ANIMA
BRSKI

Bootstrapping Remote Secure Key Infrastructure

An option for HOMENET security

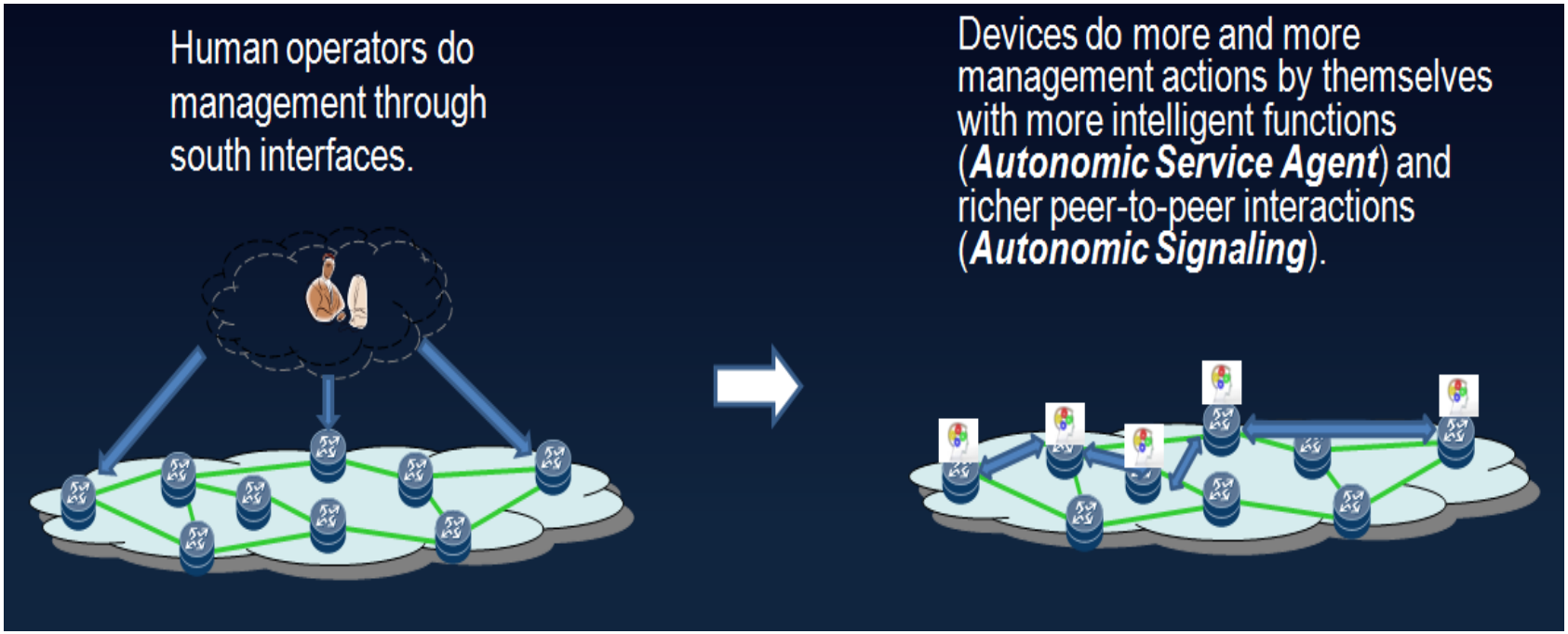
Michael Richardson
mcr+ietf@sandelman.ca

https://www.sandelman.ca/SSW/ietf/meeting/ietf101/ietf101_anima_brski_homenet

Slide from Leo Liubing

Anima's approach towards autonomics

- **A**utonomic **N**etworking **I**ntegrated **M**odel **A**pproach
- "Integrated Model Approach" indicates that Anima is not a "Clean Slate"; rather, it could be integrated into current networks (e.g. co-exist with NMS/SDN).
- According to current charter, Anima aims at developing some "re-useable components", which means some common technologies that could be used among different scenarios.



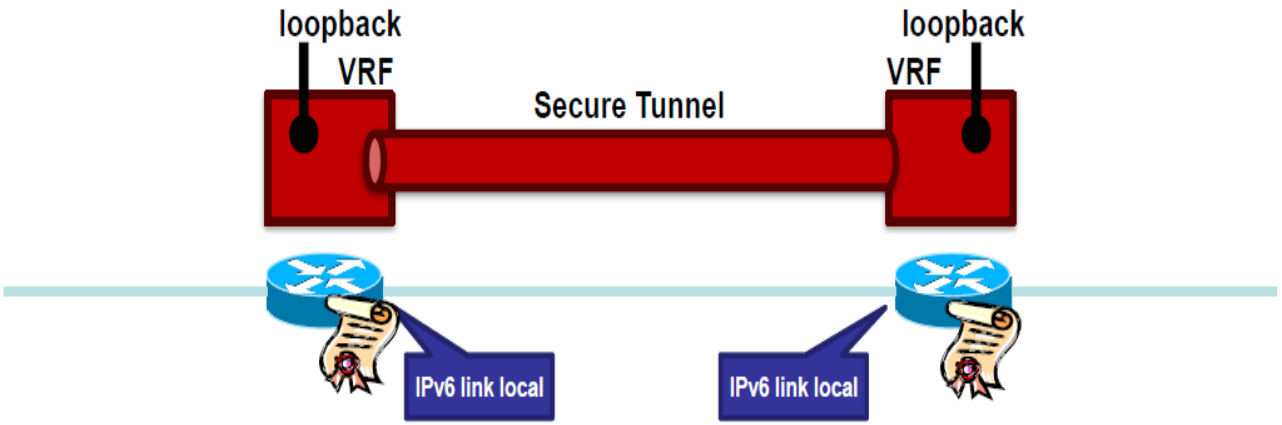
Slide from Leo Liubing

Two Anima Groupsets: ANI & ASA

- **ANI (Autonomic Network Infrastructure)**
  - Three fundamental functions
    1) Secure bootstrap (aka. BRSKI)
    2) A secure and dedicated channel (VPN) for management/control (aka. ACP)
    3) A generic signaling protocol (aka. GRASP)
  - Could be used by most of the scenarios
  - Started at the initial stage

- **ASA (Autonomic Service Agent)**
  - Specific functions regarding to various configurations/services
  - Run on top of ANI
  - Use GRASP for communication
    - Need defining GRASP options (called “Objectives” in GRASP) for each kind of service

Self-Creation of the Autonomic Control Plane
6) Addressing



- Auto-create IPv6 loopback address
- Suggestion: Use IPv6 ULA
  - Global ID: Hash of domain name
  - Subnet and interface ID: Device specific, unique in network
    - Derive from device name, or
    - Assign at time of first registration of device

Copied from https://www.ietf.org/proceedings/92/slides/slides-92-anima-7.pdf

How to bootstrap trust?

- Devices come out to the box with a trust anchor linking them to the manufacturer.
- End user convinces manufacturer that device belongs to them, and manufacturer issues voucher: see draft-ietf-anima-voucher
- Device now trusts end user
  - How is end-user identified? (Issue for later slide)

Join (Enroll) Problem

How to securely let new devices into a network without destroying the network.

- The goal is to provision new nodes with certificates, at which point “traditional” methods may be used to secure network (802.1x/EAP)
- Nodes are uninitialized
- They are “drop shipped” directly from the warehouse.

Why not use EAP?

- Why didn’t you use 802.1x/EAP/PANA?
  - Hasn’t it “solved” this problem?

- Well… no.
  - EAP is a mechanism to get a network key, or authenticate an existing node.
  - BRSKI is about both *finding* the right network, and getting the credential that you’d need to do a 1x method.

- We also want to do this for the *routers* and *switches* that will be providing 1x services later on. The authenticator/authentication-server back-haul is usually radius, and requires at a minimum, a secret to be configured. It’s also often stateful. We felt that there were too many conflicts with existing 1x uses.

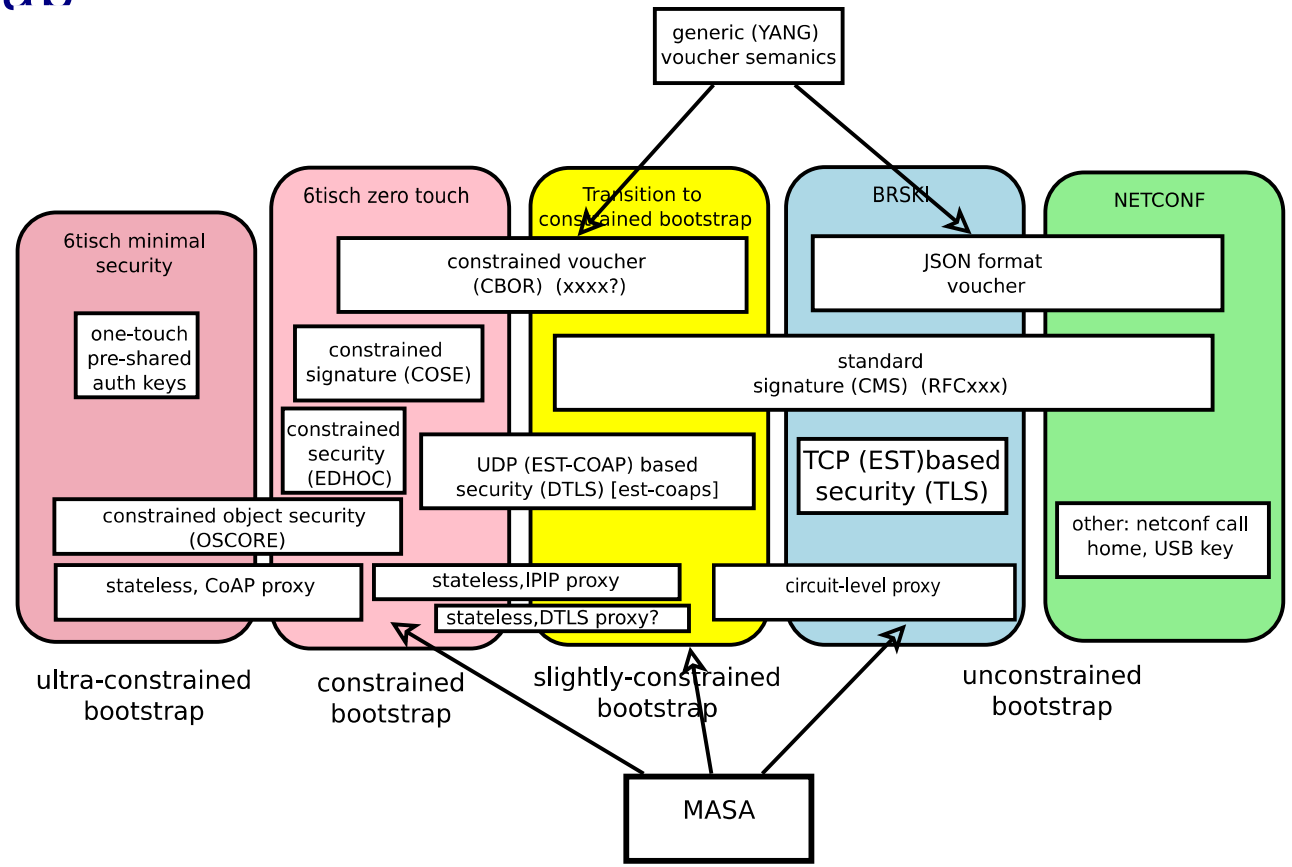
Enrollment at IETF

(many things in many places)

- From draft-richardson-enrollment-roadmap-01 – Iot-dir suggested a wiki for now
  - https://trac.ietf.org/trac/int/wiki/EnrollmentRoadman
-

Insert homenet Enrollment Story

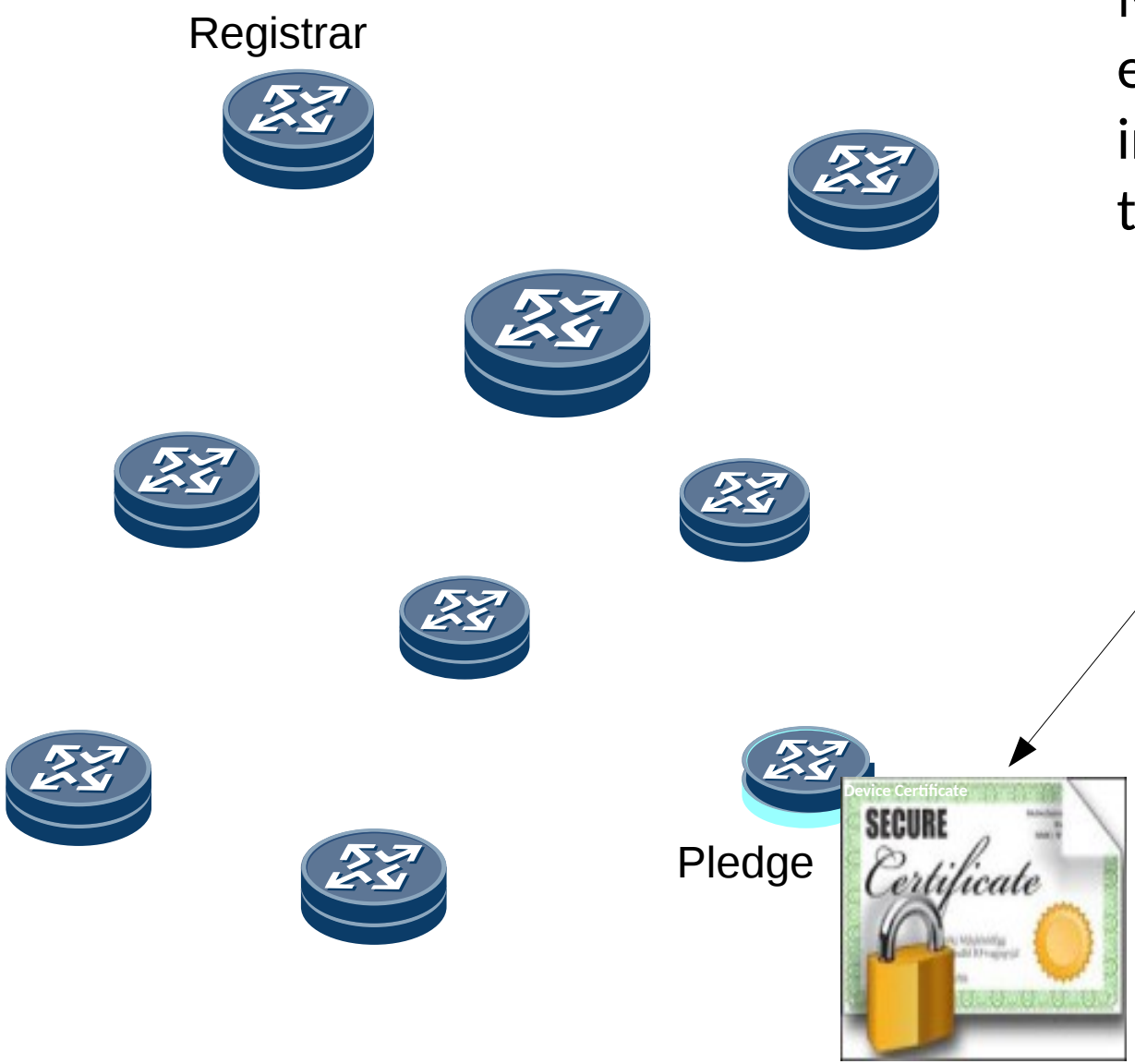
Add To Diagram



Bootstrapping Remote Secure Key Infrastructures (BRSKI)
New Device getting Online

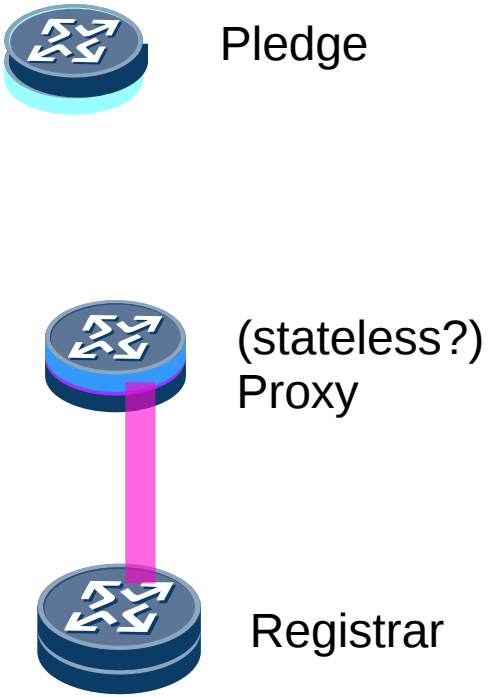
Slide from Leo Liubing

- Every device that supports ANI MA Bootstrapping is pre-installed a device certificate, which is in the form of 802.1AR certificate.



Terminology – synchronized/negotiated between ANIMA, 6tisch, and NETCONF

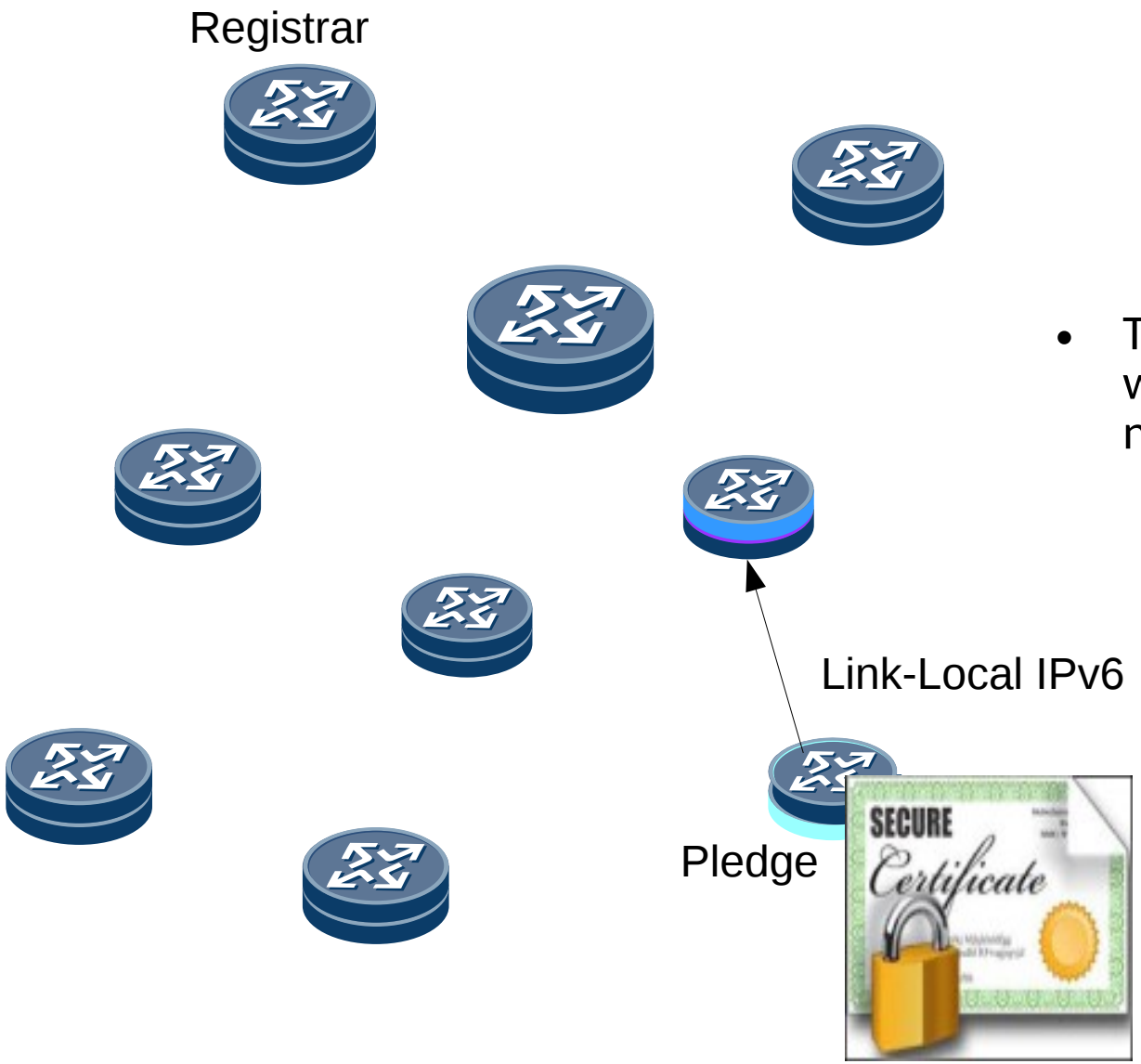
- PLEDGE: the new device
- Join Proxy: the helper.
- Join Registrar/Coordinator(JRC)
- Sometimes s/Join/Enrollment/
  - Because ROLL people use the world “Join” in a different context.



Slide from Leo Liubing

Connects to BRSKI Join Proxy

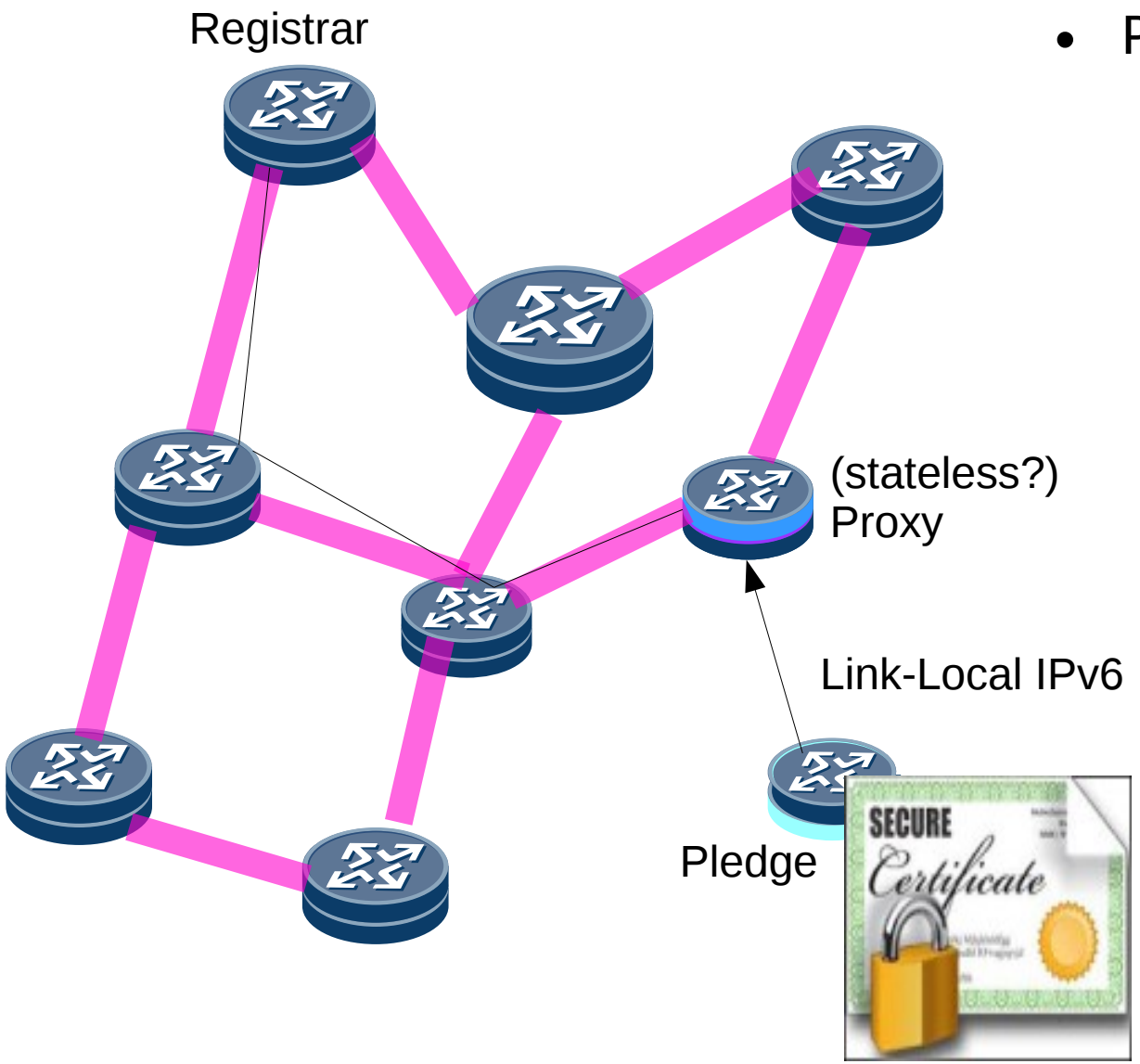
- Every device that has already got online ac ts as a BRSKI Proxy by default.
  - They broadcast the GRASP Flood me ssages periodically so that they can b e found.
  - (New device can remain sealthy)
- The new device chooses one proxy which will relay the communication between the new device and the Registrar.



Slide from Leo Liubing

Enrollment to the Registrar

- Registrar authenticates device using IDevID certificate.
- Pledge
  - They use EST protocol for se cure certificate exchange.(ES T: Enrollment over Secure Tr ansport, RFC7030)



Vouchers

```
module: ietf-voucher
  yang-data:
  voucher-artifact
      +---- voucher
         +---- created-on                       yang:date-and-time
         +---- expires-on?                      yang:date-and-time
         +---- assertion                        enumeration
         +---- serial-number                    string
         +---- idevid-issuer?                   binary
         +---- pinned-domain-cert               binary
         +---- domain-cert-revocation-checks?   boolean
         +---- nonce?                           binary
         +---- last-renewal-date?               yang:date-and-time
```

```
{
  "ietf-voucher:voucher": {
    "created-on": "2016-10-07T19:31:42Z",
    "assertion": "logged",
    "serial-number": "JADA123456789",
    "idevid-issuer": "base64encodedvalue==",
    "pinned-domain-cert": "base64encodedvalue==",
    "nonce": "base64encodedvalue=="
  }
}
```

Signed with CMS
(CBOR+COSE soon)

Things Homenet does not need

- ACP is overkill
  - Just use BRSKI
    - 6tisch join/enrollment process will do that
- Intent-based policy
  - But ANIMA hasn’t got it anyway, and SUPA is dead,
    - Intent is implicit in HOMENET anyway.
- Maybe even PK*I* is unnecessary
  - Just use the secure transport to exchange PSKs, or exchange RPK.
    - BRSKI with vouchers to make secure transport.

Things HOMENET probably wants

- Vouchers
- Integration of BRSKI + MUD
  - MUD might be the “killer” app that makes this worth it.
    - Manufacturer Usage Description Specification
    - https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/
- Manufacturer involvement!
- “push-button” extensions (see section 6) to BRSKI to operate with reduced security.

Challenges for HOMENET

non-professionally managed network --- no infrastructure!

- “unprofessional”? “amateur”? “un-managed”?
  - Key is probably that infrastructure is very hard to fund.
- So… who/what will run the Join Registrar (JRC)?
  - Is there any PKI?
  - If so, what happens when the PKI machine is replaced?
    - Perhaps, quite abruptly.
    - His/Her JRCs?

- Interactions with “SmartHome”, etc. IoT things.
  - Having BRSKI would be good, as it would provide an anchor in the home.
  - Maybe IoT network will provide JRC?
- What is the fallback when there is no JRC?
  - Chicken and egg situation
- Can the Join Registrar be cloud-located?
  - Can it be outsourced?

Layer-8 and layer-9 issues

- Relates to entire HOMENET challenge: who is gonna pay for ongoing maintenance?
  - Does the end-user want to be beholden to that entity?
- Is there a fax-effect we are missing?
  - Can providing HOMENET security enable other things?

While often an IETF tradition to claim this is out of scope, too many of our good ideas die because we did not figure how the incentives would work

If the home user is in fact the “product” for another entity, we might want to think hard about privacy issues sooner.

Some additional thoughts/hopes
http://hubofallthings.org/

- Aims to be a place to keep one's personal data, self-owned.
- Seems an obvious place for a JRC function!
- Currently cloud-based, for pragmatic reasons.
  - London based, some cross-over of people
- Suffers from same layer-9 issues as HOMENET

My experimental JRC/hubofallthings

- OxDroid HC1 (2cm x 5cm), with old laptop HD.
  - HD is superfluous, but is the “media” container.
  -
- Functionally identical, GnuBEE home NAS, but better packaging.
- Good for hacking, but how to get one into every household?
  - A regular homenet problem!
  - Pushing string.

How to proceed - 1

- Finish current work!
- Help ANIMA and 6tisch review our current documents.
  - Are there MUST NOTs that you think would have to change for Homenet?
  - SHOULDs which HOMENET can not do, likely are less of a problem.
    - Write a profile

How to proceed – 2 - profile

- Write a profile of BRSKI for HOMENET.
  - Do you want full BRSKI (HTTPS, JSON format vouchers + CMS signatures)
  - Or constrained voucher (CoAP +{DTLS,EDHOC}, CBOR format vouchers, COSE signatures)
  - May have to support both to enable the “home office” to use enterprise equipment, while still speaking to IoT.
  - What kind of join proxy will you make MTI?
    - BRSKI default is **stateful**, trivial to code (just a “port forward”), constrained default is **stateless**, a bit harder to code.
      - Type of proxy used is between Proxy and JRC; Pledge does not change.

How to proceed – 3 – Legacy/fallback considerations

- Figure out what a BRSKI-HOME device will do in a legacy home.
  - Probably call home with NETCONF zero-touch!
  - If it is too good, maybe that’s all that will ever occur.

Questions/Discussion

?

Michael Richardson
mcr+ietf@sandelman.ca

https://www.sandelman.ca/SSW/ietf/meeting/ietf101/ietf101_anima_brski_homenet

How to proceed – step 0
find cool acronym (an IETF tradition)

- Find a way to expand the acronym
  - Suggestion: “RADLER”
    - a nice summer beer (BRSKI) with grapefruit juice
  - Remote ADder for Lots of Exciting Routers