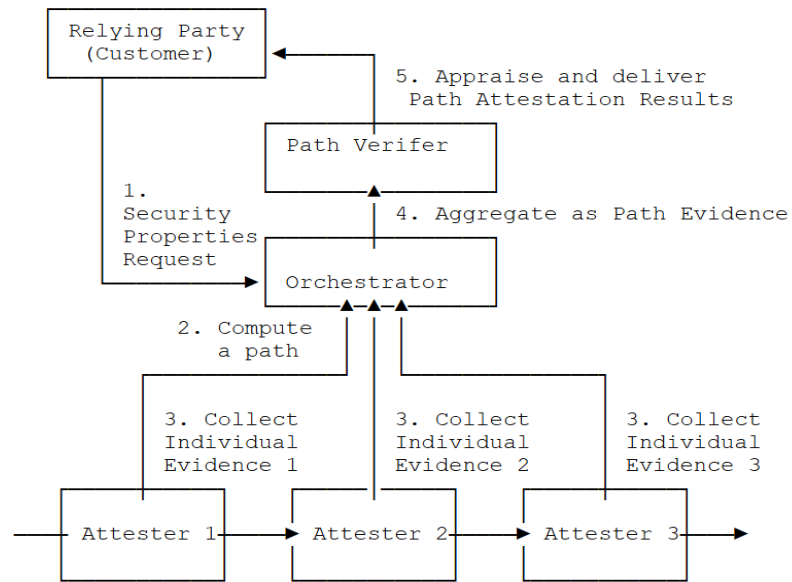
Possible Requirements for Anima

- **Auto-Discovery of trusted devices**
 - ✓ Attestation results (signed report of the device' s trust evaluation) exchange between devices
- **Distributed trust evaluation**
 - ✓ Attestation evidence (original trust measurement, hasn' t been evaluated&signed) exchange between devices
- **Trusted path set up**
 - ✓ To set up the path which combined by a set of trusted devices in a distributed manner

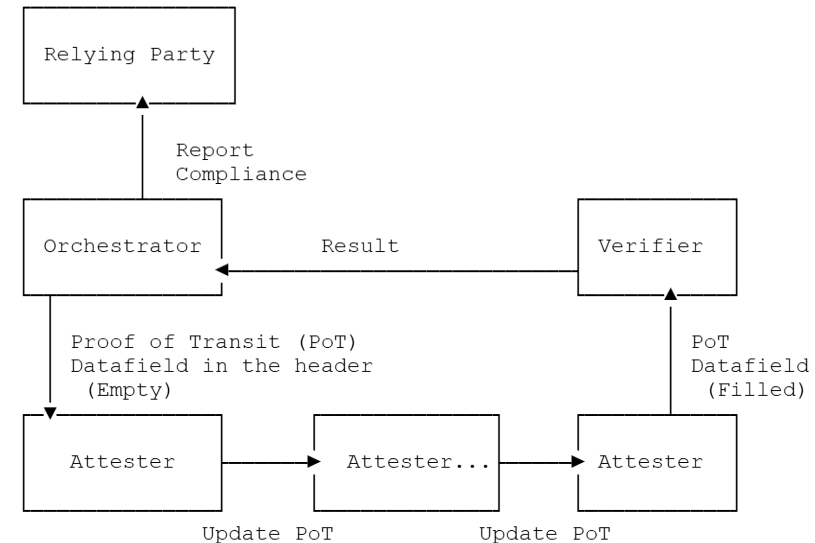
Current Architecture

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) by controller, collectively verified through attestation, create baseline
 - **ANIMA USE CASE HERE:** Centralized source routing path → Decentralized path computation, creation, cross-attestation?
3. [During Use] the behavior can be audited and (continuously) verified (e.g., Proof of Transit).



Step 1 and 2 (YANG example)



Step 3

Thank You!