IETF 117 – LAMPS Update for PQUIP

draft-ietf-lamps-cms-kemri-01 is in WGLC. The vast majority of the comments have been resolved, and a few last details are being worked out.

The PQC for PKIX and PQC for CMS documents are simple. We have all the placeholders and we are waiting for NIST to make standards and assign OIDs.

As always, crypto transitions are hard. KEMs are easier than signatures.

Composite KEM is moving along. For those using multiple PKIs, follow draft-ietf-lamps-cert-binding-for-multi-auth.

Composite signatures are not dead, but the problem is significantly harder than expected. This is an area where additional thought and analysis would be helpful.