From: Moody, Dustin (Fed)
To: Bassham, Lawrence E. (Fed); Alperin-Sheriff, Jacob (Fed)
Cc: Perlner, Ray A. (Fed)
Subject: RE: All KAT and RNG and API files
Date: Thursday, September 7, 2017 1:37:31 PM

Sara has the files all posted, except the KAT.pdf that Jacob is re-writing. She'd like it today, as she will be out tomorrow.

What should we say on the forum?

Scripts to generate KATs are now available (give link). Read KAT.pdf to know what to do. Let us know if you have any questions.

Anything else?

From: Bassham, Lawrence E (Fed)
Sent: Thursday, September 07, 2017 11:16 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

From: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Date: Thursday, September 7, 2017 at 11:13 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

Nope, in the one Dustin attached I only see declarations for

seedexpander_init

seedexpander

print_Bstr

From: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Date: Thursday, September 7, 2017 at 11:12 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

It's the second-to-the-last declaration in the file. Is that not in your copy?

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