Bootstrapping Key Infrastructures

Max Pritikin

IETF 95, 4 April 2016

Summary of Diffs 01 - 02

- Named the protocol “BSKI”
- s2 Clarified ‘proxy’ role
- s3 Normative choices made for functional flow
- s3.2 Expanded Proxy discussion
- s3.2.1 CoAP discussion begun
- s5.1 Expanded client identity discussion
- s6.1 Added some trust model discussion
- A bunch of text clarifications etc

Upcoming Discussion items

- Proxy/CoAP methods to be finalized
- Finalize json message formats

  Including “ownership voucher” which is undefined by NETCONF
- s5.4 Initial configuration distribution

  – example: AN-Domain-ID or info for certificates

  This section has been a place holder and final role/integration needs to be decided
- Incorporate lessons from implementation experience

MASA Log discussion item

- The MASA log provides a privacy protected global log of the device imprints. There are implementation choices:

1. The MASA service is a fully trusted entity. It simply logs and is trusted to not mess up. **This is the current method of the draft.**

2. The MASA service NOT trusted. It logs using a “certified log” approach, like a Merkle hash tree, and can be checked.

3. A distributed logging mechanism using buzzword compliant block chains etc could be used.

[[EDNOTE]]s

- During your reading any paragraph called out with this tag is soliciting your feedback!
- s5.1 EAP-EST is a mistake. Consider it deleted.