From:	Moody, Dustin (Fed)
To:	Alperin-Sheriff, Jacob (Fed); Bassham, Lawrence E. (Fed); Perlner, Ray A. (Fed)
Subject:	RE: All KAT and RNG and API files
Date:	Thursday, September 7, 2017 3:51:01 PM

I'm heading home now – can somebody post to the forum about this today? If not, I'll do it tonight if there are no objections.

From: Moody, Dustin (Fed)
Sent: Thursday, September 07, 2017 3:46 PM
To: Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: RE: All KAT and RNG and API files

In order to be able to post to the forum today, we need to put something in place of the KAT.pdf on the Example Files page. Sara won't be here tomorrow, so I sent her the following to use. It's not really detailed, but I think we can then at least let the forum know the scripts are there, and many submitters can probably figure it out. If not, they'll start asking us questions, and we can update our stuff as needed.

I'm thinking that for a forum post, we can simply say:
Submitters should use the scripts available at http://csrc.nist.gov/groups/ST/post-quantum-crypto/example-files.html
to generate their KAT files.

It would helpful to also provide a few examples with several intermediate values for debugging purposes. An example of such an example is in the file Intermediate Values, which can also be found at the url above.

Let us know if you have any questions.

Do we need to have a FAQ question for this?
Dustin

KAT.pdf text:
Test vectors are to be generated that can be used to determine the correctness of an implementation. These files come in two types: Known Answer Tests (KAT) files and Intermediate files. The KAT files are for general use to determine an implementation's correctness. The Intermediate values are useful for debugging an incorrect implementation. KAT files shall be provided to test different aspects of the algorithm, e.g., key generation, encryption, decryption.

Submitters should use the scripts available at http://csrc.nist.gov/groups/ST/post-quantum-crypto/example-files.html

to generate their KAT files.

It would helpful to also provide a few examples with several intermediate values for debugging purposes. An example of such an example is in the file Intermediate Values, which can also be found at the url above.

From: Alperin-Sheriff, Jacob (Fed)
Sent: Thursday, September 07, 2017 2:59 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: All KAT and RNG and API files

Also, on closer inspection, given the way the API notes file is written, it doesn't appear that the current script files will work properly, since there's nothing in the API notes file about declaring the

crypto_sign_keypair, crypto_sign, crypto_sign_open, crypto_encrypt_keypair, etc. etc. in the api.h file.

Is this what they are supposed to do? I assume so, since otherwise PQCgenKAT_*.c files won't be able to find the appropriate functions when compiling and linking.

Very difficult to write anything for the KAT files without resolving this …

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, September 7, 2017 at 2:17 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Subject: RE: All KAT and RNG and API files

Larry,
Jacob had a question about the submitters needing to edit the files to give their algorithm name :

```
char    AlgName[] = "My Alg Name";
```

He was wondering if there was some other way to read it in, so the submitters wouldn't need to edit our files. Any thoughts?

Dustin

From: Alperin-Sheriff, Jacob (Fed)
Sent: Thursday, September 07, 2017 12:47 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: All KAT and RNG and API files

Oops they do.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, September 7, 2017 at 12:25 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Subject: RE: All KAT and RNG and API files

Do we provide that? Or the submitter?

From: Alperin-Sheriff, Jacob (Fed)
Sent: Thursday, September 07, 2017 12:26 PM
To: Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: All KAT and RNG and API files

Where is api.h?

From: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Date: Thursday, September 7, 2017 at 12:06 PM
To: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Subject: Re: All KAT and RNG and API files

Final version – for now.

Larry

From: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Date: Thursday, September 7, 2017 at 11:46 AM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Subject: RE: All KAT and RNG and API files

I see a couple of spots in the KEM and PKE scripts that still have “crypto_sign_xxx” in either a function call or a print statement. Please check these.

From: Moody, Dustin (Fed)
Sent: Thursday, September 07, 2017 11:27 AM
To: Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
Cc: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: RE: All KAT and RNG and API files

Ray, let me know when you are okay with us posting these.

From: Alperin-Sheriff, Jacob (Fed)
Sent: Thursday, September 07, 2017 11:25 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
Cc: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: All KAT and RNG and API files

The only “obvious” I saw doesn’t seem to be a problem now that I got an updated version of rng.h

---

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, September 7, 2017 at 11:19 AM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Cc: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Subject: RE: All KAT and RNG and API files

We can release it now – I just wanted you and Ray to take a look first to see if there was anything obvious. Sounds like you’re giving it the okay.

From: Alperin-Sheriff, Jacob (Fed)
Sent: Thursday, September 07, 2017 11:19 AM
To: Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: All KAT and RNG and API files

No, just release it as it is now and let people test it on their own stuff that they’ve already presumably at least partially written, and then let them find some complaints to make that we can then fix!

e.g. sounds like you’ve done as much testing as we can really hope for without the VM set up and “beta testers” to find problems with it.

From: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>

Date: Thursday, September 7, 2017 at 11:17 AM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Cc: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Subject: Re: All KAT and RNG and API files

Do what? Test with one of the submissions that came in already? Because I don't have the VM all set up and ready to go yet. That's for next week.

From: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Date: Thursday, September 7, 2017 at 11:15 AM
To: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Cc: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Subject: Re: All KAT and RNG and API files

Why don't we just do that then?

From: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Date: Thursday, September 7, 2017 at 11:15 AM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Cc: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Subject: Re: All KAT and RNG and API files

I haven't tested with other algorithms, but I made some dummy XOR based stuff to try them (the KAT gen files) out. I did a bit more testing of randombytes and the seed expander. I'm sure people will find problems and have complaints. We can update things as necessary.

From: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Date: Thursday, September 7, 2017 at 10:55 AM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Cc: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Subject: Re: All KAT and RNG and API files

Shouldn't randombytes be declared in rng.h?

How are they going to include it in their submissions otherwise …

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, September 7, 2017 at 10:54 AM

To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Cc: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Subject: RE: All KAT and RNG and API files

Rng.h is attached. Larry has done some testing – maybe he can explain

---

From: Alperin-Sheriff, Jacob (Fed)
Sent: Thursday, September 07, 2017 10:53 AM
To: Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: All KAT and RNG and API files

Did we get rng.h yesterday? I don't see it here.

Also, what have we tested these on already?

From: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Date: Thursday, September 7, 2017 at 9:55 AM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Cc: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Subject: All KAT and RNG and API files

Here they are. Take a look.

Larry