

18 March 2024

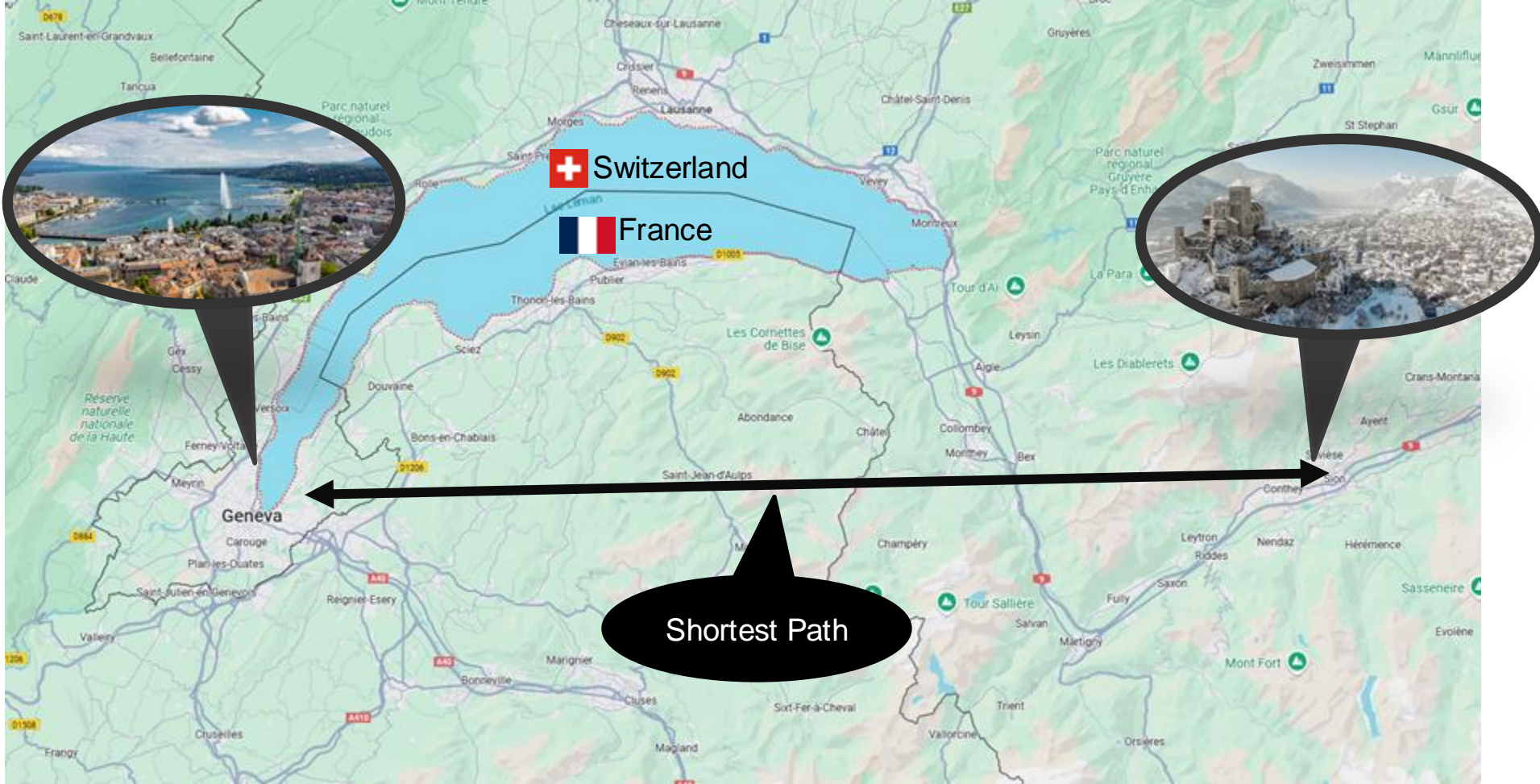
IETF 122 NASR

Network Attestation for Secured foRwarding

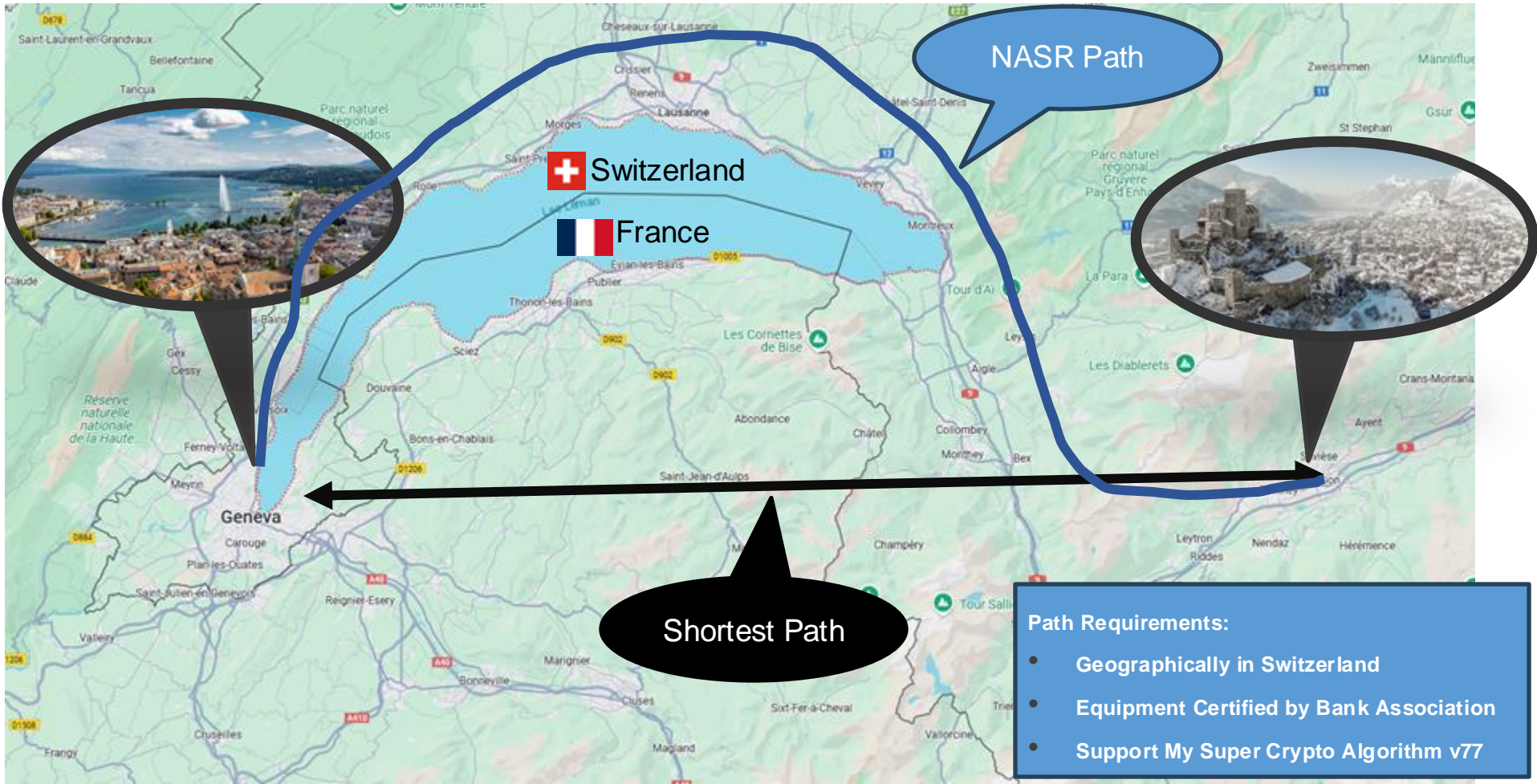
Use Cases

- **Diego Lopez**, Meiling Chen, Cuicui Wang

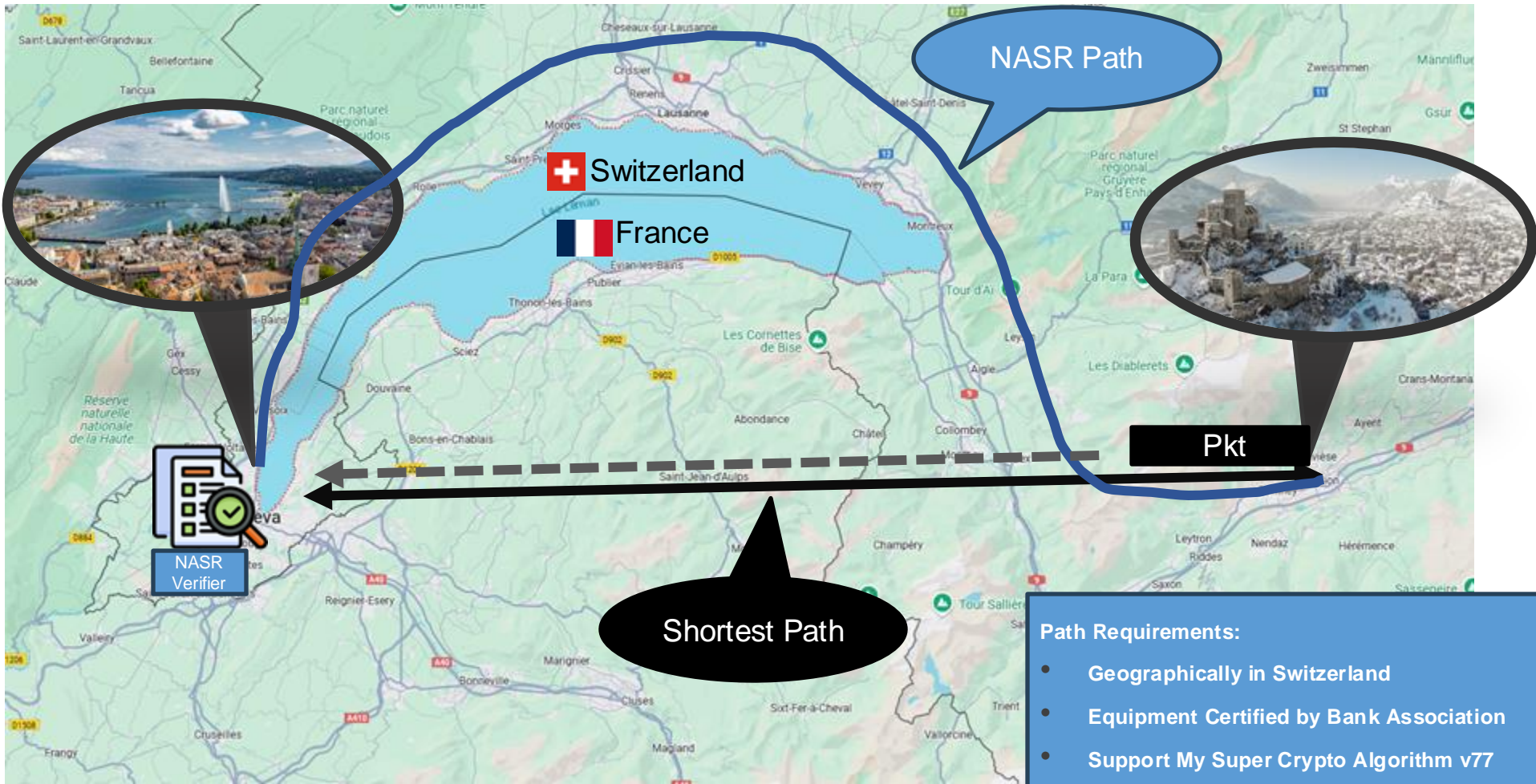
Swiss Bank Use Case: SION-GENEVA Transaction



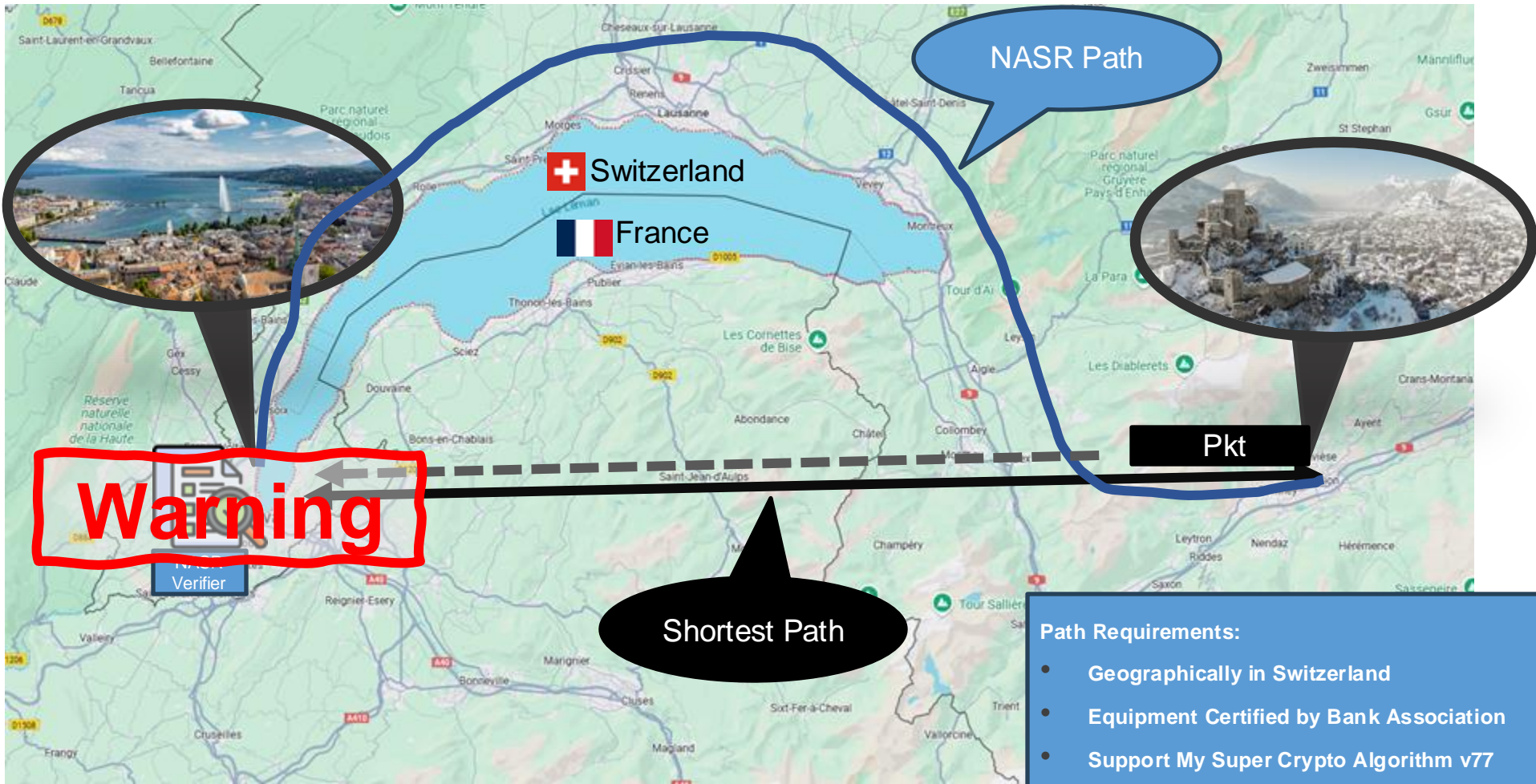
Swiss Bank Use Case: SION-GENEVA Transaction



Swiss Bank Use Case: SION-GENEVA Transaction



Swiss Bank Use Case: SION-GENEVA Transaction



NASR Path

 Switzerland

 France

Warning

Verifier

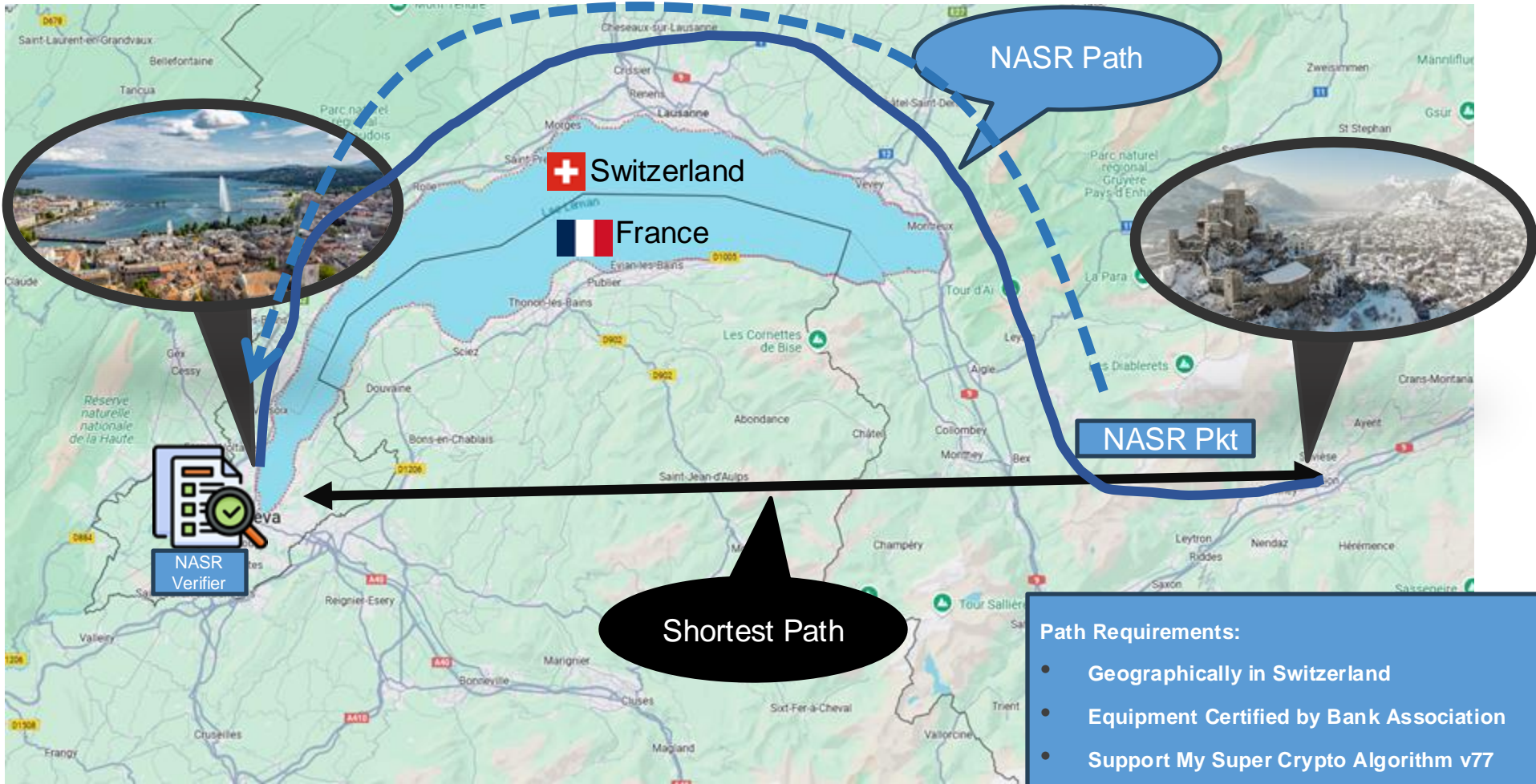
Pkt

Shortest Path

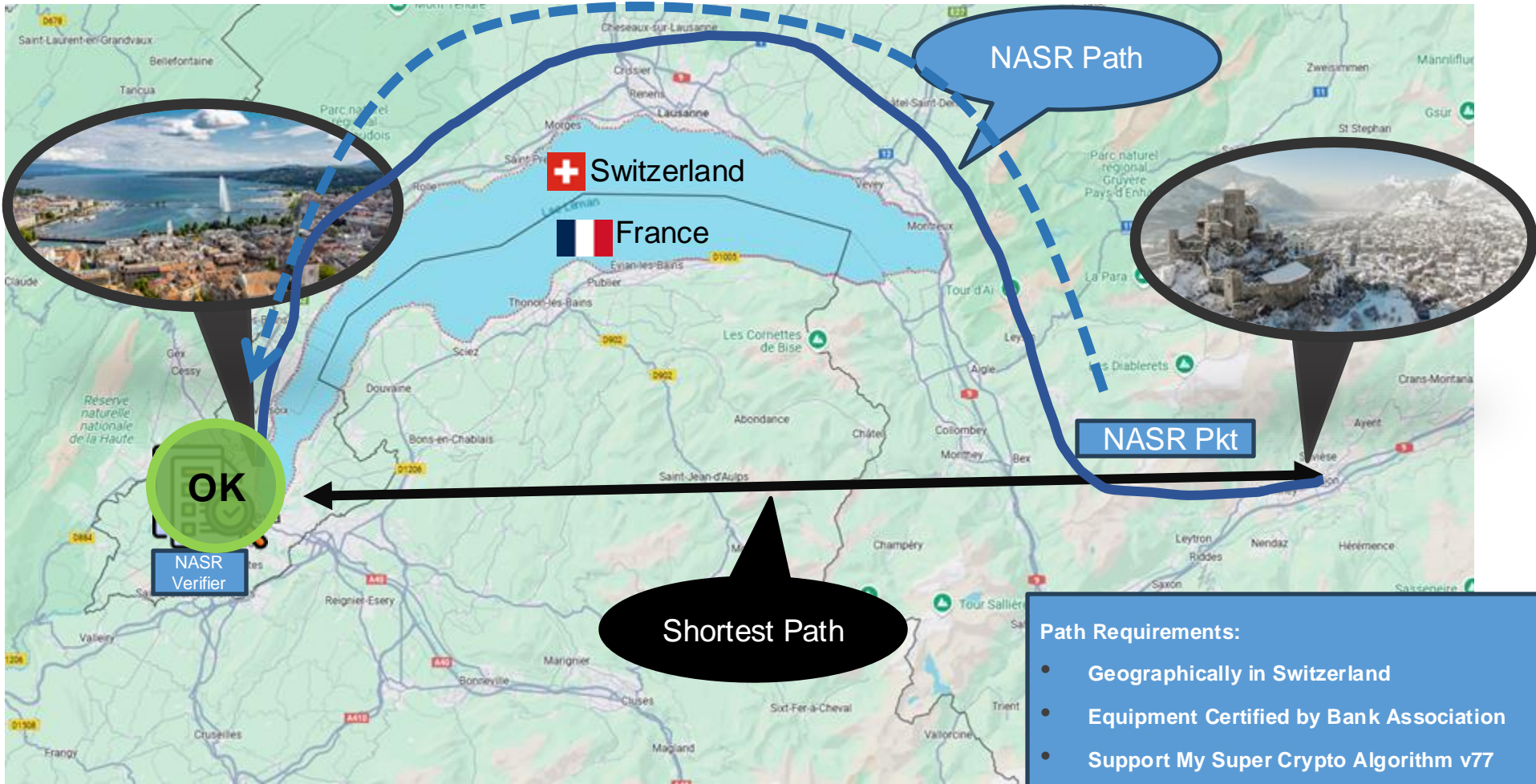
Path Requirements:

- Geographically in Switzerland
- Equipment Certified by Bank Association
- Support My Super Crypto Algorithm v77

Swiss Bank Use Case: SION-GENEVA Transaction



Swiss Bank Use Case: SION-GENEVA Transaction



NASR Path

Switzerland

France

NASR Pkt

OK

NASR Verifier

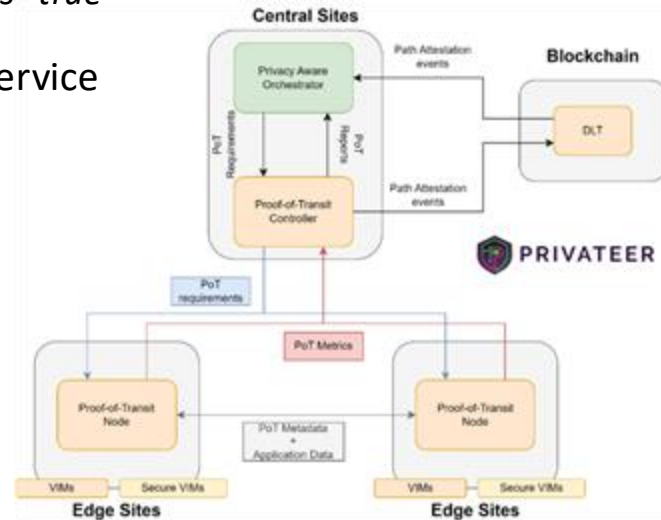
Shortest Path

Path Requirements:

- Geographically in Switzerland
- Equipment Certified by Bank Association
- Support My Super Crypto Algorithm v77

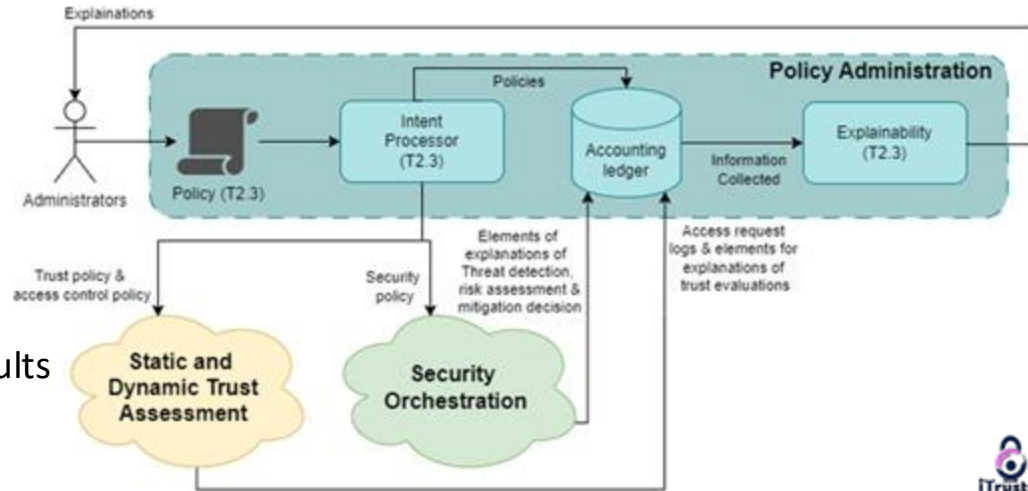
Levels of Compliance - LoC

- Based on the LoA (Level of Assurance) concept, widely used in identity
 - *The certainty with which a claim to a particular identity during authentication can be trusted to actually be the claimant's "true" identity*
- Further applied in NFV to assess the certainty on a (virtual) service deployment
 - Based on applying attestation to infrastructures, images, and connectivity
- Generalized for network service trustworthiness assessment
 - Several research projects with participation of Telefónica
 - Demonstrated as the base for security requirements in SLAs
- Suitable to be generalized even further
 - Via intents, smart contracts, third-party auditing
 - For the data and control planes, and even for telemetry and control flows



The Ingredients for LoC Application

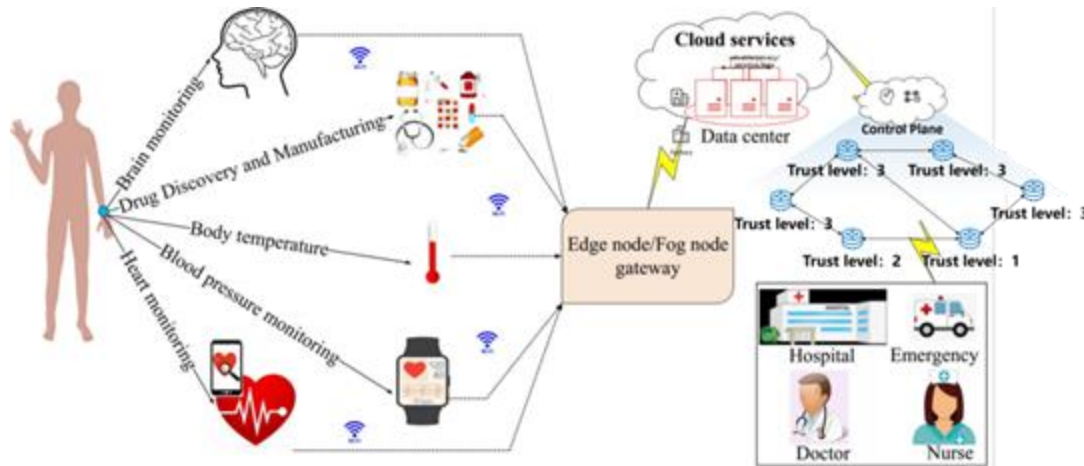
- Means for **assessing specific properties on a particular network path**
 - Whatever their nature, generally related to a security posture
 - Geolocation
 - Versioning / patch level
 - Supported features
 - ...
- Attestation of the **path components**
 - When constructing the path
 - **Remote attestation mechanisms**
- Attestation of the **path compliance**
 - During its use
 - **Proof of transit techniques**
- Transparent repository for attestation results
 - Trust assessment
 - Auditing



Use Cases

Secure and Reliable Routing requirement for Internet of Things for Healthcare

The aim of healthcare monitoring which is based on China Unicom Network, is to track the patient's body parameters and provide fixed and reliable data to medical teams to better diagnose diseases, which will be particularly a great help to patients and elderly users when needing medical services in an unexpected and dangerous situation.



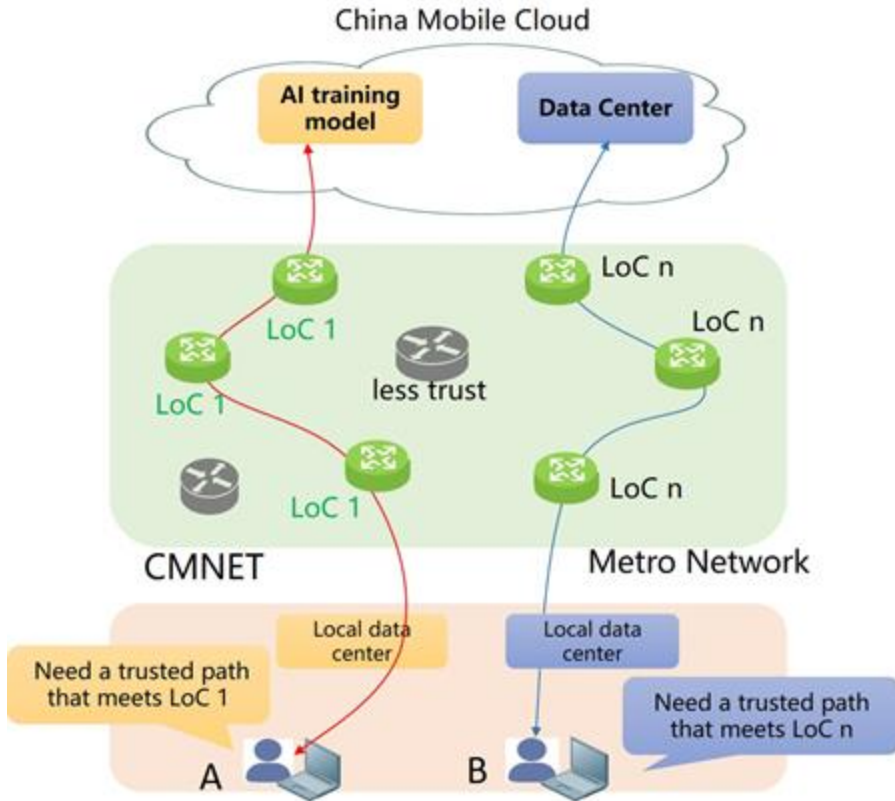
Security Requirement

- Wearable healthcare applications distribute personal and private data and hostile nodes may obtain and analyze medical data. For this reason, security requirements such as privacy and data integrity should be provided against invaders.
- Therefore, **it is important to have a trusted and secure routing scheme that prevents the choice of high-risk nodes as intermediate nodes in the routing path.**
- **The secure routing protocols to secure data transfer to IoT health devices is required.**

Reliability Requirement

- **Reliability (such as Maximal Occupancy Level, Diversity) is a critical requirement** for routing schemes due to the increasing number of connected devices and the need for real-time data processing.

Use Case: Sensitive Data Routing



Customer A

Role: AI big model user

Operations: AI training

Needs: a trusted path at LoC 1:

- ❖ Data can not be leaked
- ❖ Data can not go abroad
- ❖ Data can not be exposed to network
- ❖ ...

Customer B

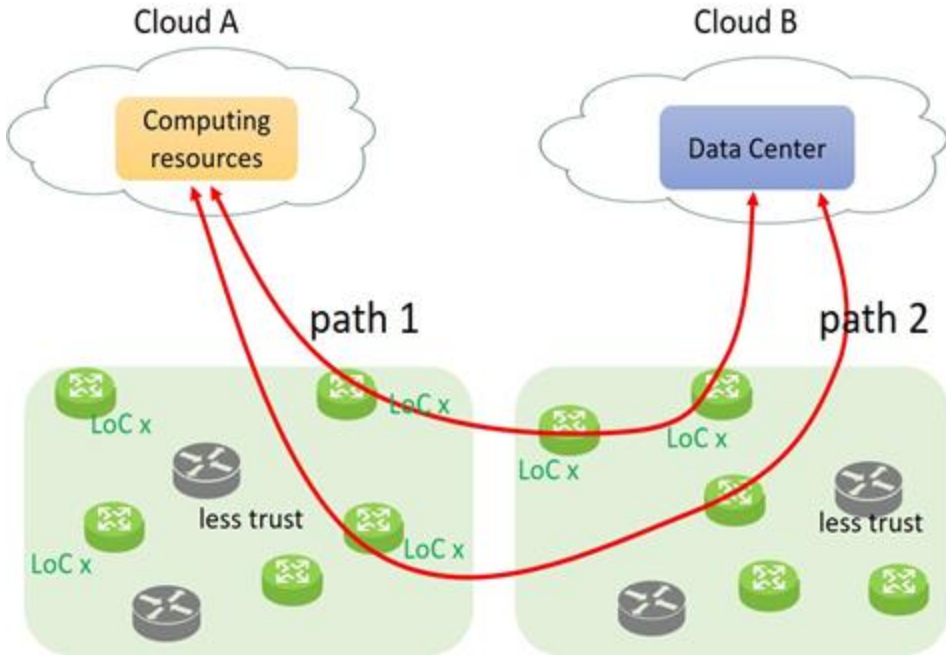
Role: Data storage

Operations: Store data

Needs: a trusted path at LoC n:

- ❖ Data can not be leaked and analyzed
- ❖ Data can not go abroad
- ❖ Can not be DDoS
- ❖ ...

Use Case: Sensitive Data Routing



Customer C

Role: Mobile cloud users

Operations: Computing and data storage

Needs: trusted paths at LoC x:

- ❖ Data can not be leaked and copied
- ❖ Cross domain regulations
- ❖ Path backup
- ❖ ...

What they ask for ISPs

1. Generate a trustworthy, secure and controllable forwarding path meets their LoCs;
2. Attestations of the path and service compliance, to prove the path is indeed trustworthy and the security service is in compliance with the commercial agreement.

Policy Drivers

- Privacy concerns and regulation on personal data
 - EU: GDPR
 - Germany: TTDSG/TDDDg
 - China: Data Security Law (DSL)
- Emerging regulations on data and digital sovereignty
 - Use of public networks for critical services
- Customer requirements
 - In the light of network service virtualization
- Edge-cloud scenarios
 - In application of regulations mentioned above

<https://piwik.pro/glossary/ttdsg/>



THANKS!