From: Moody, Dustin (Fed)
To: Chen, Lily (Fed)
Subject: RE: 2nd draft of Submission Merging Guidelines
Date: Monday, April 30, 2018 9:31:00 AM

I think I shall replace several places I use the word scheme with submission:

NIST would like to encourage any submissions which are quite similar to consider merging. It would be helpful if any such merger is 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. While the selection of candidates for the second round will primarily be based on the original submissions, NIST may consider a merged submission more attractive than either of the original schemes if it provides improvements in security, efficiency, or compactness and generality of presentation. At the very least, NIST will accept a merged submission to the second round if either of the submissions being merged would have been accepted. If the merged submission is accepted to the second round, the actual specification of the merged scheme should be ready by the deadline for tweaks to other round 2 submissions, and must meet the same standards.

A few points regarding this:

- Submissions should only merge which are similar, and the merged submission 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.
- Submissions which are KEMs or PKEs can be merged into one submission. Submissions 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.

From: Chen, Lily (Fed)
Sent: Monday, April 30, 2018 9:22 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: 2nd draft of Submission Merging Guidelines

Then, that means to merge to one submission, not one scheme. For example, when using the essential primitive for PKE (static public key) it can be CCA. Then using the same primitive for KEM (one-time public key) it can be CPA. These can be considered as two schemes, not one scheme.

Lily

From: Moody, Dustin (Fed)
Sent: Monday, April 30, 2018 9:20 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: RE: 2nd draft of Submission Merging Guidelines

I'm not sure I understand. Should I use a different term than scheme?

I intended to mean that a submission can have different schemes (i.e. CPA or CCA, KEM or PKE) inside of it. So that you don't need to have two submissions, one for CPA and one for CCA.

Dustin

From: Chen, Lily (Fed)
Sent: Monday, April 30, 2018 9:17 AM
To: Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Cc: daniel-c.smith@louisville.edu <dcsmit11@exchange.louisville.edu>
Subject: RE: 2nd draft of Submission Merging Guidelines

> Apologize for not questing in one-pass. This is another question. By statement "Schemes which are KEMs or PKEs can be merged into one scheme. Schemes which are CPA or CCA can also be combined" we assume that the different ways to use a primitive can be considered as ONE scheme. For a given way of using the essential primitive, it can be CPA or CCA but not both. This is related to the term "scheme". Maybe this is not a problem at all.
>
> Lily

From: Alperin-Sheriff, Jacob (Fed)
Sent: Monday, April 30, 2018 8:52 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Cc: daniel-c.smith@louisville.edu <dcsmit11@exchange.louisville.edu>
Subject: RE: 2nd draft of Submission Merging Guidelines

I'd say you can post this.

-------- Original Message --------
From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>

Date: Mon, April 30, 2018 3:31 PM +0300
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, internal-pqc <internal-pqc@nist.gov>
CC: "daniel-c.smith@louisville.edu" <dcsmit11@exchange.louisville.edu>
Subject: RE: 2nd draft of Submission Merging Guidelines

(Here's the current version, incorporating everybody's changes…)

NIST would like to encourage any submissions which are quite similar to consider merging. It would be helpful if any such merger is 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. While the selection of candidates for the second round will primarily be based on the original submissions, NIST may consider a merged submission more attractive than either of the original schemes if it provides improvements in security, efficiency, or compactness and generality of presentation. At the very least, NIST will accept a merged submission to the second round if either of the submissions being merged would have been accepted. If the merged submission is accepted to the second round, the actual specification of the merged scheme should be ready by the deadline for tweaks to other round 2 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.

From: Moody, Dustin (Fed)
Sent: Monday, April 30, 2018 8:11 AM
To: Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; internal-pqc <internal-pqc@nist.gov>

Cc: daniel-c.smith@louisville.edu <dcsmit11@exchange.louisville.edu>
Subject: RE: 2nd draft of Submission Merging Guidelines

If there are no objections, I'll post this message sometime this afternoon.

Dustin

From: Alperin-Sheriff, Jacob (Fed)
Sent: Thursday, April 26, 2018 4:20 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Cc: daniel-c.smith@louisville.edu <dcsmit11@exchange.louisville.edu>
Subject: Re: 2nd draft of Submission Merging Guidelines

Will this be mentioned before Eurocrypt?

-------- Original Message --------
From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thu, April 26, 2018 1:52 PM -0400
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, 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.