From: Moody, Dustin (Fed)
To: Peralta, Rene (Fed)
Subject: RE: 2nd draft of Submission Merging Guidelines
Date: Monday, April 30, 2018 8:09:00 AM

Thanks Rene.

As to the line you quoted, we mean that by necessity a merging will require many changes. The teams can therefore update their parameters. However, our decision as to which submissions move into the 2nd round will also factor into account the original parameters from the original submission(s). Meaning, we don't want anybody to merge just as a way to make some changes, because they were attacked and want to increase their parameters. In our CFP we said we weren't allowing changes before the 2nd round, so this is just a hint that we are trying to keep a level playing field.

Not sure if that makes sense. Yi-kai explained it better at our meeting last week.

Dustin

From: Peralta, Rene (Fed)
Sent: Friday, April 27, 2018 7:40 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: 2nd draft of Submission Merging Guidelines

Hi Dustin,

"It would be helpful if any such merger be announced (to NIST) before "

-->

"It would be helpful if any such merger is announced (to NIST) before "

I am not sure what this means:

"Parameters may be updated, but we will still be considering the parameters from the original submissions."

Rene.

From: Moody, Dustin (Fed)
Sent: Thursday, April 26, 2018 1:52 PM
To: internal-pqc
Cc: daniel-c.smith@louisville.edu
Subject: 2nd draft of Submission Merging Guidelines

I incorporated Jacob's and Ray's comments. Let me know if anybody has any other thoughts….

Dustin

NIST would like to encourage any submissions which are quite similar to consider merging. It would be helpful if any such merger be announced (to NIST) before November 30th. Along with a statement of which schemes are merging, merging teams should submit a separate brief document which highlights which aspects of each of the merged schemes are to be used, referring if possible to the already submitted Supporting Documentation for each of the schemes.   The actual specification of the merged scheme should be ready by the deadline for round 2 tweaks to other submissions, and must meet the same standards.

A few points regarding this:

- Schemes should only merge which are similar, and the merged scheme should be in the span of the two original submissions.
- While merging will obviously necessitate some changes, we do not want substantial re-designs.   Parameters may be updated, but we will still be considering the parameters from the original submissions.
- Schemes which are KEMs or PKEs can be merged into one scheme. Schemes which are CPA or CCA can also be combined.
- The merged submission should be sent to pqc-submissions@nist.gov, and should satisfy the requirements set forth in the NIST Call For Proposals (available at www.nist.gov/pqcrypto). In particular, the merged submission will need to include a reference and optimized implementation (which can be the same), as well as new signed IP statements.

- NIST will review the merged submission to verify that it meets the acceptability requirements from the Call For Proposals, as well as to check that the changes are not too major and are in scope.
- Teams may contact us at pqc-comments@nist.gov for more specific questions regarding merging.