From:	Alperin-Sheriff, Jacob (Fed)
To:	Perlner, Ray A. (Fed); Moody, Dustin (Fed); internal-pqc
Subject:	Re: Guidelines for merging submissions
Date:	Wednesday, April 25, 2018 4:30:45 PM

I think Ray is right, that we shouldn't spring this on them and expect something huge. So something like,

By November 30th, merger should be announced to NIST. 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 to , referring if possible to the already submitted Supporting Documentation for each of the schemes.

1. 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

---

From: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Date: Wednesday, April 25, 2018 at 3:24 PM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: RE: Guidelines for merging submissions

We should say what needs to be ready when.

I would propose that in order to be considered for round 2:

1. An announcement and brief description of the merger should be ready by a month or so before any plausible NIST announcement of the round 2 candidates (e.g. the submitter should announce by November 30th)
2. The actual specification of the merged scheme, patent statements etc. should be ready by the deadline for round 2 tweaks to other submissions.

From: Moody, Dustin (Fed)
Sent: Wednesday, April 25, 2018 2:45 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Guidelines for merging submissions

Here's a draft of what we could say:

NIST would like to encourage any submissions which are quite similar to consider merging. It would be helpful if any merges could be done in the next several months, so that we would have time to consider the newly merged scheme for the 2nd round. 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.

Any suggestions?

Dustin