draft-richardson-6tisch-dtsecurity-secure-join-00

Michael Richardson
+ authors TBD
Status

• Secure join design team rebooted May 2016.

• -00 ID posted this week. Outline created, expect to do motivation/problem statement as Introduction.
  – Kramdown for draft, at: https://github.com/ietf-roll/6tisch-secure-join

• Design team meets every two weeks, on Wednesdays at 1400UTC via JITSI.
Draft outline

- Introduction
  - Terminology
  - Credentials
    - One-Touch Assumptions
      - Factory provided credentials (if any)
    - Credentials to be introduced
  - Network Assumptions
  - Security above and below IP
    - Perfect Forward Secrecy
  - Join network assumptions
    - Number and cost of round trips
    - Size of packets, number of fragments
  - Target end-state for join process
- Diagram of Join Process
  - Description of States in Join Process
- Protocol Overview
  - New node announcement
    - use of EARO messages
    - Proxy to JCE
  - JCE initiates to new node
  - Use of ACE Token for Ownership
- Security Details (Security protocol? Security process?)
  - Security options
    - EDHOC and OSCOAP
    - DTLS/CoAP
    - ???-insert-yours
  - Forward Secrecy
    - Rekeying of networks
    - Rekeying of nodes
    - Per-link key
  - Node decommissioning
    - Voluntary Revocation
    - Emergency Revocation
    - Expulsion of hostile node
- Certificates and Authorizations
  - Assymetric credentials
    - chain of certificates from vendor trust anchor to network operator
    - possession of public key (resurrecting duckling model)
    - Symmetric credentials
  - Use of ACE Token for Ownership
Draft outline

- Introduction
  - Terminology
  - Credentials
    - One-Touch Assumptions
      - Factory provided credentials (if any)
    - Credentials to be introduced
  - Network Assumptions
  - Security above and below IP
    - Perfect Forward Secrecy
  - Join network assumptions
    - Number and cost of round trips
    - Size of packets, number of fragments
    - Target end-state for join process
  - Diagram of Join Process
  - Description of States in Join Process
  - Protocol Overview
    - New node announcement
      - use of EARO messages
    - Proxy to JCE
    - JCE initiates to new node
    - Use of ACE Token for Ownership

- Security Details (Security protocol? Security process?)
  - Security options
    - EDHOC and OSCOAP
    - DTLS/CoAP
    - ???-insert-yours
  - Forward Secrecy
    - Rekeying of networks
    - Rekeying of nodes
    - Per-link key
  - Node decommissioning
    - Voluntary Revocation
    - Emergency Revocation
    - Expulsion of hostile node
  - Certificates and Authorizations
    - Assymetric credentials
      - chain of certificates from vendor trust anchor to network operator
      - possession of public key (resurrecting duckling model)
      - Symmetric credentials
    - Use of ACE Token for Ownership