ANIMA

Constrained Voucher and BRSKI extensions to COAP-EST

For ANIMA WG

Michael Richardson
mcr+ietf@sandelman.ca
Peter van der Stok
<consultancy@vanderstok.org>
Panos Kampanakis
<pkampana@cisco.com>

Why are we here?

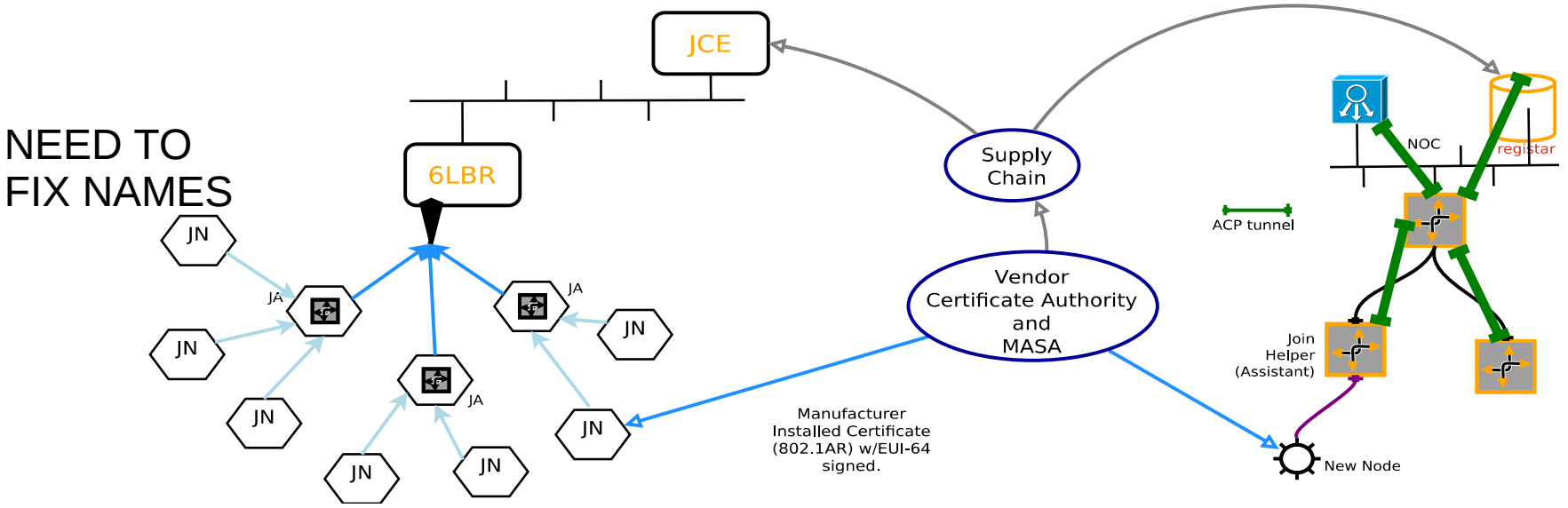
- To tell you about draft-richardson-anima-ace-constrained-voucher-03
  - we'd like it to be draft-ietf-anima-constrained-voucher.

802.1x/EAP/PANA has this "solved" for initialized nodes which know which network they want to join; need to be pre-provisioned with certificates.

- needs EAP-TLS to make this work, which then includes new layers of fragmentation. This code is used once!
- PANA/1x authenticator function scales with number of nodes attempting to join, is subject to DoS attack, defending against may be too expensive for constrained nodes
- 1x function for ANIMA **ACP** bootstrap may interfere with 1x function being provided by routers/switches for end-hosts!

BRSKI is for HTTP

- (HTTP for “big devices” and “big networks”)
- Now want to use it for constrained devices
- But, ACE only wants to do EST over COAPS (DTLS), while others want to use CoAP with EDHOC



How do the vouchers change?

- Serialized to CBOR using SIDs
- Signed with CMS (just like ietf-anima-voucher)
- Signed with COSE (new)
- BRSKI extensions to EST need to applied to EST-COAPS – draft-{ietf,vanderstok}-ace-coap-est

Who is going to use it?

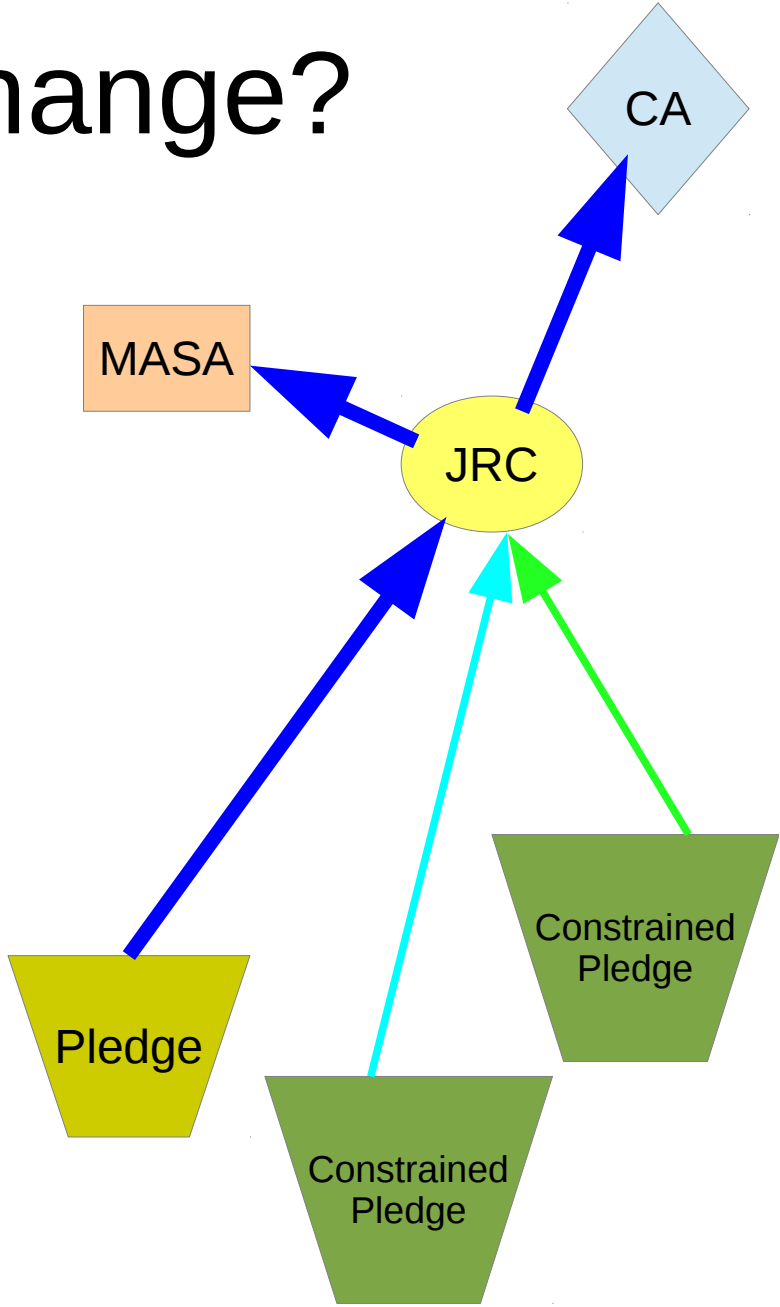
- Fairhair – building control
  - Maybe integrated with Thread stack
- Zero-touch in 6tisch
- Retail lighting

How does MASA change?

- MASA remains mostly the same
  - Must learn to create constrained vouchers
  - MASA<->JRC communication is still HTTPS

How does JRC change?

- Join Registrar/Coordinator (JRC) also remains mostly the same
  - Same interface to CA/PKI backend
  - Still speaks HTTPS to MASA
- Differences
  - Has to audit constrained vouchers and create constrained voucher requests
  - Speaks COAPS (CoAP over DTLS) and/or EDHOC over COAP.
    - (maybe others in the future, see ATLAS WG)
  - May perform JOIN process only, and not enrollment to PKI.
    - draft-ietf-6tisch-minimal-security Join Request
    - Coordinator role will issue 2-byte L2 assignments
    - Rekeying of network keys (e.g., draft-richardson-6tisch-minimal-rekey-02)



Open Issues

- Some issues with SID allocation which are unresolved in CORE/YOT:
  - Does “ietf-voucher” get a SID assignment,
  - Or does ietf-cwt-voucher get a SID assignment
    - (including ietf-voucher that was inside)
    - Ietf-cwt-voucher-request has a different SID assignment?
- So, is ietf-cwt-voucher.expire-on the same SID as ietf-cwt-voucher-request.expire-on, because they both inherit from ietf-voucher?
  - We THINK NOT. But, this is not yet well documented.

Example of constrained voucher

- **Example (in CBOR diagnostic notation):**

```
{
   1001031: {
     +2 : "2016-10-07T19:31:42Z",                  / SID = 1001033, created-on /
     +4 : "2016-10-21T19:31:42Z",                 /   SID = 1001035, expires-on /
     +1 : "verified",                               / SID = 1001032, assertion /
     +10 : "JADA123456789",                       / SID = 1001041, serial-number /
     +5 : h'0102030405060708090A0B0C0D0F',     / SID = 1001036,  idevid-issuer /
     +8 : h'0102030405060708090A0B0C0D0F', / SID = 1001039, pinned-domain-cert /
     +3 : true,                    / SID = 1001034, domain-cert-revocation-checks /
     +6 : "2017-10-07T19:31:42 Z"            / SID = 1001037, last-renewal-date /
   }
 }
```

Parent SID

Delta against Parent SID

-
- Delta encoding keeps CBOR dictionary keys to one byte!
- Wrap this with CMS Signed object (just like ietf-anima-voucher),
  - or use COSE to sign it (RFC8152)