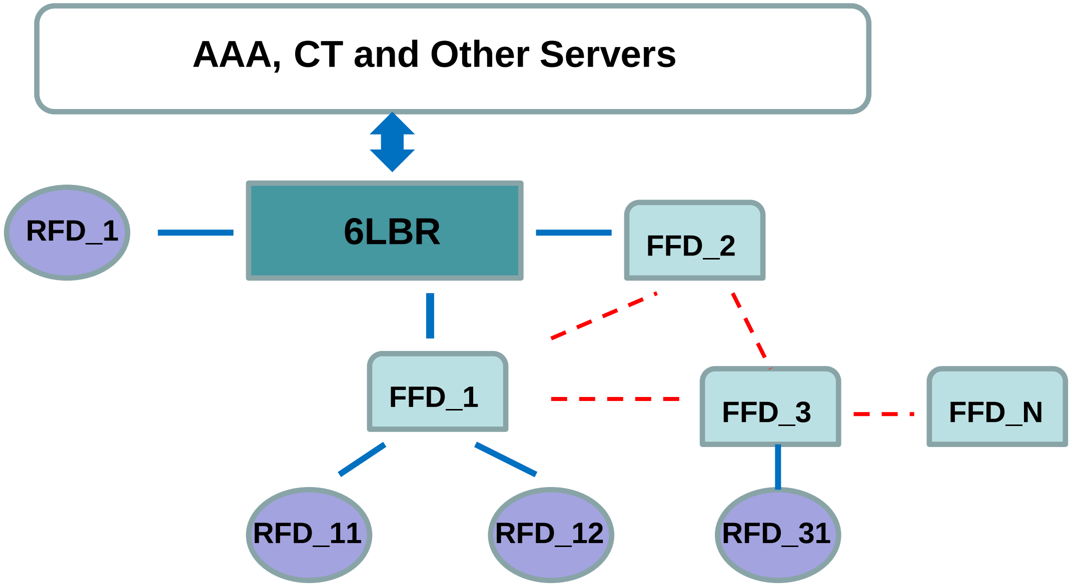
IoT Security Bootstrapping: Survey and Design Considerations

draft-he-6lo-analysis-iot-sbootstrapping

Ana(Danping) He	ana.hedanping@huawei.com
Behcet Sarikaya	Sarikaya@ieee.org

What is the Problem?



IEEE 802.15.4
Low rate, Low power
Different types of devices
Mix topologies: star, mesh, cluster-tree

Users are not experts
Devices without sufficient input interface
Scale can be large

Protocols e.g. 6LoWPAN ND, IPv6 over 802.15.4, RPL, AODV, DSR, DTLS, CoAP can be selected for different applications

Security self-bootstrapping is fundamental to Self-Organizing IoT

A new device joining the network securely
The bootstrapping of all other information can be conducted securely

What is Proposed So Far?

- **[I-D.pritikin-anima-bootstrapping-keyinfra]** EAP-EST, EAP-TLS, 802.1X, EAP-IKEv2 for 802.1 AR certificate
- **[I-D.kwatsen-netconf-zerotouch]** Same authentication methods can be used for X.509 certificate
- **[I-D.struik-6tisch-security-considerations]** Undefined joining protocol for certificate
- **ZigBee IP stack based Smart Energy** EAP-TLS, PANA for certificate
- **[I-D.sarikaya-6lo-bootstrapping-solution]** EAP-TLS for Raw public key
- **[I-D.he-iot-security-bootstrapping]** EAP, PANA for various credential material
- **[I-D.kumar-6lo-selective-bootstrap]** DTLS for various credential material, order selected by Commissioning Tool (CT)

What is the credential issue?

- **Certificate:**

  high security, mutual authentication, PKI infrastructure, (de)centralized architecture, high computation and communication cost, should avoid complex trust dependency and circular dependency

- **Raw public key/self signed certificate:**

  high security, no authentication, decentralized architecture, high computation and communication cost

- **Pre-shared key:**

  high security, mutual authentication, decentralized architecture, low computation and communication cost

- **Product installed code(?) Thread Group:**

  high security, one-way authentication, centralized architecture, low computation and communication cost

How should a good design be like?

- Able to clearly define security dependency and trust domains
    - Clear Security dependency
    - Mutual authentication
    - Agreement on security association
- Cross-layer design
    - Security bootstrapping in collaboration with other layers is likely to produce a comprehensive solution.
- Reduce human interaction to the minimum
- Able to resist attacks
- Low computation cost and communication overhead

What remains to be done?

- 802.1AR certificates or something else to authenticate?
- Need AAA server or CT?
- EAP-IKEv2 supports multiple credential materials, should we use it?
- Bootstrap first and then configure IP or
- IP and untrusted routing before device authentication and key distribution
- A single default solution for all cases or different solutions for each environment?
- → We need a standard solution/solutions
- → 6lo to work on this?

Thank you!

Any Comments?

Ana(Danping) He	ana.hedanping@huawei.com
Behcet Sarikaya	Sarikaya@ieee.org