ELASTIC Project
Secure Systems Group, Aalto University

Henrik Niskanen (Aalto University), Huy Ngo (Aalto University) , Lachlan J. Gunn (Aalto University)

Beyond the Pod: Attested Kubernetes deployment of systems of Confidential Containers

1. Building Blocks of Confidential Computing & Protecting data-in-use

Trusted Execution Environment
A hardware-isolated, secure area within a CPU that protects the confidentiality and integrity of code and data, even from the host operating system. **(TEE)**

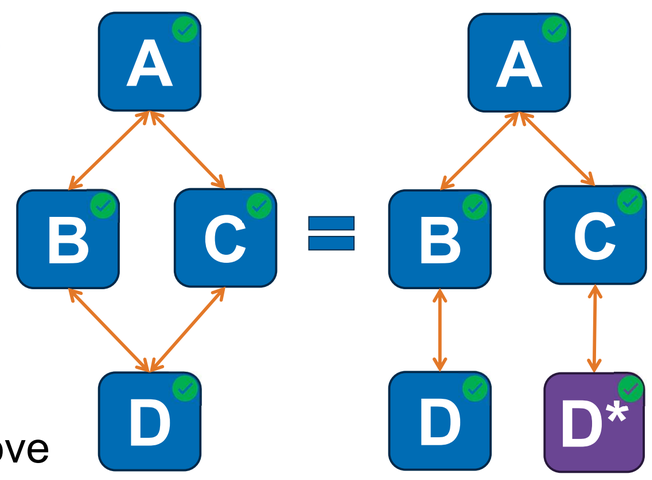
Remote Attestation
The process by which a TEE provides verifiable proof of its identity, HW and SW integrity, and current security state to a remote party to establish trust. **(RA)**

Confidential Containers
Kubernetes pods running inside TEE-backed VMs (CVM) that isolate them from the untrusted host. Provides tools for attestation and policies **(CoCo)**

2. The Granularity Gap

Because security of TEEs and RA is tied to physical hardware, the boundary of protection inherently fits within a single machine or VM.

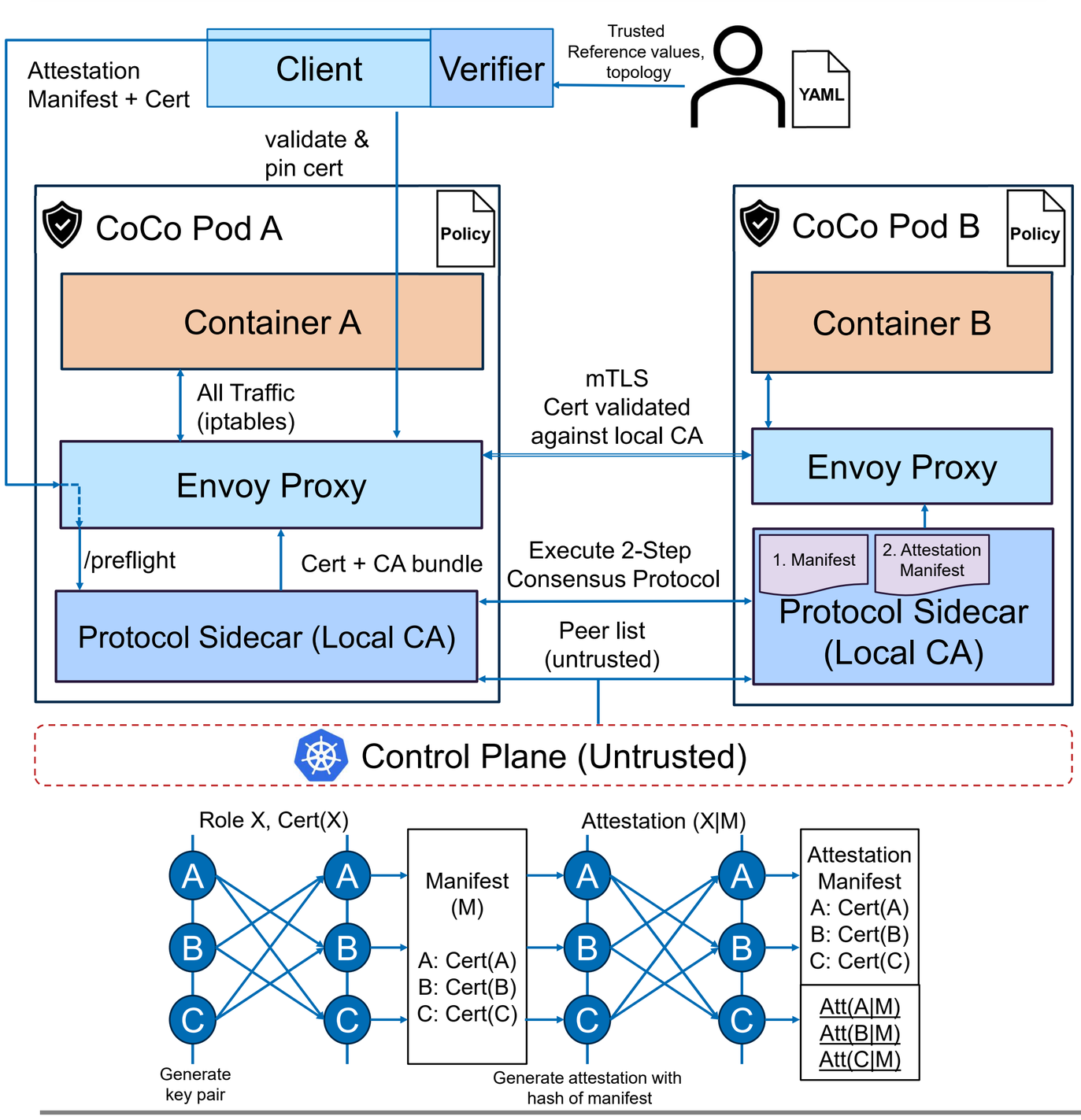
- Traditional methods only attest individual pods in isolation.
- Remote attestation alone cannot prove the structural topology of a multi-component distributed application.



3. The Goal

To implement a mechanism for application components to prove that the entire distributed application is correct, including both topology and structural integrity, operating under the assumption that control plane is inherently untrusted

4. Pluggable Distributed Trust



Confidential Containers: Pods run in a CoCo CVM. It enforces a policy restricting images and commands and the policy is included in the hardware quote

Two-Phase Protocol: Sidecars exchange freshly minted CA certificates, then embed the full topology manifest into their hardware quote.

Attestation gate: Envoy starts only after the pod's leaf cert and peer CA bundle are delivered. No traffic flows before.

Transparent Interception: iptables redirects all pod traffic through Envoy proxy with no application code changes required.

mTLS Enforcement: Envoy presents its leaf cert, validates peers against the attested CA bundle, and rejects any cert not in the manifest at handshake.

External Verifier: Any client validates the full application by fetching the attestation manifest, verifying the hardware quotes commit to the manifest, and pinning the CA for TLS.

5. Open Questions

- How does the protocol handle scaling, restarts and ephemeral workloads
- How to handle persistent storage in the solution

Aalto University

Co-funded by the European Union

The ELASTIC project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe programme, Grant Agreement No. 101139067. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or SNS-JU. Neither the European Union nor the granting authority can be held responsible for them.