XMPP DNA

IETF 83

Matthew Miller

Existing Work

draft-hildebrand-dna-00 (2009/10)

draft-ietf-xmpp-dna-00 (2010/01)

draft-barnes-dna-00 (2010/08)

draft-ietf-xmpp-dna-01 (2011/03)

The Problem

How to trust a connection is authorized for traffic intended for a given domain

Building Blocks

- Determine Trust
- Delegation & Piggybacking

Approaching Trust

- Multiple approaches
- well-defined belief suspension

Proof Types

- DANE
  - certificate from TLSA _xmpp-server._tcp.capulet.lit
- HTTPS/.well-known
  - certificate from HTTPS://capulet.lit/.well-known/_xmpp-server._tcp...
- PKI
  - cache all the names

Approaching Delegation

- stream:feature to signal “don’t freak out”
- Connection has a “allowed-names” list
- start empty, signal for additions

Signaling Delegation

- dialback
  - maybe without keys 
- what about c2s?

Outcomes

- “federation” document
- DANE proof type document
- HTTPS/.well-known proof type document