From: Bassham, Lawrence E (Fed)
To: Perlner, Ray A. (Fed); Alperin-Sheriff, Jacob (Fed); Moody, Dustin (Fed)
Cc: internal-pqc
Subject: Re: Unless You Have Serious Objections
Date: Friday, December 1, 2017 4:54:43 PM

Ok. Just wasn't sure how serious of an issue(s) Jacob was addressing.

On: 01 December 2017 16:50, "Perlner, Ray (Fed)" <ray.perlner@nist.gov> wrote:

We've previously said on the forum that we would be lenient regarding minor coding issues: See e.g. Dustin's September 14th email:

"We recognize that the API discussion has probably gone on too long for many on the list. We could have done more behind the scenes, but we wanted to be as open and transparent as possible. Nonetheless, we think the discussion was quite useful to us, and we think we have now arrived at a stable version. We will not change the API anymore.

Please note that even if a submission does some minor thing, not quite how we want, we are not going to kick submissions out for things like that. We will work with submitters to handle such issues, including potentially after the submission deadline if necessary. If possible, we will fix it entirely on our end. We would still appreciate if submitters follow our advice so this process can go as smoothly as possible, but we understand if it is too difficult to modify existing code. (With regards to the directory structure, please follow the original guidance in the CFP. We agree that our post indicating otherwise should be ignored, although this is an example of a minor thing that shouldn't be problematic).

Regarding third party test platforms: we have tried to make sure that we are compatible with both SUPERCOP and Open Quantum Safe (the two most developed platforms that are available). We designed our KAT scripts to work with both of them insofar as possible, so that submitters would not need to make different implementations if they wish to submit implementations there. Nonetheless, all that is required on our end, at least initially, is that we can get the submitted code to run well enough to confirm the KAT values provided.
"

From: Bassham, Lawrence E (Fed)
Sent: Friday, December 01, 2017 4:34 PM
To: Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Re: Unless You Have Serious Objections

How much are we allowing people to change things now? That was the point of the early review. I thought if they don't have things correct now they are out.

Larry

On: 01 December 2017 15:42, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov> wrote:
Starting Monday I will be letting people know of any problems I find with the optical media as I find them, so that they don't have to wait on getting the technical completeness review to fix anything; otherwise I feel like it will take far far too long to get all these things shipshape if we have to wait on everyone to finish reviewing and then have to tell them what to fix and then

I will be sure to stress that these may not be the only problems with their submission but we wanted to let them know about the compilation/KAT issues ASAP so that they could get started on fixing them.

(Alternatively we can urge all of our people to expedite their technical reviews of the ones I've found optical media problems with).

Enjoy Hong Kong.

—Jacob Alperin-Sheriff