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

Henk Birkholz {henk.birkholz@sit.fraunhofer.de},
Eric Voit {evoit@cisco.com},
Wei Pan {william.panwei@huawei.com}

November 2021, RATS WG
Relationship to other RATS drafts

**RATS Language**
- draft-ietf-rats-architecture
  - Terminology
  - Topological models
  - Timing definitions

**Profile**
- draft-ietf-rats-tpm-based-network-device-attest
  - Use case
  - Operational prerequisites
  - Call flow
  - Evidence evaluation

**Interface Specification**
- draft-ietf-rats-yang-tpm-charra
  - YANG definitions & RPCs for Attester
  - TCG Algorithm registry

**Attestation Evidence via Telemetry**
- draft-ietf-rats-network-device-subscription
  - Provably fresh events
  - RFC-8639 based YANG subscriptions

**Enables WG discussion via shared context**
- draft-ietf-rats-reference-interaction-models
  - Interaction models

**Routers / Switches**

- **Use case**
- **Operational prerequisites**
- **Call flow**
- **Evidence evaluation**

**Just Adopted**

**In progress**

**WGLC Complete**
Purpose & Scope

- 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 for the Evidence going into TPM PCRs, and when the PCRs are extended.

- Result
  - Verifier is pushed new verifiably fresh Evidence whenever PCRs change.
Contents

1. Introduction ................................................................. 3
2. Terminology ................................................................. 5
3. Operational Model ........................................................ 5
   3.1. Sequence Diagram .................................................. 5
   3.2. Continuously Verifying Freshness ............................... 7
4. Remote Attestation Event Stream ...................................... 9
   4.1. Subscription to the <attestation> Event Stream .............. 9
   4.2. Replaying a history of previous TPM extend operations ... 10
       4.2.1. TPM2 Heartbeat .............................................. 11
   4.3. YANG notifications placed on the <attestation> Stream ... 11
   4.4. Filtering Evidence at the Attester ............................. 14
   4.5. Replaying previous PCR Extend events ....................... 14
   4.6. Configuring the <attestation> Event Stream ................. 14
5. YANG Module ............................................................... 15
9. References ..................................................................... 22