Status

• Goal: Zero-touch join protocol, inspired from ANIMA BRSKI work.

• News:
  – ANIMA voucher document (“ownership claim token”) is almost in WGLC. (GRASP is in RFC-editor queue)
  – ANIMA BRSKI document was rewritten in April/May, and is much more readable.
  – Area Directors will find a home for EDHOC this week.

•
Status – Next Steps

• Rewrite dtsecurity-secure-join to parallel BRSKI document with:
  – TLS → EDHOC,
  – HTTP → CoAP
  – minimal-security Join Request bootstrapped

• There should be a virtual 1:1 between sections in BRSKI and dtsecurity-secure-join.
  – This could result in some empty sections: tell me this makes sense.
  – The title should change to include the words “zero-touch”
Related documents: Enhanced Beacon

- IEEE802.15.4 Informational Element encapsulation of 6tisch Join Information
- draft-richardson-6tisch-join-enhanced-beacon-01
- Authors: Michael Richardson and Diego Dujovne.
  - Awaiting WG adoption.
  - Enhancements suggested by 6tisch minimal to permit 0xff join preference to indicate “turn off join” (proxy).
Related documents:

• Minimal Security rekeying mechanism for 6TiSCH
  – draft-richardson-6tisch-minimal-rekey-02
• Authors: Michael Richardson, Peter van der Stok.
  – Needs revision and work.
  – Intended to be COMI based, using keys setup from minimal-security and/or EDHOC. Details of keying are not yet stable.
• Covers case of network that either lives long enough to need a rekey, or any network that might need to remove a malicious/p0wned node from it’s network.
Some details: zero-touch

0. 802.11AR
   IdevID
   Installed in factory

1. Voucher request

2. (signed) Voucher

3. Voucher validated
Some details: ANIMA BRSKI

1. Voucher request

2. (signed) Voucher

3. Voucher validated

pledge

EST(TLS) proxy

JRC

MASA

Manufacturer

0. 802.11AR

IdevID

Installed in factory
Some other contrasts

6tisch

- Pledge discovers Proxy vis Enhanced Beacon
- Proxy provisioned with Pledge address via JoinRequest
- CoAP/EDHOC/OSCOAP

ANIMA/BRSKI

- Pledge discovers Proxy vis GRASP M_FLOOD
- Proxy discovers JRC via GRASP
- TLS/EST
  - Leading to LDevID, and creation of ACP.
BRSKI diagram from TXT

```
+------------------------+
| Vendor Service        |
| +--------------------+
| | Manufacturer       |
| | | Authorized       |
| | | Ownership        |
| | | Signing           |
| | | Authority        |
| | +------------------+
| V
| +------------------------+
| | Pledge               |
| | | Circuit            |
| | | Proxy              |
| | | Domain             |
| | | Registrar          |
| | +-------------------+
| | X.509               |
| | | IDevID             |
| | | | Key Infrastructure|
| | | | {e.g. PKI Certificate|
| | | | Authority}        |
| | +--------------------+

"Domain" components
```