BRSKI overview and issues

- Very short BRSKI overview.
- recap of incoming/outgoing discussion
- audit token, nonce-full/nonce-less versions
- online view, offline view
- ownership voucher details: Kent

The cast

Manufacturer
Manufacturer Authorized Signing Authority (MASA)
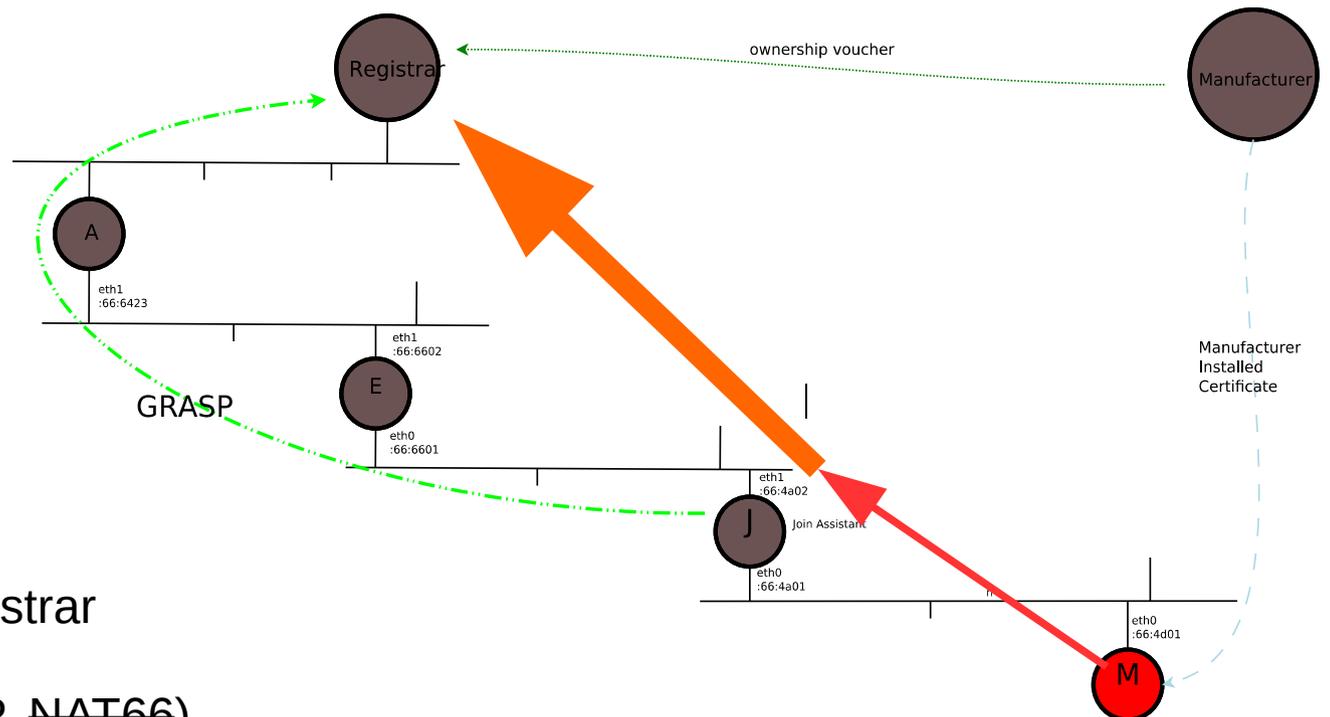Registar
Join Assistant/Proxy
New Node (pledge)
(ownership) voucher

LL
fe80::123-
>fe80::proxy
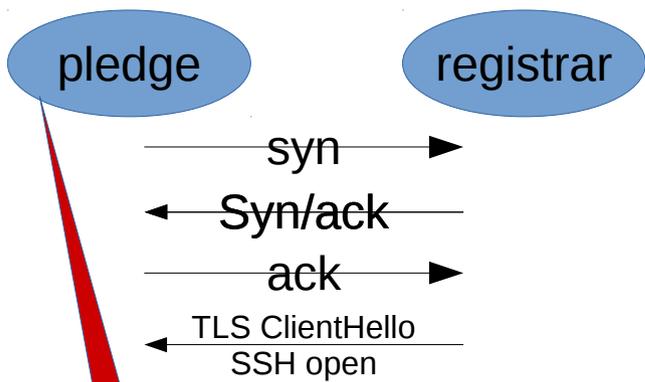
ULA
fd12:345::1-> registrar

(circuit proxy, IPIP, ~~NAT66~~)

Incoming (callhome) / Outgoing Debate
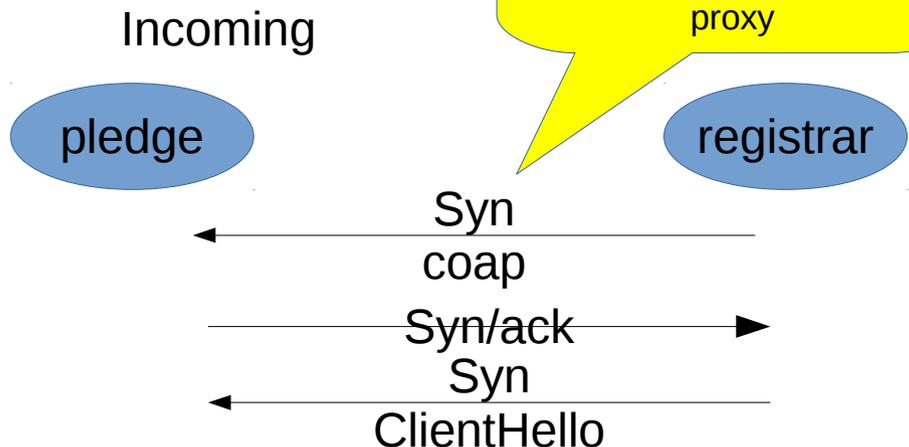
I-D.ietf-netconf-call-home

Call Home
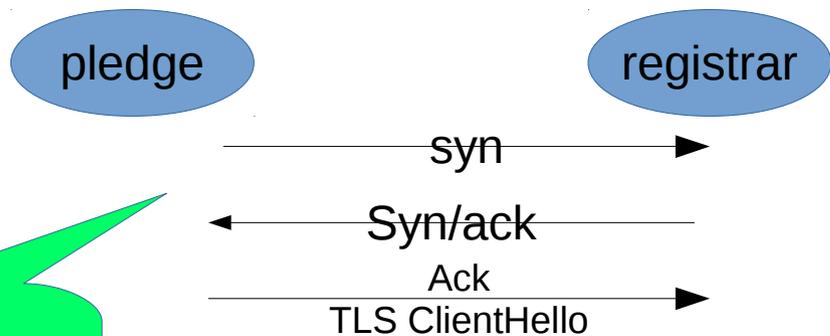
- outgoing TCP, followed by swap of client/server

pledge

registrar

syn →

← Syn/ack

ack →

← TLS ClientHello
SSH open

Tcp client
TLS server

Incoming

pledge

registrar

6tisch
Will use incoming,
With COMI+
System-keystore
proxy

← Syn
coap

Syn/ack →

← Syn
ClientHello

Outgoing

pledge

registrar

syn →

← Syn/ack

Ack →
TLS ClientHello

ANIMA
Decided to stick
With outgoing via
proxy

Audit tokens and ownership
Mix of contradictory requirements!

Audit Token

- Weak to no link to owner

  - May be bearer token!

  - Likely contains link to owner's public key.

  - May link to some DN/CN of owner

- Uses MASA to serve as registration, providing audit trail to subsequent "owners"

-

Ownership Voucher

- Strong link to owner

- MASA either produces the voucher (possibly "online"), or provides access to already created voucher.

- MASA stores history of previous vouchers.

- (controversial), may include Voucher Revocation List!

Token Requirements

- Online validation
  - May include NEA-type assessment of current firmware of device (remote attestation) back to vendor.
  - Strong connection to supply chain to provide proof of ownership.
- Offline validation
  - Need to collect all Tokens/Vouchers onto stable storage for use offline.
    - National security concerns, disaster recovery, protection against vendor going out of business
  - Uncooperative/immature supply chain
    - Need to include voucher in bearer token form inside packaging as QR code
    - Supporting re-sale of devices, transitive trust of ownership vouchers