On the Different Kinds of Rodents in the IETF Ecosystem
Gathering at the RATS Bar BoF
July 2018

TIME & PLACE:

Thursday, July 19th
7pm (after Afternoon Session III)
Room: Square Dorchester
On Remote Attestation (RA)

- **Remote** Attestation is providing cryptographic evidence (proof) that a
  system entity is a trusted and trustworthy system (RFC4949) to other
  entities via an interconnect.

- A set of basic, related activity definitions:
  - Attestation: An object integrity authentication facilitated via the creation of a
    claim about the properties of an Attestor, such that the claim can be used as
evidence
  - Conveyance: The transfer of evidence from the Attestor to the Verifier via an
    Interconnect.
  - Verification: The appraisal of evidence by evaluating it against declarative
    guidance
  - Remote Attestation: A procedure composed of the activities attestation,
    conveyance and verification

- Though we are starting to think about a better, more accurate and less
  (ab)used term
  - Related with a measurement of system health and trustworthiness
A General Model for Remote Attestation

[Attestor]

| ←----------------- Nonce, Shared Secret ID, [Additional Info] |
| Collect Integrity Claims |
| Sign Claim Set (Evidence) |
| Evidence, Identity, Nonce, Signature ------------------------> |

[Verifier]

Appraise Evidence
Here We Stand

• IETF Reference Terminology for Remote Attestation Procedures (RATS)

• Current Topics that are work in progress:
  – Different flavors of Root of Trust
  – Procedures to proof freshness
  – How to include terms as Claim and Claimant that will be in sync with Concise Identities
  – Binding of differentiations wrt to Principal/Issuer, and "Possessor“
  – More flexible binding of Roles and Actions/Activities

• Platforms for discussing and progressing general RA matters
  – https://www.ietf.org/mailman/listinfo/rats
  – https://github.com/ietf-rats

• We believe this is a relevant matter for IETF

• If you are interested, join us on Thu 19th 7:15pm in Square Dorchester