Intro to DNA

Joe Hildebrand

XMPP WG, IETF 76, Hiroshima
Domain
Name
Assertions

• Delegate hosting your domain?
• Typical X.509 identities are not enough
  • Secrecy/liability of private keys
• Scale
Dramatis Personæ

- Alice owns `alice.example`, running an XMPP server
- Bob owns `bob.example`, running an XMPP server
- Cho owns `cho.example`, running a hosting provider for XMPP
- Dho owns `dho.example`, running a hosting provider for XMPP

Note: “own” is shorthand for both controlling the DNS for the domain and being able to get a widely-trusted CA to sign a cert for you with that domain name in it.
Alice talks to Bob (today)

• Alice and Bob host their own XMPP servers on their own machines

• SRV, X.509 tie identity to each end of a connection

• One connection each way

• Each check “from” addresses to
Today

From Alice, To Bob

From Bob, To Alice
Alice Decides to Host with Cho

- Alice trusts Cho to protect her data, within reason
- Alice points her SRV to Cho’s machine
- Alice’s private key?
  - Cho doesn’t want it (potential liability)
  - Alice doesn’t want to give it (secret)
Today, with hosting
DNA: Alice gives Cho a “Proof”

- Safe for Cho to hold
- Proves to Bob that Alice trusts Cho
- First proof defined is Attribute Certificates
- Proofs are extensible
Cho: I’m Alice
Bob: Prove it!
Cho: Here’s my AC
Bob: Hiya, Alice!
Bob Decides to Host with Dho

- Without DNA:
  - Two sockets per domain pair
  - Remember: identity tied to connection
- Cho and Dho both host many domains
  - Example: 10k * 10k * 2 = 200M sockets!
- >one should be deployment choice
DNA: Scale

Cho: I’m Alice
Dho: Prove it!
Cho: Here’s my AC
Dho: Hiya, Alice!
Dho: I’m Dave
Cho: Prove it!
Dho: Here’s my AC
Cho: Hiya, Dave!

Bob
Dave
Deployment Choice

- One socket?
- Socket per cluster?
- Socket per data center?
- 10 sockets, for queuing?