DNSSEC validation chain TLS extension (draft-ietf-tls-dnssec-chain-extension)

Melinda Shore, Willem Toorop, Shumon Huque, Richard Barnes

November 17, 2016

Summary & status

- Deliver a DNSSEC validation chain in a TLS extension, eliminating DNS round-trips
- We need to finish up:
  - record ordering
  - client certificate
  - TLS 1.3
- We believe the document will be ready for WGLC before Chicago

record ordering

- validation order is not always possible because of CNAME and DNAME indirection
- but we need to specify what the server needs to use as the first RRset
- Viktor proposed having the server present the records in the order it received them from its own DNS server, or
- collapsing everything into a ”jumbo” packet

client certificates

- see draft-huque-dane-client-cert (expired) for background on client certificates in DANE
- similar to server certificate chain delivery, but extension delivered in Client Certificate message

TLS 1.3

- validation chain delivered in either Encrypted Extensions or in Certificate message (looking for feedback)
- if a client certificate is present, delivered in Certificate message
- implementation depends on availability of TLS 1.3 support in OpenSSL (not sure when 1.1.1 will be released)