Trusted Computing Future: Emerging Use Cases and Solutions

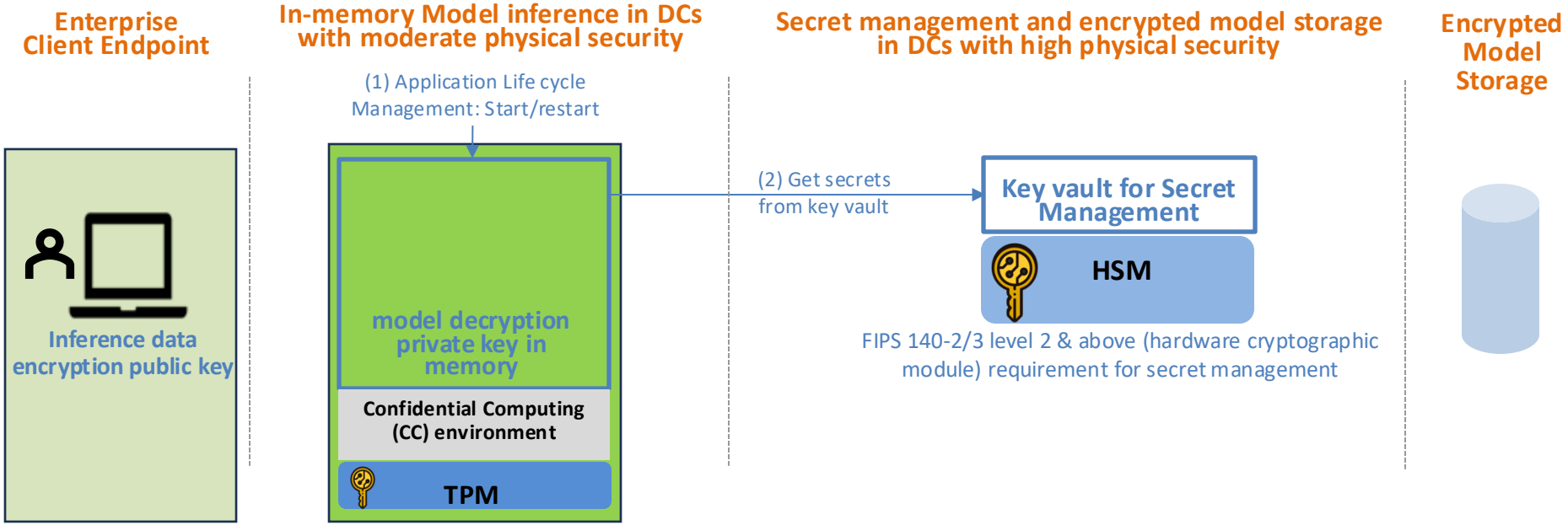
Keynote in Austin, USA, 2025 TCG meeting

Ramki Krishnan, Ned Smith (Intel)
Diego Lopez (Telefonica)
Ghada Arfaoui (Orange)

Agenda

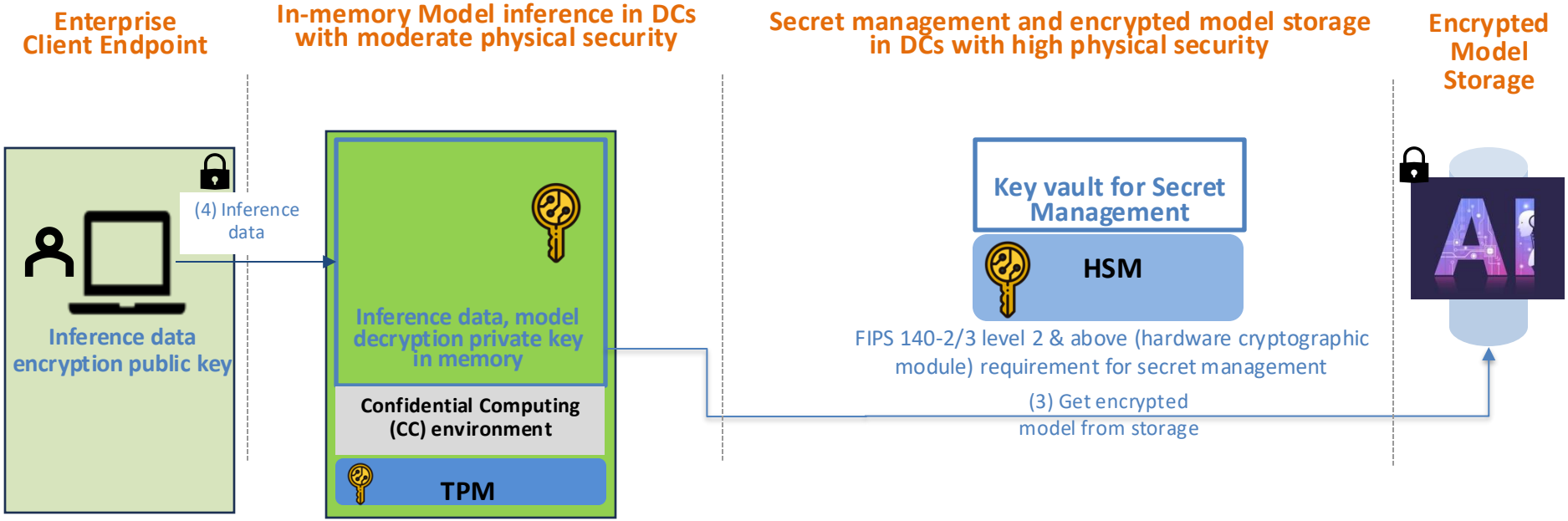
- Data residency
  - Use case and Requirements
  - Security and compliance value for servers and clients
- Challenges - End-to-end trusted computing and Host-affinity
- Trusted Confidential Computing (TCC) Architecture
- Data residency use case end-to-end value
- Call to Action

Data residency - use case



Exemplary deployment model for Confidential AI inferencing

Data residency - use case



Exemplary deployment model for Confidential AI inferencing

Data residency - use case requirements

Technical and legal challenges

- **Data protection Regulations:** EU GDPR, US HIPPA, PCI DSS etc.
- **Data protection in all its lifecycle management:** creation, process, usage, storage, destruction.
- **Data protection in all its status:** in transit, in use, at rest.

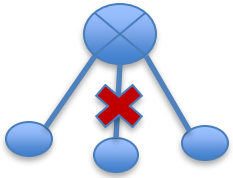
Requirements

- **Host affinity** requirement
  - Need for data to be tied to specific computing environments or hosts where it is stored and/or processed.
- **Geo-Location affinity** requirement
  - Data not to be transferred out of a defined geographic region. Includes country local legal mandates on data localization (China, Russia, India etc.).

Data residency – security and compliance value for servers



Network DNS Cache

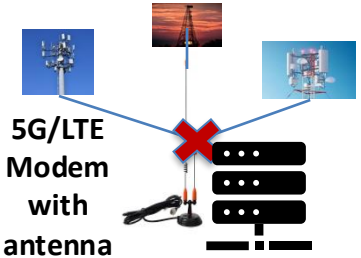


Data in transit attack: Compromise Endpoint DNS cache to redirect traffic to less secure server host/DC

Solution: Host location affinity detects misdirection.



Confidential Compute



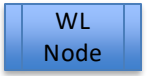
5G/LTE Modem with antenna

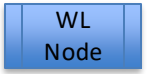
Physical Attack: Detach / Move / Replace modem device

Solution: Host-based / RoT integrity check detects device swaps.





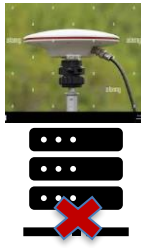




SW Infrastructure Attack: Workload orchestrator compromise redirects workloads on less secure hosting node

Solution: Host affinity knows expected nodes for workload.

GPS-based location HW



Data in transit attack: Compromise DC API GW to redirect traffic to unsafe geo-location

Solution: Location affinity know expected geo-location for workload.



Physical Attack: Detach/Move storage

Solution: Storage affinity integrity check detects device swaps.

Compliance: Verifiable host/geo-location attestation that data is processed only in vetted server geo-location(s)/host(s).

Note: The described attacks are typical and not meant to be exhaustive

Data residency – security and compliance value for clients

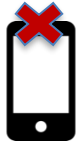
Embedded geo-location HW



Old HW issue: Old HW or HW without latest firmware patch returns inaccurate geo-location.

Solution: Host-based / RoT integrity check detects out-of-date HW.

External geo-location HW



Physical Attack: Detach or Replace with un-approved device.

Solution: Host-based / RoT integrity check detects device swaps.

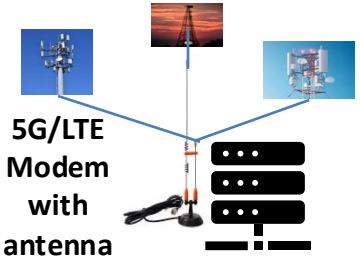
Geo-location SW

Old SW issue: Un-patched SW returns inaccurate geo-location.

Solution: Host-based / RoT SW integrity check detects out-of-date SW.



Confidential Compute

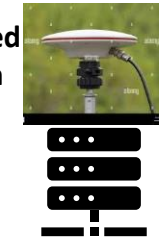


5G/LTE Modem with antenna

Key vault for Secret Management

HSM

GPS-based location HW



Compliance: Verifiable host/geo-location attestation that data is processed only in vetted client geo-location(s)/host(s).

Note: The described attacks are typical and not meant to be exhaustive

End-to-end trusted computing challenges

- Need to ensure that a host component (physical TPM, location sensor etc.) is **used only by an application running on the host**.
- Need to ensure that the **communication** between host component (location sensor etc.) and application **cannot be tampered**.
- Need to ensure that the **location sensor hardware cannot be spoofed**.
- **Source IP address-based geo-location is inaccurate**. Enterprises can move their IANA assigned IP addresses anywhere in the world.

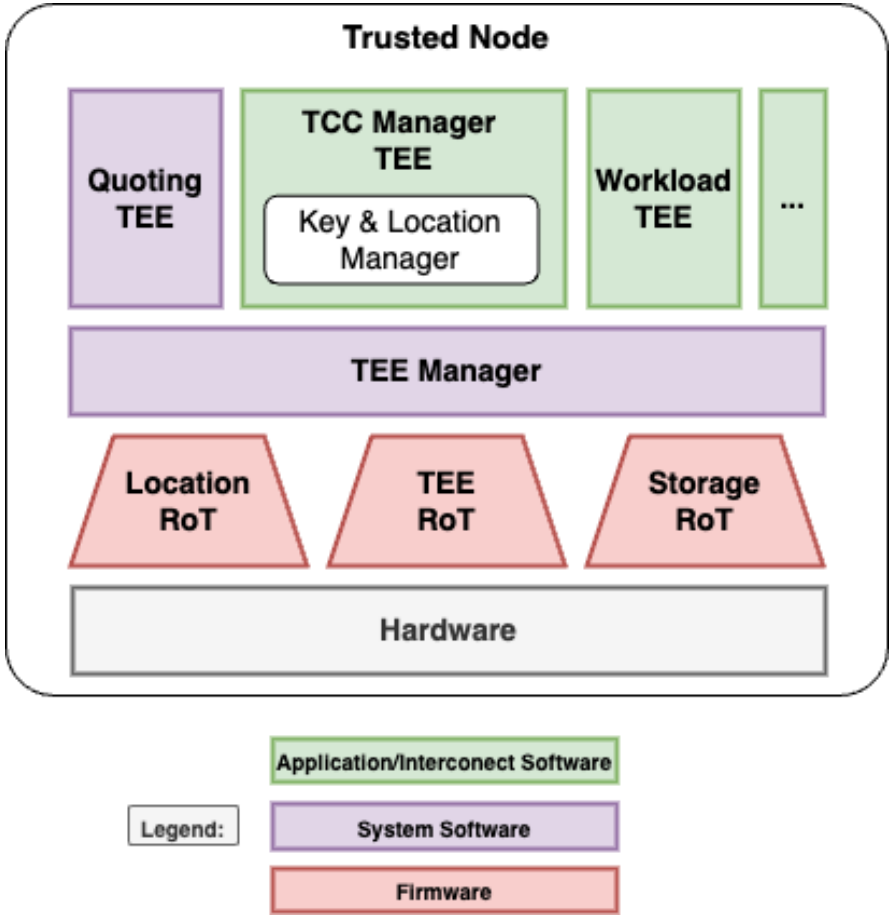
Host Affinity Challenges

- Confidential Computing (CC) nodes with a Trusted Execution Environment (TEE) need **host-native secure secret storage for keys**; essential for host-affinity.

- A physical TPM as **host-native key storage provider** on the **motherboard** has challenges:
  - Sharing the host TPM with CC workloads **brings the host (Firmware/Hypervisor/OS) into the CC trust boundary**, potentially expanding the attack surface.
  - A single physical TPM **lacks multi-tenant scalability** for effective key management.

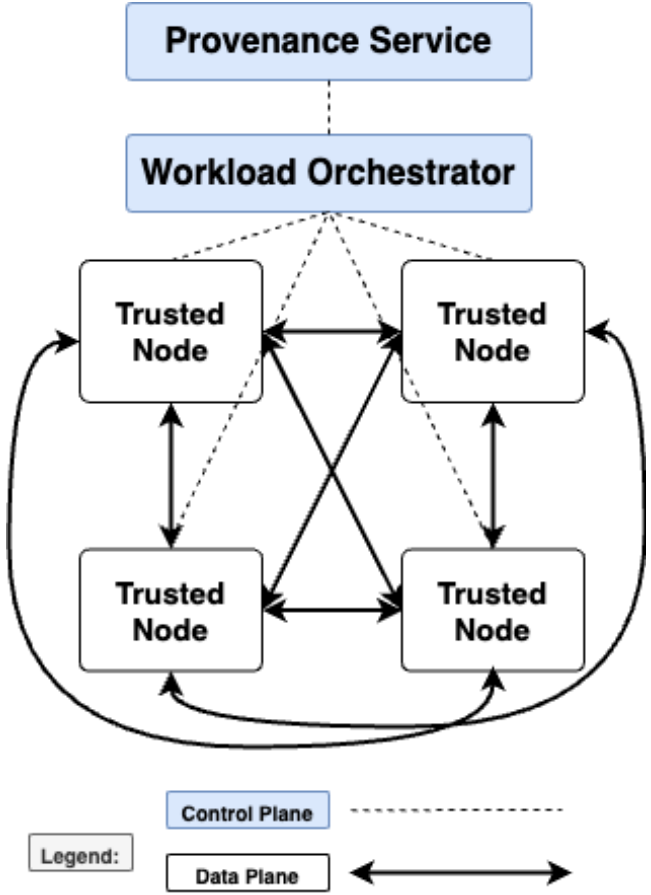
- **TPM lacks a flexible interface** for connected partitioned HSM usages:
  - RFC7512 exposes HSM as **Web-aware** PKCS11 interface.
  - CXL, SPDM and TLS transports have emerging attestation evidence conveyance capabilities that extend to **a wide variety of trusted endpoints** (memory, sensors, io, CC nodes).

Trusted Confidential Computing (TCC) Architecture



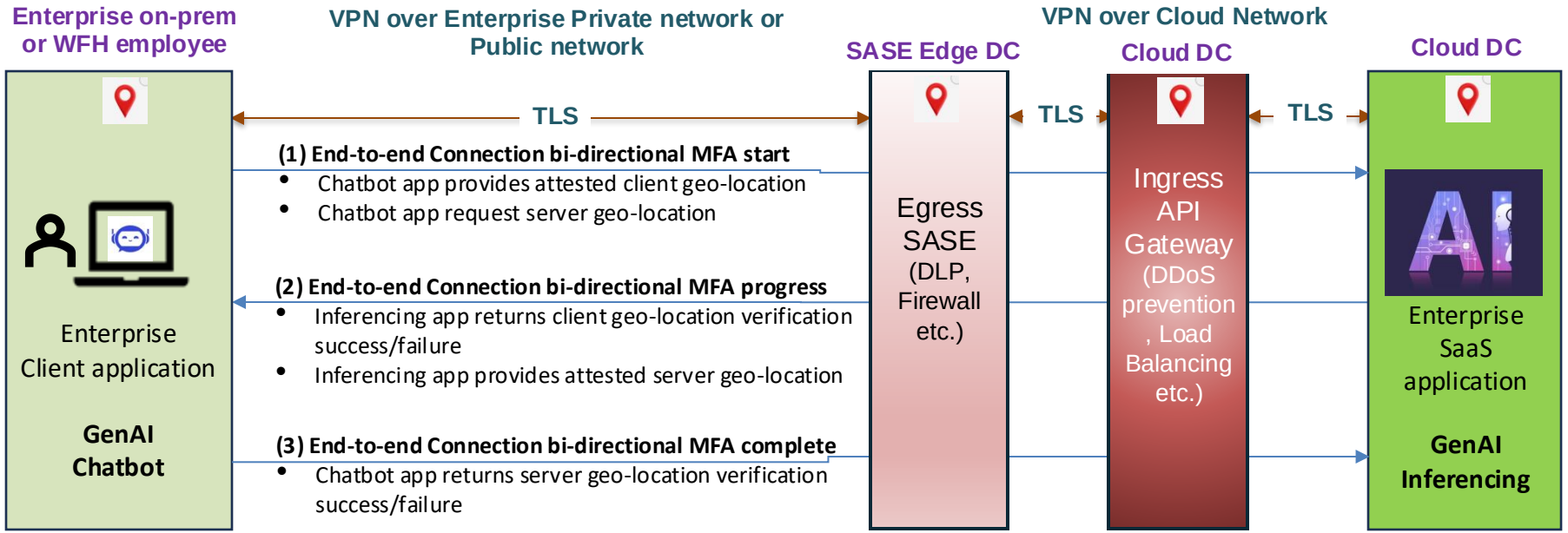
- **TEE RoT:** Ensures the TCC Manager, TEE Manager, and other system components are measured as part of system initialization.
- **Location RoT:** TCC Manager performs IO subsystem (location sensor etc.) integrity checks as a prerequisite to binding IO devices to workload TEEs.
- **Key Storage RoT:** TCC Manager performs storage subsystem integrity checks as a prerequisite to binding storage resources to workload TEEs.

Trusted Node Interconnect



- **Trusted Nodes:** Tenant workload execution and data are isolated from host system software while retaining host-affinity.
- **Orchestrator:** Workload nodes can be distributed and coordinated following a trusted lifecycle.
- **Provenance Service:** Workloads, Identities, TEEs, Platforms.
- **Trusted Workloads:** Before workload processing begins, trust between nodes and orchestrator is established, and the workload is bound to trusted node interconnect fabric.

Data residency use case - end-to-end value



- **Precise, 3rd party verifiable client/server application geo-location as part of bi-directional MFA between**
  - **Enterprise client application and Enterprise SaaS application (depicted above, end-to-end connection)**
  - Enterprise client application and Egress SASE application (TLS connection)
  - Egress SASE application and Ingress API gateway application (TLS connection)
  - Ingress API gateway application and Enterprise SaaS application (TLS connection)
- **Addresses the data residency requirements and mitigates sophisticated threats while driving compliance.**

Call to Action

- Data residency is needed to drive future trusted computing innovation, and an *end-to-end perspective* is essential for trusting confidential computing workloads.
- Trusted Computing is evolving to include:
  - Trusted location that expands root-of-trust underpinnings beyond traditional RTS, RTR, and RTM capabilities.
  - Connected trusted execution environments that are flexibly partitioned and dynamically bound to HW roots with host and location affinity.
  - Active trust management in the form of attestation appraisal, risk assessment, and trusted resource lifecycles overseen by a *TCC Manager, Workload Orchestrator and Provenance Service*.