RATS Architecture

https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/

Henk Birkholz {henk.birkholz@sit.fraunhofer.de},
Dave Thaler {dthaler@microsoft.com},
Michael Richardson {mcr+ietf@sandelman.ca},
Ned Smith {ned.smith@intel.com},
Wei Pan {william.panwei@huawei.com},

IETF 108, 2nd Virtual Session, July 29th 2020, RATS WG

Who & When

- Henk Birkholz(*)
- Thomas Fossati
- Andrew Guinn
- Thomas Hardjono
- Sarah C. Helble
- Eliot Lear
- Peter Loscocco
- Laurence Lundblade
- Nicolae PALADI
- Wei (William) Pan(*)
- Michael Richardson(*)
- Paul Rowe
- Ned Smith(*)
- Dave Thaler(*)
- Eric Voit
- Monty Wiseman
- Ling (Frank) Xia
- Giri Mandyam

Tuesdays 10am EST
(+ a few Fridays/adhoc)

24 meetings
since IETF106

Issues: 10 open
39 closed

Pull requests: 4 open
78 closed

Open Issues and Pull-Requests

- #111 Appendix A: Time Consideration regression
  https://github.com/ietf-rats-wg/architecture/issues/111
- #101 Confusing phrasing in the ML use case description
  https://github.com/ietf-rats-wg/architecture/issues/101
- #82 Security Considerations for Implicit Trust Model
  https://github.com/ietf-rats-wg/architecture/issues/83
- #72 What are “role compositions”?
  https://github.com/ietf-rats-wg/architecture/issues/73
- #71 Section 4.2 and 4.3 should use similar conventions for section names and figures
  https://github.com/ietf-rats-wg/architecture/issues/71
- #67 Class of claims for messages that “transit” entities involved in Role interactions
  https://github.com/ietf-rats-wg/architecture/issues/67
- #66 Have preferred serialization formats
  https://github.com/ietf-rats-wg/architecture/issues/66
- #65 More thorough definition of Endorser or Endorsement
  https://github.com/ietf-rats-wg/architecture/issues/65
- #57 Trust Model Section, Evidence consumed by an Endorser
  https://github.com/ietf-rats-wg/architecture/issues/57
- #54 Attestation Results description too limited
  https://github.com/ietf-rats-wg/architecture/issues/54
- #131 attempt to use structured yaml to acknowledge contributors
  https://github.com/ietf-rats-wg/architecture/pull/131
- #130 Revise Privacy Considerations
  https://github.com/ietf-rats-wg/architecture/pull/130
- #123 time sequences diagram changes (was issue #111)
  https://github.com/ietf-rats-wg/architecture/pull/123
- #94 More description of Endorsements
  https://github.com/ietf-rats-wg/architecture/pull/94

Summary of Changes since IETF 107

- Discussed comments from Hannes about **intrinsic complexity** → there is a little bit more to it
- Discussed and addressed **comments from Kathleen** → a few did not resulted in changes to the text, but most of them did
- Overall polish of **defined terms** → Endorsement is still under scrutiny
- Polish to **use cases** based on feedback and discussion
- Improved structure of the **Trust Model**, addressing each defined role individually now
- Significant improvement of the **Freshness** section
- Ongoing improvement of the **Privacy Consideration** section
- Ongoing improvement of the **Time Considerations** appendix

Two prominent current topics (part1)

- **Endorsement & Endorser**
  - What about Key Provisioning?
  - Should the scope of Endorsements be extended or are there more than one Conceptional Message types conveyed from the Endorser to the Verifier?
  - In the planned 2nd phase of the RATS charter Conceptual Messages can also be conveyed from the Endorser to the Attester (as provisioning a step).

Two prominent current topics (part2)

- **Time-Keeping based on nonces** (with or without clocks involved)
  - Is the current scope highlighting the purposes of nonces sufficient?
  - What is the impact of correct use of nonces as illustrated on the security of resulting solutions?
  - Is it okay to infer the use of nonces from the existing examples or might that lead to misconceptions?

RATS Trustworthiness Vectors

for the SUIT Workflow Model

https://datatracker.ietf.org/doc/draft-birkholz-rats-suit-claims/

Henk Birkholz {henk.birkholz@sit.fraunhofer.de},
Brendan Moran {brendan.moran@arm.com},

IETF 108, 2nd Virtual Session, July 29th 2020, RATS WG

Rodents in Formal Wear

- A **RATS Attester** processing a **SUIT Manifest** can change its security characteristics during an ongoing update or after a successful update procedure.
- A SUIT Manifest and the corresponding **SUIT Workflow Model** can be used as a **remediation** procedure.
  - If a RATS Attester's **Evidence shows non-compliance** for its firmware, a SUIT Workflow can be triggered to **update** the relevant components of the **composite Attester**.
- RATS already supports Evidence for **before and after** the update.
- The recently defined **SUIT Report** now enables the appraisal of resulting **SUIT Records** generated during a **SUIT Update Procedure**.

Trustworthiness Levels

- The Claims defined include SUIT-specific assertions about the hardware components and software components as referred to in a SUIT Manifest (**System Property Claims**).
  - Some of these Claims are **specializations or generalizations** of the Claims defined in **EAT**.
  - A semantic mapping with the EAT I-D could be a next step.
    - The Claims about the outcomes of **Update Procedures** and **Boot Procedures** are based on the records in a **SUIT Report** (**Interpreter Record Claims**).
  - Every record is associated with a **pass or fail** result (**Record Success Claim**).
  - This representation is based on the **Trustworthiness Levels** defined in the RATS Trusted Path Routing I-D.

Trustworthiness Vectors

- Every **Record Success Claim** associated with other **Interpreter Record Claims** generated during an **SUIT Update Procedure** represents a single **Trustworthiness Level**.
- All acquirable **Trustworthy Levels** (pass or fail for each command) concatenated in a sequence represent a **Trustworthiness Vector** based on a **SUIT Command Sequence**.
- Trustworthiness Vectors can be **conveyed as Evidence**.
- Application-specific **subsets** of the Trustworthiness Vectors can be refined by the **appraisal** of a Verifier.
- Trustworthiness Vectors specific to a **Relying Party** can be **conveyed as Attestation Results** that are far more fine grained than "binary trust decisions".

RATS UCCS

Unprotected CWT Claims Sets ("Unendorsed Tokens")

https://datatracker.ietf.org/doc/draft-birkholz-rats-uccs/

Henk Birkholz {henk.birkholz@sit.fraunhofer.de},
Nancy Cam-Winget {ncamwing@cisco.com},
Carsten Bormann {cabo@tzi.de},
Jeremy O'Donoghue {jodonogh@qti.qualcomm.com},

IETF 108, 2nd Virtual Session, July 29th 2020, RATS WG

A Secure Channel „As Good As“ a Signature – an Example

- An **exemplary requirement** (instead of a recap is the secure conveyance of **unsigned Evidence.**
- In this example the Evidence is framed in an UCCS and a **substitute** for the COSE envelope **is required**.
- Simply describing what the **UCCS CBOR tag** does is not enough.
  - The use of the COSE envelope in this scenario had **semantics and security implications**.
  - These semantics and implications are **usage scenario specific**.
  - As a result, an UCCS **must not be specified standing alone**, but always in the scope of a usage scenario.
- The **initial usage scenario** the UCCS CBOR tag is specified in is **RATS**.
- Evidence in RATS must be authentic and tamper-proof (sometimes it must also be obfuscated)
- In RATS, the conveyance of an UCCS requires a **Secure Channel**
- Not only the **characteristics** of the Secure Channel but also **of the RATS roles** that establish the Secure Channel are important.
  - The **key material** used to create the Secure Channel must be **equally protected** as the key material that signs Evidence.
  - The **source** of a UCCS must be **authenticated** before a UCCS may be send in RATS.
  - The conveyance must support the **obfuscation of the content**, e.g., via encryption methods.

Summary of Changes since IETF 107

- Improved document structure including the required
  - **UCCS CBOR tag**,
  - **RATS usage scenario**, and the required
  - **Characteristics of the Secure Channel**.
- Aligned the text with requirements coming from "Unendorsed Tokens" as defined by **Global Platform**.
- A section on **Privacy Preserving** Channels was added.
- Most importantly, a RATS-specific **Security Consideration** was added.