

Can RATS Architecture Help in Security Analysis of Attestation Frameworks?

Muhammad Usama Sardar¹

Based on joint work with Thomas Fossati²,
Hannes Tschofenig³ and Simon Frost⁴

¹TU Dresden, Germany

²Linaro, Lausanne, Switzerland

³University of Applied Sciences Bonn-Rhein-Sieg and Siemens, Germany

⁴Arm, Cambridge, UK

September 27, 2024

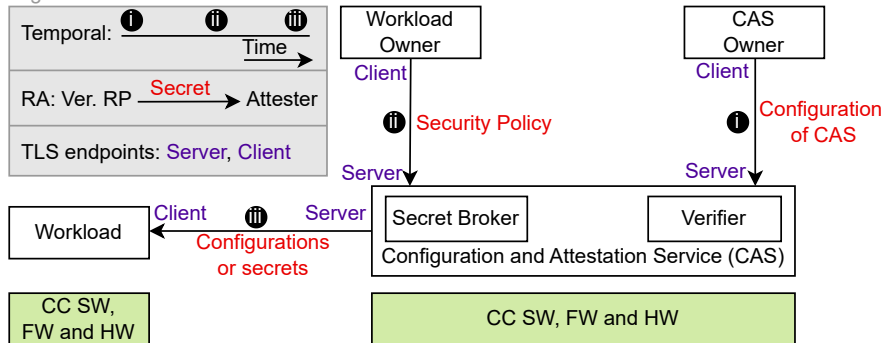


Challenge

- Closed-source and Un(der)specified
- Context: Confidential Computing

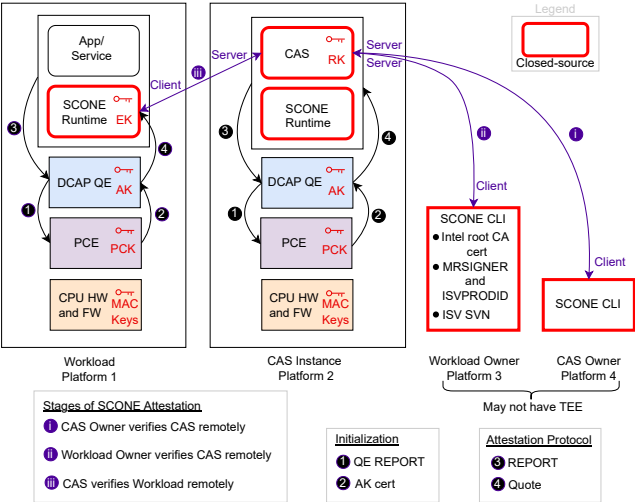
SCONE Attestation Architecture

Legend



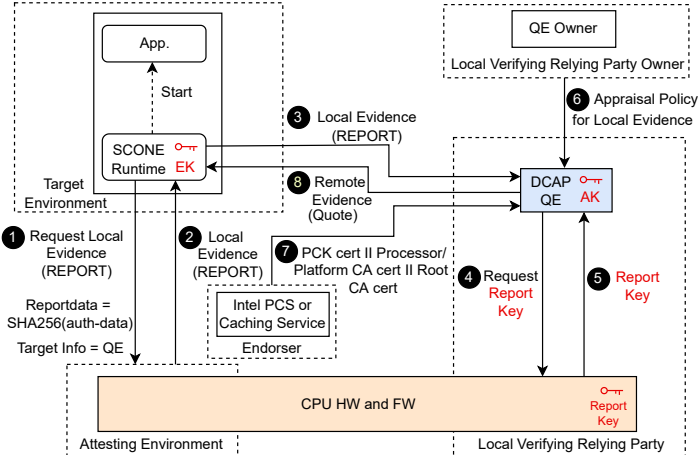
- **Closed-source** and **Unspecified**: Functionality of SCONE QE?
- **Unspecified**: Structure of SCONE Quote?

DCAP-based SCONE Attestation



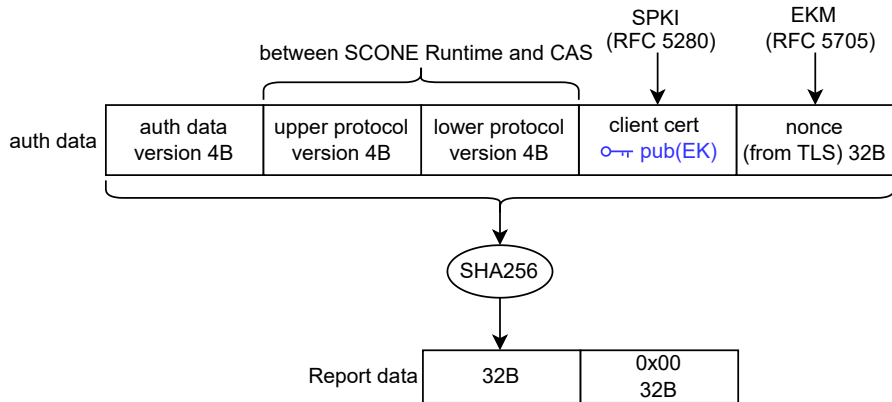
- App + SCONE Runtime in **one** enclave
- **Unspecified:** Bootstrapping of CAS

Generation of Remote Evidence (Stage iii)



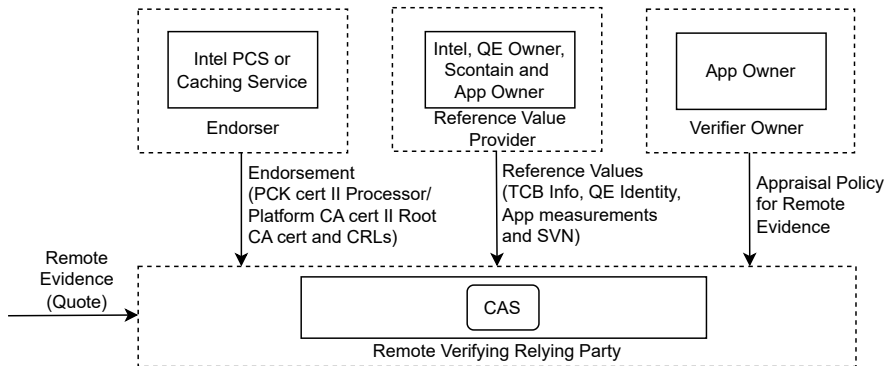
- How can app owner be sure that SCONE Runtime is not **malicious**?
- **Unspecified**: Conveyance of Evidence

Report Data for Stage iii



- Protocol for agreement of versions **unspecified**
- SPKI is **not** cert!
- EKM should **not** be used as nonce in the general case!
- Claim: several properties, such as **state at rest**, are attested.

Appraisal of Remote Evidence (Stage iii)



- App Owner may not really be the RVP!

Summary

- Closed-source
 - SCONE QE
 - SCONE Runtime
 - CAS
 - SCONE CLI
- Unspecified
 - Functionality of SCONE QE (vs. DCAP QE)
 - Structure of SCONE Quote
 - Protocol for agreement of versions
 - Conveyance of Evidence
 - KDF for RK in stage ii
 - Report data for stage ii
 - Certificate chain for CAS
 - Bootstrapping of CAS

ACK

- Nikolaus Thümmel (Scontain)
- Ionut Mihalcea (Arm)
- Yaron Sheffer (Intuit)
- Thore Sommer (Kiel University)
- Henk Birkholz (Fraunhofer SIT)
- Giridhar Mandyam (Mediatek USA)
- Anonymous ICFEM reviewer # 1