IETF dance update

oej 2022-11-08
Three wg documents

- draft-ietf-dance-architecture-00
- draft-ietf-dance-client-auth-00
- draft-ietf-dance-tls-clientid-00
My vision

Dancing
TLS changes
How to dance
Dancing with XXX

Architecture
Secure dancing
Requirements on protocol implementations
Protocol-specific dances
Architecture-xx is a mess

• A mixture of a lot of things

• How do we clean it up?

• Some protocol-specific parts need to become separate "protocol-specific" or "implementation-specific" docs, like IoT
DNS trees

- Most of our docs document a flat namespace
- DNS gurus suggest a more hierarchical namespace, like ENUM or PTR records
- For me, this is "how to dance"
Privacy

- If we’re looking at using Dance for protocols with email style addresses, then we can’t use the URI as the index in the DNS

- Check RFC 7929 (DANE/OpenPGP) for hints

For example, to request an OPENPGPKEY resource record for a user whose email address is "hugh@example.com", an OPENPGPKEY query would be placed for the following QNAME: "c93f1e400f26708f98cb19d936620da35 eec8f72e57f9ee0c01c1af6._openpgpkey.example.com". The corresponding RR in the example.com zone might look like (key shortened for formatting):

```
c9[...].d6._openpgpkey.example.com. IN OPENPGPKEY <base64 public key>
```
Reorganize

• Make "draft-huque-dane-client-cert-08" into a DANCE implementation requirement document - "how to dance"

• Find candidates for protocol specific documents - "Dancing with xxx" and find energy there

• Focus where there’s energy

• We need one for _service and one for _device at least, if we still want them both

• Are there other patterns to explore on how to code an identity into a DNS name?
Time to code?

• Ash had some code somewhere

• Demo with Curl (libcurl) + Openssl + <server> ?

• Demo with <COAP library> ?

• Dance extension needs to exist in libraries in order to become successful and used.