From: Moody, Dustin (Fed)
To: Kerman, Sara J. (Fed)
Subject: RE: Today"s Meeting Notes
Date: Tuesday, December 19, 2017 11:19:03 AM

We just cleared HK17. We said we'd check something in their spec, and we checked it.

So we still have 2 pending.

From: Kerman, Sara J. (Fed)
Sent: Tuesday, December 19, 2017 11:08 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Today's Meeting Notes

Thanks for clarifying. I only had FAPKC as one algorithm row previously (didn't realize they were two)! ☺

From: Moody, Dustin (Fed)
Sent: Tuesday, December 19, 2017 10:54 AM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: RE: Today's Meeting Notes

The other pending was pqNTRUsign.

Note – FAPKC was 2 separate algorithms (like Post Quantum RSA). We're saying NO to both.

We're also going to say NO to LEDAsig.

Everything else looks correct.

From: Kerman, Sara J. (Fed)
Sent: Tuesday, December 19, 2017 10:34 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Today's Meeting Notes

I heard 9 that we said no to:

1. Edon-S
2. FAPKC
3. GuessAgain
4. Kayawood KAP
5. KAZ
6. KERUS
7. NTRU Prime IIT Ukraine
8. Theory of Mathematical Defense to …
9. TPSIG

Two pending

1. Asymmetric Cryptosystem Based
2. ??

Post-Quantum RSA (Encryption/KEM/Signature) will be two separate algorithms

1. Post-Quantum RSA-Encryption
2. Post-Quantum RSA-Signature