Client Authentication Recommendations for Encrypted DNS (CARED)

draft-jaked-cared-00

Tommy Jensen (Microsoft)
Jessica Krynitsky (Microsoft) [presenter]
Jeff Damick (Amazon)
Matt Engskow (Amazon)
Joe Abley (Cloudflare)

Updates since 120

- Edited language to be more precise and define scenario scope
- Added terminology section for “encrypted” vs. “protective” DNS
- More clearly delineate when DNS resolvers and clients SHOULD vs. SHOULD NOT request client authentication
- Formatted normative recommendations into a list
- Recommends mTLS with x.509 certificates and provides considerations for using PSKs
- Calls out TLS 1.3 must be supported

Open Issues

- TBD: what to do with EDSR destinations · Issue #4
- Specify that recommended client auth mechanisms are resistant to replay attacks · Issue #7
  - This is already covered by existing TLS drafts, but may want to include
- Off-list suggestions to add PSKs for IoT use-cases
  - Co-authors want to avoid defininig all possible use cases, but we have added a callout to PSKs
- Some feedback in 120 to remove normatives and refactor to informational draft
  - Without normatives, we would not be able to accomplish our goals of interoperable solutions to locked-down DNS without vendor lock-in
- UTA suggestions to use other HTTP authentication mechanisms
  - Avoid DoH-specific options and mTLS would enable more interoperability

Next Steps

- IETF area chairs have determined this fits best in UTA charter
- Seeking another round of feedback via mailing lists or GitHub
- Call for adoption with UTA? (likely after 1 more iteration)