Zero-Trust Sovereign AI – RATS impact:

Verifiable Geofencing & Residency Proofs for Cybersecure Workloads

- **Reference**: WIMSE https://github.com/nedmsmith/draft-klspa-wimse-verifiable-geo-fence/blob/main/draft-lkspa-wimse-verifiable-geo-fence.md
- **Authors**: Ramki (Presenter), Ned, Diego, Prasad, Srini

Agenda

- Sovereign cloud data residency requirements
- Key industry problems and solution summary with “Sovereign Cloud AI inferencing” as an example
- Summary of key protocol changes and suggested next steps

Sovereign cloud data residency requirements

Technical and regulatory challenges

- **Data protection regulations**: EUDR, US HIPPA, PCI DSS, Local legal mandates (Saudi Arabia, China …)
- **Data protection in all its lifecycle management**: creation, process, usage, storage, destruction.
- **Data protection in all its status**: in transit, in use, at rest.

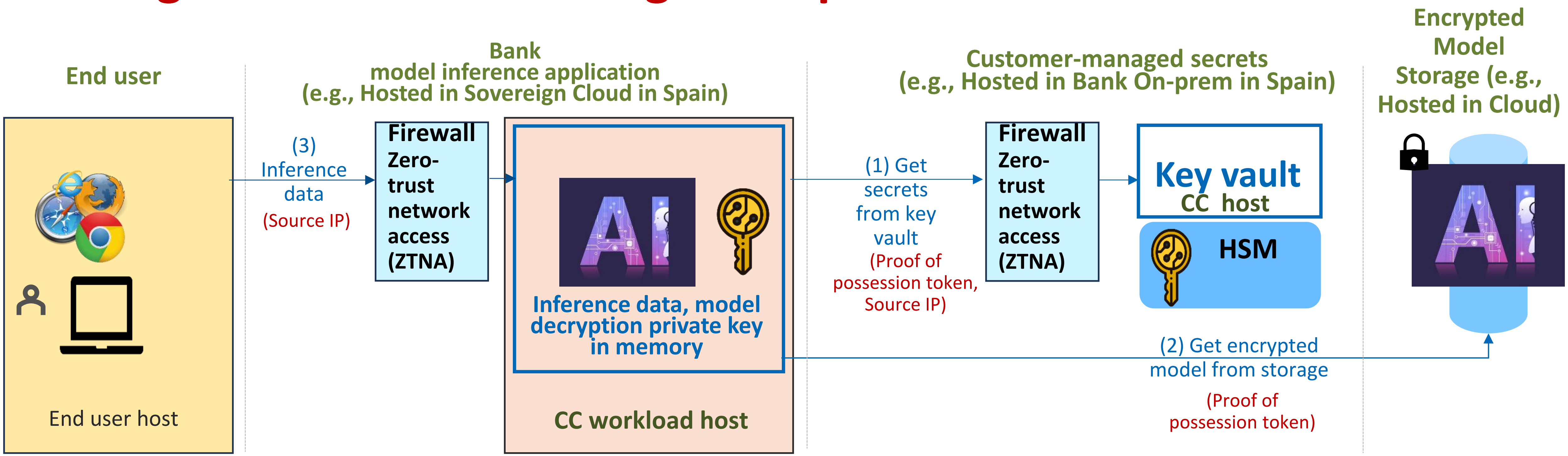
Data residency technical requirements

- **Host affinity** requirement
  - Data must storage and processing must be tied to specific hosts.

- **Geolocation affinity** requirement
  - Data must be stored/processed only in a defined geographic region.

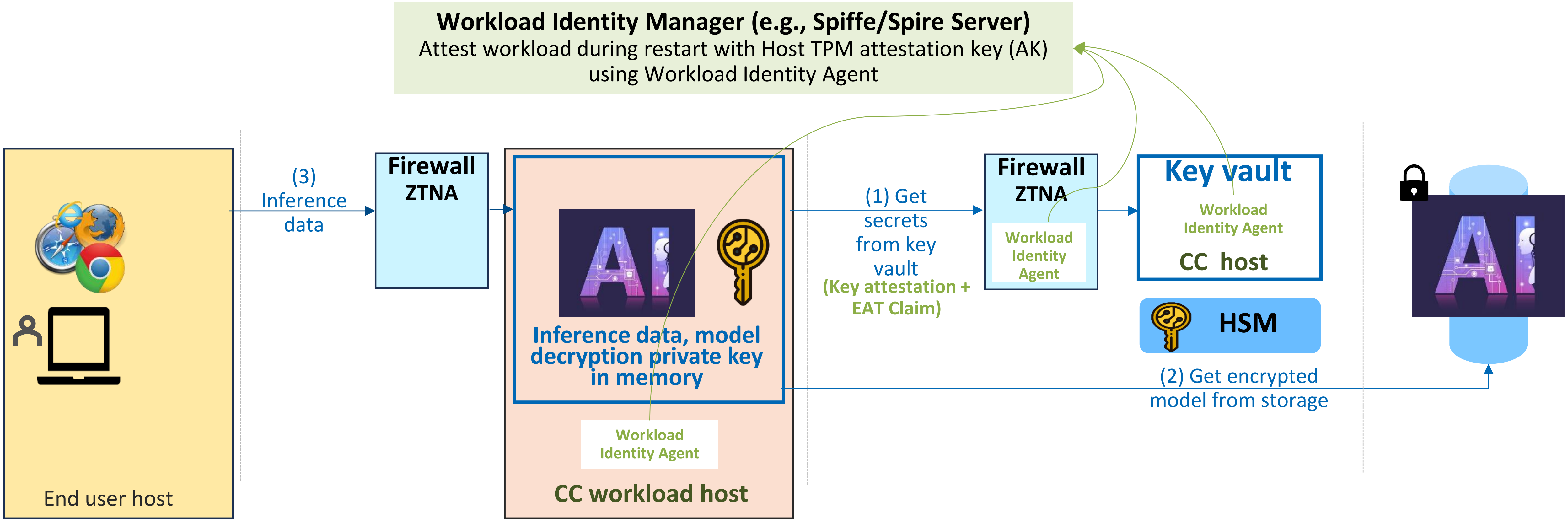
- **Host geolocation affinity (aka geofencing)** requirement
  - Host is bound to defined geographic region(s)

Sovereign Cloud AI inferencing: Example use case & Problem



- **Host-Affinity Realization Challenges**
  - **Proof-of-Possession tokens** (RFC 7800) bind a private key to the token. However, workload orchestrator security misconfigurations (OWASP security misconfiguration) can still undermine them by private key being used by unauthorized workloads
  - RATS Key attestation draft missing pieces (1) Movement of key from key vault to CC workload host (2) HSM binding to CC
- **Geolocation-Affinity Realization Challenges**
  - **IP-based geofencing** (firewall rules that check source IP) offers only weak location guarantees. Attackers easily bypass it using VPNs, proxies, or IP spoofing.

Sovereign Cloud AI inferencing: Example use case & Solution



Key attestation is a solution to host affinity (gaps below)

- Proof that HSM (therefore the private key) is bound to a specific CC host through attestation
- Proof that the key vault interaction exists for the CC workload

EAT claim is a solution for geolocation affinity (gaps below)

- Proof that geolocation sensor is trustworthy
- Proof that geolocation sensor is bound to a specific CC host through attestation

Suggested next steps

- **Address key attestation solution gaps**
  - Proof that HSM (therefore the private key) is bound to a specific CC host through attestation
  - Proof that the key vault interaction exists for the CC workload

- **Address EAT gap in expressing a non-GPS location and geofence**
  - Currently only precise geolocation is defined
  - Missing Telco DC network triangulation (mobile sensor is part of a server host)