



IETF COSE TSA-TST Header Parameter

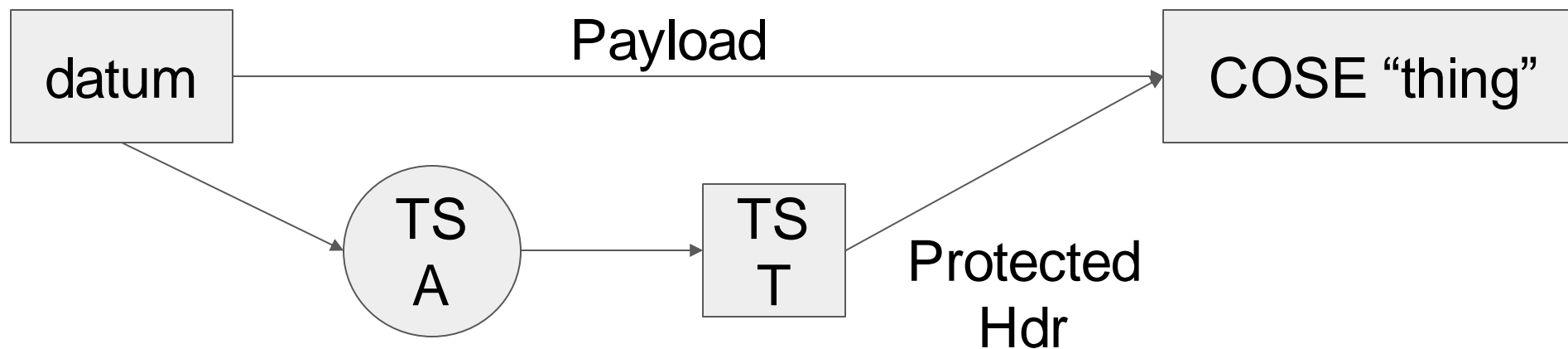
**IETF 117
July 24th, 2023
San Francisco, USA**



- Goal: reuse existing RFC3161 timestamping infra with COSE
- Two basic modes:
 - Timestamp then apply COSE processing (e.g., Sign1)
 - Apply COSE processing, then timestamp

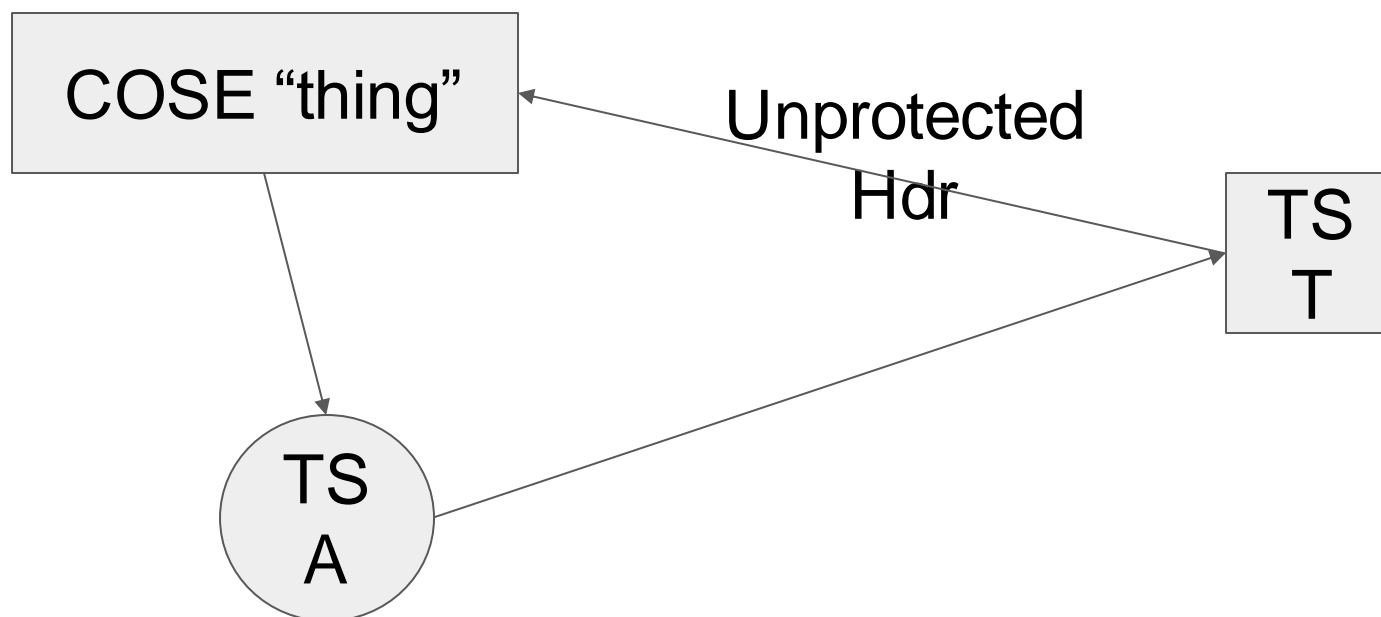
Case #1: Timestamp then apply COSE processing

- “Traditional” use cases – TODO(henk) expand
- Protected header



Case #2: Apply COSE processing then timestamp

- ~Countersign + (trusted) time
- Unprotected header



Questions

- Interested?
 - If so, which case?
- Different semantics and processing
 - Same or different COSE header key?