elastic

Efficient, portabLe And Secure orchesTration for reliable servICes

T3.3

Remote Attestation.

Anne-Marie Parden / Thales DIS

Co-funded by
the European Union

6GSNS

T3.3: Remote Attestation

Lead: THD; Participants: ERF, UVC, AAL, LUN

Objective:

Develop and enhance **remote attestation mechanisms** for **TEEs** to establish trust between remote entities and ensure **a secure, uncompromised environment.**

Key Focus Areas:

- **Leverage standardisation efforts** (e.g., RATS) for compatibility and interoperability
- **Strengthen security & robustness** using hardware root of trust and cryptographic mechanisms
- **Explore lightweight, efficient protocols** for distributed and heterogeneous systems

This work will enhance the reliability and scalability of **Confidential Computing (CC)** in modern infrastructures.

Co-funded by
the European Union

6GSNS

T3.3: Remote Attestation

elasstic

State of the Art Analysis: Remote Attestation

- **Explored Implementations in:**
  - **TEEs** (e.g., AMD SEV-SNP, Intel SGX & TDX, Keystone, COVE)
  - **Cloud Platforms** (e.g., Microsoft Azure, AWS, Google Cloud Platform)
  - **Open-Source Projects** (e.g., OpenTitan, Enarx, Confidential Computing Consortium)

Enhancement Exploration (Post-SOTA Analysis)

- **Strengthening security & robustness** of attestation mechanisms
- **Developing efficient & lightweight** attestation protocols
- **Defining a Hardware Abstraction Layer** for WASM runtime
  - Ensures **interoperability** across confidential computing environments
  - Supports **large-scale deployment** of secure attestation processes

Co-funded by the European Union

6GSNS

elastic

Thank you for your attention!

https://elasticproject.eu/ https://www.linkedin.com/company/elastic-project/

https://www.instagram.com/elastic_project/ https://twitter.com/ElasticProject_

Co-funded by
The European Union

6GSNS