Wentao Xie(Aalto, Ericsson), Jimmy Kjällman (Ericsson), Lachlan J. Gunn (Aalto)

Platform-Agnostic Remote Attestation with WebAssembly Components

1 Introduction

- Remote attestation establishes trust between distributed nodes.
- However, different hardware platforms(AMD SEV-SNP, Intel TDX, etc.) produce evidence in incompatible formats, forcing a central verifier to maintain multiple, platform-specific tools.
- We encapsulate each platform's verification logic into a sandboxed WebAssembly component, which a central node can load and use through a single, uniform interface with minimal overhead.

2 Background

- WebAssembly Components are dynamically loadable modules that expose a standardized interface, defined in a WIT(WebAssembly Interface Types) file which specifies function signatures and data types. This model ensures language- and runtime-agnostic interoperability, strong sandboxing, and high portability with minimal overhead.
- The WebAssembly System Interface (WASI) is a standardized API that enables WebAssembly modules to perform system-level operations in a secure, sandboxed manner.

3 Solution

- We decouple platform-specific tasks from platform-agnostic operations. Each platform's specific logic is compiled into a WebAssembly component exposing a predefined interface. Each component is signed by a trusted authority to guarantee its integrity. At runtime, the component is dynamically loaded into the unified verifier, enabling validating evidence from any supported platform.
- The WebAssembly component encapsulating platform-specific logic accepts attestation evidence and expected measurements as inputs, verifies the evidence signature, parses the report, validates measurements against expected values, and emits a claim map.
- Although the underlying implementations differ significantly across attester hardware platforms, each WebAssembly component exposes these capabilities through a uniform interface.

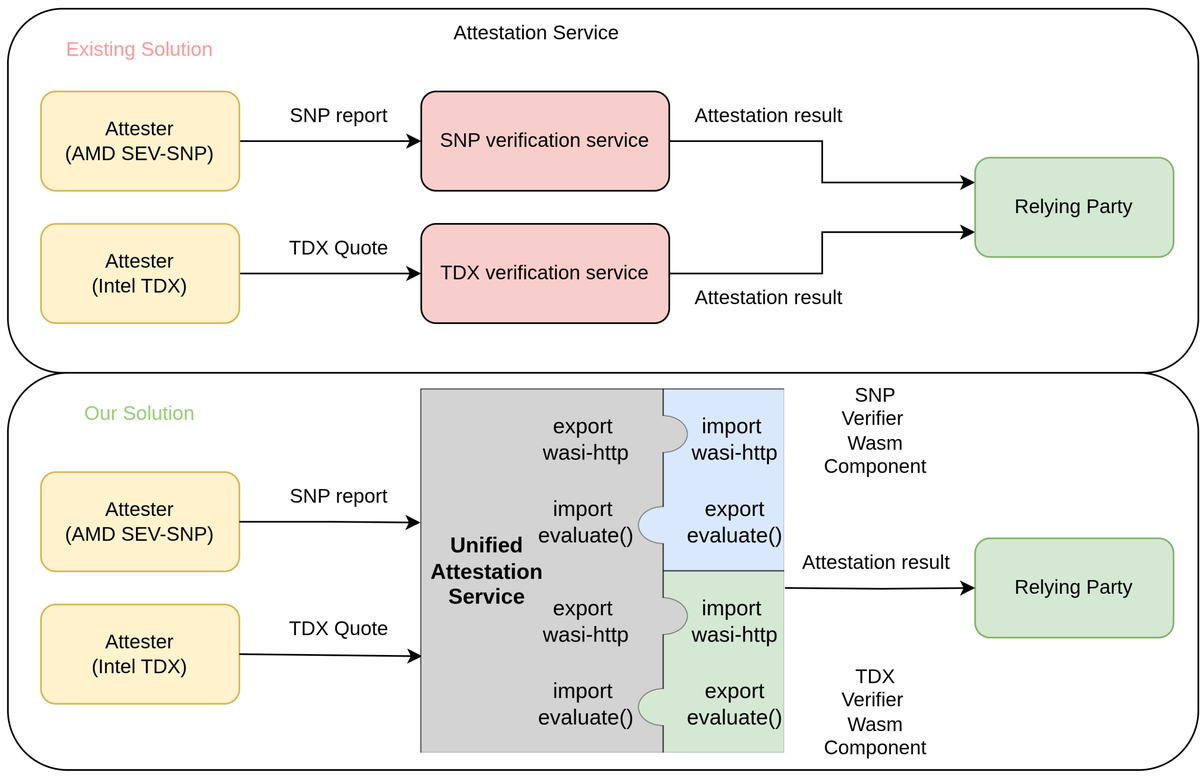

Figure 1: Comparison between our solution and existing solutions

4 Application

- Data fabric is an architectural framework that provides unified access and management of data across heterogeneous sources.
- To demonstrate our platform-agnostic attestation service, we integrate it into a data fabric implementation. When a data consumer requests access to sensitive data, the fabric initiates a remote attestation of the consumer and validates the resulting evidence using our embedded attestation service.

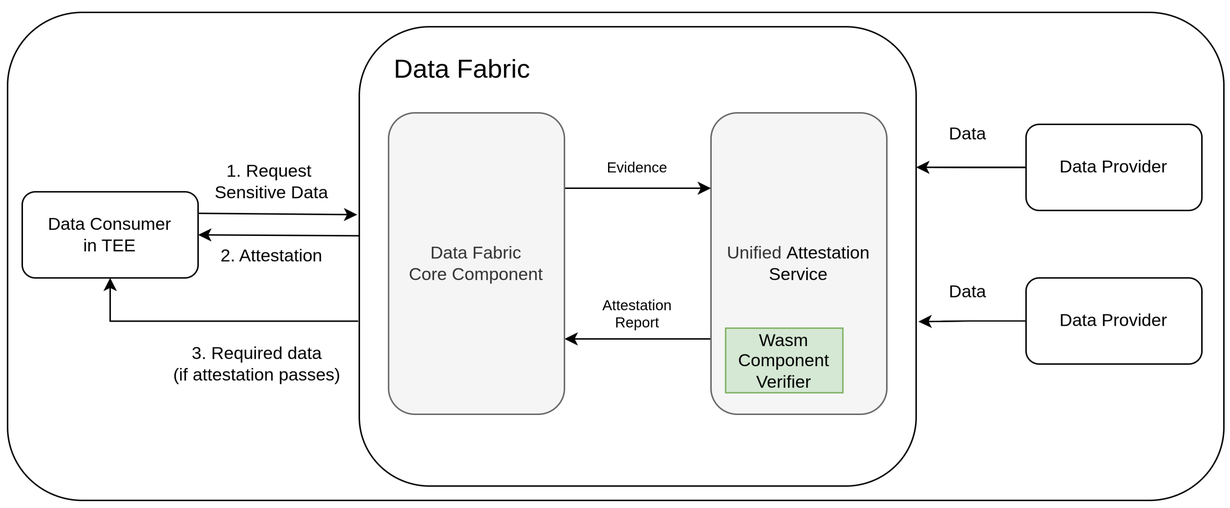

Figure 2: Integration with Data Fabric

Aalto University
ERICSSON
elastic
6GSNS
Co-funded by the European Union