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

draft-ietf-rats-yang-tpm-charra-02

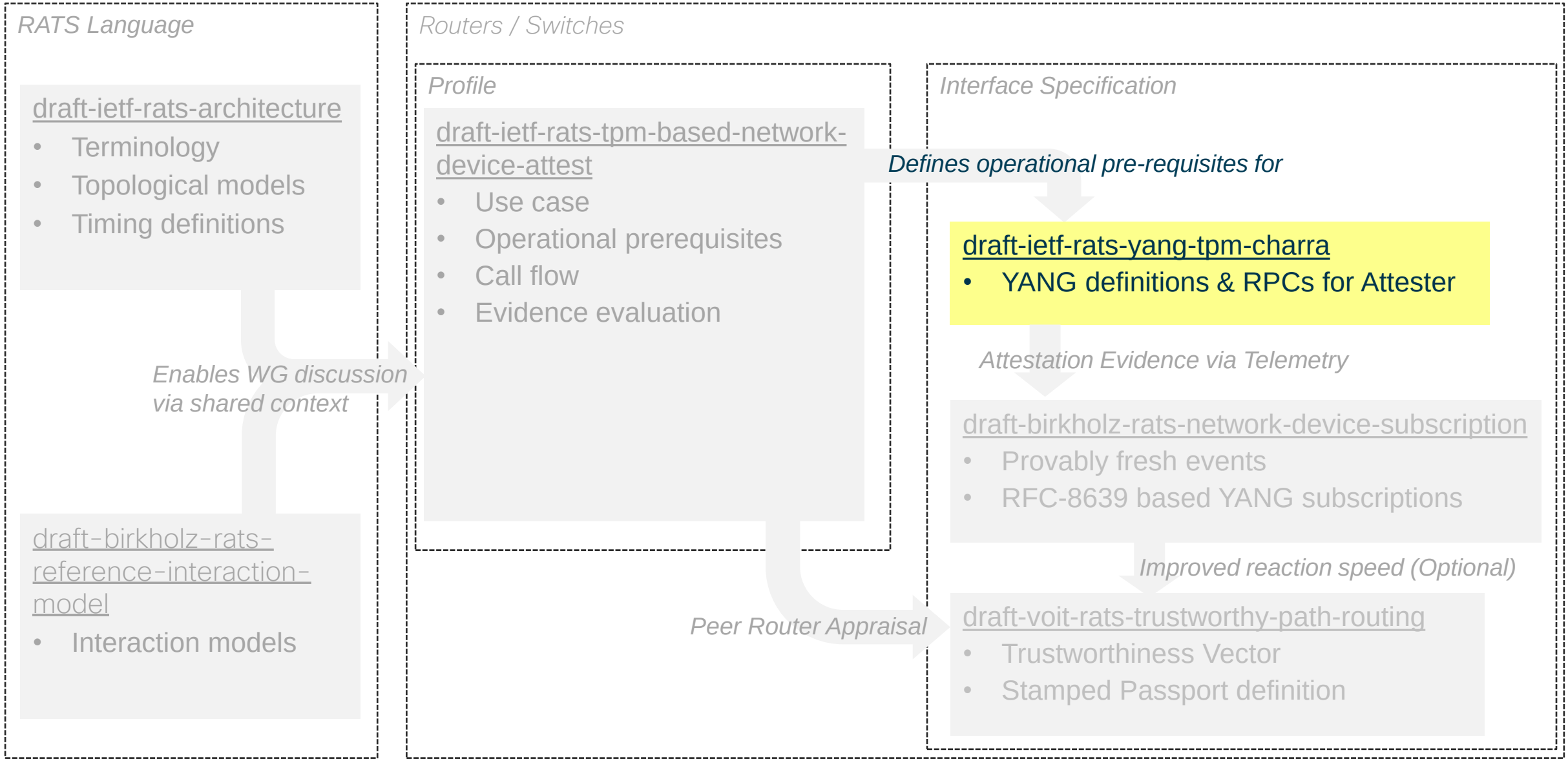
Henk Birkholz {henk.birkholz@sit.fraunhofer.de},
Michael Eckel {michael.eckel@sit.fraunhofer.de},
Shwetha Bhandari {shwethab@cisco.com},
Bill Sulzen {bsulzen@cisco.com},
Eric Voit {evoit@cisco.com},
Liang Xia (Frank) {frank.xialiang@huawei.com},
Tom Laffey {tom.laffey@hpe.com},
Guy C. Fedorkow {gfedorkow@juniper.de},

IETF 108, 1st Virtual Session, July 28th 2020, RATS WG

Purpose & Scope (recap)

- Context
  - A lot of **network equipment devices** use YANG-based management interfaces.
  - A lot of corresponding tool-chains & software **agents already exist**.
  - 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.
  - This YANG module supports multiple **Roots-of-Trusts** (TPMs) in **composite devices**.
  - This YANG module enables **trustworthy evidence telemetry**.

Relationship to other RATS drafts



Issues Addressed

1. PCR numbers have their own type (not a UINT8)
2. Identities instead of strings for TCG and IETF crypto algorithm types. Strings allow lots of errors to be introduced. (Question #1)
3. Removal of nested keys of [node id] [tpm name]. Add a Mandatory leafref back to node-id when compute-nodes is not null.
4. Eliminate TPM-Name of "ALL".
5. Added leaf for a unique TPM-Path.
6. Optional YANG features for TPM1.2 and TPM2.0 (RPCs won't be unnecessarily exposed.)
7. New grouping for log algorithm types. And other grouping tweaks.

Issues Addressed & a Couple Questions

8. 'Certificate-name' used as a TPM identifier for RPCs. This allows for a cleaner certificate migration path (and re-identification of a specific TPM).
9. Extracted into a group TPM2_ALG_ID
10. Separate out crypto-algorithm types into a separate YANG model (Question #1)
11. Removed choices for IETF algorithm types as the TPMs by definition need to follow TCG types. Mappings can still be made in Identities.
12. Leafrefs for certificate datastores should simplify the storage of this information should people not want to create separate structures.
13. vTPM support added
14. New log type for network devices boot? (Question #2)

ietf-tpm-remote-attestation.yang

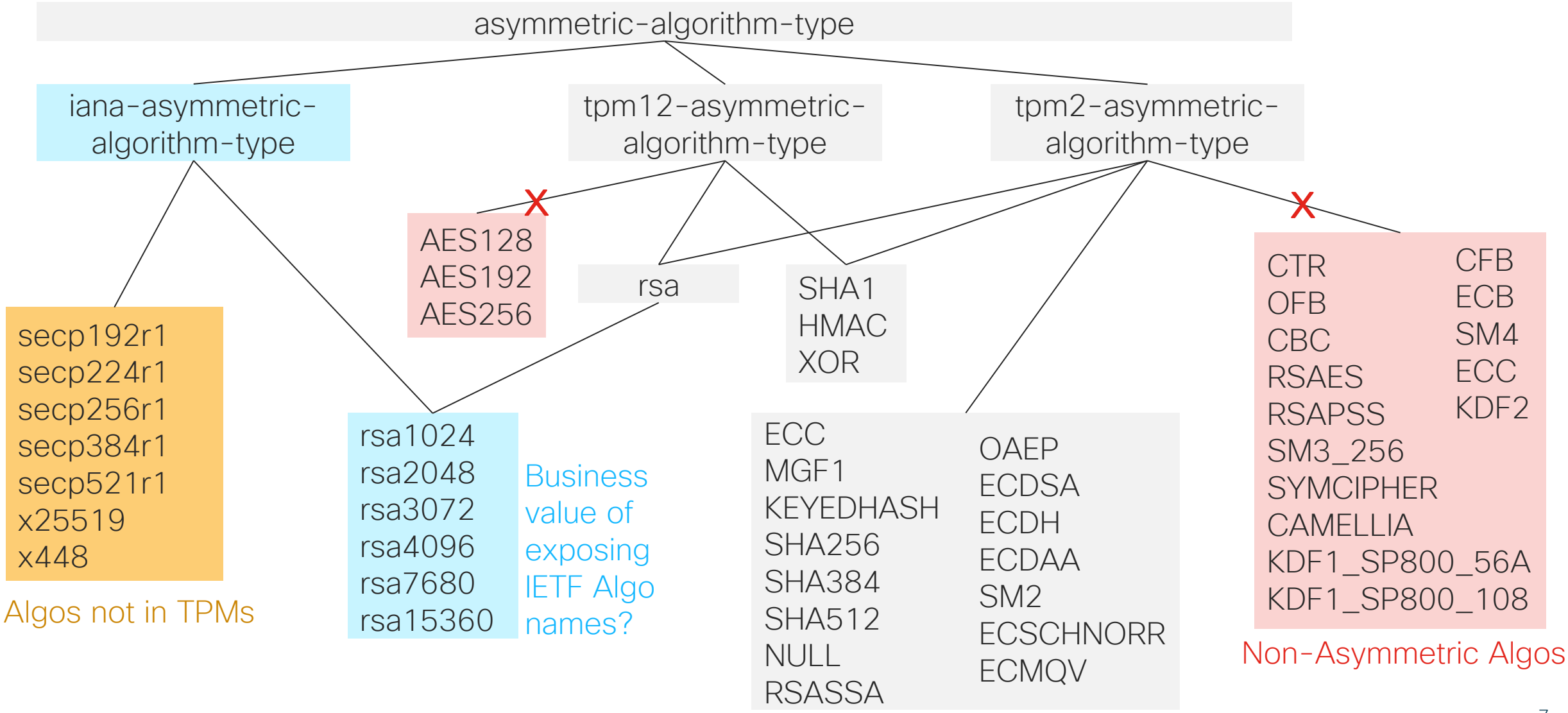
```
    +--rw rats-support-structures
       +--rw supported-algos*   identityref
       +--ro compute-nodes* [node-id]
       |  +--ro node-id                        string
       |  +--ro node-physical-index?           int32 {ietfhw:entity-mib}?
       |  +--ro node-name?                     string
       |  +--ro node-location?                 string
       +--rw tpms* [tpm-name]
          +--rw tpm-name                       string
          +--ro hardware-based?                boolean
          +--ro tpm-physical-index?            int32 {ietfhw:entity-mib}?
          +--ro tpm-path?                      string
          +--ro compute-node                   compute-node-ref
          +--ro tpm-manufacturer?              string
          +--ro tpm-firmware-version?          string
          +--ro tpm-specification-version      identityref
          +--ro tpm-status?                    string
          +--rw certificates
             +--rw certificate* [certificate-name]
                +--rw certificate-name         string
                +--rw certificate-ref?         leafref
                +--rw certificate-type?        enumeration
```

Only needed when multiple TPMs per device

A new certificate-name appearing in RPC response allows mapping to TPM here (easier key migration)

to ietf-keystore.yang

ietf-asymmetric-algs.yang
Question 1: Reduce YANG Identities just to those in Grey?



Question 2: New log type for network devices boot?

```
grouping netequip-boot-event {
  leaf event-number
  leaf filename-hint
  leaf filedata-hash
  leaf filedata-hash-algorithm
  leaf file-version
  leaf file-type
  leaf pcr-index
}
```

```
grouping network-equipment-boot-event-log {
  list boot-event-entry {
    key event-number;
    description
      "Boot-time event log, order by event-number.";
    uses netequip-boot-event;
  }
}
```

Next

- Close Questions
- Any other questions / concerns ?
- Submit for YANG Doctor Review