

From: [Perlner, Ray \(Fed\)](#)
To: [Moody, Dustin \(Fed\)](#)
Subject: RE: Sample documents for PQC Call For Proposals
Date: Thursday, June 2, 2016 2:27:00 PM

sure

From: Moody, Dustin (Fed)
Sent: Thursday, June 02, 2016 2:27 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Subject: Re: Sample documents for PQC Call For Proposals
Can I forward this to Larry?

From: Perlner, Ray (Fed)
Sent: Thursday, June 2, 2016 2:26:19 PM
To: Moody, Dustin (Fed); Liu, Yi-Kai (Fed)
Subject: RE: Sample documents for PQC Call For Proposals
I'm not sure if "DH-Functions" really covers our description of key exchange, as it assumes a symmetry between initiator and responder that may not be present for submitted cryptosystems. Also, it seems a little funny to include randomness as an input for decryption and signature verification (that said I don't think it does any harm, and I can vaguely imagine reasons one might want a randomized algorithm for either of these functionalities. It's just not all that typical.)

From: Moody, Dustin (Fed)
Sent: Thursday, June 02, 2016 10:18 AM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Subject: Fw: Sample documents for PQC Call For Proposals
Here is Larry's API text. I don't know what they are supposed to look like, but it seems fine to me. Let me know if you think it needs anything.
Dustin

From: Bassham, Lawrence E (Fed)
Sent: Wednesday, June 1, 2016 2:23 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>
Date: Tuesday, May 24, 2016 at 1:31 PM
To: "Bassham, Lawrence E (Fed)" <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>

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> 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