MTL Mode Experiments

IETF 118

4-5 November 2023

Prague

Hackathon Plan

- Need easy way to experiment with MTL Mode and evaluate concepts.
  - Leverage new library https://github.com/verisign/MTL which was mentioned as forthcoming at IETF-117 and published recently.

Drafts

- draft-harvey-cfrg-mtl-mode

Note well obligation

Verisign announced a public, royalty-free license to certain intellectual property related to the Internet-Draft

- IPR declarations 6170-6176 give the official language (datatracker link)

What got done

- Demonstrated open-source MTL library and included example application
- Discussed the need for future collaborations
- Discussed how MTL mode works as described in draft-harvey-cfrg-mtl-mode

What we learned

- We are very early in the cycle of growing technical community understanding of how MTL Mode Signatures are constructed and can be used to address use cases where PQC signature size will have adverse impact
- Next Steps
  - Cryptographic Library Integration/Implementation
  - Library bindings for other languages may be useful
  - Create an I-D on using MTL Mode with DNSSEC
  - Seek partners for future hackathon on MTL Mode with DNSSEC
  - Follow-up discussions on other MTL Mode use cases

Wrap Up

Team members:

Joe Harvey

Andy Fregly

<Other links, contacts or notes>