

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

- 1. Introduction
- 2. Architectural Overview
- 3. Functional Overview
 - 3.1. Behavior of a Pledge
 - 3.2. Behavior of a Join Proxy
 - 3.3. Behavior of the Registrar
 - 3.4. Behavior of the MASA Service
 - 3.5. Leveraging the new key infrastructure / next steps
 - 3.6. Interactions with Network Access Control
- 4. Domain Operator Activities
 - 4.1. Instantiating the Domain Certification Authority
 - 4.2. Instantiating the Registrar
 - 4.3. Accepting New Entities
 - 4.4. Automatic Enrollment of Devices
 - 4.5. Secure Network Operations
- 5. Proxy Discovery Protocol Details
- 6. Registrar Discovery Protocol Details
- 7. Protocol Details
 - 7.1. Request Voucher from the Registrar
 - 7.2. Request Voucher from MASA
 - 7.3. Voucher Response
 - 7.4. Voucher Status Telemetry
 - 7.5. MASA authorization log Request
 - 7.6. MASA authorization log Response
 - 7.7. EST Integration for PKI bootstrapping
- 8. Reduced security operational modes
 - 8.1. Trust Model
 - 8.2. New Entity security reductions
 - 8.3. Registrar security reductions
 - 8.4. MASA security reductions
- 9. Security Considerations
- 10. Acknowledgements

Omitted
Many lines
To fit on slide

Organized by
Who does what

• DRAFT 07

- 1. Introduction
 - 1.1. Other Bootstrapping Approaches
 - 1.2. Terminology
 - 1.3. Scope of solution
- 2. Architectural Overview
 - 2.1. Secure Imprinting using Vouchers
 - 2.2. Initial Device Identifier
 - 2.3. Protocol Flow
 - 2.4. Lack of realtime clock
 - 2.5. Cloud Registrar
- 3. Protocol Details
 - 3.1. Discovery
 - 3.2. Request Voucher from the Registrar
 - 3.3. Request Voucher from MASA
 - 3.4. Voucher Response
 - 3.5. Voucher Status Telemetry
 - 3.6. MASA authorization log Request
 - 3.7. MASA authorization log Response
 - 3.8. EST Integration for PKI bootstrapping
 - 3.8.1. EST Distribution of CA Certificates
 - 3.8.2. EST CSR Attributes
 - 3.8.3. EST Client Certificate Request
 - 3.8.4. Enrollment Status Telemetry
 - 3.8.5. EST over CoAP
- 4. Reduced security operational modes
 - 4.1. Trust Model
 - 4.2. Pledge security reductions
 - 4.3. Registrar security reductions
 - 4.4. MASA security reductions
- 5. IANA Considerations
 - 5.1. PKIX Registry
- 6. Security Considerations
- 7. Acknowledgements

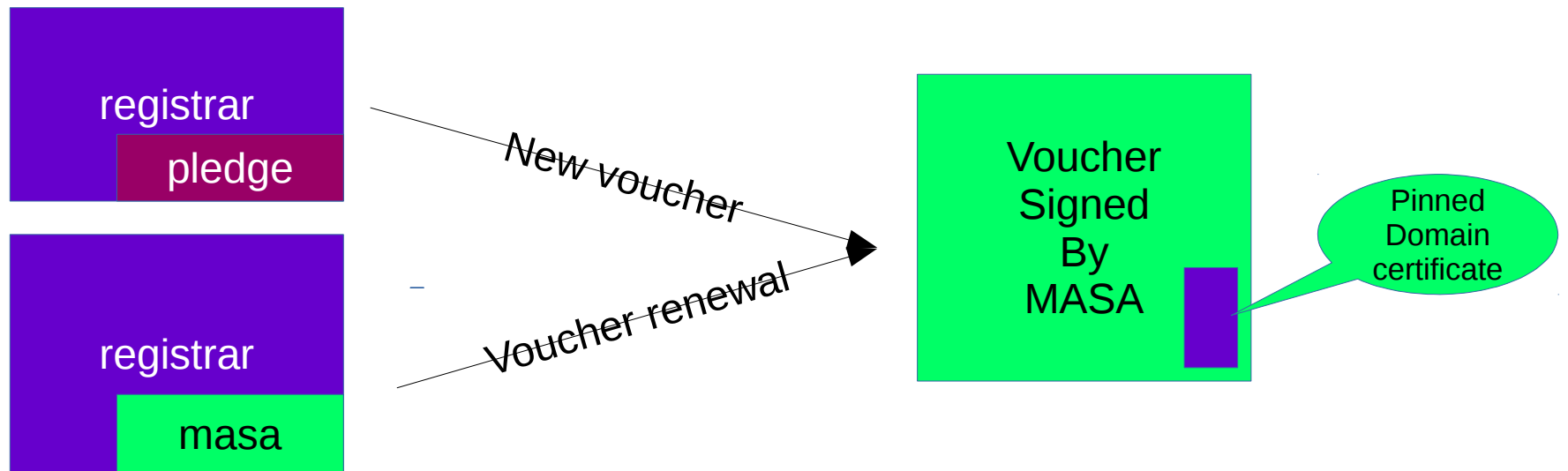
Shrunk
From 54 pages
To 42 pages

Omitted
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 possession 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

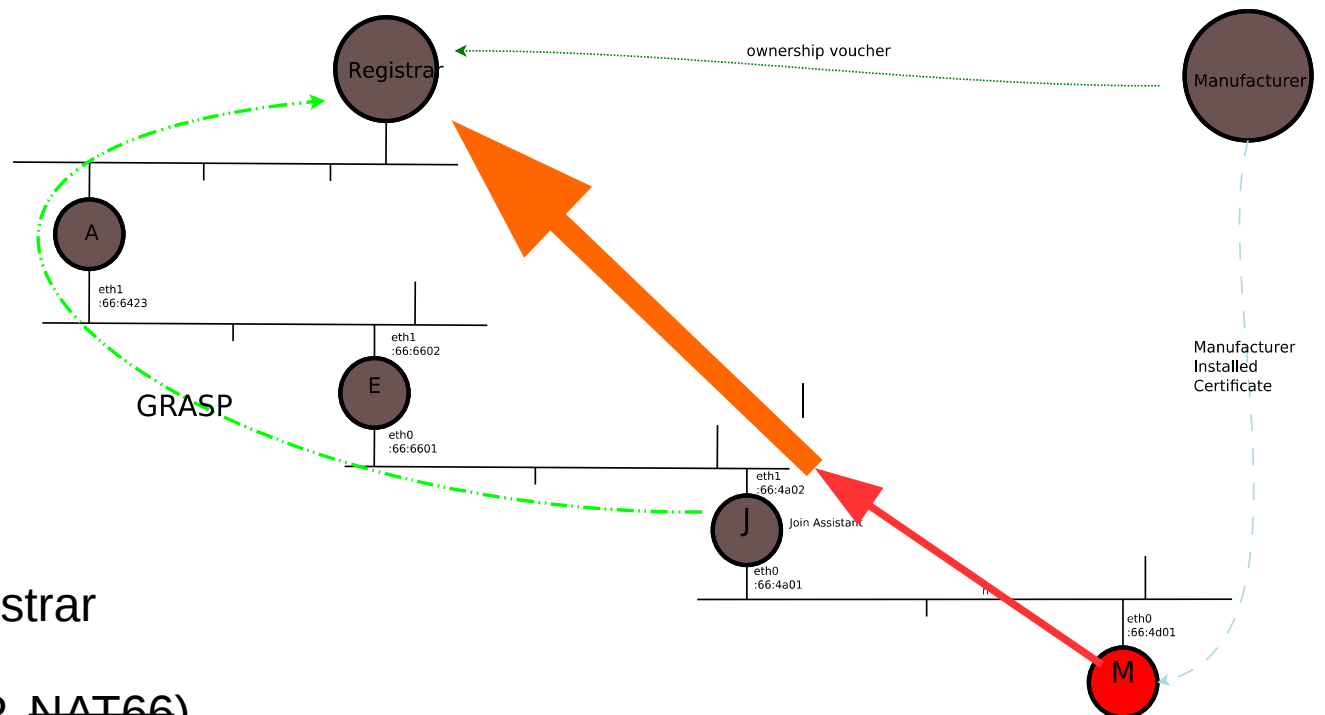
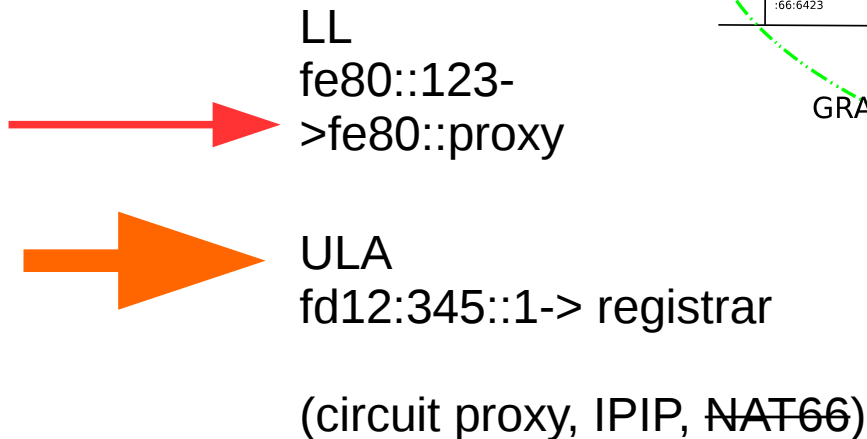
Manufacturer Authorized Signing Authority (MASA)

Registrar

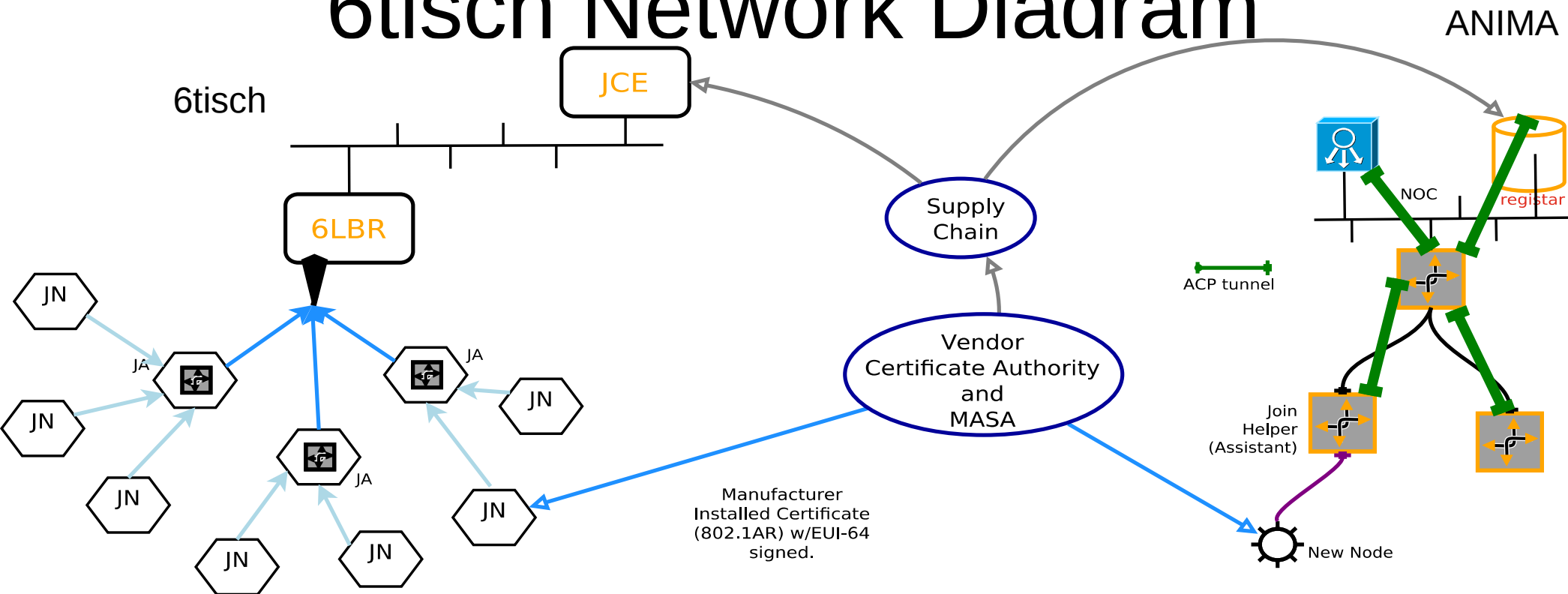
Join Assistant/Proxy

New Node (pledge)

(ownership) voucher



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

