Redefining “secure channel” for DNS64 in RFC 7050

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

Tommy Jensen (Microsoft)

Context

- Jen Linkova and I are writing a CLAT Recommendations draft
  - https://datatracker.ietf.org/doc/draft-ietf-v6ops-claton/
- It talks about when nodes should enable CLAT, the client-side of 464XLAT, which transports IPv4 packets inside IPv6 packets
- RFC 7050 is one way for CLAT to learn the IPv6 prefix needed for CLAT to function by querying a DNS64 server

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."

Problem

- That definition was written before the TLS-based encrypted DNS standards were defined
- We also have network advertisement of TLS-based encrypted DNS server configuration now (DNR, defined in RFC 9463)
- So long as we are writing new drafts that refer to RFC 7050, we should modernize its concept of securing DNS communication

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)

Next Steps

- List discussion kicked off the question of “should we update 7050 or just deprecate use of DNS64 anyway?”
- Should 7050 be updated in some way to update how the communication is trusted?
- If so, is dnsop the right home for a draft on this topic to be adopted?