Attestation Event Stream Subscription
draft-birkholz-rats-network-device-subscription-00

Henk Birkholz henk.birkholz@sit.fraunhofer.de

Eric Voit evoit@cisco.com

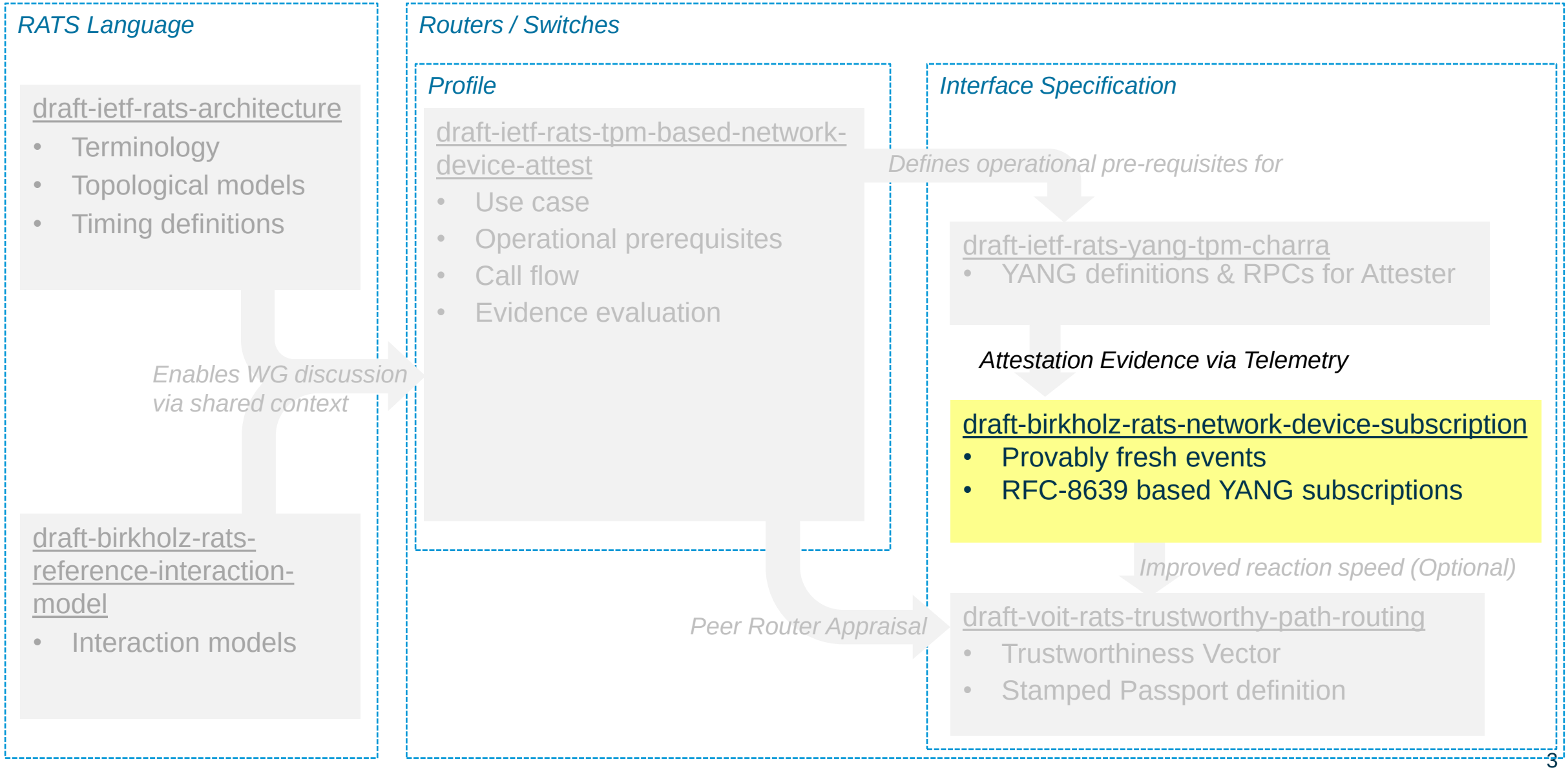
Wei Pan william.panwei@huawei.com

IETF 108, July 28th & 29th 2020, RATS WG

Purpose & Origin

- Defines how to subscribe to a stream of attestation related Evidence on TPM-based network devices.
  - When subscribed, a Telemetry stream of verifiably fresh YANG notifications are pushed to the subscriber.
  - Notifications are generated when TPM PCRs are extended
- This draft integrates:
  - Section 5 of draft-voit-rats-trusted-path-routing-01
  - draft-xia-rats-pubsub-model

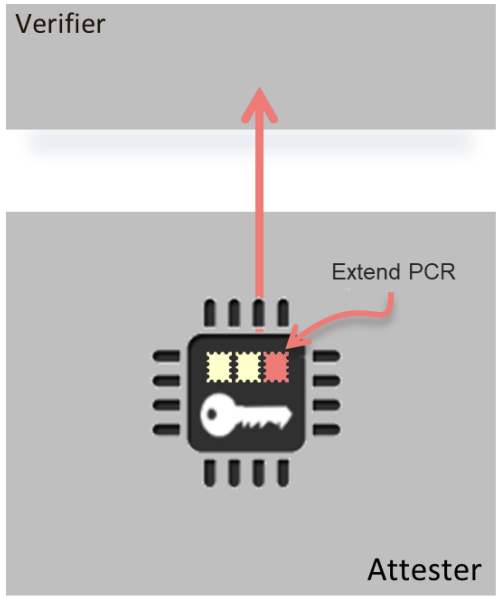
Relationship to other RATS drafts



TPM PCR Evidence as Telemetry

draft-ietf-rats-yang-tpm-charra

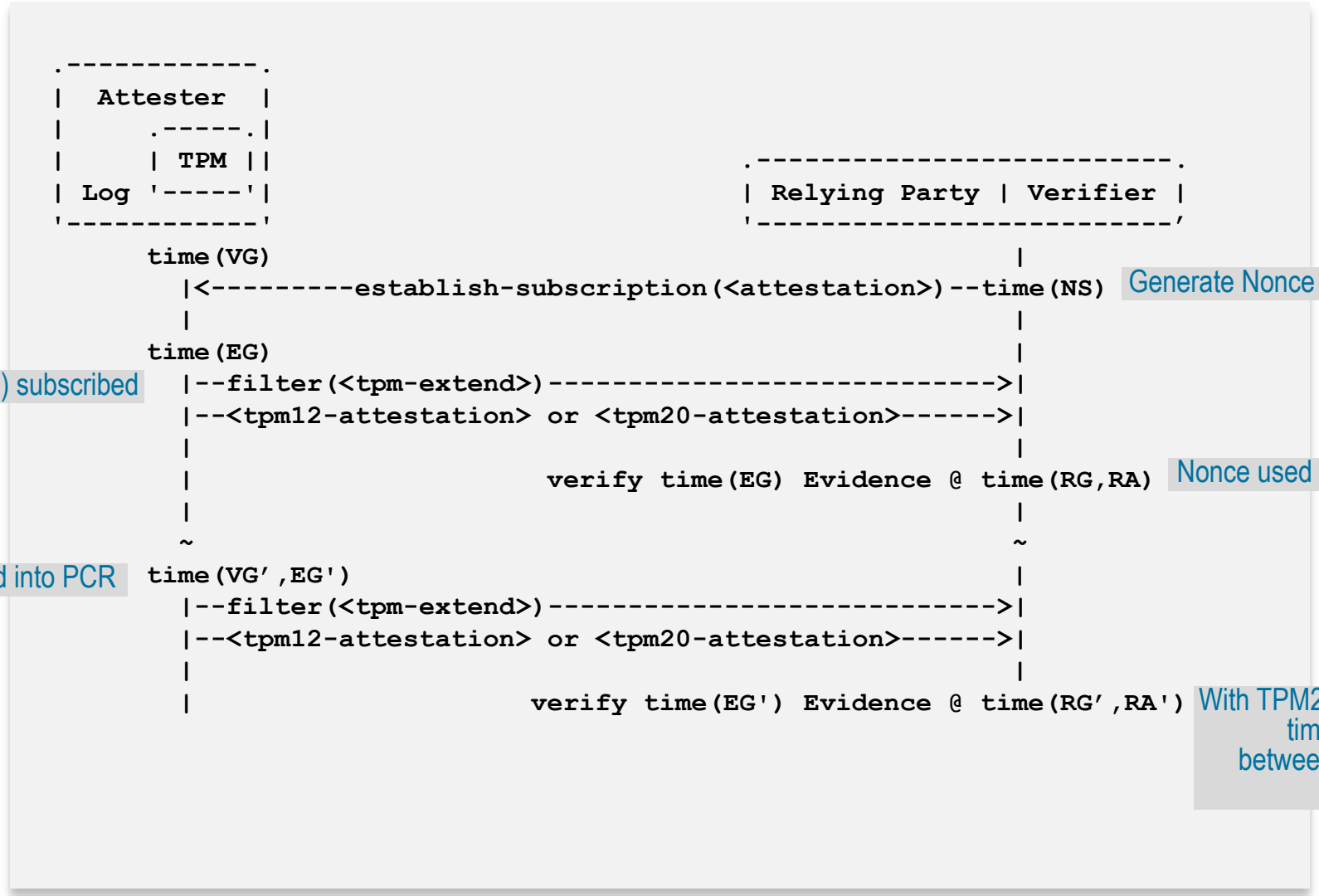
- Periodic polling
- Reboot loses info/state



draft-birkholz-rats-network-device-subscription

- Events & PCR changes streamed as they happen
- Subscription established right at Boot checks:
  - Hardware integrity
  - Unique identity
  - Boot integrity
  - Filesystem integrity
- Telemetry streaming after Boot checks:
  - New software installed
  - Suspect log message detected
  - Privilege level escalation
  - Etc...

Fresh Security Telemetry



<attestation> Event Stream

- Fresh, streaming Evidence
  - Based on draft-ietf-rats-yang-tpm-charra & YANG subscriptions (RFC-8639)
- YANG Notifications
  - <tpm12-attestation>
  - <tpm20-attestation>

  } Objects defined in draft-ietf-rats-yang-tpm-charra

  - <tpm-extend>

  } Measurements which have extended a PCR
- <replay> of all Notifications since boot
- Verifier can subscribe to PCRs / Notifications of interest via XPATH
- Extensible with other Notifications

ietf-tpm-remote-attestation-stream.yang

```
      +--rw rats-support-structures
         +--rw rats-support-structures
          +--rw supported-algos*
          +--rw tpms* [tpm-name]
          |  +--rw tpm-name
          |  +--rw leafref-to-keystore?
          |  +--rw (subscribable)?
          |     +--:(tpm12-stream) {tpm:TPM12}?
          |     |  +--rw tras:tpm12-pcr-index*
          |     +--:(tpm20-stream) {tpm:TPM20}?
          |        +--rw tras:tpm20-pcr-index*
          +--rw marshalling-period?
          +--rw tpm12-subscribed-signature-scheme?
          +--rw tpm20-subscribed-signature-scheme?
 +--rw tpm20-subscription-heartbeat?
```

Charra

This draft

Attestation Key to be used

PCRs allowed to be subscribed

Maximum delay to bundle evidence

Algorithm for signed results

Keepalive PCR state

Next

- Interest?
- Your suggestions to the mailing list.
- Potential for adoption call @ IETF 109?