RATS Reference Interaction Models for

Challenge-Response/Time-Based/Streamed Remote Attestation

Henk Birkholz {henk.birkholz@sit.fraunhofer.de},
Michael Eckel {michael.eckel@sit.fraunhofer.de},
Liqun Chen {liqun.chen@surrey.ac.uk},
Christopher Newton {cn0016@surrey.ac.uk},

IETF 109, 1st Virtual Session, November 17th 2020, RATS WG

Interaction Models

- Challenge-Response Remote Attestation
  - In general, initiated „by the Verifier“ using a nonce
  - BCP 205 Implemation Status https://github.com/Fraunhofer-SIT/charra
  - **NEW** Code for the Verifier role: https://github.com/veraison/
    - Continious tracking of progress and alginment with I-D
- Time-based Remote Attestation
  - In general, initiated „by the Attester“ using sync-tokens and timestamps
- Streamed Remote Attestation
  - In general, initiated „by the Verifier“ using a nonce, then maintained „by the Attester“ using sync-tokens and timestamps („hybrid“ CHARRA & TUDA)

Recent Activities (recap)

- Adopted shortly after IETF 108
- Recently updated
- Better alignment with the wording used in the RATS architecture I-D
  - Examples: ~~creation~~ -> generation of Evidence
  - Split of the Conceptual Messages "Reference Values"
  - Highlighted the intrinsic relationship to Layered Attestation

Current Activities

- Request for Review on the list
  - Review required on Section 6. Normative Prerequisites
    - This section intends to highlight only the most essential prerequisites
    - Primarily focused on the Attester
    - Is content and scope appropriate?
  - Review required on Section 7. Generic Information Elements
    - This section intends to highlight only the most essential Information Element required for implementing protocols based on the interaction models
    - Focused on Attester and Verifier as creators of protocol messages
    - This sections exceeds the scope of Claims included in Conceptual Messages
    - Is content and scope appropriate?