From: Moody, Dustin (Fed)
To: Peralta, Rene C. (Fed)
Subject: Re: Status update on PQC CFP
Date: Friday, October 14, 2016 7:56:38 AM
Attachments: image001.png
OutlookEmoji- .png

Rene,
I think of the whole thing as a standardization process. The writing of the standard is only the final stage at the end. We are plagued a bit by not having a good word like "competition".

Dustin

From: Peralta, Rene (Fed)
Sent: Friday, October 14, 2016 7:39:13 AM
To: Moody, Dustin (Fed)
Cc: Peralta, Rene (Fed)
Subject: Re: Status update on PQC CFP
Hi Dustin,

On page 12 there is

>>
and display such implementations for the purposes of the post-quantum algorithm public review and evaluation process
>>

and later

>>
To be considered as a “proper” post-quantum public-key cryptosystem (and continue further in the standardization process), the scheme shall meet the following minimum acceptability requirements:
>>

The stuff in parenthesis made me think we were discussing two "processes" in the document. After your mail I think we are not. Maybe we can just remove the word "standardization" from the stuff in parenthesis?

Please feel free to ignore. My ability to misunderstand stuff seems boundless 😕 .

Regards, Rene.

From: Moody, Dustin (Fed)
Sent: Friday, October 14, 2016 7:10 AM
To: Peralta, Rene (Fed)
Subject: Re: Status update on PQC CFP

Rene,
I think the same as you - that the write up of standards documents will come after the evaluation process. Was there something that made you think otherwise?

The only exception I can think of is hash-based signatures, which we might standardize before.

Dustin

From: Peralta, Rene (Fed)
Sent: Thursday, October 13, 2016 3:25:30 PM
To: Moody, Dustin (Fed); Alperin-Sheriff, Jacob (Fed); Ray Perlner; Bassham, Lawrence E (Fed); Chen, Lily (Fed); Daniel Smith-Tone; Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed); Miller, Carl A. (Fed); Perlner, Ray (Fed); Smith-Tone, Daniel (Fed)
Cc: Peralta, Rene (Fed)
Subject: Re: Status update on PQC CFP

Thanks, I had been thinking that the write-up of standards documents will start after this evaluation process, not concurrently with it. But I guess we can decide that on the way.

Regards, Rene.

From: Moody, Dustin (Fed)
Sent: Thursday, October 13, 2016 1:55 PM
To: Alperin-Sheriff, Jacob (Fed); Peralta, Rene (Fed); Ray Perlner; Bassham, Lawrence E (Fed); Chen, Lily (Fed); Daniel Smith-Tone; Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed); Miller, Carl A. (Fed); Perlner, Ray (Fed); Smith-Tone, Daniel (Fed)
Subject: RE: Status update on PQC CFP

In our intro (to the CFP) we say:
NIST is beginning a process to develop new post-quantum cryptography standards, including digital signature schemes specified in Federal Information Processing Standards Publication (FIPS) 186 and key establishment schemes specified in NIST Special Publications (SP) 800-56 A and B. The process is referred as *post-quantum cryptography standardization*. The standards will be published as Federal Information Processing Standards (FIPSs) or Special Publications (SPs).
NIST is soliciting proposals for post-quantum cryptosystems and it will solicit comments from the public as part of its evaluation process. NIST expects to perform multiple rounds of

evaluation, over a period of three to five years. The goal of this process is to select a number of acceptable candidate cryptosystems for standardization.

From: Alperin-Sheriff, Jacob (Fed)
Sent: Thursday, October 13, 2016 1:51 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>; Ray Perlner (b) (6) ; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Daniel Smith-Tone <daniel-c.smith@louisville.edu>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Miller, Carl A. (Fed) <carl.miller@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>
Subject: Re: Status update on PQC CFP

I guess “NIST intends to standardize” has a weaselly way out that if we get nothing decent, then despite our best intentions, we don’t?

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, October 13, 2016 at 1:50 PM
To: "Peralta, Rene (Fed)" <rene.peralta@nist.gov>, Ray Perlner (b) (6) "Alperin-Sheriff, Jacob M. (Fed)" <jacob.alperin-sheriff@nist.gov>, "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>, Daniel Smith-Tone <daniel-c.smith@louisville.edu>, "Jordan, Stephen P (Fed)" <stephen.jordan@nist.gov>, "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, "Miller, Carl A. (Fed)" <carl.miller@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Smith-Tone, Daniel (Fed)" <daniel.smith@nist.gov>
Subject: RE: Status update on PQC CFP

I think we’ve said that we plan on standardizing what comes out of this, although, we’ve left open the possibility that if we aren’t satisfied at the end of the process, then we are not required to standardize anything.

From: Peralta, Rene (Fed)
Sent: Thursday, October 13, 2016 12:29 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Ray Perlner (b) (6) ; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Daniel Smith-Tone <daniel-c.smith@louisville.edu>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Miller, Carl A. (Fed) <carl.miller@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>
Subject: Re: Status update on PQC CFP

We use "evaluation process" and "standardization process" in the CFP. Are we using these interchangeably? Have we committed to a standardization process to accompany this public discussion (avoiding the term competition)?
Rene.

From: Moody, Dustin (Fed)
Sent: Wednesday, October 12, 2016 1:26 PM
To: Ray Perlner; Alperin-Sheriff, Jacob (Fed); Bassham, Lawrence E (Fed); Chen, Lily (Fed); Daniel Smith-Tone; Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed); Miller, Carl A. (Fed); Moody, Dustin (Fed);

Peralta, Rene (Fed); Perlner, Ray (Fed); Smith-Tone, Daniel (Fed)
Subject: Status update on PQC CFP
Everyone,
Thanks for everybody's time and effort to finalize our CFP. Here's a few notes and assignments following our second internal meeting yesterday.

- I think we resolved most of the minor comments, which have been reflected in the attached updated CFP. Please review it. The changes are marked and easy to see. Let me within a week if anybody sees something that needs to be addressed/fixed.
- Larry and Ray have written some new FAQ questions. See the attached. I will have Sara post them to the FAQ section next week, unless I hear anything back from anyone. Daniel is going to write one on how our process is different than a competition.
- Larry is working on resolving the API comments. For some of that, he will work with Ray. Also need to make sure how we change our key-exchange/KEM stuff is reflected in the API.
- Yi-Kai will work with Ray to revise the security section (4.A.4). Yesterday, we agreed with Yi-Kai that it might be best to remove security levels 2 and 4. Possibly discuss this on the pqc-forum.
- Jacob will work with Ray to re-write the portions of the CFP dealing with key-exchange. We agreed to add an ephemeral version. Jacob has suggested some text for 4.A.2, which could be split into 2 sections. They also need to look at 2.B.1 and section 3. We need to agree on our terminology. Would probably also be good to discuss on the pqc-forum.
- We had a meeting with the NIST lawyers. They said we need to keep our IPR statements as they currently are (meaning we can't have only royalty free algorithms). There will probably be a few lines added into the CFP strengthening our language that we have a strong preference for royalty-free, and that it will be used as an evaluation criteria. Andy would also like to add a line that we will commit to having at least one algorithm of each type be royalty-free.
- We will need to have a 2nd FRN announcing our final version of the CFP, but it will be very short, just pointing to our webpage. We will also want to have a short report which summarizes the comments received (text of the comments will also be published), and the main changes we made as a result.
- We will have a meeting next Wednesday (10/19), 10am til noon. The main topics of discussion will be the above items.

Thanks!
Dustin