BRSKI document status

Authors:

Max Pritikin,

Michael Richardson

and

Kent Watsen

BRSKI document – significant editorial changes

- Version -06: major rewrite of document.
  - We took most content and put it into an appendix, and then rescued content back into document in a new order.
  - RFC tools diff, 05 to 07: https://goo.gl/m3wMhD
- Significant changes to precisely align with voucher document WGLC text.

Editorial review: Table of Contents

DRAFT 05

Ommitted
Many lines
To fit on slide

Organized by
Who does what

DRAFT 07

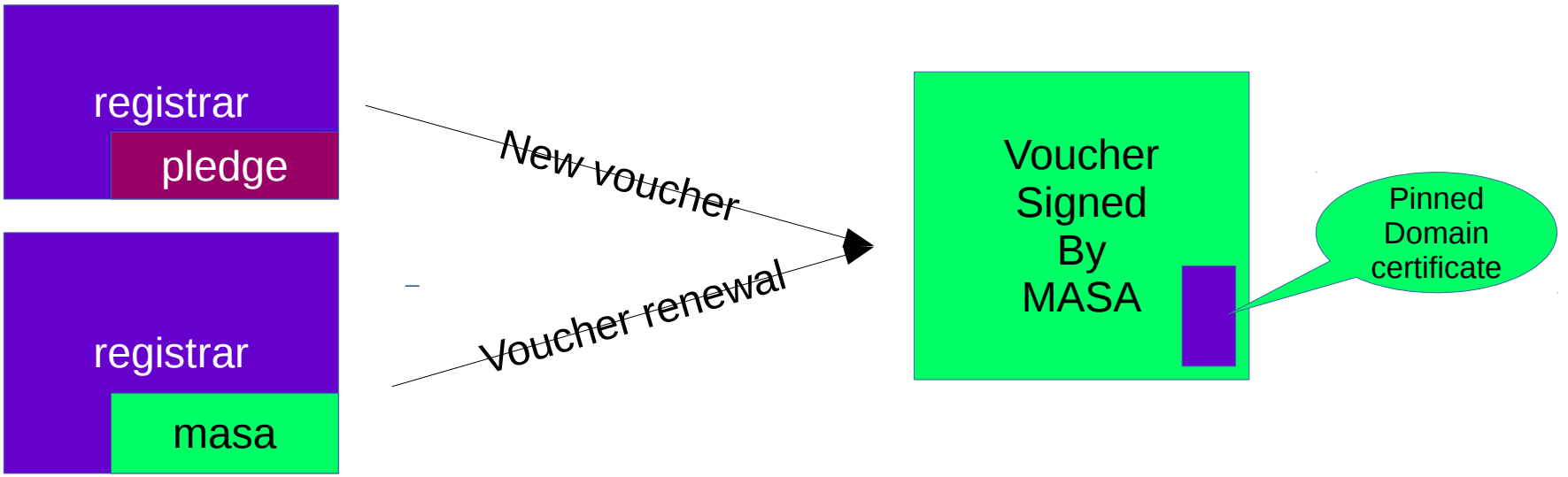
Shrunk
From 54 pages
To 42 pages

Ommitted
Only two lines
To fit

Organized by
Time sequence
Of activities

Technical changes to document

- In support of the non-contiguous voucher renewal model, the voucher request is a voucher signed by the requestor.
  - Provides proof of posession of private key
  - It may include previously signed vouchers
    - It may include signed voucher from pledge



Registrar Identity

- It was previously vague as to how MASA received the Registrar identity.
  - Assumed by some that it was the TLS ClientCertificate used by Registrar to connect.
- Signed request voucher now clarifies that entity that signed the request voucher is relevant entity.

Voucher format: PKCS7+JSON

- Our initial voucher format will be PKCS7 signed JSON.
  - Architecture permits evolution easily to JOSE signed JSON.
    - Not the same as JWT due to differences in claims
  - JWT and CWT are also obvious next steps
- Registrar needs to be aware of formats, but MASA and Pledge can implement only one.
  - Pledge determines format that will be used when it does it’s voucher request. Registrar must cope (or fail).

Questions and Comments

?

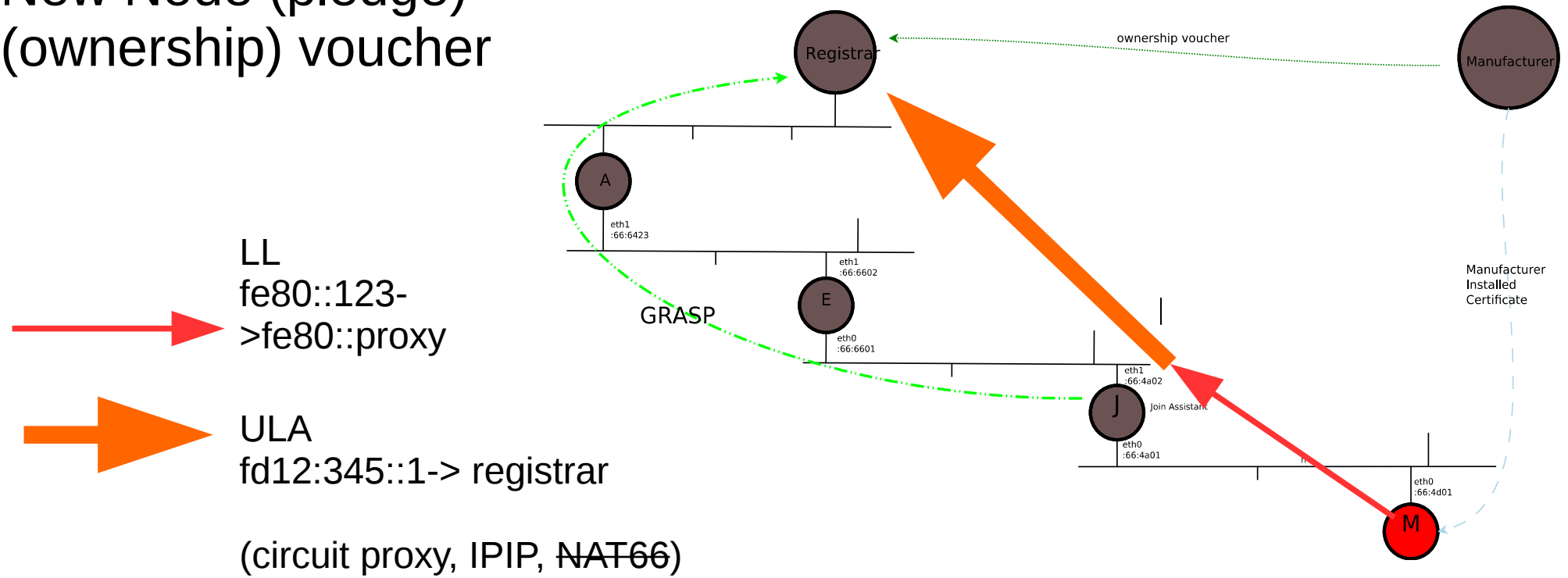
Are design team summaries useful?

Next Steps

- Get feedback on appropriateness of MIME types,
  - Fill in MIME registry template
- Review rest of “Appendix D”, determine what additional text should be rescued.
- Design team will continue to meet weekly (after short IETF recover break), Tuesdays at 1400UTC (10am EDT).
- Anticipate WGLC by fall, to be done by IETF100.

Extra sides: The cast

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

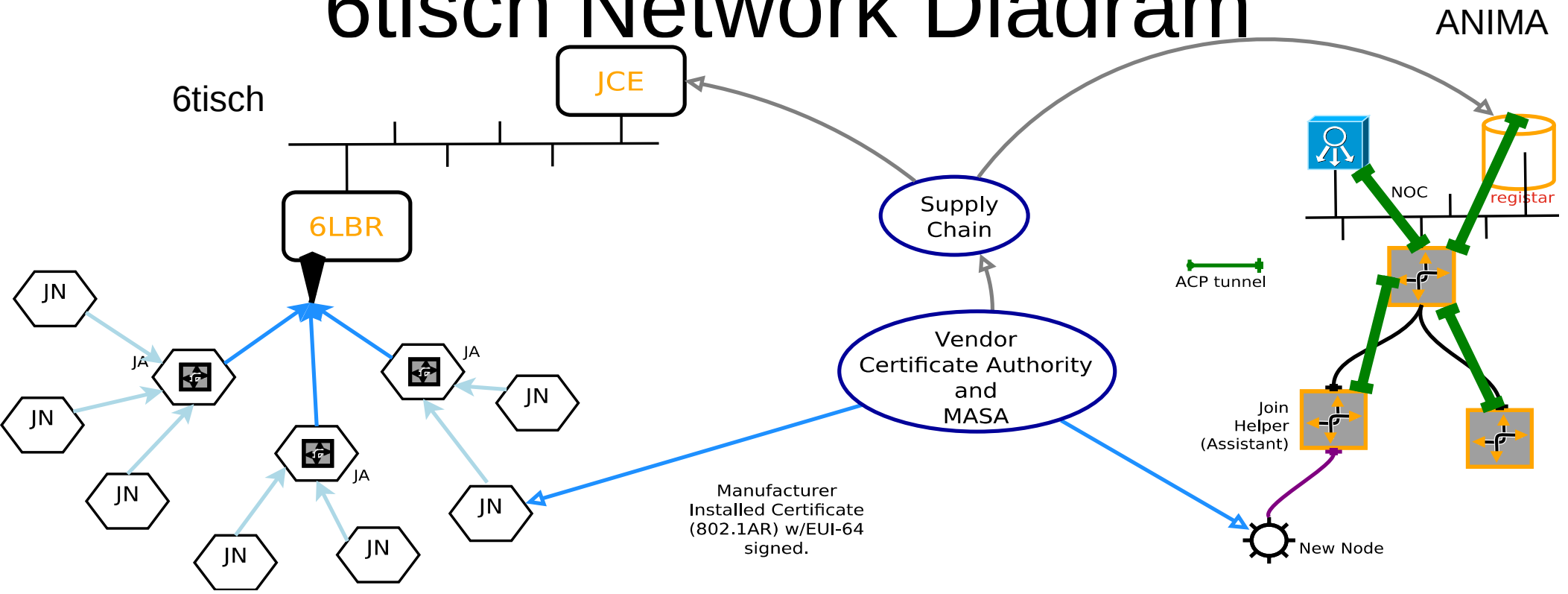


LL
fe80::123->fe80::proxy

ULA
fd12:345::1-> registrar

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

Extra slides: 6tisch Network Diagram



Both 6tisch/LLN, ANIMA and NETCONF share Manufacturer Installed Certificates (“MIC”) [IDevID], and have a supply chain relationship with network operator via which Ownership Vouchers can be communicated.

Network Diagram: NETCONF