Proof of Presence Endorsement

Michael Richardson
<mcr+ietf@sandelman.ca>

IETF 123

draft-richardson-rats-pop-endorsement-00

What is a typical Endorsement...

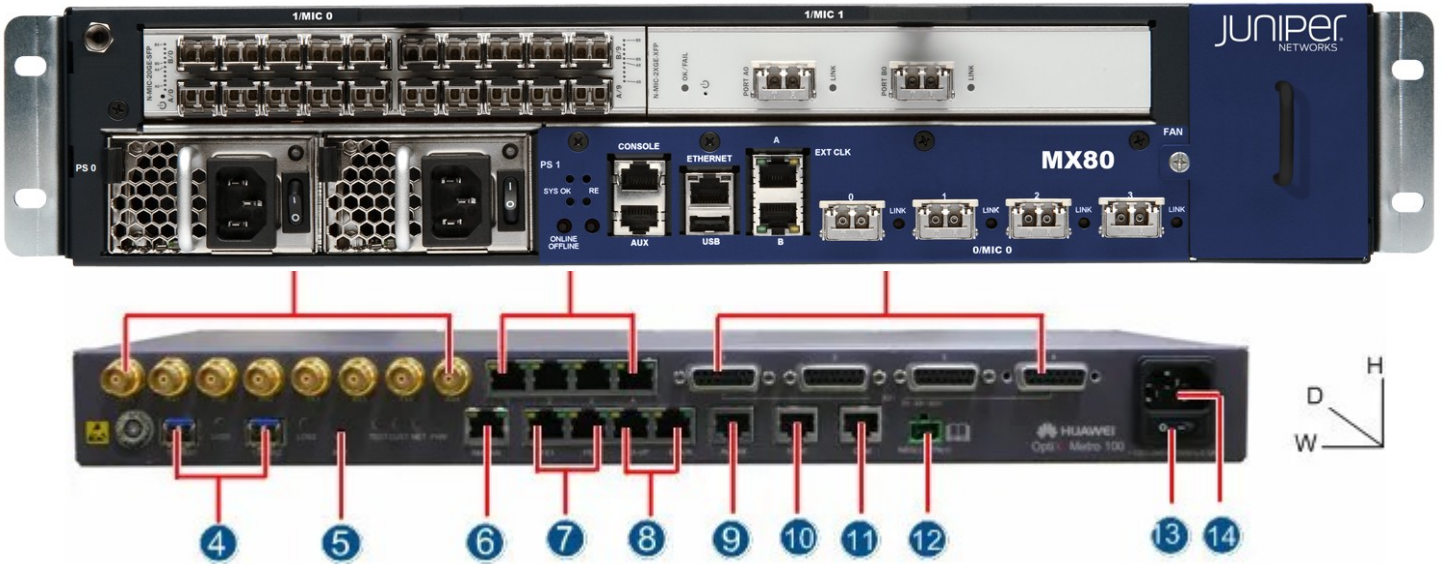
- for instance: EUDI Wallet (wscd+wsca)
- Needs to be certified by a Conformity Assessment Body
- The qualification is about the category

What is the router problem?

- There is a need for certain information to be available in the form of an Endorsement
- ~~“My car is Red”~~
- Car 438ABC is Red

Router bdi2.core.rtr.storm.ca

- Located at 151 Front Street, Toronto.
- But, what's the device's public key/identity?
- How can auditor be sure? All Juniper MX5 look the same.
- Which cable is plugged into which port?



How do we find out?

- walk up to the device
- plug something in
- exchange some signed data...
- **D**evice **U**nder **T**est
  - “DUT”

USB OTG cable

draft-richardson-rats-pop-endorsement

- a serial console protocol... probably.
- wait for login:/username:
- login with “endorsementaudit” (no password)
- could be just a “shell”
  - better to have it run a custom program.

- commands: “attestation-key”, “port-flash”, “port-down”, “port-up”,
- “endorsements”
- “exit”

Product is EAR

- signed by device under audit's (DUA) IDevID
- so links up to PKI for vendor's device identity
- https://datatracker.ietf.org/doc/draft-richardson-rats-pop-endorsement/

- verifier is **auditor** and auditor's device
  - auditor is trained CPA.
  - Yes, think KPMG,Deloitte, but also government regulator
- verifier will add additional information.
  - like a picture of the device
  - a list of cables/fibers/networks attached
- Attestation Result is **EAR**
- Result either goes up to cloud/infrastructure for later use.
- Or: gets loaded into the DUA, having been signed by the audit/auditor's infrastructure.

A connection to MUD, Ethernet

- Since an IDevID is used, and can be returned, it can contain a MUD URL, which gives one many details about device type and access!
-

- Many devices do not have console port.
- Would one want to do this over ethernet?
  - IPv6-LL?
  - LLDP?
- Need to avoid being physically spoofed.
  - ISO27001 connection