SoK: Attestation in Confidential Computing

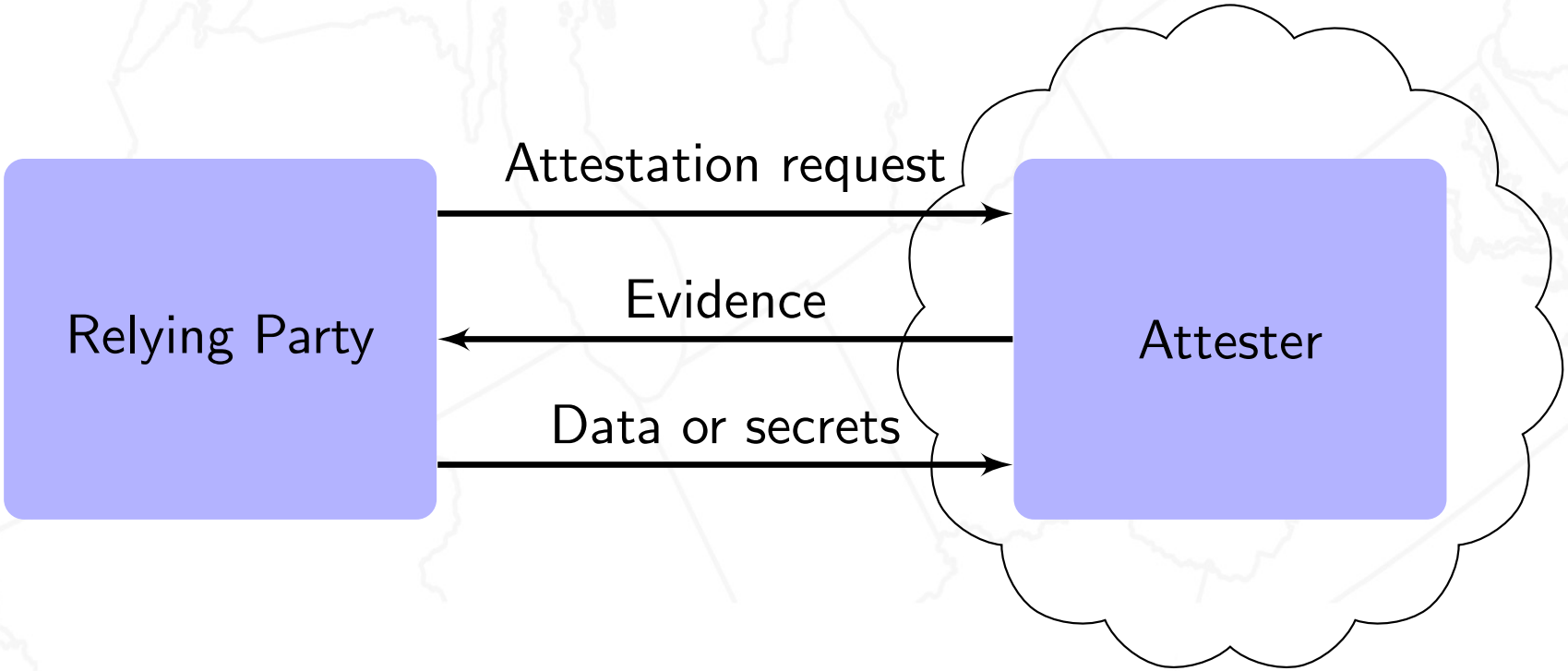
Muhammad Usama Sardar[1] Thomas Fossati[2] Simon Frost[2]

[1]TU Dresden

[2]Arm Ltd.

HOTSOS 2023
10TH ANNUAL
HOT TOPICS in the SCIENCE OF SECURITY
APRIL 3 - 5, 2023 | Virtually hosted by The National Security Agency
hotsos.org

Attestation in Confidential Computing



Contributions

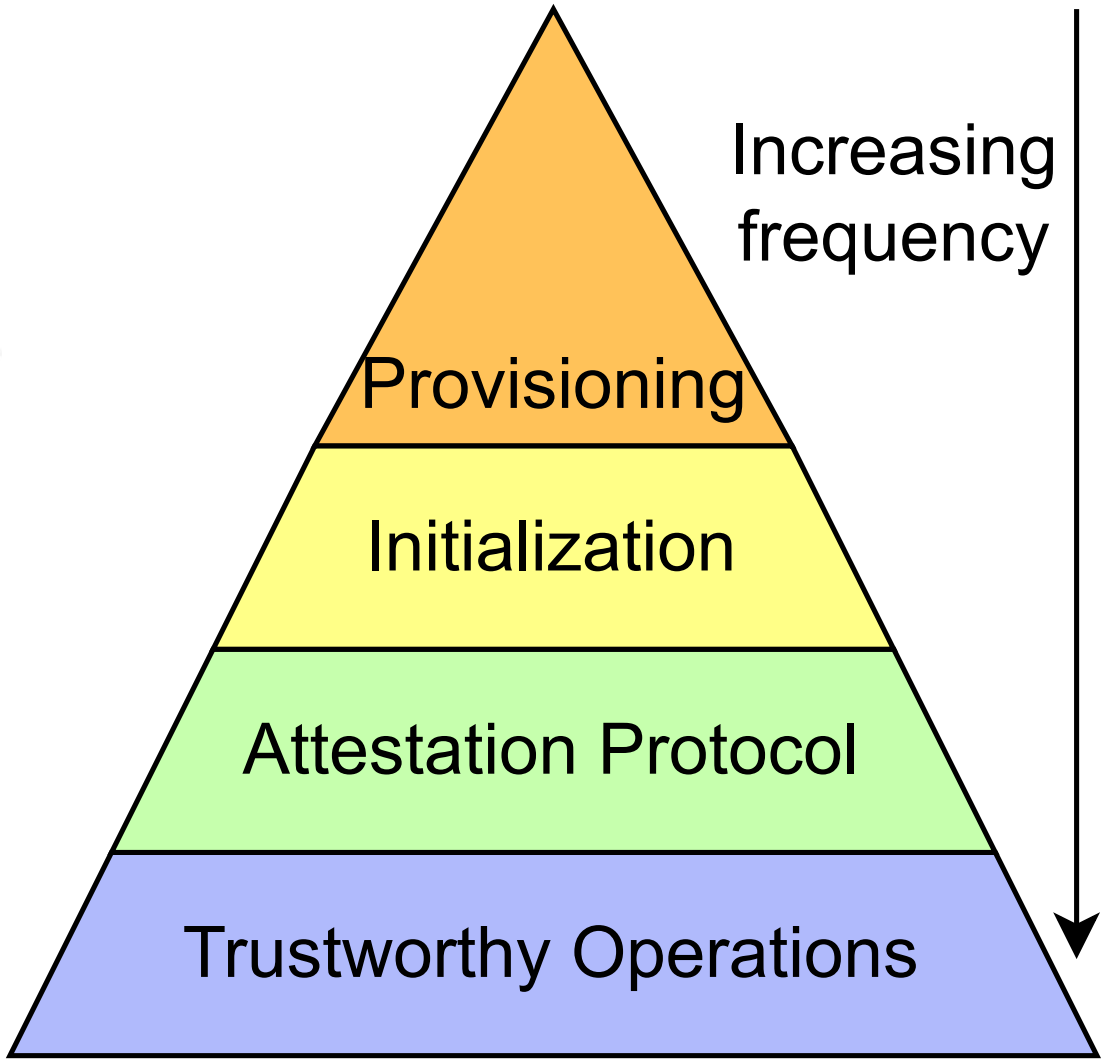
Holistic view of attestation

TEE-agnostic attestation architecture

Mappings to attestation architecture

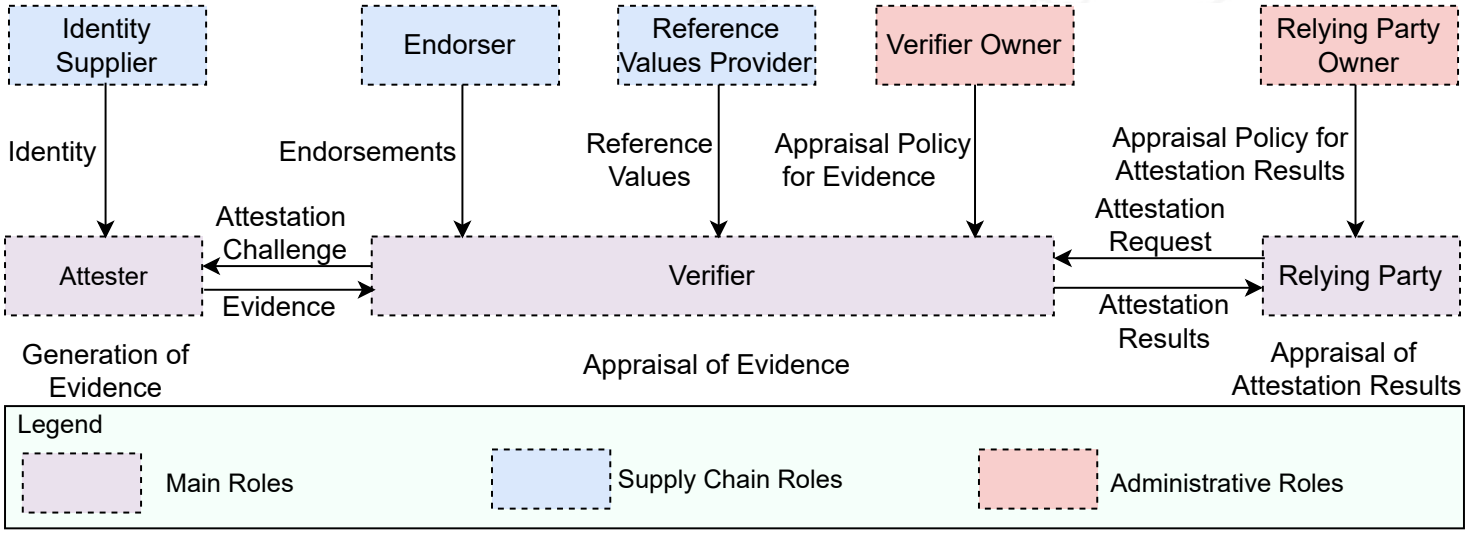
Formal specs

Holistic View of Attestation

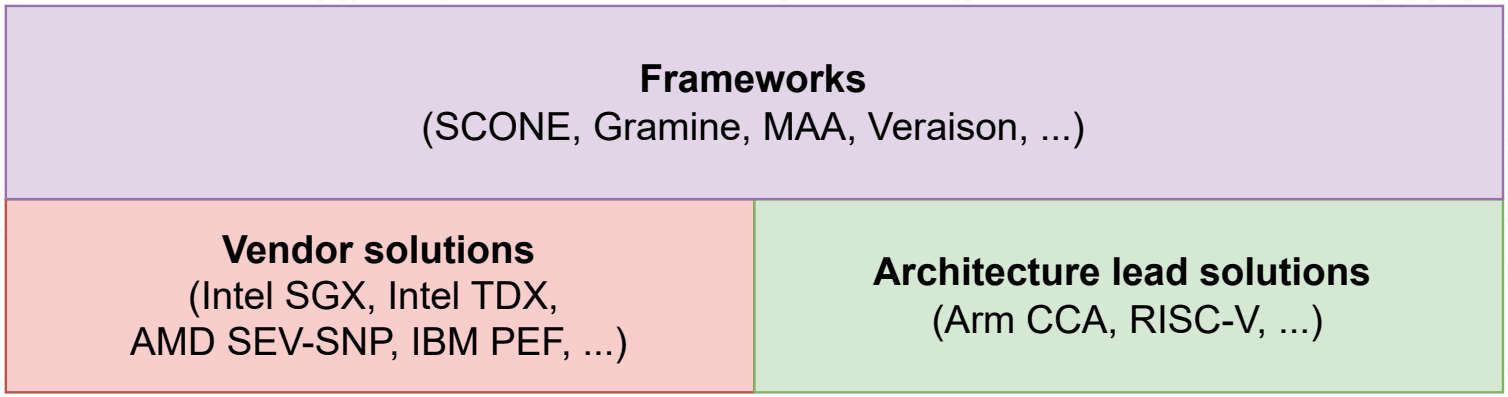


Attestation Architecture

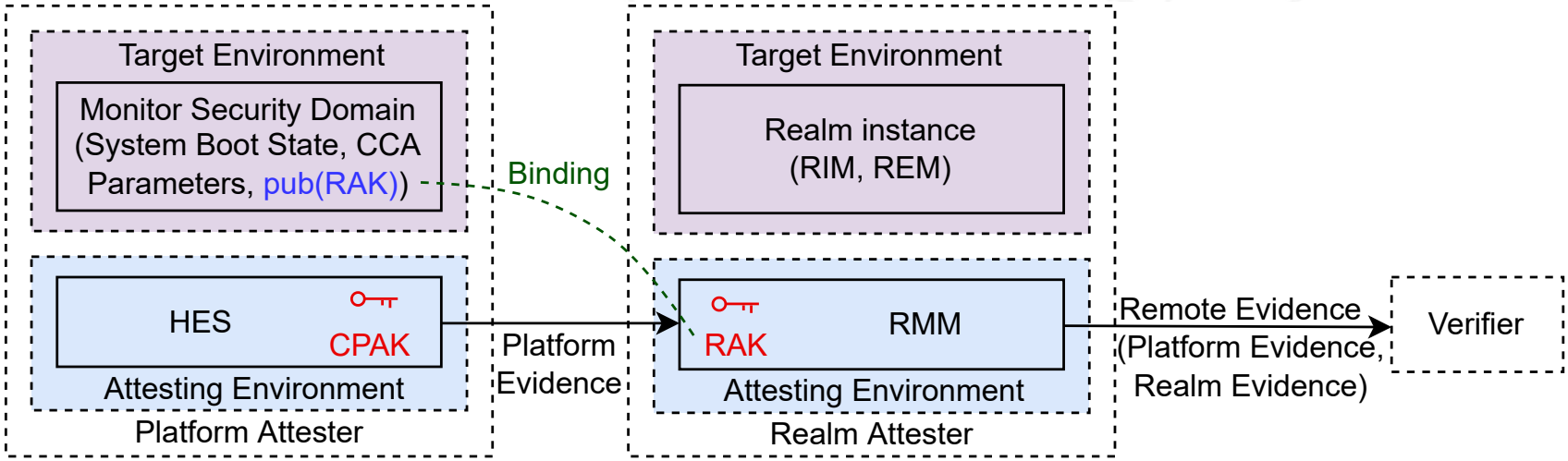
- Limitations of IETF RATS standard
  - Local attestation out of scope (cannot express Intel's attestation mechanisms)
  - Cannot express anonymous attestation (Intel EPID)
  - Various ambiguities, e.g., role vs. entity
- Errata submitted for RATS
- Our proposed TEE-agnostic architecture



Groups for Mappings



- Example: mapping for Arm CCA



Formal Analysis in ProVerif

- Assumptions
  - Verifier has preconfigured pub(CPAK) for signature verification
  - Secure channel between HES and RMM to transport the RAK key pair
- Integrity of Platform and Realm Evidence

```
query data : bitstring;
event (accepted(data)) ==> inj-event (sent(data)).
```
(1)

- For further details and security issues found, please see the draft