XMPP DNA

Matt Miller / Peter Saint-Andre

IETF 88 – Vancouver

Draft Changes …

~~draft-saintandre-xmpp-dna~~

→ draft-ietf-xmpp-dna

~~draft-miller-xmpp-posh-prooftype~~

→ draft-miller-posh

~~draft-miller-xmpp-dnssec-prooftype~~

→ draft-ietf-dane-srv

POSH BoF

“I read your draft, but didn’t understand it.”

- Held in Berlin
- Helpful feedback incorporated
  - Detail the problem
  - Two modes (pointer vs. keys)
  - Hash instead of cert chain
  - Expiration hints

Early POSH Implementations (version -01)

- Prosody module
  - Verify server-to-server
- psyced (fippo's branch)
  - Verify server-to-server
- node-posh
  - Generate keys documents
  - Verify POSH keys document

DNSSEC/DANE

- Some advice incorporated into DANE WG draft …
- … which has expired
- Contacting DANE WG chairs about progressing

DNA

- Incorporated lessons from POSH
  - Clearer intro
  - Better order of operations
  - IANA registrations
- Dependent on DNSSEC/POSH
  - … or is it?
- Waiting on implementation feedback

Next Steps

- Finish up POSH
- Finish up DNSSEC/DANE
- Implementations and Feedback
  - Actively soliciting implementations
  - Actively soliciting feedback