# Client Authentication Recommendations for Encrypted DNS (CARED)

https://datatracker.ietf.org/doc/draft-tjjk-cared/

Tommy Jensen (Microsoft)
Jessica Krynitsky (Microsoft)
Jeff Damick (Amazon)
Matt Engskow (Amazon)

# Context

- Enterprises are increasing encrypted DNS deployments
- Applying client policy often relies on the client's IP address
- Enterprises want to only allow their own clients to connect
- Addressing both when clients can be work-from-home requires client authentication (or per-client tunnel gateways…)

# Draft in a nutshell

- Requirements considered when evaluating client auth mechanisms:
  - SHOULD be per-connection, not per-query
  - SHOULD use existing open standards
  - SHOULD be reusable across encrypted DNS protocols
  - SHOULD NOT require human interaction to complete

- Rationale: avoid vendor lock-in, optimize for long-running connections, solve the problem once for DoT, DoH, and DoQ, avoid the “click through” effect

# Redefining “secure channel” for DNS64 in RFC 7050

https://datatracker.ietf.org/doc/draft-jens-7050-secure-channel/

Tommy Jensen (Microsoft)

# Context

- RFC 7050 says a client “SHOULD communicate with a trusted DNS64 server over a *secure channel* or use DNSSEC.”

"a communication channel a node has between itself and a DNS64 server protecting DNS protocol-related messages from interception and tampering.  The channel can be, for example, an IPsec-based virtual private network (VPN) tunnel or a link layer utilizing data encryption technologies."

# Proposal

This draft updates RFC 7050 in two major ways:

- Redefine “secure channel” to mean using name-validating encryption such as TLS (such as DoT, DoH, or DoQ) with configuration advertised using DNR (or pre-configured)

- Deprecate/remove the DNSSEC fallback mechanism (an unnecessary complication when “secure channel” is now strongly defined and DNS-associated)