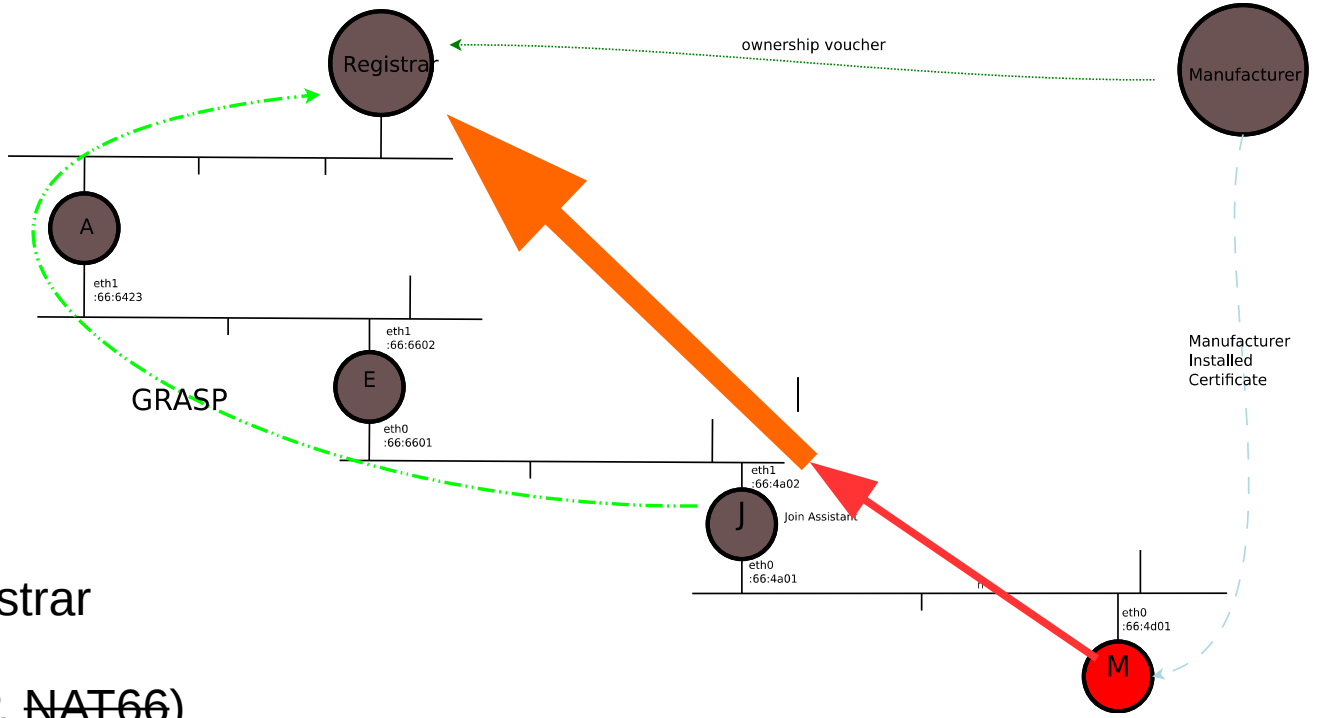
BRSKI overview and issues

- 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

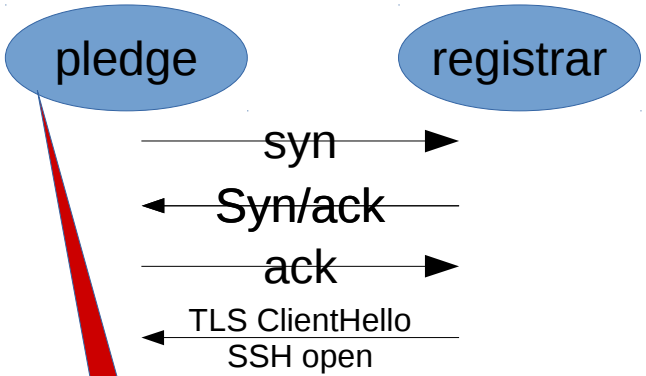
(circuit proxy, IPIP, ~~NAT66~~)

Incoming (callhome) / Outgoing Debate

I-D.ietf-netconf
-call-home

Call Home

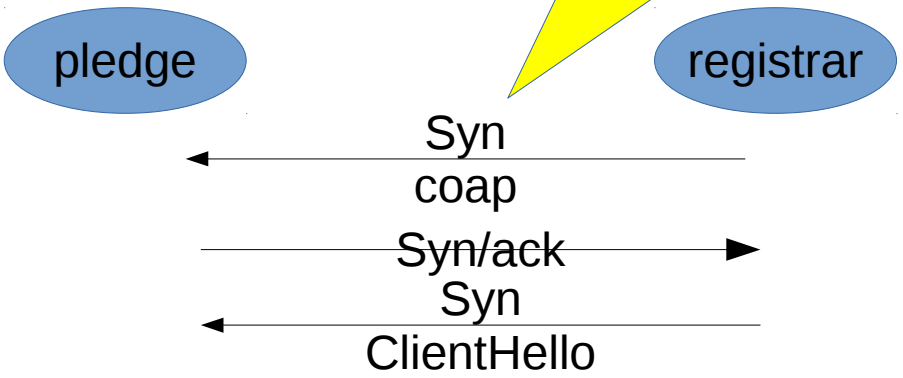
- outgoing TCP, followed by swap of client/server



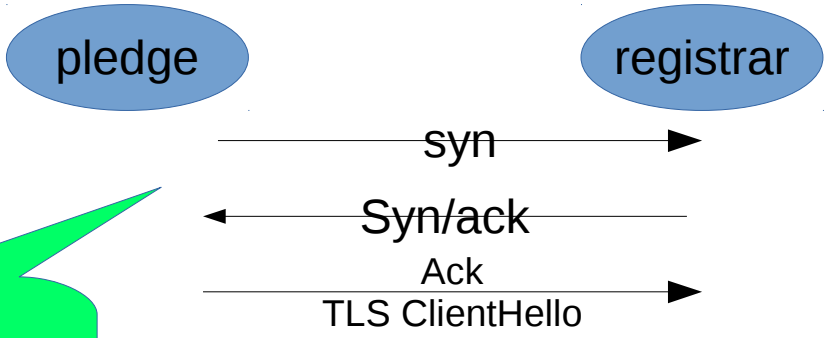
Tcp client
TLS server

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

Incoming



Outgoing



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!

Audit vs **Ownership** Voucher

YANG description		
module: ietf-voucher		
+--rw voucher	**Audit**	**Ownership**
+--rw assertion	**trust anchor for Registrar**	
+--rw trusted-ca-certificate	**id of Registrar**	**id of Registrar**
+--rw certificate-id		
| +--rw cn-id? string		
| +--rw dns-id? string		
+--rw unique-id*	**id of Pledge**	**id of Pledge**
+--rw nonce	**Real Time Clock proofing**	Real Time Clock proofing
+--rw created-on	if RTC available on Pledge	**if RTC available on Pledge**
+--rw expires-on	if RTC available on Pledge	**if RTC available on Pledge**
+--rw revocation-location	under consideration	**under consideration**
+--rw additional-data	future proofing	

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