From:	Moody, Dustin (Fed)
To:	Petzoldt, Albrecht R. (IntlAssoc)
Subject:	RE: PQC and ECC 2017 Annual Reports
Date:	Monday, October 30, 2017 1:36:00 PM

Thank you!

From: Petzoldt, Albrecht R. (IntlAssoc)
Sent: Monday, October 30, 2017 1:35 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: PQC and ECC 2017 Annual Reports

From: Moody, Dustin (Fed)
Sent: Monday, October 30, 2017 11:19 AM
To: Barker, Elaine B. (Fed) <elaine.barker@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>; Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>; Cooper, David A. (Fed) <david.cooper@nist.gov>; Calik, Cagdas (IntlAssoc) <cagdas.calik@nist.gov>; Miller, Carl A. (Fed) <carl.miller@nist.gov>; Mouha, Nicky W. (IntlAssoc) <nicky.mouha@nist.gov>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Petzoldt, Albrecht R. (IntlAssoc) <albrecht.petzoldt@nist.gov>
Subject: PQC and ECC 2017 Annual Reports

Everyone,
I'm attaching the write-ups for PQC and ECC. Let me know of any comments or suggestions.
Thanks,

Dustin

Hi Dustin,
I think that the reports are good.

However, I would change some things in the table of PQC

- I don't know if may be needed is enough (for AES key size)
- In the last row, DSA is only a signature algorithm (so delete key exchange or add something like DH)
- I would swap line 4 and 5 (RSA and DSA both work over the integers) and maybe line 1 and 2 (hash functions are different from the other schemes)

Best,
Albrecht