Why P-256 and RSA hybrids are needed in industry

Mike Ounsworth
Entrust

A migration stepping-stone

- Consider private PKIs serving bespoke certificate-based protocols.
  - There is still a very large number of private environments on legacy ‘90’s era technology.
  - These environments can be serving millions of endpoints with critical applications.
  - PQC offers a forcing function to modernize, but …
  - **Fact:** these environments do not move quickly
  - These environments have a lot of momentum, long QA times (~ 2 years of QA not uncommon), patching and hardware replacement cycles that can be many years long, etc etc.
- The FIPS queue is currently like ~ 18 months. This will not get shorter with the flood of new PQC modules.
  - When will we have a broad selection of FIPS / CC certified ML-KEM implementations? 2 years (2026)? 3 years (2027)?
- {ML-KEM + RSA} or {ML-KEM + P256} hybrids allow for direct use of existing crypto code as part of migration.
  - Lowers QA and FIPS-re-certification lead-times.
  - Lowers deployment risk by using existing battle-hardened code.

A migration stepping stone

- Open questions about RSA-KEM vs RSA-OAEP vs RSA-PKCS1v1.5.
- Nobody is arguing that {ML-KEM + RSA} is good, but rather that it's a stepping stone to help these environments adopt ML-KEM sooner.
- Similar argument for ECDH-P256.

- People are (likely) to do this anyay, so CRFG can help avoid the pitfalls of "roll-your-own" crypto here.