RATS Architecture & Terminology

Henk Birkholz {henk.birkholz@sit.fraunhofer.de}
Ned Smith {ned.smith@intel.com}

IETF RATS WG Virtual Interim, October 8th

Major Refactoring

- New **architectural constituents**, e.g...
  - RATS Roles & Principals, and
  - Roles Messages
- ...help to avoid specification text about **RoT & TA**,
- and **disambiguate** terms that are as **simple** as “attestation” or “to attest”.

- Attester Role now includes:
  - **Attesting** Computational Environment
  - **Attested** Computational Environment
- Next to their RATS Duties, these two contexts are specified to be “**separate**” and no more detail is provided, intentionally.

Simplification of Terms

- Terminology was **boiled down** to **four roles** and **five message** types.
  - Is more simplification possible? E.g.: Currently, use case semantics sometimes only differ due to the **composition of RATS Roles**, already.
  - The current Role & Message **definitions map** appropriately to TEEP, FIDO & TCG subsets of RATS, as well as to solutions, such as EAT, OPv2 (that may become TEEPv1), the RIV use case, CHARRA, and the YANG realm.
  - RATS terms are already adopted in other SDO and vendor solutions, while the architecture I-D is still in some churn – the current improvements look very promising.
- **Next steps** to improve readability are a **restructuring** early parts of the I-D (learning curve) and the **continuation of convergence with use cases** (some of which are still a bit abstract).

Structure / Sequence of Content

- To improve readability and comprehensibility, there are two major action items:
  - “All **terms go up**”, including a concise definition of various roles and messages that today appear too late in the text will also be in the **Terminology section**.
  - “Clarifying exemplary **diagram(s) go(es) up**” to complement the to be up-leveled Terminology section, creating a better intuitive understanding **how terms are related**.

STD or Informational

- Most recent discussions focused on how this document is **intended to be referenced** in the future.
- While the architecture **is** (and will be a tad bit more) **prescriptive** wrt to what solutions that specify RATS Principals or Roles have to adhere to,
- That **does not mean it has to be standards track**, though, as it seems today.
  - This has to be confirmed by AD, most likely. Roman? :-)

- In essence, the architecture I-D is intended to specify things, such as:
  - “A RATS Attester Role MUST be able to create attestation Evidence”
  - “Attestation Evidence MUST have [insert here] qualities.”
- This is as far as the “perscriptiveness” of the architecture I-D should ever go.
- Thoughts? Is that an appropriate scope?

RATS Interaction Model(s)

Henk Birkholz {henk.birkholz@sit.fraunhofer.de}
Michael Eckel {michael.eckel@fraunhofer.de}

IETF RATS WG Virtual Interim, October 8th

Terms & Implementation

- The current version of the Interaction Model I-D is now **better aligned** with the Architecture Terminology (but still needs work).

- There is now **running code** – using CoAP, CBOR and CDDL.
  - https://github.com/Fraunhofer-SIT/charra
  - BSD 3-Clause "New" or "Revised" License
  - Out-of-the-box development/testing environment (docker)

More Than One Model

- Up to today, the focus was on the **often used**, but **difficult to reference** challenge/response interaction between the Attester Role and the Verifier Role.
- More Interaction Models are now in the queue:
  - Direct Anonymous Attestation (**DAA**)
    - Different attestation provenance
  - **DICE**-based Attestation
    - Different semantics of keys and certificates
  - Time/Clock-Based Attestation (**TUDA**)
    - No nonce required, but trustworthy time synchronization and/or a TSA

RATS YANG Module

Henk Birkholz {henk.birkholz@sit.fraunhofer.de}
(presenting as editor)

IETF RATS WG Virtual Interim, October 8th

Status Update

- There were two reviews, which is great – but one or two more are better!
- Parallel prototyping efforts in production environments have started.
- Introduction & Background text is in the queue and should be done until the next IETF meeting.
- Composite Device definitions (such as IEEE 802.1AR aggregate device) are almost finished.
  - Is there a benefit to introduce the concept of composite device (for RATS Principals taking on the Attester Role) in the Architecture I-D?