DANCE into _user space

Rick van Rein
rick@openfortress.nl

Usage patterns for DANCE

- _device for hardware
- _user for human users (and services)

- _device identity 1:1 mapped into DNS
- _user identity is mapped via a CA

Indirection via a CA

- Domain-controlled root certificate
- DNS(SEC) validates the root CA

- Quick offline update to the user base
- DNS can be iterated, userid should be private

Client Certificates

- Hold a uid attribute [RFC4519, LDAP]
- Stored in subjectAltName
- *Not quite sure:* Is this proper use of this field?

Example Use

- Connect to LDAP with DANE Client Identity
- dane_clientid must be ok and start with “_user.”
- TLSA lookup for CA, included in TLS cert req
- Client ID ends in @ with domain (less “_user.”)
- LDAP receives Client ID via SASL EXTERNAL

Useful about this Pattern

- SASL-within-TLS works for many protocols
- User ID setup is each domain’s prerogative
- This is a pattern for Realm Crossover
  - Never met you before, nice to know who you are
- Allows fine Access Control (data privacy!)
- Authentication as a common global pattern

Optional Extras

- Named services under a domain
- S/MIME certificates for email sign/crypt
- ENUM infra for user/phone certification