

A YANG Data Model for Challenge-Response-based Remote Attestation Procedures using TPMs

draft-ietf-rats-yang-tpm-charra-03

Henk Birkholz {henk.birkholz@sit.fraunhofer.de},

Michael Eckel {michael.eckel@sit.fraunhofer.de},

Shwetha Bhandari {shwetha.bhandari@thoughtspot.com},

Eric Voit {evoit@cisco.com},

Bill Sulzen {bsulzen@cisco.com},

Liang Xia (Frank) {frank.xialiang@huawei.com},

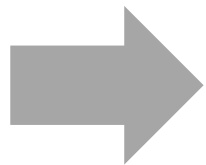
Tom Laffey {tom.laffey@hpe.com},

Guy C. Fedorkow {gfedorkow@juniper.de},

Nov 17th 2020, RATS WG

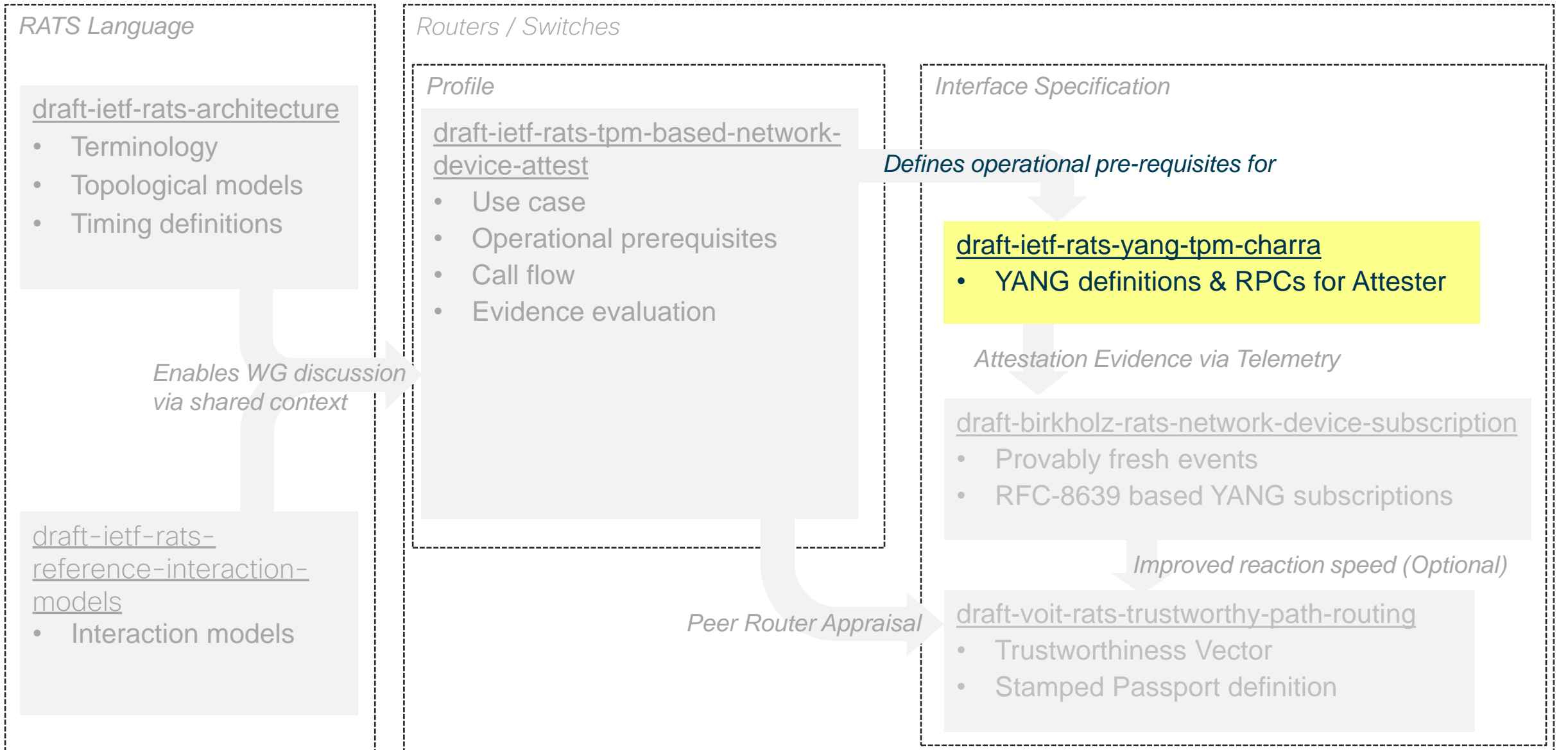
Purpose & Scope (recap)

- Context
 - A lot of **network equipment devices** use YANG-based management interfaces.
 - Adding Remote Attestation as procedures to **existing and implemented management interfaces** significantly reduces the threshold of adoption.
- Contribution
 - This YANG module defines **RPCs** and a concise **datastore** implementing the Challenge-Response Remote Attestation Interaction Model.



IETF YANG Doctor review, discussions underway

Relationship to other RATS drafts



Issues Addressed (review from interim)

Overall document:

1. Added text describing purpose and context of YANG model

Within YANG model:

2. Added ietf-tcg-algs.YANG, and created error checks around them.
3. Added support for netequip_boot logs
4. Significantly refined model to eliminate redundancies and sources of configuration error
5. Removed key establishment RPC
6. Descriptive text added throughout model
7. Inserted high level containers to align with YANG practices

Open Issues

Within YANG model:

- XPATH expressions to which perform configuration data integrity validation need review.
- Any (tbd) YANG Doctor comments to be addressed
- Maximize commonality between TPM1.2 & TPM2.0 RPCs
 - Expert review has been requested to ensure TPM1.2 Quotes are accurate

Closed: Include tpm-name and node-id in RPCs?

```
+-- rats-support-structures
+-- compute-nodes!
| +-- compute-node*
|   +-- node-id ←
+-- tpms
  +-- tpm* [tpm-name]
  +-- tpm-name
  +-- compute-node
  +-- certificates
    +-- certificate*
      +-- certificate-name
```

certificate-name is assumed unique on a multi linecard attester. It can indicate which TPM and which linecard (node-id)

No objections to this subsequent to our interim

Option 1: Minimize RPC complexity

```
+---x tpm20-challenge-response-attestation
+---w input
| +---w tpm20-attestation-challenge
|   +---w certificate-name*
+---ro output
  +---ro tpm20-attestation-response*
  +---ro certificate-name?
```

Option 2: Allow variations input and output parameters.

```
+---x tpm20-challenge-response-attestation
+---w input
| +---w tpm20-attestation-challenge
|   +---w tpm-name
|   +---w node-id
+---ro output
  +---ro tpm20-attestation-response*
  +---ro tpm-name
  +---ro node-id
  +---ro certificate-name?
```

Next

- Await YANG doctor comments
 - XPATH scrub
- Still need someone to validate TPM1.2 structures
- Then propose WGLC