RATS WG
Report on Adopted I-Ds

Henk Birkholz <henk.birkholz@sit.fraunhofer.de>

IETF 113

22 March 2022

Vienna

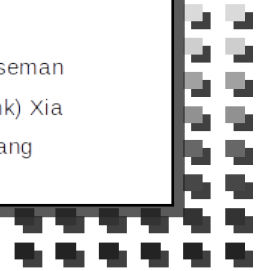# RATS Architecture (I)

https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/
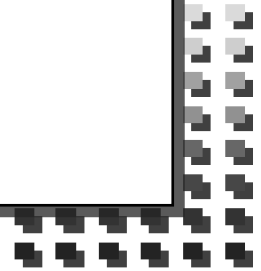
- When: Tuesdays 10am EST
  (+ a few Fridays/adhoc)
- Issues: 185 total (none remaining)
- Pull requests: 216 total (one remaining)
- No edits until the start of the next
  review phase

WHO:
- Henk Birholz(*)
- Thomas Fossati
- Yogesh Deshpande
- Andrew Guinn
- Thomas Hardjono
- Sarah C. Helble
- Xinxin Fan IoTeX
- Eliot Lear
- Peter Loscocco
- Laurence Lundblade
- Nicolae Paladi
- Wei (William) Pan(*)
- Michael Richardson(*)
- Paul Rowe
- Ned Smith(*)
- Dave Thaler(*)
- Akura Tsukamoto
- Eric Voit
- Monty Wiseman
- Ling (Frank) Xia
- Penglin Yang

I E T F

RATS Architecture (II)

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

- Latest Diff: https://www.ietf.org/rfcdiff?url1=draft-ietf-rats-architecture-12&url2=draft-ietf-rats-architecture-15

- 3.1 Added: Two Types of Environments of an Attester

- References added: DAA, PSA-Token, NIST-800-57p1, RFC8086, TCG-DICE-SIBDA

- Already had AD review, state is "Submitted to IESG for Publication"

- **What is happening next?**

I E T F

RATS Reference Interaction Models
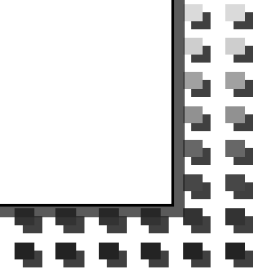
https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/

- 7.1.1. Added: Models and example sequences of Challenge/Response Remote Attestation

  - Background Check & Passport model basedon emerging requirements coming from C2PA (LF project: Coalition of Content Provenance and Authenticity)

- Anything else then consistency polish, diagram maintenance and... **is now the time to ask for dedicated area and dir review?**

I E T F
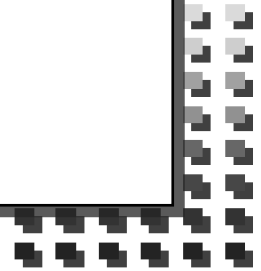
RATS Unprotected CWT Claims Sets
https://datatracker.ietf.org/doc/draft-ietf-rats-uccs/

- Addressed early review comments from Thomas Fossati

- Recap: while UCCS is for all CWT an UCCS document must never be shipped with an application specific Security Consideration – RATS is the initial context

  - Follow-up I-Ds can reuse the core definitions of this document and introduce their own specific Sec-Con.

- Added a proposal that combines the CDDL .feature control with a generic type definition to allow for a choice between JSON & CBOR – potentially allowing for UJCS.

I E T F

RATS Direct Anonymous Attestation
https://datatracker.ietf.org/doc/draft-ietf-rats-daa/

- In the middle of multiple open issues
- Next steps:
    - Relate DAA Issuer flows to RATS Endorsements
    - Introduce the related TCG concept of "Privacy CA"
    - Explore relationships to TCG DICE and maybe add corresponding sections
    - Address issues of undermining anonymity by injecting re-identifiable information via CHARRA interaction models

I E T F