Zainab Ahmad (Aalto, Ericsson), Jimmy Kjällman (Ericsson), Lachlan J. Gunn (Aalto)

Multi-Platform Attestation Verification

- Trust in remote devices can be established via **remote attestation.**
- Currently **hardware specific solutions** exist.
- Our solution converts the proprietary evidence format to standard format in **WebAssembly**.

Introduction

- A security mechanism by which an entity i.e. Attester provides information about its hardware and software configurations to a remote entity i.e. Relying Party.
- The Remote ATtestation procedureS (RATS) architecture provides a standardized framework to support the attestation process (Figure 1).

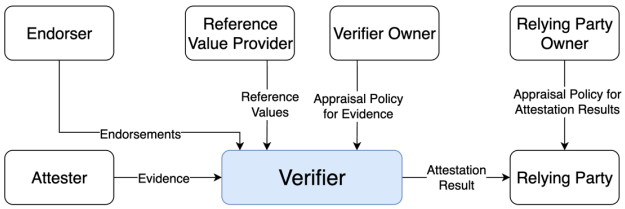

Figure 1: Remote Attestation (RATS Architecture).

The problem

- Current solutions are primarily hardware-specific, tailored to individual Trusted Execution Environments (TEEs) using proprietary mechanisms.

EAT, Trust, Verify

- Converts the proprietary evidence format to a standard EAT format after signature verification.
  - A module for verifying the evidence signature and converting it can be sent alongside the evidence from Attester.
  - The Verifier can dynamically acquire the capability to verify evidence for new hardware platforms.
- Verifies and signs the result within the Verifier i.e. VERAISON.

Implementation

- Our approach converts proprietary evidence into a standard format inside a WebAssembly module (Figure 2).
- Evidence signature verification is also done inside the WebAssembly module (Figure 2).
- Different WebAssembly modules loaded for different proprietary evidence formats without affecting the entire system.
- The sandboxed nature of WebAssembly ensures portability and security.

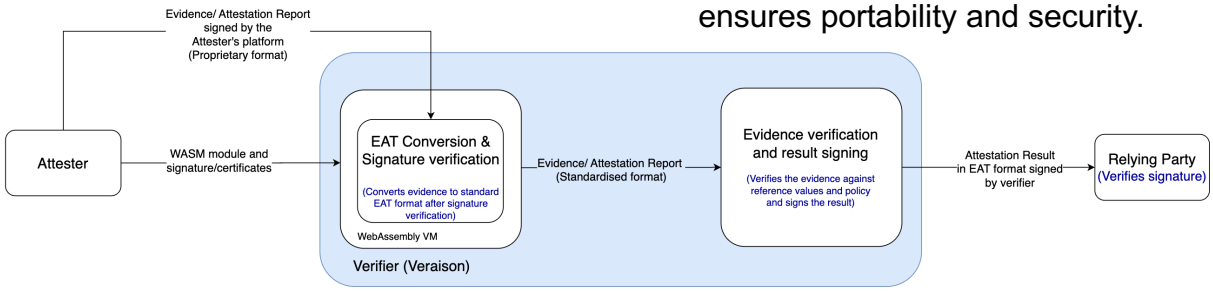

Figure 2: Attestation Flow.

Aalto University
This work is supported in part by the Academy of Finland (decision 339514).
ERICSSON