draft-lmo-dprive-phase2-requirements-01

1. Overview of the draft

   Latest markdown at https://github.com/alex-nicat/ietf-dprive-phase2-requirements/blob/master/draft-lmo-dprive-phase2-requirements.md

2. Update from interim meeting

3. Specific areas of feedback / WG discussion needed

draft-lmo-dprive-phase2-requirements-01

FYI: We will do a gap analysis – looking at Section 5, Perspectives and Use Cases – to see if we are missing any requirements. (And then the section might be possible to move to an appendix with an RFC Editor note that it can be removed later.)

draft-lmo-dprive-phase2-requirements-01

[10 mins]

Is anything missing from Section 4, Threat Model & Problem Statement?

draft-lmo-dprive-phase2-requirements-01

[5 mins]

Is DoT always required? Or is it possible in some use cases to have other privacy-protective mechanisms (e.g. QNAME minimization)?

draft-lmo-dprive-phase2-requirements-01

[15 mins]

Trust anchor/authority: Should this depend only on the DNS, such as DANE, or also on Certification Authorities?

draft-lmo-dprive-phase2-requirements-01

[15 mins]

Downgrade Prevention & Preferences: Should the user (e.g. stub, app, resolver) be able to say only ever use DoT and never downgrade? Or should the authoritative domain be the only one? Or should both be permitted and let the app/stub decide what to do based on that info?

draft-lmo-dprive-phase2-requirements-01

[10 mins – or list if needed]

Discovery: What requirements do we have for a recursive to determine availability of encryption on an authoritative server? (e.g. loose coupling vs. whitelists are okay)

draft-lmo-dprive-phase2-requirements-01

Next Steps:

- We will make all these changes and revise the draft.
- Should this become a WG draft?