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 108, 1st Virtual Session, July 28th, 2020, RATS WG
Three RATS Interaction Models

- **Challenge-Response Remote Attestation**
  - In general, initiated „by the Verifier“ using a nonce
  - Referenced by:
    - **BCP 205 implementation** https://github.com/Fraunhofer-SIT/charra

- **Time-based Remote Attestation**
  - In general, initiated „by the Attester“ using sync-tokens and timestamps
  - Referenced by:

- **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)
  - Referenced by:
Direct Anonymous Attestation (DAA)

• Welcome Liqun and Chris! (from Surrey University)
• A few details on the mapping of DAA to the interaction models: (a comprehensive description of DAA can be found at [1])
  • DAA enables the generation of anonymized Evidence by a group of Attesters.
  • Adds a new capability to the Endorser role: DAA Issuer
• In essence:
  • An Authentication Secret associated with a single Attester is replaced by Authentication Secrets used for a group of Attesters.
  • Attesters are associated ("joined") in a group of Attesters that share the same characteristics.
• Appraisal of evidence requires the DAA Issuer certificate and the "randomized" credential from the Attester.

Where Do Interaction Models Go?

- Inquiry to the list: https://mailarchive.ietf.org/arch/msg/rats/tVi1UTacN_X_2qSg9NSQQmSAhSs
- The open question is: where should this content about interaction model go?

**Option 1**: standalone (one I-D for each model)

**Option 2**: standalone (one I-D for all models)

**Option 3**: all three models merged into the architecture I-D

**Option 4**: each model merged into a separate solution I-D