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, Virtual Interim, October 23\textsuperscript{rd} 2020, RATS WG
Interaction Models

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

• 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)
Direct Anonymous Attestation (DAA)

• DAA enables anonymizable creation of Evidence for a class of Attesters
• Adds a new capability to the Endorser role: DAA Issuer
  • In a nutshell, an Authentication Secret associated with a single Attester is replaced by Authentication Secrets used for a group of Attesters. Then associated ("joined") with set of multiple roots of trust that share the same characteristics.
  • Appraisal of evidence requires the DAA Issuer certificate and the "randomized" credential from the Attester
• A "group signature" scheme
Current Status of the Document

• Recently adopted
• Quite recently updated
• Better alignment to wording used in the RATS architecture I-D
  • Examples: creation -> generation of Evidence
  • Use of the Conceptual Message Reference Values
  • Highlighted the strong relationship to Layered Attestation
• Referenced by four RATS documents
Next Steps

• 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?