TLS Working Group Virtual Interim September 14, 2018

NOTE WELL

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.

As a reminder:

- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process),
- BCP 25 (Working Group processes),
- BCP 25 (Anti-Harassment Procedures),
- BCP 54 (Code of Conduct),
- BCP 78 (Copyright),
- BCP 79 (Patents, Participation),
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

Agenda

- Problem statement recap
  - Discuss client-side caching semantics and use cases.
  - Discuss need (or not) for extension pinning.
- Review open gaps:
  - Lack of a port number in the client side of the extension
  - Lack of downgrade protection for existing applications
  - Lack of discussion of virtual hosting
  - Needless complexity from RRset ordering requirements.
- Wrap up

Problem Statement

draft-ietf-tls-dnssec-chain-extension

- What is the fundamental security issue? What is the purpose of this extension?
- Under what circumstances should dnssec_chain be cached and reused for future use?
- Is pinning required? If so, what is pinned, and at what layer(s) should it be implemented?