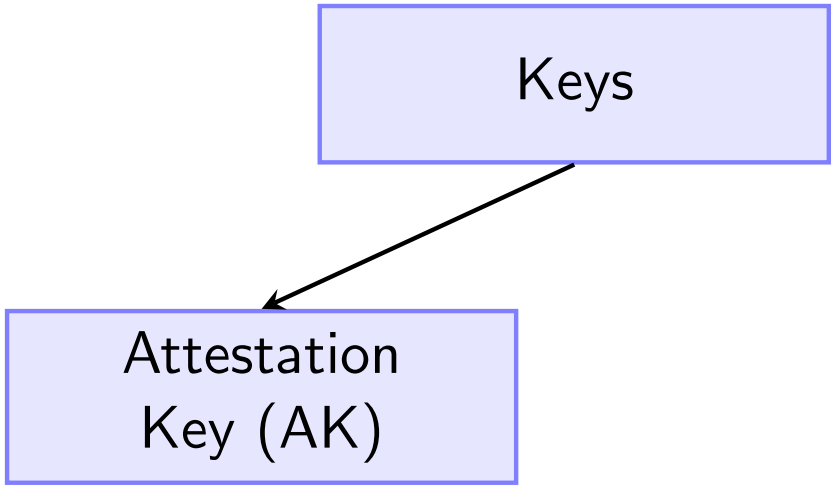
Open Questions for Discussion

Muhammad Usama Sardar

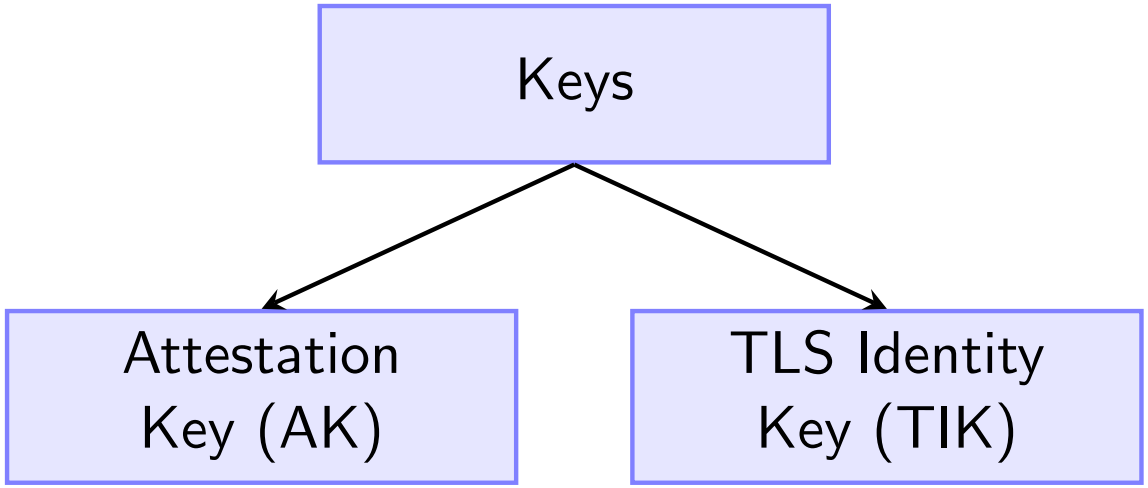
TU Dresden, Germany

January 28, 2025

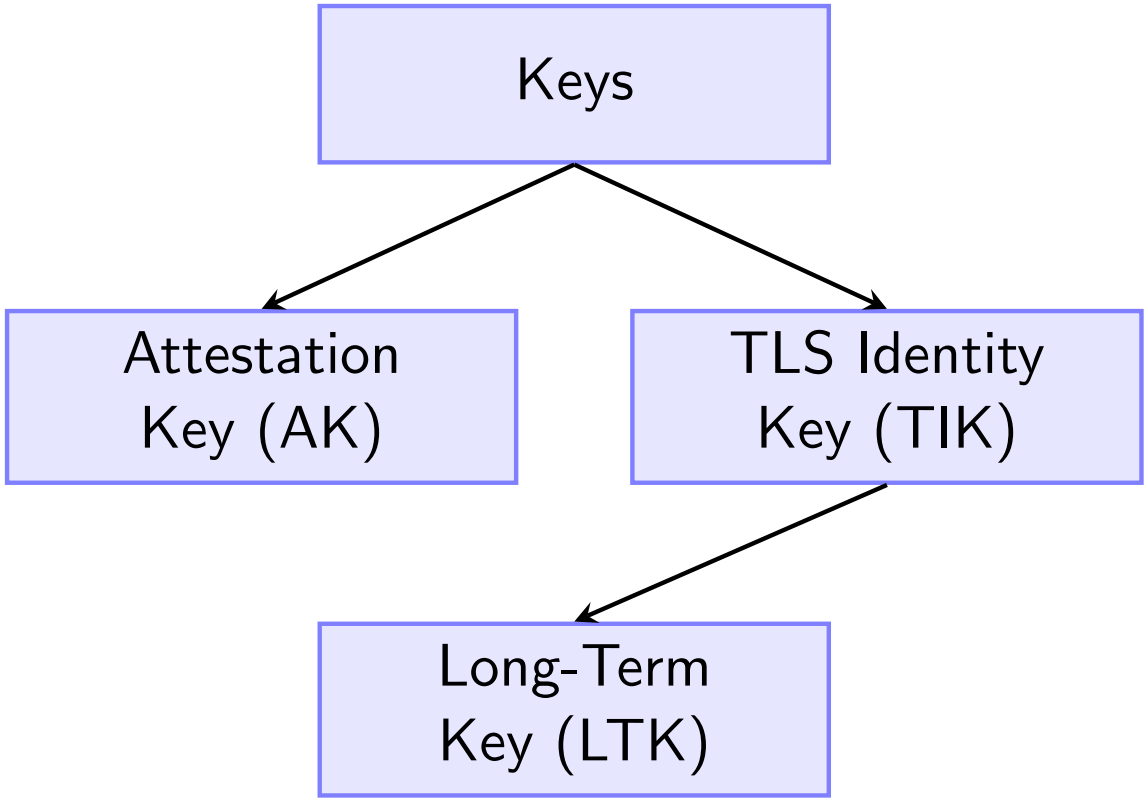
Authentication vs. Attestation?



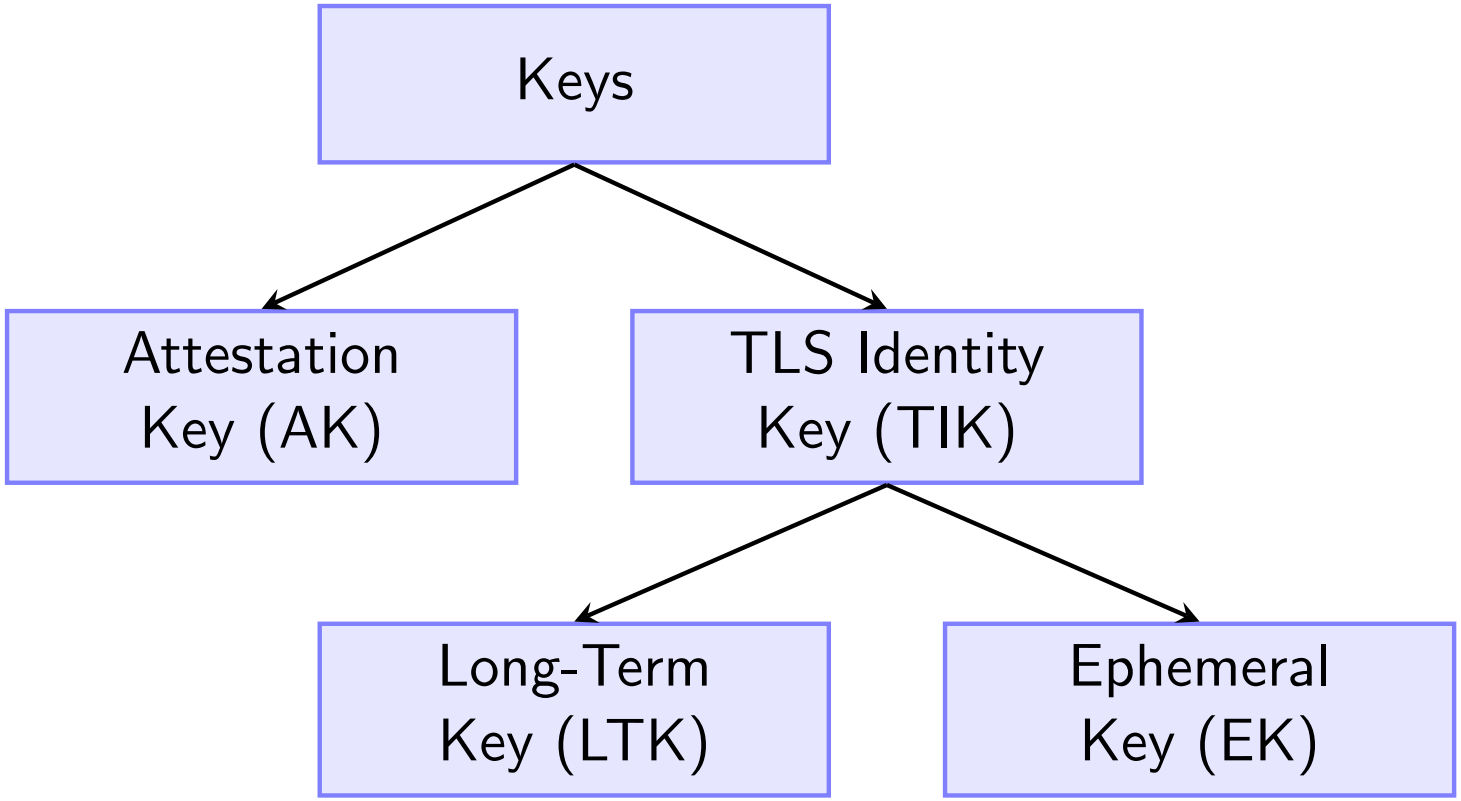
Authentication vs. Attestation?



Authentication vs. Attestation?

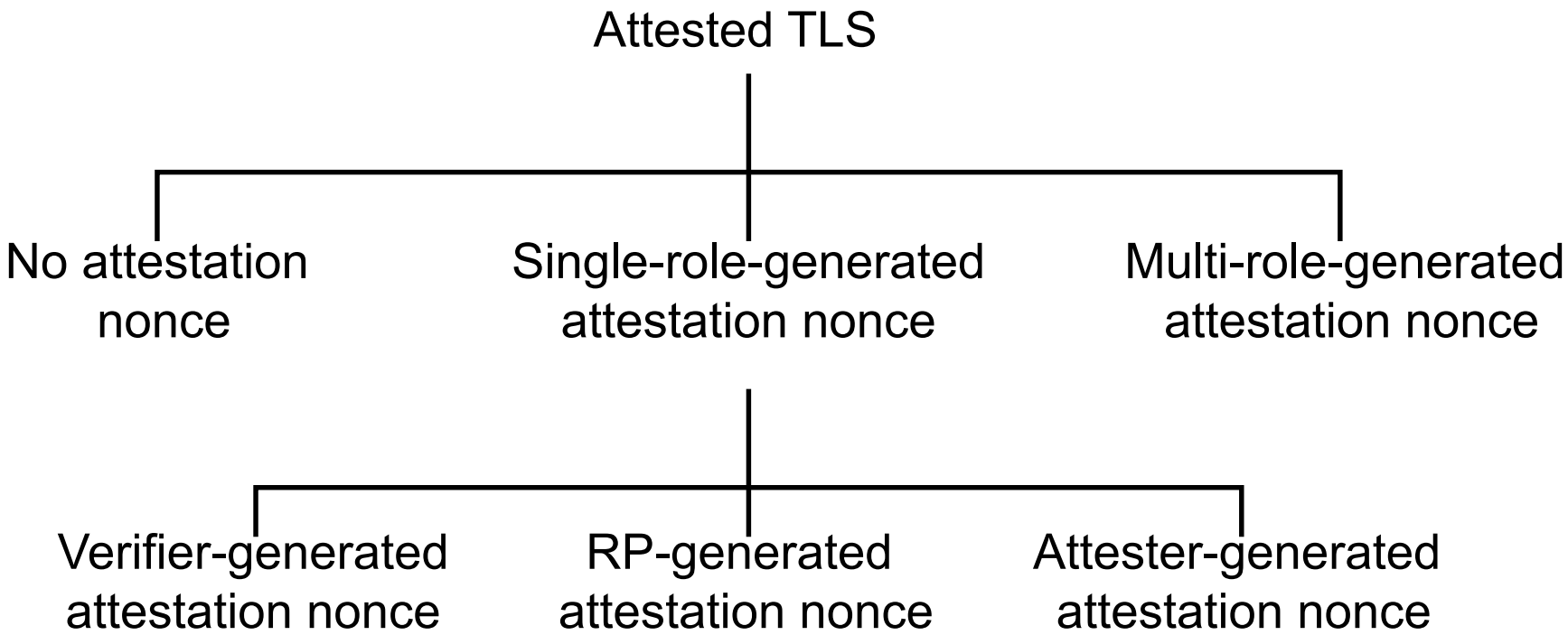


Authentication vs. Attestation?

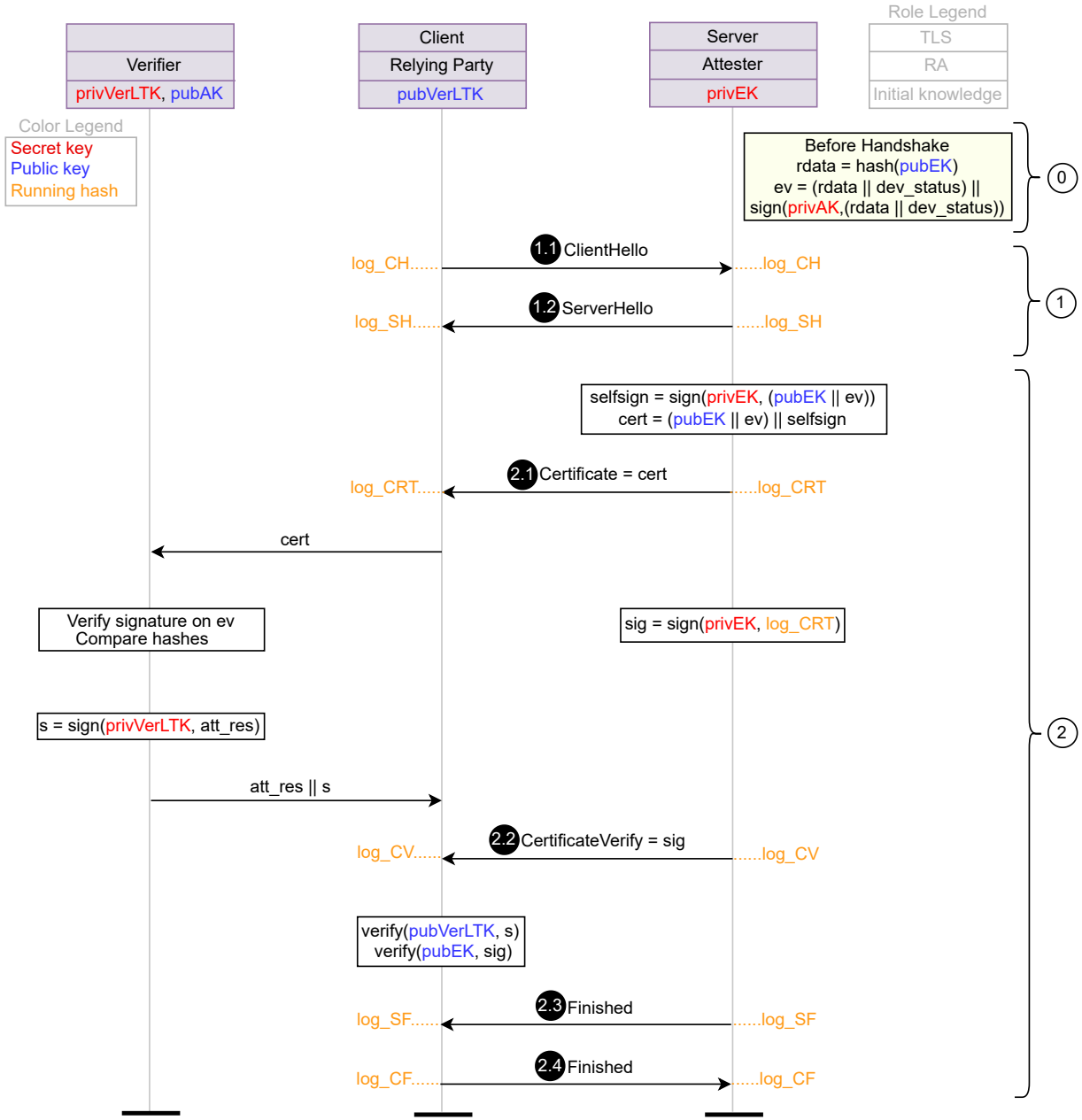


Attester-generated nonce?

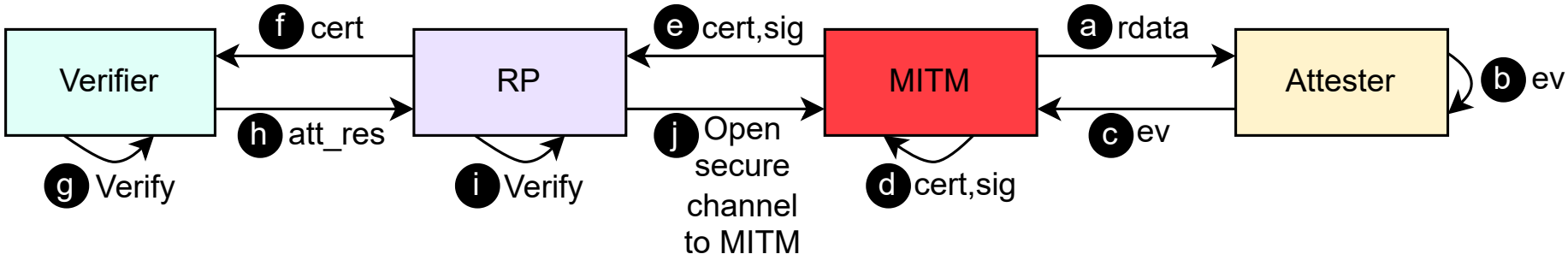
- Context: one-way (vs. mutual) attestation
- Single layered Attester



Interoperable RA-TLS



What *exactly* is measured? (Kernel, OS, App?)



Discussion

- Identity of VM-based TEE?

Discussion

- Identity of VM-based TEE?
  - Instance of VM or owner?

Discussion

- Identity of VM-based TEE?
  - Instance of VM or owner?
- Freshness of Evidence: long-lived workloads

Discussion

- Identity of VM-based TEE?
  - Instance of VM or owner?
- Freshness of Evidence: long-lived workloads
- How to provide both authentication and attestation in TLS?