YANG model for ANI

IETF101

draft-eckert-anima-enosuchd-raft-yet-99

Toerless Eckert, Huawei (tte@cs.fau.de)

Why Yang model

- Configure ANI
  - ANI != fully autonomic. Some things to configure
  - Enable/Disable ANI – global/per interface
    - Superset of enable/disable BRSKI and ACP
  - BRSKI:
    - Registrar + EST server (renewal) (separate ?):
      - enable, define domain certificate parameters
      - CA authentication/URL
      - Simplifications ? Automatically instantiate local CA upon instantiating registrar
      - Parameters for MASAs
        - Allow learning from IDevID part of BRSKI – policies for this ?!
        - Explicit configured MASA (for legacy IDevIDs)
      - GRASP parameter for registrar/EST server announcements
  - ACP:
    - “acp connect” interfaces, explicit configured neighbors/ACP tunnels
  - GRASP (in ANI nothing) ?

How Yang model

- Strategy to allow modularity ?
  - Build Yang models for ACP, BRSKI, GRASP separately + ANI model ?
    - Would like to make sure these components can be reused in other solutions, (including reuse of yang model)
  - ACP without BRSKI
    - Existing models to provision Certificates ?
    - Everything else to configure in ACP same if ACP is with or without BRSKI ?
  - BRSKI without ACP
    - Additional (from prior slide ANI variant) - configured proxies ?
  - GRASP without ACP
    - ??? Not sure yet.

Why Yang model (2)

- Manage / observe ANI (read(-only) data)
  - Prio 1: Read “configuration” of ANI
    - Will require additional “state” of functions representation
  - Prio 1: ANI operational data
    - E.g.: step-by-step BRSKI, step-by-step ACP neighborship build
    - Current state representation (ACP neighbor table, discovered GRASP objectives,…)
  - Prio 2: For underlying components
    - ACP has most components it uses, e.g.: VRF, “secure channels”, GRASP
    - Probably need to scrape IETF docs:
      - Which component already has MIB and/or operational YANG model
    - EST also “underlying” component of BRSKI
      - Anything for it ?
      - If not… should Yang mode for BRSKI be built as an extension to a to-be-built EST model ?
        - Would allow to re-use then for EST-only servers (MCR: renewal may be EST-only…)
    - GRASP: unchanged question from prior slide
- Main issue:
  - Operational Yang == better version of “show” CLI.
  - Issue: Often you can not do live “show” in automated networks.

Logging

- Q: can we define some trace/log model
  - Yang version of syslog ? (Yang push ? What else are the options ?)
- How about logging locally for later retrieval ?
  - Pledge not enrolling, something wrong, but can not verify in actual target deployment
  - Need to be able to retrieve logs from some on-pledge limited storage later.
  - Except similar issues also in e.g.: Proxy, small device environment (no good generic diagnostics environment).

BRSKI Enrolment control

- How to express policy which pledges are allowed into domain ?

- Whitelist / blacklist of IDevID serials on registrars ?
  - Flexibility too limited:
    - Want to be able to trigger some action before making decision (ask operator,…)
    - Decision not binary – may also want to be able to define per-pledge parameters of the cert (address type, subdomain, cert lifetime,…)

- Most simple & flexible solution ? :
  - RPC type call from registrar to external server to make decision
  - RPC(IDevID) -> (enrol, cert-parameters)
  - Define yang model for RPC, server connection parameters
  - Similar for EST renewal ?

BRSKI Enrolment control (2)

- Minimum complexity solution ?
  - ANI does not know which pledges are enrolled.
    - Only “external” server and CA
    - Do not model server (only RPC) or CA into ANI model
    - No need to model/track pledges inside ANI, ni modelling whitelist/blacklist
  - With just parameters of registrar enrolment RPC and EST renewal RPC, one can easily build management (“SDN”) server using e.g.: RestConf from Registrar/EST server
    - Useful separation – SDN server can, but usually do not like to implement specific protocols (e.g.: BRSKI, BRSKI-MASA,… ?)
    - EST/BRSKI already HTTP protocol, so a lot closer to what SDN controller like, but:
    - Registrar needs to be connected to ACP. For easy building of system it is very helpfull to be able to have the SDN server be able to live outside of ACP

Structuring Yang work

- One draft ?
  - Data model
    - ANI, ACP, BRSKI, GRASP
    - Or multiple ?
  - Concept explanations..

- Looking for collaborators to this work!
- Can form design team if interest ?