Operational Considerations for BRSKI Registrar

draft-richardson-anima-registrar-considerations

M. Richardson

Liang Xia

Jie Yang(presenting)

IETF 107, ANIMA

Reference of BRSKI Registrar connection

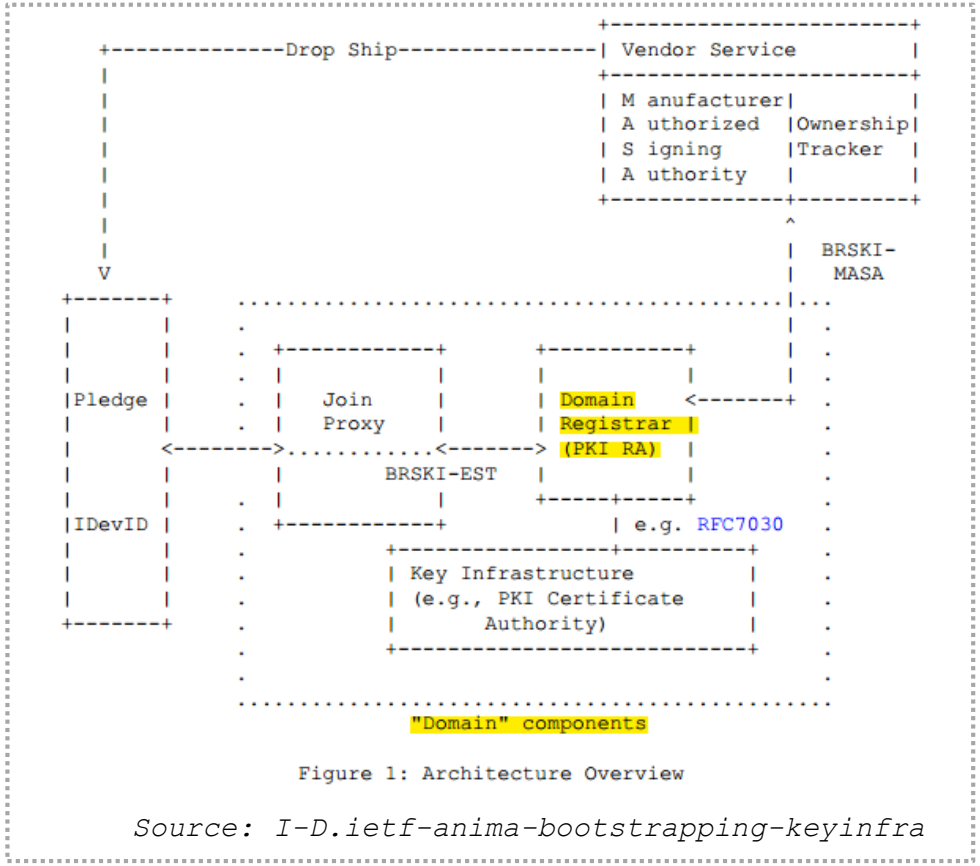


Figure 1: Architecture Overview

Source: I-D.ietf-anima-bootstrapping-keyinfra

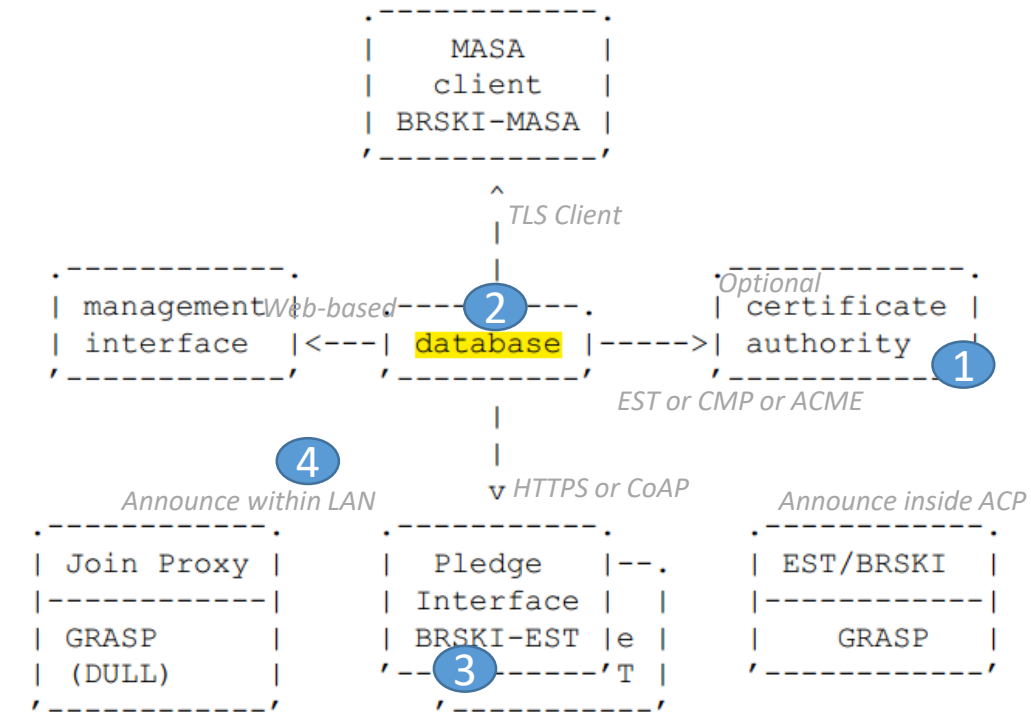
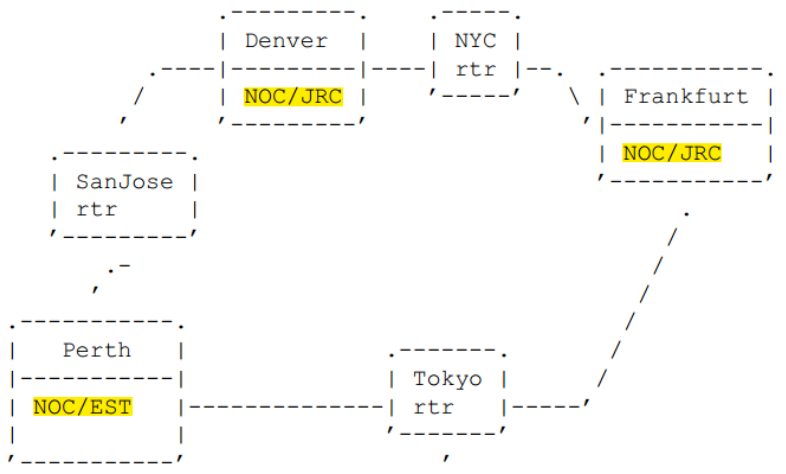


Figure 2: Reference Internal Architecture for Registrar

- BRSKI Registrar is the component that implement the domain, authorizing the pledges to join
- BRSKI Registrar have four major Interfaces Connected by common database, and four considerations need to be discussed more

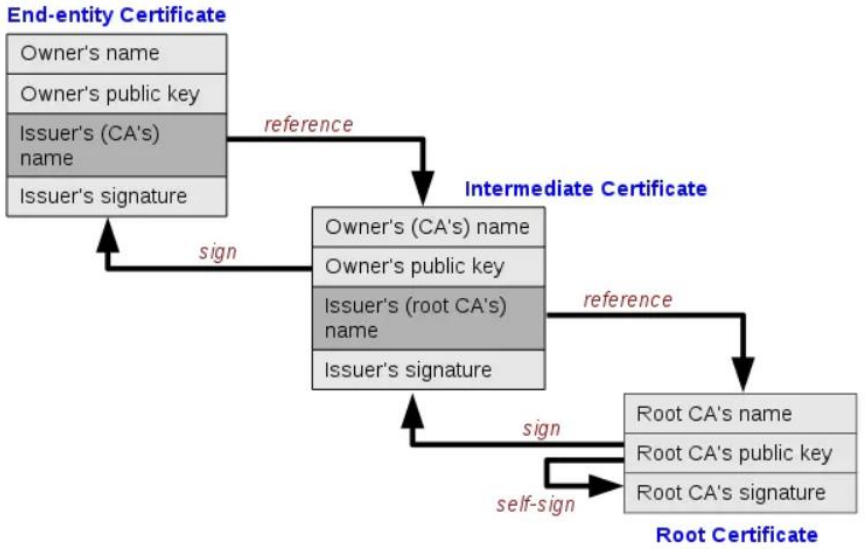
1. PKI Recommendations: Infrastructure CA for Registrar in ISP

- Tier-1/ISP Networks
  - **Three-tier** PKI infrastructure : **Good practice**
    - **Root CA** with the private key kept offline, longer lifetime
    - Multiple **Intermediate CA** with a common root and the keys online, shorter periods, sign local **End-entity** certification
    - Registrar need Client certification for MASA and Server certification for EST, Recommend issued by **NOC Infrastructure(Intermediate) CA**
- Enterprise Network
  - Multiple NOCs : Same Three-tier PKI infrastructure as ISP
  - All NOC in a single locations:
    - Three-tier PKI for operational continuity, with root CA installed in VM and the private key kept offline
- Home Network
  - Three-tier PKI infrastructure with the private key offline is Redundant
  - Registrar should be initialized with a single key pair used as CA
  - Where to locate PKI and registrar? One device owned by home user …

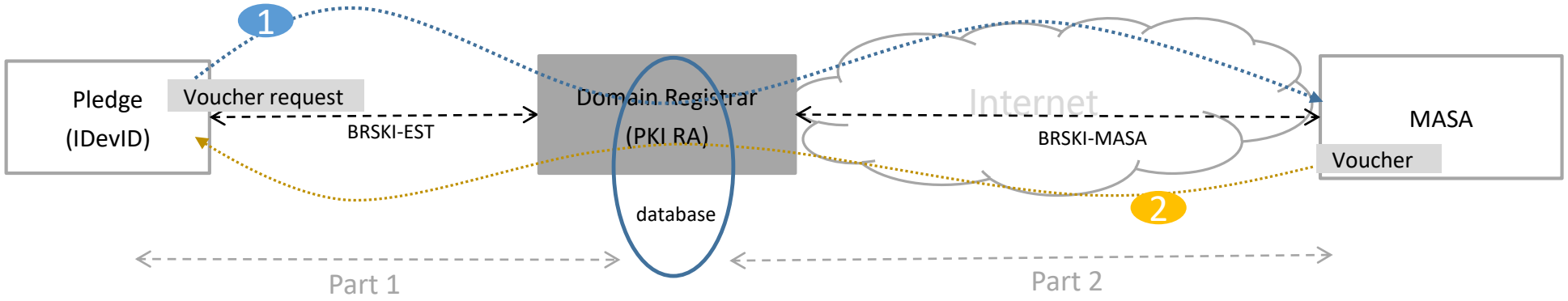


Multiple NOCs in different locations

Figure 1: Reference Tier-1 ISP network

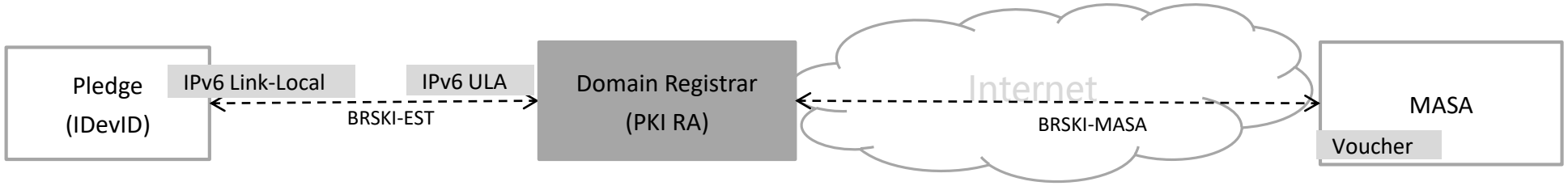


2. Scalability: Voucher Calling mechanism choosing on Registrar



- Optional Calling Mechanism:
  - Completely Synchronous Registrar
    - Operate as a single thread for the voucher-request and fresh voucher
    - Depend on the thread timeout, and share the same database
  - Asynchronous Registrar
    - Have a higher latency with secure advantages
      - the internal facing Registrar never connects to the Internet
      - deal with a high number of malicious or lost internal clients independently
  - Partially Synchronous Registrar

3. ACP Addressing for Pledge



- ACP required In ISP use cases
  - The certifications returned by Registrar Must contain a unique IPv6 ULA address
  - Limit the number of nodes between 32K(F=1 address) and 8M(F=0 address)
    - **which kind of address is asked for by the device? Non-standardized…**
      - Network manager can monitor the F=0 space(256 addresses per device)
      - If exceed 256, then allocate an F=1 address in the management intf.
      - Scenario: a large number VNFs connected to SDN controller separately

4. Security Consideration for Registrar

- **Issue 1** : DoS Attacks against Registrar,
  - A large number of IoT devices with access ports
  - But malware existing in some device
  - Bandwidth from Join Proxy to Registrar will be exhausted
- **Issue 2** : Loss of Keys in Home-net,
  - Fail to backup database followed by a failed CPE, which be thrown away
  - Then results in loss of control for all devices in the home …

Next Step on BRSKI Registrar Considerations

1. Where to issue certifications for Registrar?
2. For voucher calling on Registrar, Synchronize or Asychronize, which is prefer?
3. Which kind of IPv6 ULA address is for pledge in ACP process? F=0 or F=1?
4. Expanding considerations for Registrar security? Like DDoS and Key Loss…
5. …

Thank You!