**From:** Alperin-Sheriff, Jacob (Fed)
**To:** Chen, Lily (Fed); Moody, Dustin (Fed); internal-pqc; Brandao, Luis (IntlAssoc)
**Cc:** daniel-c.smith@louisville.edu
**Subject:** Re: 2nd draft of Submission Merging Guidelines
**Date:** Friday, April 27, 2018 8:47:33 AM

---

'Since we are sending the message now, I assume that we still consider the merged algorithms as "could be" second round candidates in the same as every other candidates (64 or less), then shall we tell them more clearly? For example, if A and B merge to C, then C may or may not be selected as the second round candidate.

For the candidates, this is a complicated game to play. That is, they need to think whether merge will increase the opportunity."

This is why we should guarantee that merging won't reduce their chances of 2nd round selection. I don't think that restricts US at all because it still lets us rejected merged algorithms if we would've rejected both of them separately, and similarly i don't see binding us to accept a merged algorithm if we would have accepted at least one of the components as a restriction since we can insist that the merged algorithm reflect the best component if necessary.

-------- Original Message --------
From: "Chen, Lily (Fed)" <lily.chen@nist.gov>
Date: Fri, April 27, 2018 3:34 PM +0300
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, internal-pqc <internal-pqc@nist.gov>, "Brandao, Luis (IntlAssoc)" <luis.brandao@nist.gov>
CC: "daniel-c.smith@louisville.edu" <dcsmit11@exchange.louisville.edu>
Subject: Re: 2nd draft of Submission Merging Guidelines

When do we allow people to tweak? Before or after the second round narrow down? (In SHA-3, I remember we did it after the second round are slected. That is we allow the selected second round candidates tweaking.)

Depending on when to twaek, the sentence " 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" indicate that either the merged algorithms will be selected as the second round candidates or we allow all the 64 (or less) candidates to tweak before we select the second round. We need to be clear.

Since we are sending the message now, I assume that we still consider the merged algorithms as "could be" second round candidates in the same as every other candidates (64 or less), then shall we tell them more clearly? For example, if A and B merge to C, then C may or may not be selected as the second round candidate.

For the candidates, this is a complicated game to play. That is, they need to think whether merge will

increase the opportunity.

Lily

On 4/27/18, 7:55 AM, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov> wrote:

One more last thought. We should probably note that a merged submission is at minimum as likely as the most "2nd-round worthy" of the merged schemes to make it to the 2nd round. Or in other and perhaps better language, we guarantee that merging will not reduce the likelihood of a scheme making it to the 2nd round.

-------- Original Message --------
From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thu, April 26, 2018 8:52 PM +0300
To: internal-pqc <internal-pqc@nist.gov>
CC: "daniel-c.smith@louisville.edu" <dcsmit11@exchange.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 <mailto:pqc-submissions@nist.gov>, and should satisfy the

requirements set forth in the NIST Call For Proposals (available at
www.nist.gov/pqcrypto <http://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 <mailto:pqc-comments@nist.gov> for more specific questions regarding merging.