From:	Alperin-Sheriff, Jacob (Fed)
To:	Moody, Dustin (Fed); Perlner, Ray A. (Fed); Bassham, Lawrence E. (Fed)
Subject:	Re: summary of our quick meeting
Date:	Tuesday, August 8, 2017 11:56:23 AM

We are saying, “use it if you want” for MFPQ but it needs to be included in the build? I think that’s reasonable but I just want to clarify it’s that versus “Don’t use it.” And I thought Larry still needs to check whether that Keccak package is “good” or not …

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Tuesday, August 8, 2017 at 11:45 AM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Subject: summary of our quick meeting

Ray – is going to write a post about the direction we’re going with the KAT calls, and run it by Larry

Jacob – is going to write a post about how ansi-C like does it need to be (we just care if it compiles). He will also clarify his “make install” text, and say we don’t think we need the MFPQ library or the cpucycle library (use it if you want, but we won’t have it on our system), but that the KECCAK package will be available.

Dustin – I will respond to the variable length signature post.

Thanks everyone!