

On the Different Kinds of Rodents in the IETF Ecosystem

Gathering at the RATS Bar BoF

July 2018

TIME & PLACE:

Thursday, July 19th

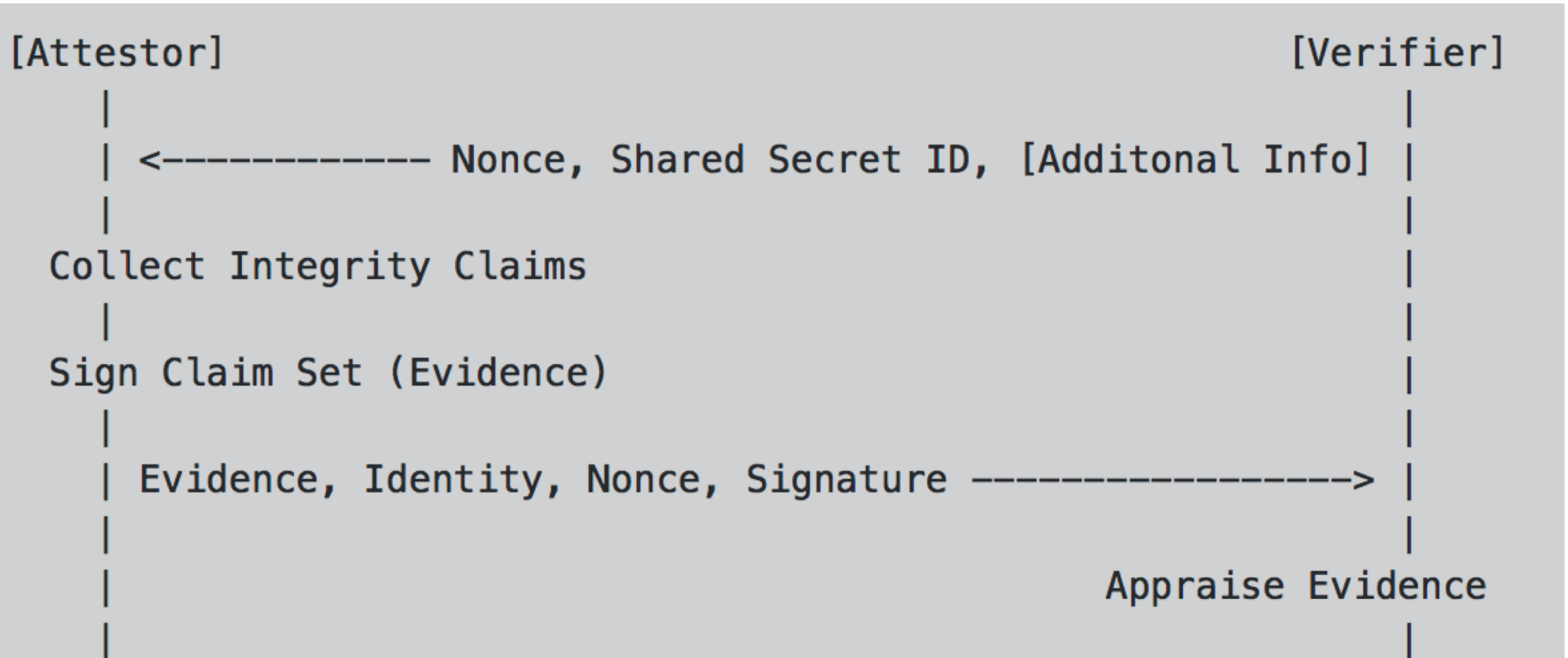
7pm (after Afternoon Session III)

Room: **Square Dorchester**

On Remote Attestation (RA)

- RA 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.
 - 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



Here We Stand

- Several drafts
 - draft-pastor-i2nsf-nsf-remote-attestation
 - draft-birkholz-i2nsf-tuda
 - draft-mandyam-eat
 - draft-mandyam-tokbind-attest
 - draft-birkholz-reference-ra-interaction-model
 - draft-birkholz-yang-basic-remote-attestation
 - draft-birkholz-attestation-terminology
 - draft-rein-remote-attestation-nfv-use-cases
- 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