Attested TLS: Use Cases

Hackathon Exploratory Session

Paul Howard, Architecture & Technology Group, Arm

Who Am I?

Paul Howard
Principal System Solutions Architect at **Arm**
paul.howard@arm.com
https://slack.cncf.io/
https://www.linkedin.com/in/paulhoward4/

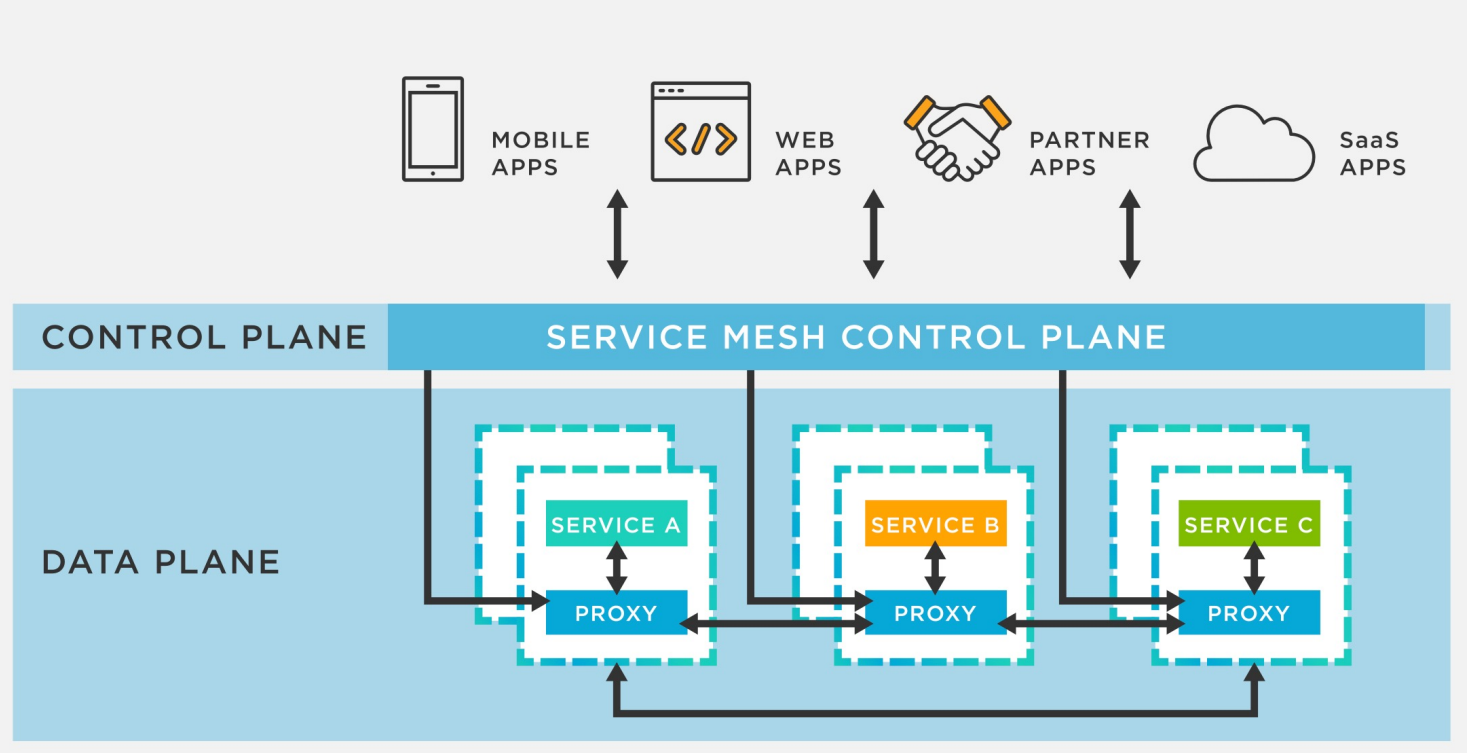
@paulhowardarm

Attested TLS In Service Mesh

Why Service Mesh?

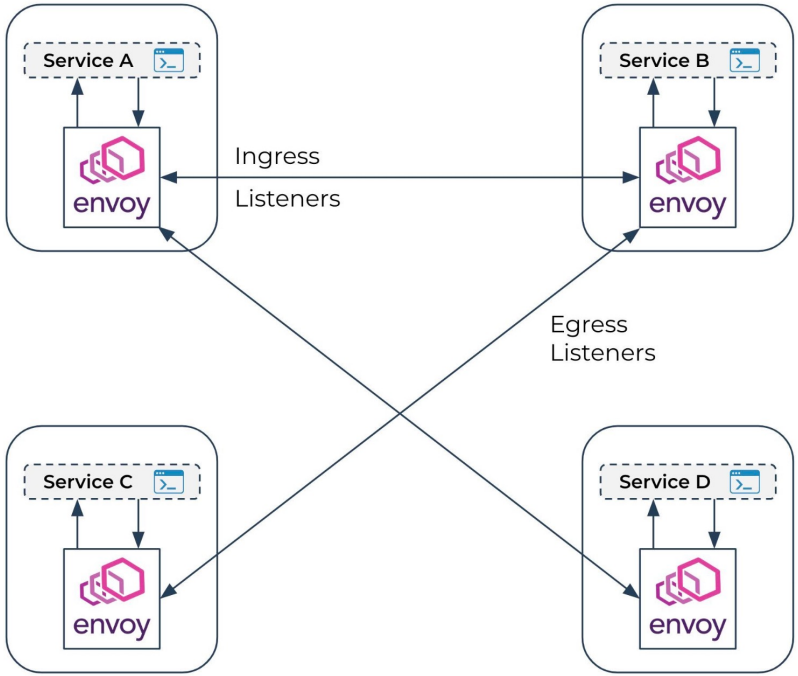
- Microservice-based applications have a common set of challenges that all services/components need to solve:
  - Secure and reliable communication between the services
  - Discovery
  - Monitoring
  - Authentication
  - Optimization and load balancing
  - Policy management
  - Rate limiting
  - Protocol translation
- Service meshes are designed to offload these requirements as a horizontal feature that all components can benefit from uniformly, allowing developers to focus on the value-add functions

Service Meshes in Cloud Native Applications



CNCF Service Mesh Landscape

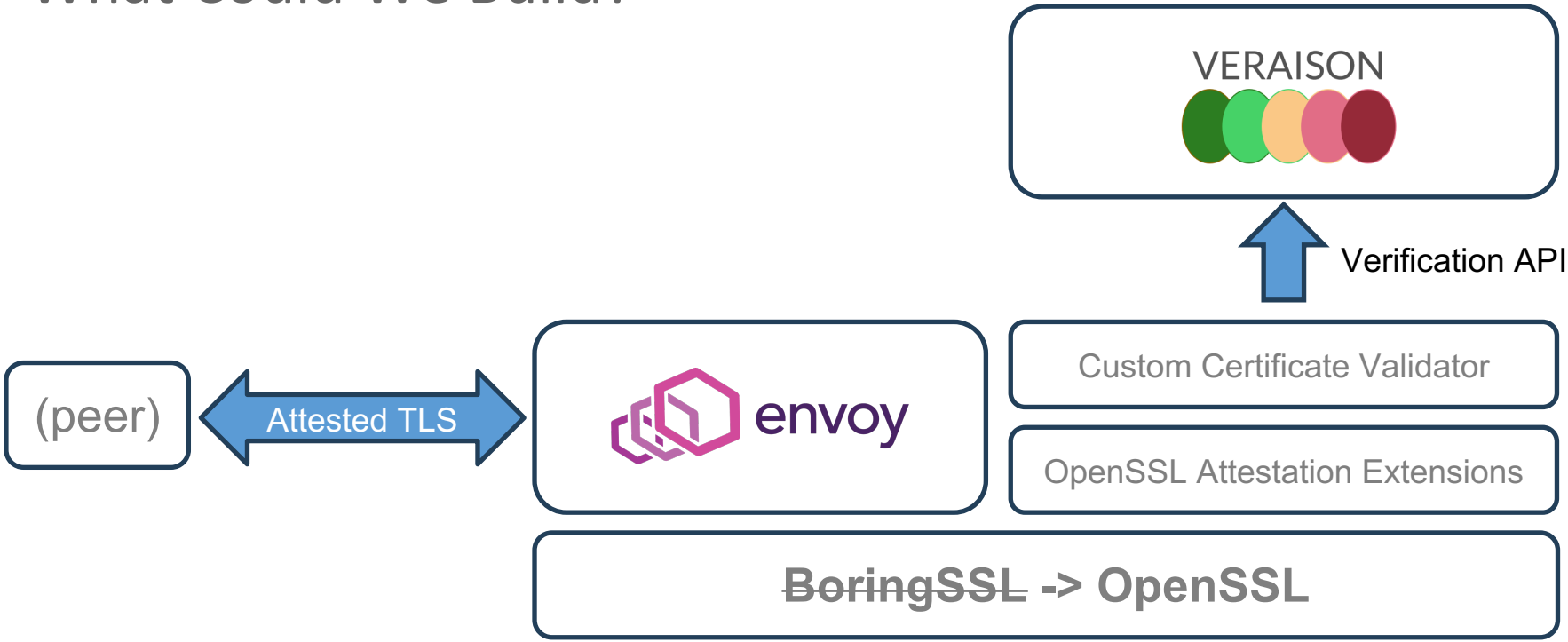
Envoy Proxy


Service A
envoy
Service B
envoy
Ingress
Listeners
Egress
Listeners
Service C
envoy
Service D
envoy

Relevance of Attested TLS

- Microservices communicate through proxies such as Envoy
- Proxy takes on the “heavy lifting” of secure communication, including TLS
- Can Attested TLS help enable use cases where we want to verify the security stance of the nodes that are hosting the microservices?

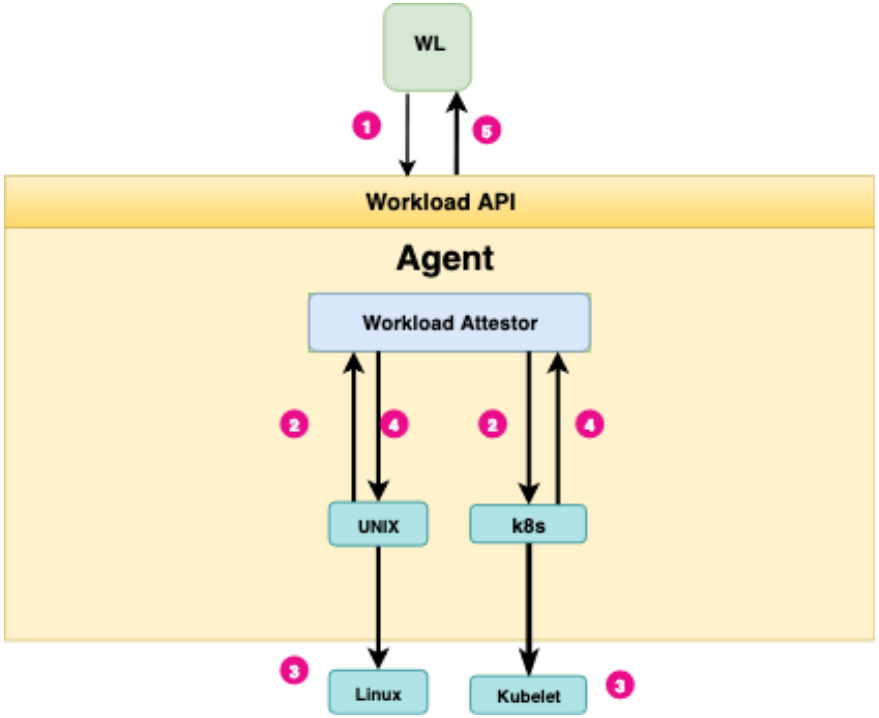
What Could We Build?



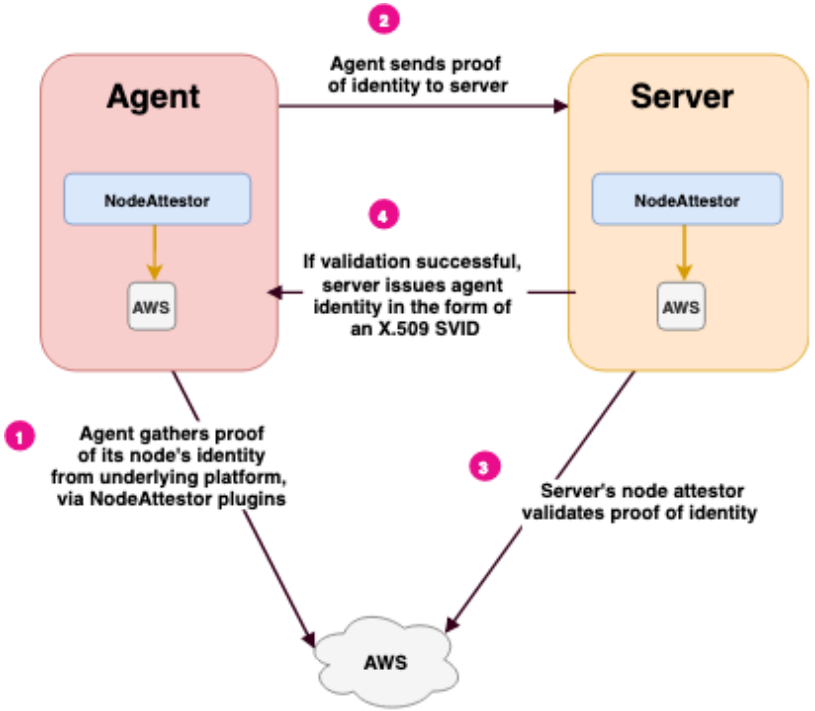
Open-ended Questions/Discussion

- Passport vs. background check – how stable is a connection between two Envoy proxy peers?
- How to blend with existing workload/node attestation ceremonies (eg. SPIFFE/SPIRE)
  - Consider different attestation patterns per peer: eg. SPIFFE/SPIRE on one end, and a EAR passport or something on the other
- Applicability to WIMSE architecture?

Appendix: SPIFFE Workload and Node Attestation



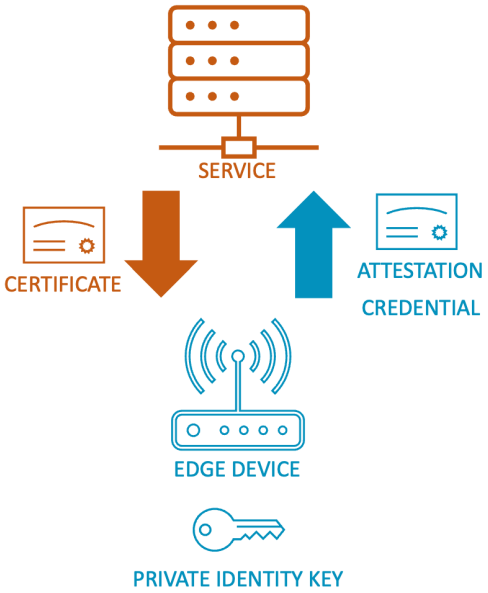
Workload Attestation



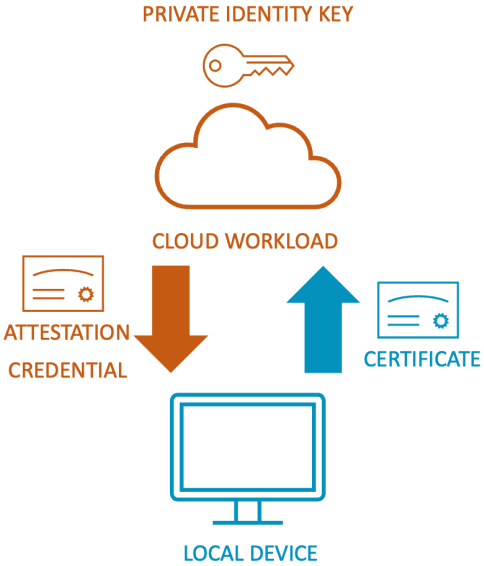
Node Attestation

“Logical TEE” Across Cloud and Edge

Flagship Use Cases for Attested TLS Today

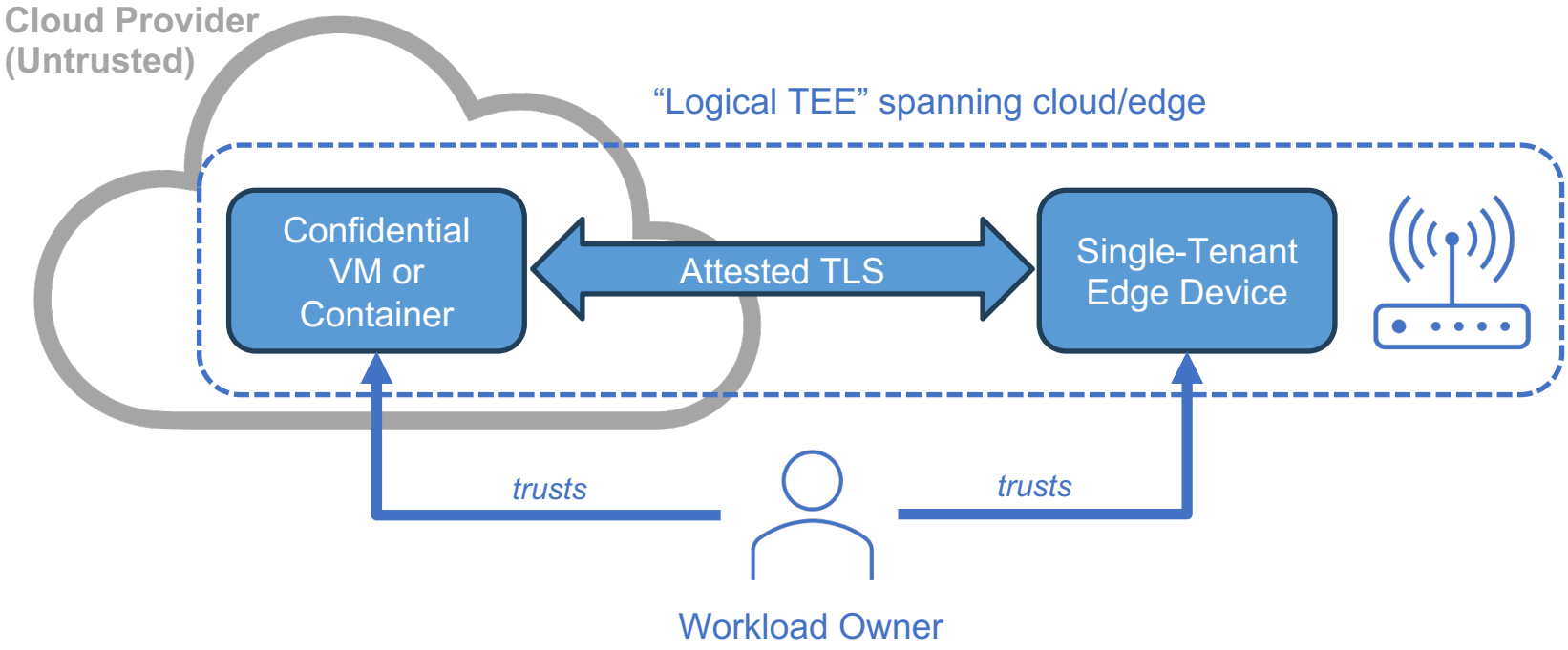


IoT/Edge Device Onboarding



Confidential Computing

Proposed Use Case: ”Logical TEE”

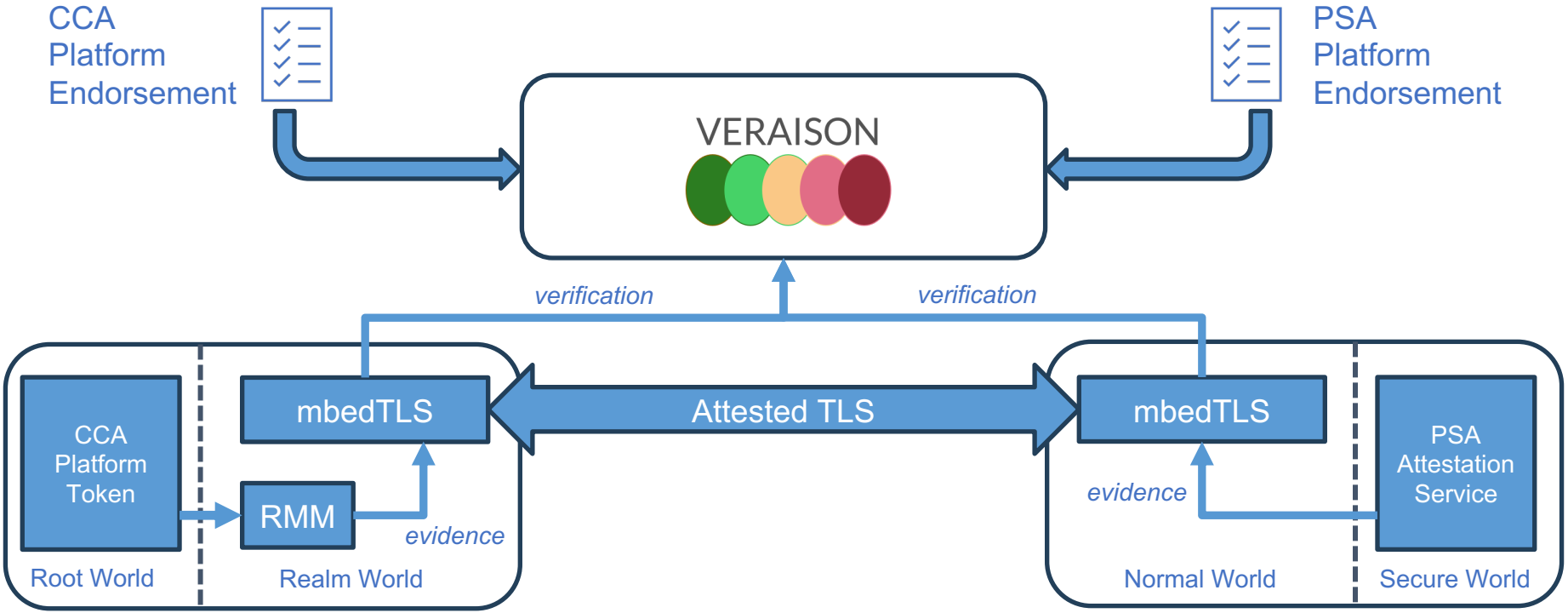


Relevant Attestation Schemes for Arm Platforms

arm CCA

psacertified™

What Could We Build?



Open-ended Questions/Discussion

- Which TLS stacks would we need to extend?
- Cloud provider awareness? (Cloud providers have existing mechanisms for orchestrating workloads onto registered edge devices)
- Who and where are the verifiers?


LinaroConnect
MADRID 2024 | MAY 12-17 2024
Thank you