Domain Name Associations

Peter Saint-Andre & Matt Miller
XMPP WG
IETF 86, Orlando
What is DNA?

• Framework for determining server identity and achieving secure delegation

• Various “prooftypes” (PKI, DANE, POSH...)

• See draft-saintandre-xmpp-dna

• Q: specify one or more prooftypes as MTI?

• Q: specify a way to signal which you support?
Multi-Domain Support

• Basically, use a prooftype (PKI, DANE, POSH...) for the first domain pair

• After that, use Server Dialback to assert / “suppose” another domain pair over the existing stream (checked using DNA rules)

• This enables us to drastically reduce the number of TCP connections for s2s
Server Dialback

• Originally in RFC 3920, now in XEP-0220
• In 3920, not an authentication mechanism
• In DNA, not a prooftype
• As noted, used only to assert / “suppose” subsequent domain pairs
• Q: re-use OK in various scenarios? (see draft-saintandre-xmpp-dna)
Proofotypes: PKI

- Proof is a PKIX certificate
- Verification material from trusted root
- Secure delegation via signed SRV records
- Follow the existing rules from RFC 6120 and RFC 6125
- Can be hard to deploy (e.g., virtual hosting)
Prooftypes: DANE

• Proof is a DANE cert / fingerprint
• Verification material from DNSSEC lookup
• Secure delegation via signed SRV records
• See draft-miller-xmpp-dnssec-prooftype
• Q: merge with draft-ietf-dane-srv?
Proofotypes: POSH

• “PKIX Over Secure HTTP”
• Proof is a certificate in JOSE format
• Verification material from HTTP URI
• Secure delegation via HTTPS redirect
• See draft-miller-xmpp-posh-proofotype
Next Steps

• Close the open issues
• Incorporate feedback from Philipp Hancke (and, we hope, others!)
• Experiment with code and deployment
• Are these three I-Ds acceptable starting points for the charter items?