From: Bassham, Lawrence E (Fed)
To: Moody, Dustin (Fed)
Cc: Liu, Yi-Kai (Fed); Perlner, Ray A. (Fed)
Subject: Re: Sample documents for PQC Call For Proposals
Date: Thursday, June 16, 2016 9:55:12 AM
Attachments: API.rtf

Dustin,
Here's the updated API file. Give that a read to make sure I didn't miss anything.
Larry

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, June 16, 2016 at 7:04 AM
To: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Subject: Fw: Sample documents for PQC Call For Proposals
Larry,
Yi-Kai had a few comments. What do you think?
Dustin

From: Liu, Yi-Kai (Fed)
Sent: Wednesday, June 15, 2016 1:20 PM
To: Moody, Dustin (Fed); Perlner, Ray (Fed)
Subject: Re: Sample documents for PQC Call For Proposals
Hi Dustin and Ray,

Just a couple more comments:

When we ask users to define CRYPTO_SECRETKEYBYTES, CRYPTO_PUBLICKEYBYTES and CRYPTO_BYTES, I still think it would also be a good idea to ask them to define CRYPTO_RANDOMBYTES to indicate how many bytes of randomness they will require. I know Larry thought this was unnecessary, but I think it will make our lives easier.

Also, I think we might want to add a sentence explaining what these constants are, this would be copied from https://bench.cr.yp.to/call-sign.html

What do you think?

Also, tell Larry thank you for putting this together!

Cheers,

--Yi-Kai

From: Moody, Dustin (Fed)
Sent: Tuesday, June 14, 2016 11:47 AM
To: Perlner, Ray (Fed); Liu, Yi-Kai (Fed)
Subject: FW: Sample documents for PQC Call For Proposals

Ray/Yi-Kai,

Take a look at what Larry sent, and let us know if there is anything that needs to be fixed. Thanks!

Dustin

From: Bassham, Lawrence E (Fed)
Sent: Tuesday, June 14, 2016 11:20 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Sample documents for PQC Call For Proposals

Dustin,

Here's what I have. Take a look and see if you think more needs to be added. Since things are kind of open as far as what can be submitted it's hard to be more specific. Let me know what you think and if things read ok.

Larry

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov<mailto:dustin.moody@nist.gov>>
Date: Tuesday, June 14, 2016 at 8:18 AM
To: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov<mailto:lawrence.bassham@nist.gov>>
Subject: RE: Sample documents for PQC Call For Proposals

Larry,
Just checking if you'll have the KAT stuff done today? Also, for the intermediate values file, here's what it says in the text:

a) If the execution of an algorithm produces intermediate results that are informative (e.g., for debugging an implementation of the algorithm), then the submitter shall include known answers for those intermediate values for each of the required security strengths. Examples of providing such intermediate values are available at: http://csrc.nist.gov/groups/ST/toolkit/index.html.

Is there where the intermediate values file should be posted? Or on the www.nist.gov/pqcrypto<http://www.nist.gov/pqcrypto> page?
Please send me the API, KAT, and intermediate values files when you can. The lawyers have signed off, so we should be able to post this later this week or next week.
Thanks,

Dustin

From: Bassham, Lawrence E (Fed)
Sent: Thursday, June 02, 2016 10:18 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov<mailto:dustin.moody@nist.gov>>
Subject: Re: Sample documents for PQC Call For Proposals

I have a sample Intermediate Values file, but I'm working on the KAT stuff. I'll have it all by Monday or Tuesday. Ok?

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov<mailto:dustin.moody@nist.gov>>
Date: Thursday, June 2, 2016 at 10:16 AM
To: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov<mailto:lawrence.bassham@nist.gov>>
Subject: Re: Sample documents for PQC Call For Proposals

Larry,

Thanks for the API page. I'll get Sara to post it when we post the Call For Proposals. Do you have the other files that you are working on? (I think it's the KAT and intermediate values).

Dustin

_____

From: Bassham, Lawrence E (Fed)
Sent: Wednesday, June 1, 2016 2:23:37 PM
To: Moody, Dustin (Fed)
Subject: Re: Sample documents for PQC Call For Proposals

Here is text for an API page. I can work with Sara on format stuff, but she usually does a good job of it.

I don't see the doc with the changed text. Can you resend that?

Larry

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov<mailto:dustin.moody@nist.gov>>
Date: Tuesday, May 24, 2016 at 1:31 PM
To: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov<mailto:lawrence.bassham@nist.gov>>
Subject: RE: Sample documents for PQC Call For Proposals

Larry,
Just checking on your progress for documents that we can post on our webpage for

? Sample files for the KAT values

? Crypto API for implementations
We will need them on the website before the CFP is posted publicly sometime in the middle of June.

Also, I edited the document to allow zip files and USB flash drives in addition to cd-rom's and DVD's. Can you check that I phrased things okay? They are mentioned in sections 2.B.3, 2.C, 2.C.2, and 2.C.4. I also changed the section from "Optical Media" to "Digital and Optical Media". Does that work? Thanks,

Dustin

From: Bassham, Lawrence E (Fed)
Sent: Thursday, April 14, 2016 9:03 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov<mailto:dustin.moody@nist.gov>>
Subject: Re: Sample documents for PQC Call For Proposals

I was talking to a couple of people about this today. I have some ideas and will start working on it.

Larry

_____

On: 14 April 2016 14:23, "Moody, Dustin (Fed)" <dustin.moody@nist.gov<mailto:dustin.moody@nist.gov>> wrote:

Larry,

Can you start working on creating the sample files for the KAT stuff? We'll also need to have a document describing the API. I don't know the best way to do it, but hopefully you do! Thanks,

Dustin