**From:** Watson Ladd <watsonbladd@gmail.com> via pqc-forum@list.nist.gov
**To:** pqc-...@list.nist.gov <pqc-forum@list.nist.gov>
**Subject:** [pqc-forum] What stops another Red Hat?
**Date:** Thursday, July 07, 2022 02:06:10 PM ET

---

Dear all,

Those of us who tried to get ECC into real working systems during the years before 2018 or so will remember that Red Hat had a uniquely unhelpful attitude towards what it considered patent threats, and it wasn't clear what could have helped. That's despite existing licenses, the RFC 6090 process, etc, and NIST licensing. While many players were satisfied that the patent risk was manageable, Red Hat was not, and it was not possible to convince them otherwise. As a result migrating to ECC was much slower than otherwise.

The existence of a few licenses doesn't mean that other claims aren't out there, and the nonexistence of other claims doesn't mean the risk perception of important entities won't be overly cautious. Unlike with ECC, we need to make a transition and unavailability of the new algorithms will be a problem. Already NIST has indicated that it might switch to NTRU to avoid patent issues, and I am wondering if there is some way NTRU might be added as an alternative to reduce the impact.

Sincerely,
Watson Ladd

--
Astra mortemque praestare gradatim

--