From: Moody, Dustin (Fed)
To: Alperin-Sheriff, Jacob (Fed); internal-pqc
Subject: RE: Are We Requiring NIST API to Get Randomness
Date: Wednesday, October 4, 2017 7:43:07 AM

If everyone but them did it the way we want, I think we were clear enough. We can ask them to make changes.

From: Alperin-Sheriff, Jacob (Fed)
Sent: Tuesday, October 03, 2017 4:44 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Are We Requiring NIST API to Get Randomness

So far Falcon is the only scheme that doesn’t seem to use the NIST API for randomness. I sort of thought we are requiring it since the only other option is to require submitters to write platform-specific code (which we explicitly do not allow). But I wanted to check with everyone anyway.

—Jacob Alperin-Sheriff