Bootstrapping Key Infrastructures

draft-pritikin-anima-bootstrapping-keyinfra-01.txt

92th IETF, 24 Mar 2015

Max Pritikin

Michael Behringer

Steinthor Bjarnason

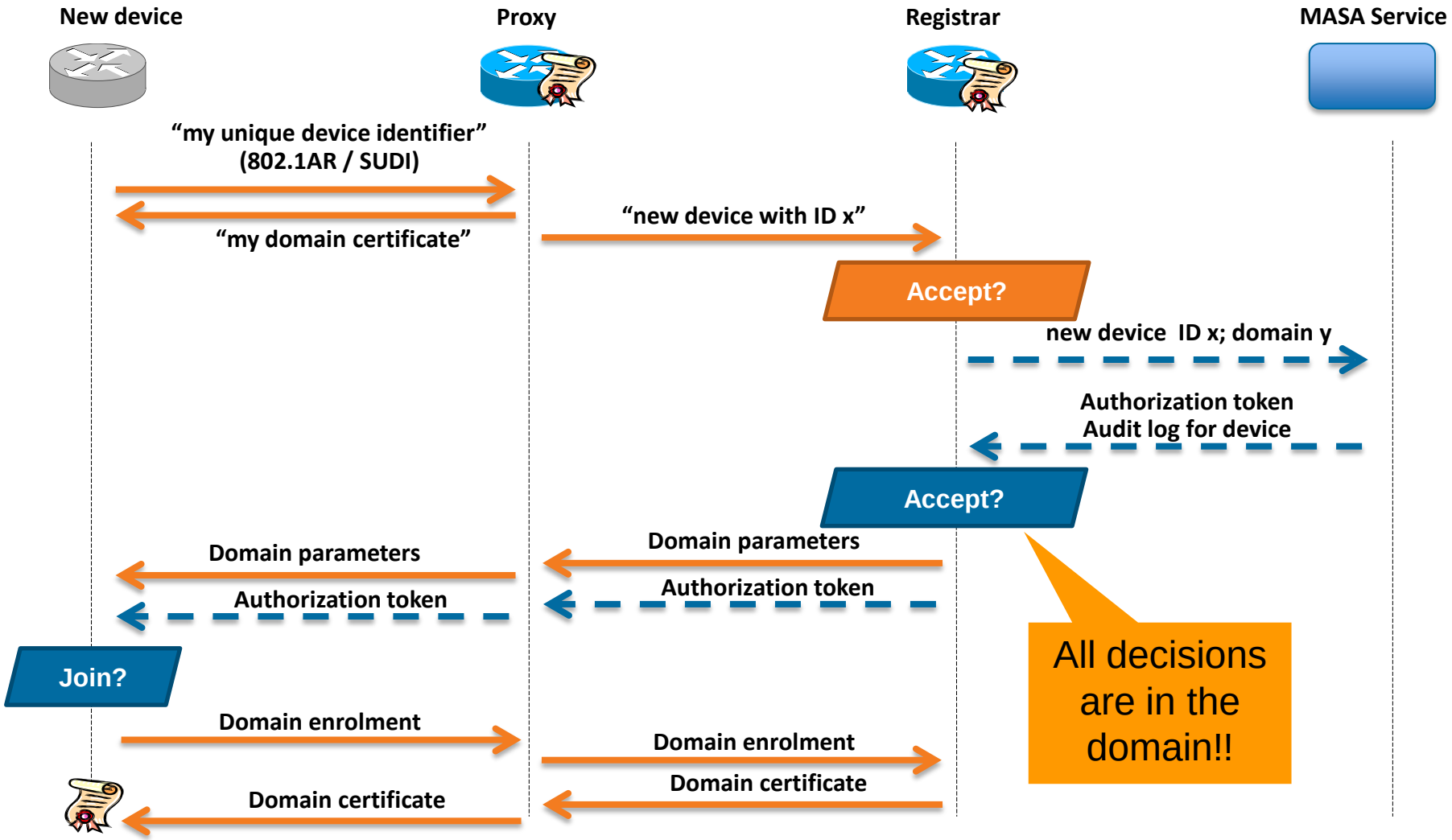
Outline

1. Introduction
2. Architectural Overview
3. Operational Overview
4. Functional Overview
5. Protocol Details
6. Reduced security operational modes
7. Security Considerations
8. Acknowledgements
9. References

Describe "optimal" approach

Describe "sub-optimal" (but pragmatic) alternatives

Secure Enrolment Process

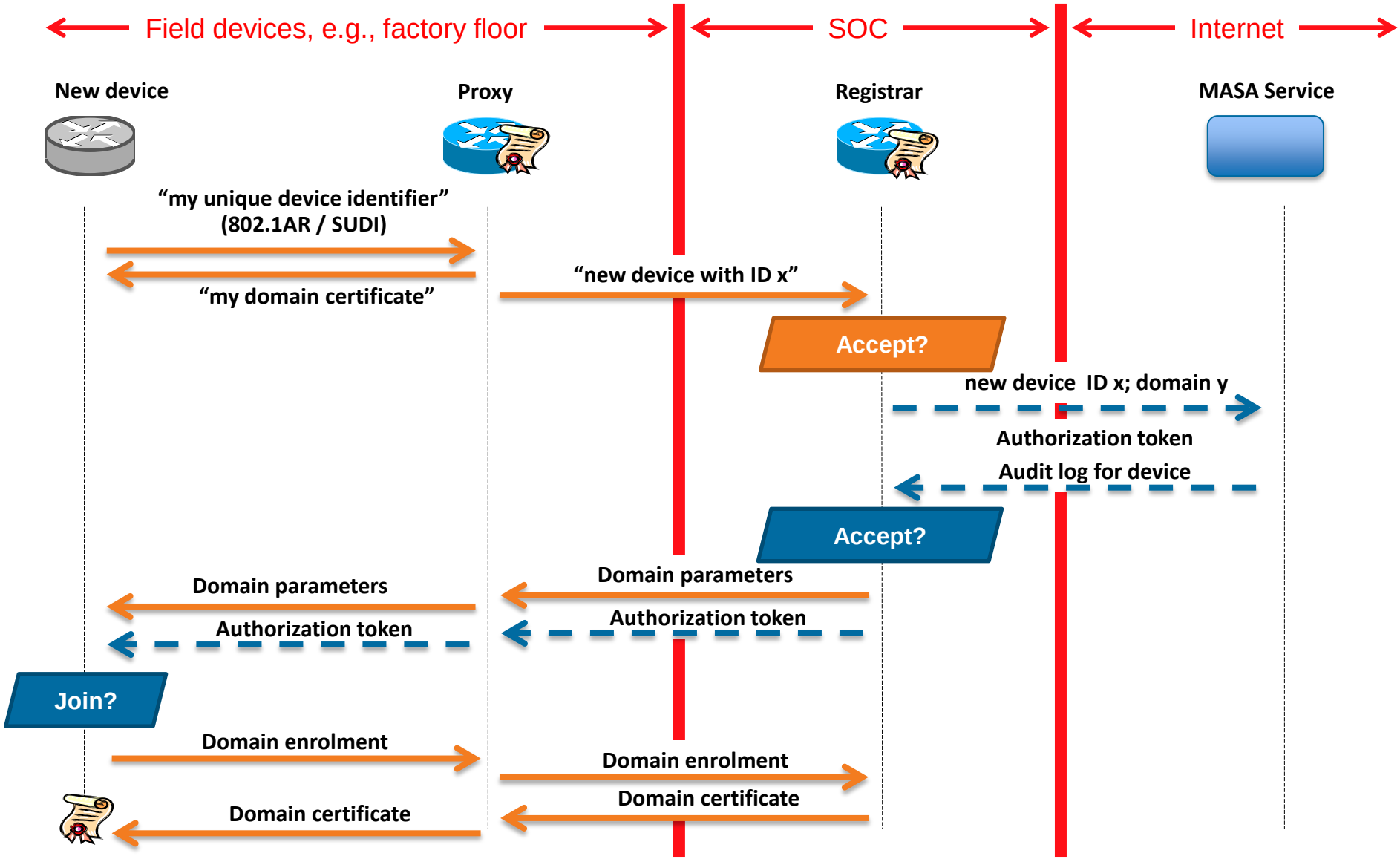


Features

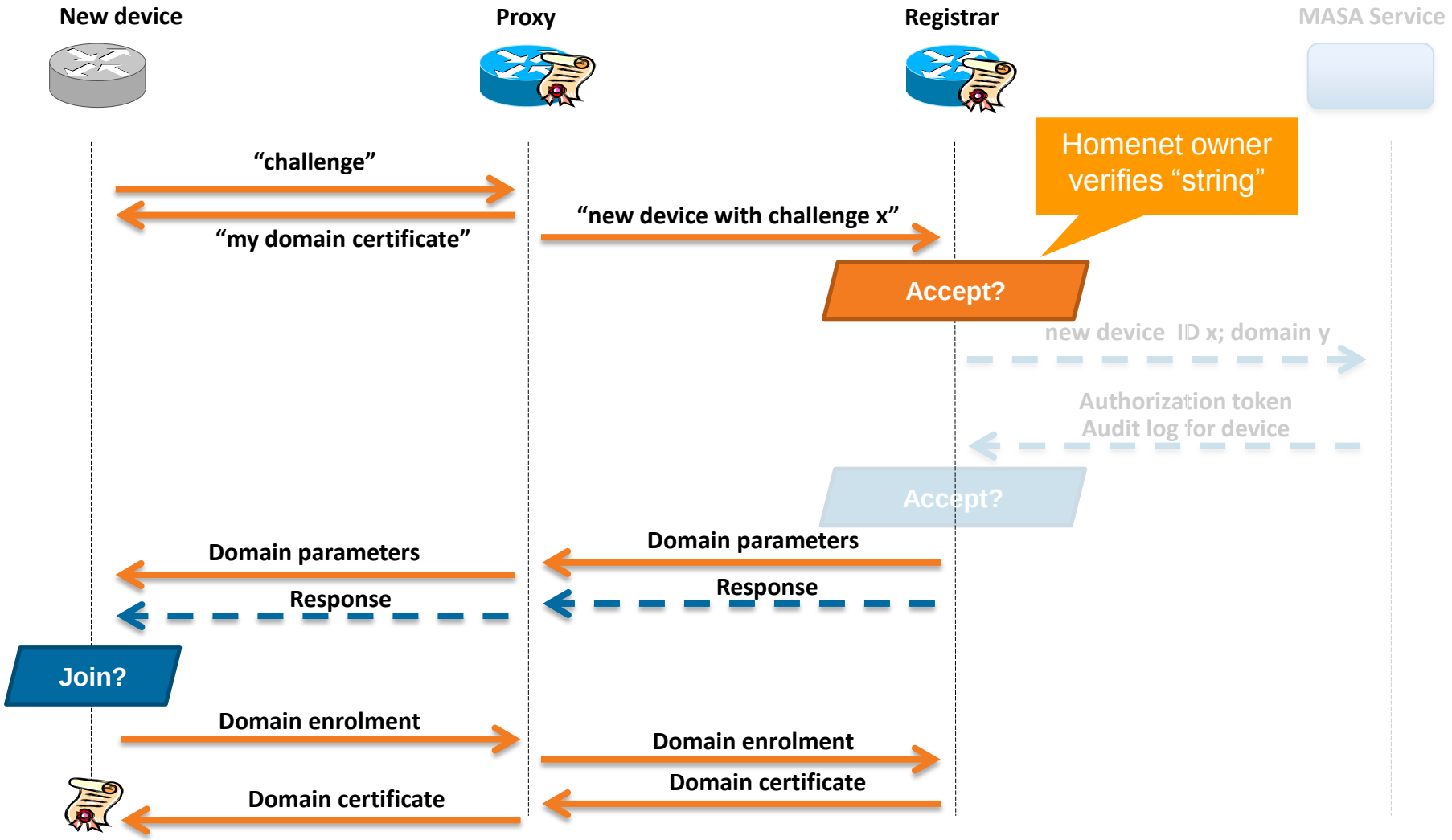
- New device has only link local connectivity
  - Can only attack first hop
- New device can be cryptographically authenticated
- New device can authenticate network
  - Join only the authorized network

- Applicability: Potentially anywhere, network devices, sensors, etc.

Possible Security Zones



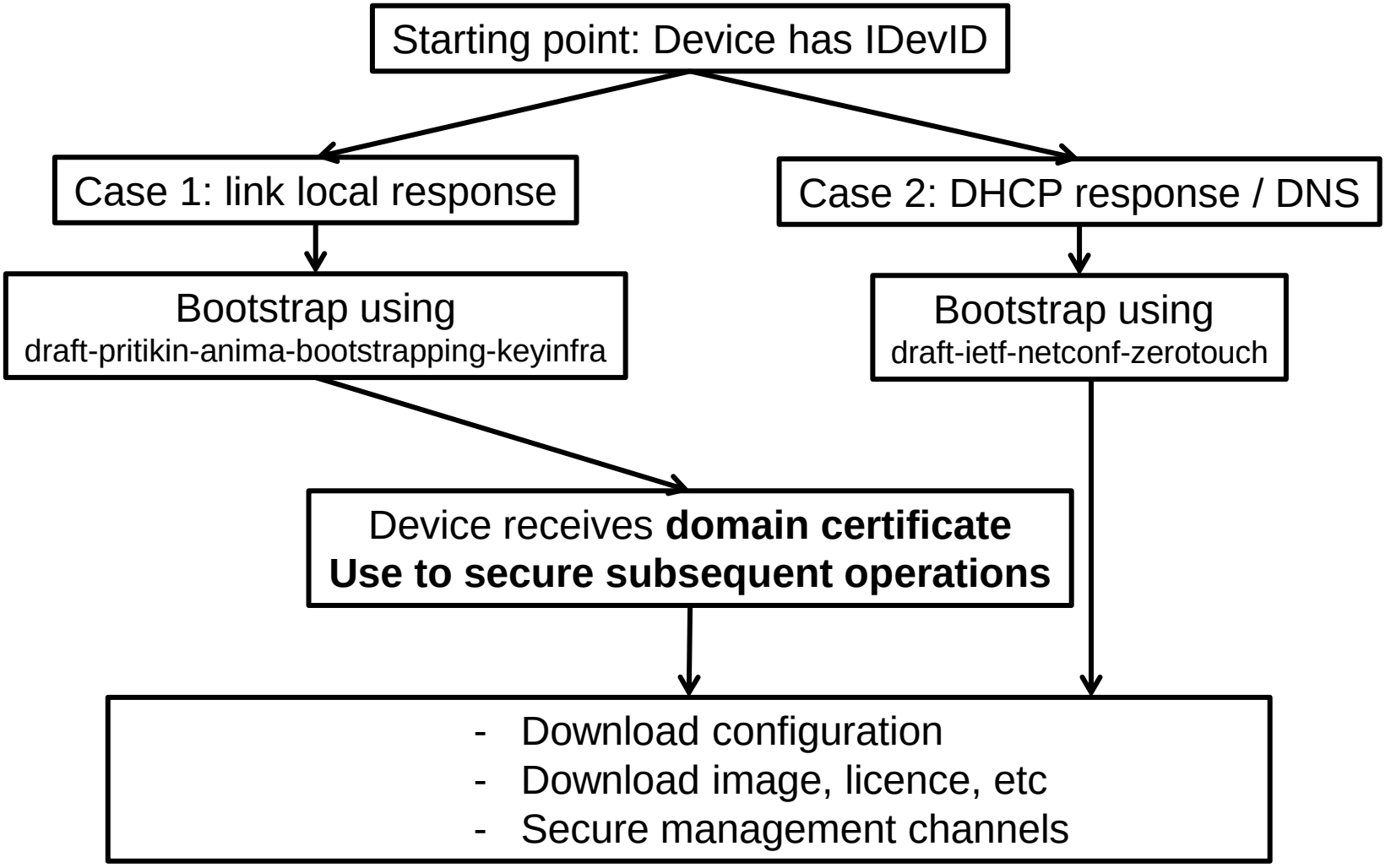
Applicability: Homenet (a possible scenario)



Discussion

- **Approach relies on a link local proxy device**
  - **Need another approach when such a proxy not available**
    Ex: draft-ietf-netconf-zerotouch
- **Still needed:**
  - **Protocol Discussions**
  - **Cover the case where vendor MASA no longer available**
    - **Solution: Trust anchors from various MASAs**
  - **Description on how symmetric schemes are supported**
- **Applicability drafts for target architectures:**
  - **Homenet (draft-behringer-homenet-trust-bootstrap)**
  - **6tisch**
  - **Others…**

Relationship with draft-ietf-netconf-zerotouch: Today



Relationship with draft-ietf-netconf-zerotouch: Possible joint approach