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

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

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

**Profile**

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

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

**Improved reaction speed (Optional)**
- **draft-voit-rats-trustworthy-path-routing**
  - Trustworthiness Vector
  - Stamped Passport definition

**Peer Router Appraisal**
- Enables WG discussion via shared context

**draft-birkholz-rats-reference-interaction-model**
- Interaction models

**Enables WG discussion via shared context**
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)
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
Question 1: Reduce YANG Identities just to those in Grey?

- asymmetric-algorithm-type
  - iana-asymmetric-algorithm-type
  - tpm12-asymmetric-algorithm-type
  - tpm2-asymmetric-algorithm-type

**Algos not in TPMs**
- secp192r1
- secp224r1
- secp256r1
- secp384r1
- secp521r1
- x25519
- x448

**RSA**
- rsa
- rsa1024
- rsa2048
- rsa3072
- rsa4096
- rsa7680
- rsa15360

**Business value of exposing IETF Algorithm names?**

**ECC**
- SHA256
- SHA384
- SHA512
- NULL

**RSA-PSS**
- RSASSA

**ECIES**
- OPAEP
- ECDSA
- ECDH
- ECDA
- SM2
- ECSCHNORR
- ECMQV

**Non-Asymmetric Algos**
- CTR
- OFB
- CBC
- RSAES
- EC
- RSAPSS
- KDF1
- SM3_256
- SYMCIPHER
- CAMELLIA
- KDF1_SP800_56A
- KDF1_SP800_108

**Key Derivation Functions**
- MGF1
- KEYEDHASH
- SHA256
- SHA384
- SHA512
- NULL
- RSA-PSS
- RSASSA

**Other**
- XOR
- ECC
- KDF2
- CFB
- ECB
- SM4
- SM3
- SM4
- ECC
- KDF1
- SP800_56A
- SP800_108
Question 2: New log type for network devices boot?

```plaintext
grouping netequip-boot-event {
    leaf event-number
    leaf filename-hint
    leaf filedatal-hash
    leaf filedatal-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