

Possible merge

draft-ietf-anima-registrar-operational-considerations
draft-ietf-anima-masa-operational-considerations

Michael Richardson,

(+Thomas Werner)

IETF 125

ANIMA Working Group

Registrar Operations

1. Introduction
 - 1.1. Terminology
 - 1.2. Reference Network and Diagrams
 - 1.2.1. Tier-1 Network
 - 1.2.2. Enterprise Network
 - 1.2.3. Home Network
 - 1.3. Internal architectural view
 - 1.3.1. Pledge Interface (Southbound Interface)
 - 1.3.2. MASA client (Northbound Interface)
 - 1.3.3. Join Proxy (Southbound Interface)
 - 1.3.4. EST and BRSKI GRASP announcements
 - 1.3.5. Certification Authority
 - 1.3.6. Management Interface
2. Connecting the Autonomic Control Plane to the Network Operations Center (NOC)
3. Public Key Infrastructure Recommendations for the Registrar
 - 3.1. PKI recommendations for Tier-1/ISP Networks
 - 3.2. Enterprise Network
 - 3.3. Home Network
4. Architecture Considerations for the Registrar
 - 4.1. Completely Synchronous Registrar
 - 4.2. Partially Synchronous Registrar
 - 4.3. Asynchronous Registrar
5. Certificates needed for the Registrar
 - 5.1. TLS Server Certificate for BRSKI-EST
 - 5.2. TLS Client Certificate for BRSKI-MASA
 - 5.2.1. Use of Publically Anchored TLS Client Certificate with BRSKI-MASA connection
 - 5.3. Certificate for signing of Voucher-Requests
6. Autonomic Control Plane Addressing
7. Privacy Considerations
8. Security Considerations
 - 8.1. Denial of Service Attacks against the Registrar
 - 8.2. Loss of Keys/Corruption of Infrastructure

History of the document: WHY?

- Implementation of Registrar and MASA from 2018 to 2022
- Issues that arose, what to do with them, dumped into two documents starting in 2019.
- Some issues/concerns that arose, such as which key is pinned in pinned-domain-cert came out of this document, and it was possible to get some changes into RFC8995, and cBRSKI contains some additional text.
- If implementations do not support some deployment models, then they operationally can't be picked. Many things are probably quality of implementation issues.
- **HOWEVER**, some things affect cross component interoperability, and then they we get intoperability issues when quality of implementation is poor.
 - For instance, can not use client-side certificate for Registrar/MASA communication if MASA framework/hosting does not support RFC9440 (“Client-Cert HTTP Header Field”) or equiv.
- Identify how operational requirements (particularly around horizontal scaling)

MASA Operations

1. Introduction
2. Operational Considerations for Manufacturer Authorized Signing Authority (MASA)
 - 2.1. Deflecting unwanted TLS traffic with Client Certificates
 - 2.2. Web framework architecture
 - 2.3. Self-contained multi-product MASA, no PKI
 - 2.4. Self-contained multi-product MASA, with one-level PKI
 - 2.5. Self-contained per-product MASA
 - 2.6. Per-product MASA keys intertwined with IDevID PKI
 - 2.7. Rotating MASA authorization keys
3. Operational Considerations for Constrained MASA
4. Operational Considerations for creating Nonceless vouchers
5. Business Continuity and Escrow Considerations
6. Privacy Considerations
7. Security Considerations
8. IANA Considerations

PKI Advice

Implementation advice, operational diversity

MASA

Operational Considerations for Manufacturer Authorized Signing Authority (MASA)

- Self-contained multi-product MASA, no PKI
- Self-contained multi-product MASA, with one-level PKI
- Self-contained per-product MASA
- Per-product MASA keys intertwined with IDevID PKI
- Rotating MASA authorization keys

- Business Continuity and Escrow Considerations

Registrar

3. Public Key Infrastructure Recommendations for the Registrar

- 3.1. PKI recommendations for Tier-1/ISP Networks
- 3.2. Enterprise Network
- 3.3. Home Network

5. Certificates needed for the Registrar

- 5.1. TLS Server Certificate for BRSKI-EST
- 5.2. TLS Client Certificate for BRSKI-MASA
 - 5.2.1. Use of Publically Anchored TLS Client Certificate with BRSKI-MASA connection
- 5.3. Certificate for signing of Voucher-Requests

Scaling Advice

PKI and security vs Horizontal Scaling

MASA

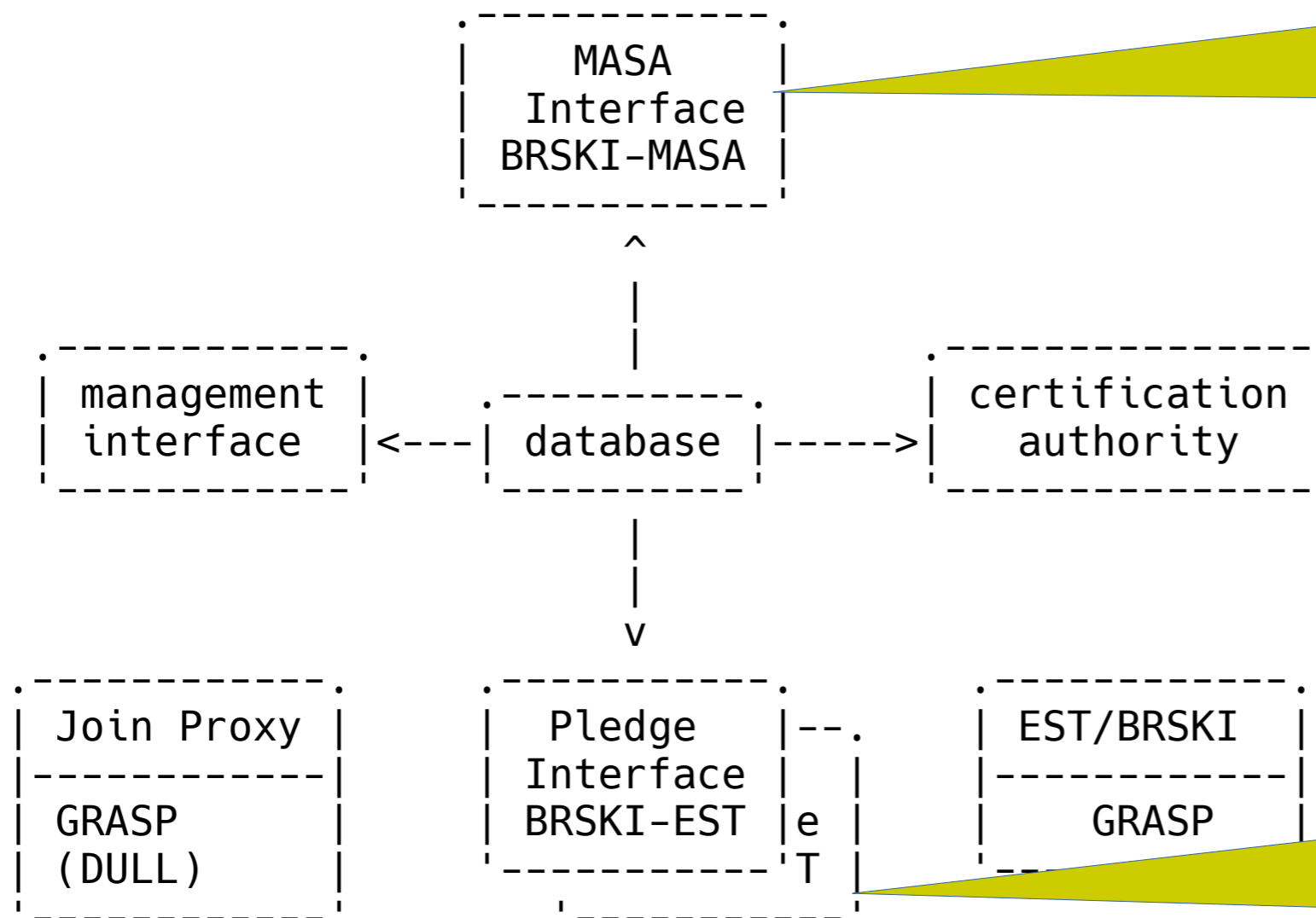
- 2.5. Self-contained per-product MASA
- 2.6. Per-product MASA keys intertwined with IDevID PKI
- 2.7. Rotating MASA authorization keys
- 3. Operational Considerations for Constrained MASA
- 4. Operational Considerations for creating Nonceless vouchers
- 5. Business Continuity and Escrow Considerations

Registrar

- 1.3. Internal architectural view
 - 1.3.1. Pledge Interface (Southbound Interface)
 - 1.3.2. MASA client (Northbound Interface)
 - 1.3.3. Join Proxy (Southbound Interface)
 - 1.3.4. EST and BRSKI GRASP announcements
 - 1.3.5. Certification Authority
 - 1.3.6. Management Interface
- 4. Architecture Considerations for the Registrar
 - 4.1. Completely Synchronous Registrar
 - 4.2. Partially Synchronous Registrar
 - 4.3. Asynchronous Registrar

Scaling Advice

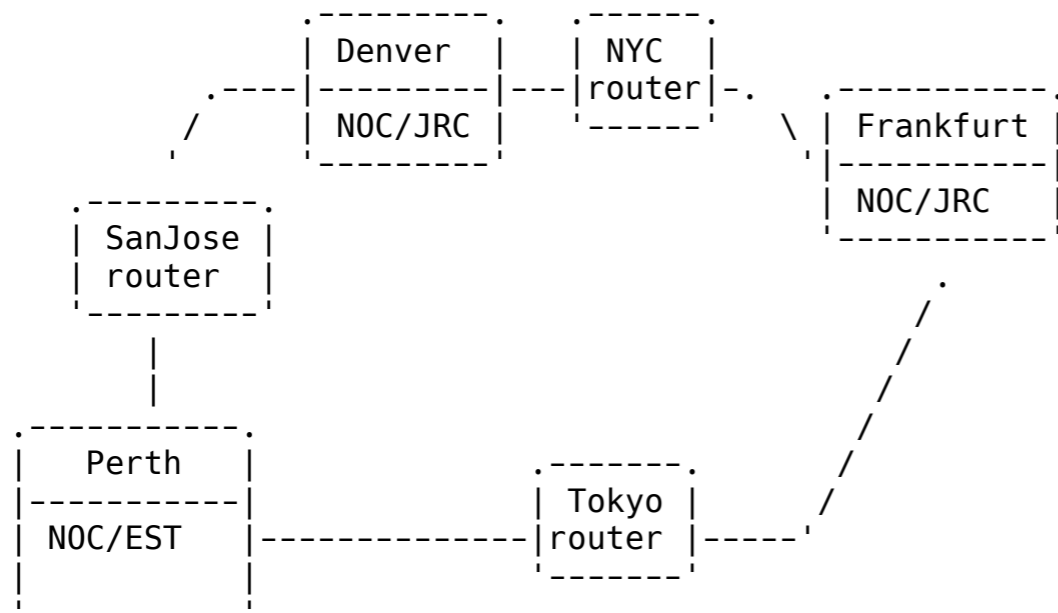
Registrar Architecture



If Client Certificate Authentication Is used, is this certificate The same as for signing The voucher-request?

Is the voucher-request Signing credential the same Across multiple (horizontally) scaled Pledge Systems?

Registrar and ACP/NOC architecture

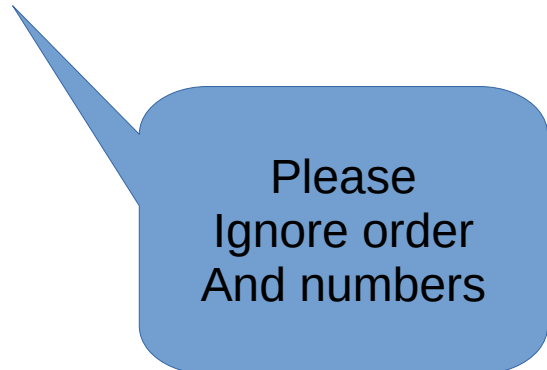


- This section/diagram was added with the intention of providing advice about how to deal with network and database partitions
- Can we onboard devices (like, core routing platforms needed to repair the partition!) when there are partitions? What preparations are necessary?
- Maybe this section was too ambitious?
-

Merged Table Of Contents

Operational Only

1. Introduction
 - 1.1. Terminology
 - 1.2. Reference Network and Diagrams
 - 1.2.1. Tier-1 Network
 - 1.2.2. Enterprise Network
 - 1.2.3. Home Network
3. Public Key Infrastructure Recommendations for the Registrar
 - 3.1. PKI recommendations for Tier-1/ISP Networks
 - 3.2. Enterprise Network
 - 3.3. Home Network
2. Operational Considerations for Manufacturer Authorized Signing Authority (MASA)
 - 2.1. Deflecting unwanted TLS traffic with Client Certificates
 - 2.2. Web framework architecture
 - 2.3. Self-contained multi-product MASA, no PKI
 - 2.4. Self-contained multi-product MASA, with one-level PKI
 - 2.5. Self-contained per-product MASA
 - 2.6. Per-product MASA keys intertwined with IDevID PKI
 - 2.7. Rotating MASA authorization keys
3. Operational Considerations for Constrained MASA
4. Operational Considerations for creating Nonceless vouchers
5. Business Continuity and Escrow Considerations
5. Certificates needed for the Registrar
 - 5.1. TLS Server Certificate for BRSKI-EST
 - 5.2. TLS Client Certificate for BRSKI-MASA
 - 5.2.1. Use of Publically Anchored TLS Client Certificate with BRSKI-MASA connection
 - 5.3. Certificate for signing of Voucher-Requests
6. Autonomic Control Plane Addressing
7. Privacy Considerations
8. Security Considerations
 - 8.1. Denial of Service Attacks against the Registrar
 - 8.2. Loss of Keys/Corruption of Infrastructure



Please
Ignore order
And numbers

Merged Table Of Contents Implementation Guidance?

1. Introduction
 - 1.1. Terminology
 - 1.2. Reference Network and Diagrams
 - 1.2.1. Tier-1 Network
 - 1.2.2. Enterprise Network
 - 1.2.3. Home Network
 3. Public Key Infrastructure
5. Business Continuity and Escrow Considerations
 - 1.3. Internal architectural view
 - 1.3.1. Pledge Interface
(Southbound Interface)
 - 1.3.2. MASA client
(Northbound Interface)
 - 1.3.3. Join Proxy
(Southbound Interface)
 - 1.3.4. EST and BRSKI GRASP
announcements
 - 1.3.5. Certification Authority
 - 1.3.6. Management Interface
2. Connecting the Autonomic Control Plane to the Network Operations Center (NOC)

Many things
Already made it
into RFC8995

Please
Ignore order
And numbers

DISCUSSION