From:	Alperin-Sheriff, Jacob (Fed)
To:	Moody, Dustin (Fed)
Subject:	Re: Only Checking KAT Correctness if They Followed API Sufficiently To Make My Compilation Script not too painful
Date:	Tuesday, October 3, 2017 2:31:05 PM

I did the noting, just didn't try to get it working to verify things.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Tuesday, October 3, 2017 at 2:26 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: RE: Only Checking KAT Correctness if They Followed API Sufficiently To Make My Compilation Script not too painful

Larry can add his thoughts, but we should first note whether or not it appears they created KATs. If their KATs don't follow our suggested scripts, then yeah, I wouldn't do anything detailed to verify them. Just look at them enough to see if they appear to make sense. Then make a note on the checklist.

Dustin

From: Alperin-Sheriff, Jacob (Fed)
Sent: Tuesday, October 03, 2017 2:16 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Only Checking KAT Correctness if They Followed API Sufficiently To Make My Compilation Script not too painful

(Or if they provided their own Makefiles that work for KATs). Most people have so far, but among others, Dan Bernstein's ntruprime didn't (defines the main functions in enc.c and dec.c instead of kem.c).

I assume this is okay?

—Jacob Alperin-Sheriff