Time-Based Uni-Directional Attestation

https://datatracker.ietf.org/doc/draft-birkholz-tuda/

Henk Birkholz @ IETF 98

Contribution

- TUDA also utilizes a trusted Time Stamp Authority (TSA) as an additional third party in the attestation activity
  - next to the attestee and the verifier.
- No nonce / challenge-response interaction model is required between attestee and verifier.

Objectives

- increase the confidence in authentication and authorization procedures,
- address the requirements of constrained-node networks,
- support interaction models that do not maintain connection-state over time, such as REST architectures [REST],
- be able to leverage existing management interfaces, such as SNMP [RFC3411]. RESTCONF [RFC8040] or CoMI [I-D.ietf-core-comi] – and corresponding bindings,
- support broadcast and multicast schemes (e.g. [IEEE1609]),
- be able to cope with temporary loss of connectivity, and to
- provide trustworthy audit logs of past endpoint states.