TPM-based Network Device Remote Integrity Verification

draft-fedorkow-rats-network-device-attestation-05

RATS Virtual
28 April 2020

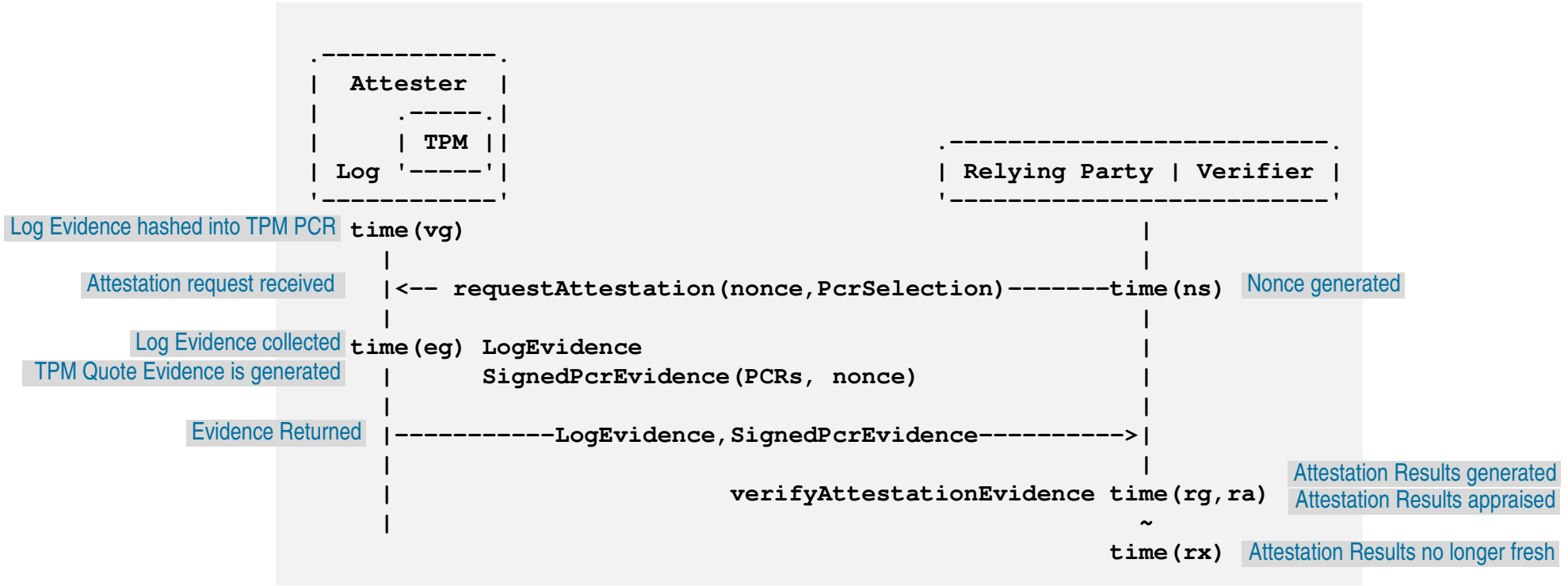
Guy Fedorkow - gfedorkow@juniper.net
Eric Voit - evoit@cisco.com
Jessica Fitzgerald-McKay - jmfitz2@nsa.gov

V3b

Objective

- Standardize operational model for today's existing but proprietary TPM-based router/switch Remote Attestation solutions.
  - Enables switches/routers to be appraised by non-proprietary controllers/Verifiers.
  - Gives Network Operators needed stability for interfacing operational systems.

Nonce based Background Check Model



New in Draft -05

- Focus on Operational Prerequisites for the RIV Use Case
- Alignment with RATS-Arch, addition of timing points
- Removal of some TCG-centric material to Appendices
- Addition of "What Evidence does RIV Appraise?"
- Addition of Peer-to-Peer to coordinate with draft-voit-rats-trusted-path-routing

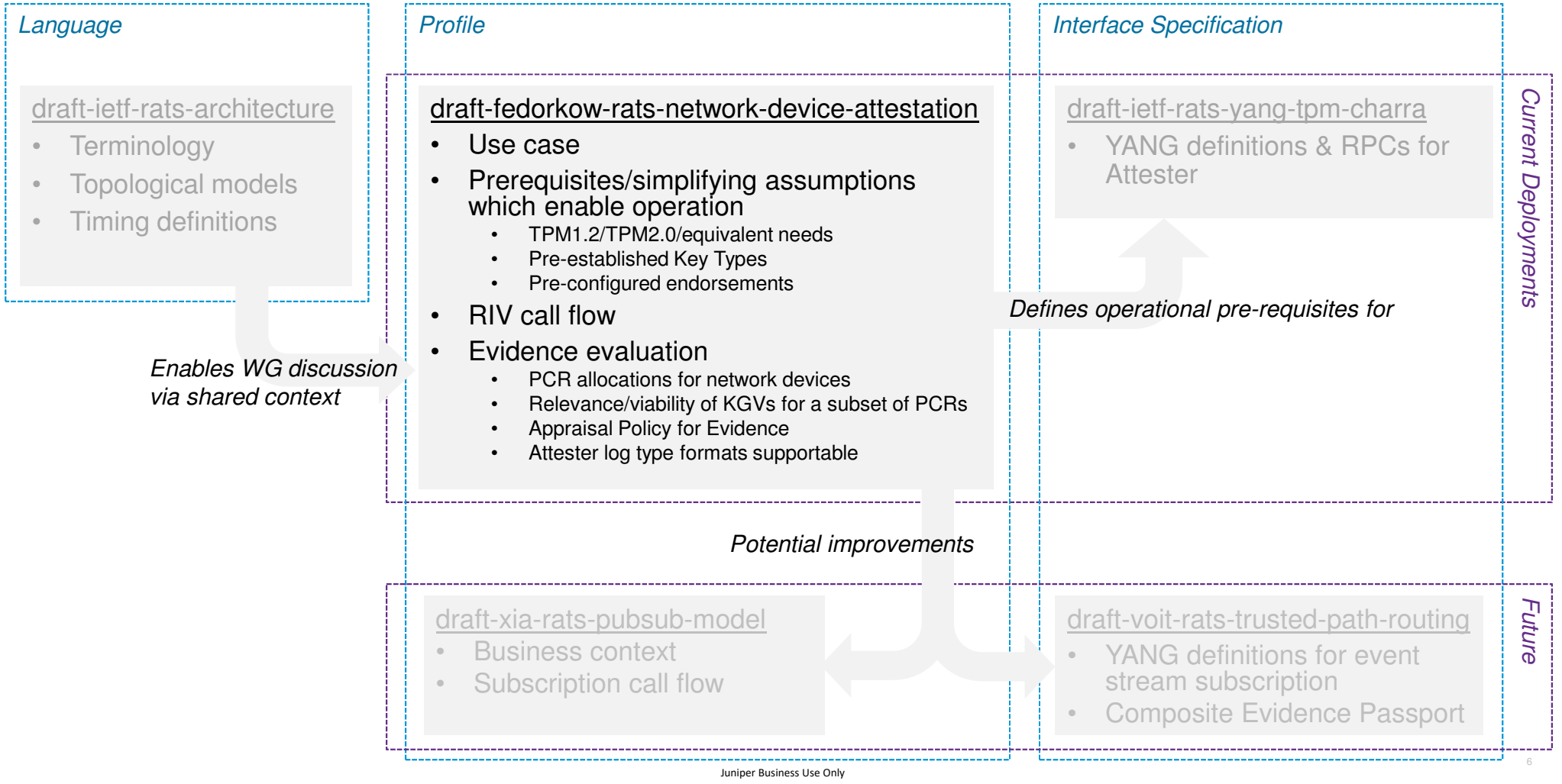
What Evidence does RIV Appraise?

Section 2.1.1 outlines what we expect to attest with RIV, including:

- Code
  - Firmware, OS loader, OS kernel and applications
- Credentials
  - Keys used to authorize operation of routers, e.g. code-signing public keys or network-access private keys (e.g. VPN keys)
- Configuration
  - Security-sensitive configuration files

RIV is intended to secure the infrastructure, so that subsequent higher-level claims can be trusted.

Relationship to other WG drafts



Assuming WG agrees such documentation is needed:

- Where should the WG document current TPM-based router/switch Remote Attestation operational prerequisites?

Option 1
Separate use case context + profile draft

Pro	Con
• Simplifies reading for different types of document users	• Precedent of two WG documents per use case?

Preferred
- If WG agrees, recommend adopting this draft

Option 2
Integrate into draft-ietf-rats-yang-tpm-charra

Pro	Con
• Fewer adopted WG drafts	• Very large merged document • Elements of the YANG model may be obsoleted based on potential improvements • Less modularity

Viable
- If WG selects, recommend merging drafts