DOTS Identities

Identities for Trusting DOTS communications

IETF 97
Seoul, KR
November 18, 2016
Robert Moskowitz
HTT Consulting

draft-moskowitz-dots-identities-00.txt

What is the problem?

- In DOTS Requirements, SEC-001:
  - Peer Mutual Authentication
- MOST of IETF protocols rely on Public Key Signing to perform mutual authentication
  - TLS, DTLS, IKE, HIP
- Two models for Public Key Signing
  - X.509 and Raw Public Keys
- Machines are not good at interacting with CA registration systems designed for people
  - Manually intensive for a person to install a certificate into a machine
- How to scale and manage and trust Identities

What is needed

- A certificate enrollment process
  - Machine orientated, but associated with the business subscription process
- Support for devices that can’t/won’t support full X.509
- Business specific PKI along with web trusted list model
- Inter business trust modeling

Draft Status

- Lots of place holders that only I know about
  - Hey, it is a -00 draft!
- Updated draft well before Interim call
- Open to other contributors

What IS in the draft

- Heavy biased to IEEE 802.1AR
  - Many vendors are implementing TPM and 802.1AR
  - Work in other areas for ‘affordable’ trusted store
  - Some attempt at enrollment
    - BRewSKI and zeroconf and 7030
- Intention of a single PKI per DOTS provider
- Support for RawPublicKey methods

What IS NOT yet in the draft

- Complete certificate enrollment process
  - 802.1AR and other certificates
- Inter-provider trust model
  - Prefer Bridge CA model
  - DANE has been mentioned
- Recommendations on LDAP or other trust lists
  - For non-business PKI
  - For RawPublicKey
- Probably other stuff

Next steps

- Rev the draft
- Get draft accepted by wg

DISCUSSION