From: Bassham, Lawrence E (Fed)
To: Perlner, Ray A. (Fed); Moody, Dustin (Fed)
Subject: Re: API doc
Date: Wednesday, August 9, 2017 2:48:43 PM

I think so. Like I said they will cover the generic tests.

On: 09 August 2017 14:26, "Perlner, Ray (Fed)" <ray.perlner@nist.gov> wrote:

Great. Can I promise such a thing when we announce the updated API?

Thanks,
Ray

From: Bassham, Lawrence E (Fed)
Sent: Wednesday, August 09, 2017 2:23 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: API doc

We can write code for generic KATs (variable plaintext and variable key types of test), but couldn't have things that test specific components of the algorithm. At this point that may not be so important. The more generic tests are probably fine. Apparently I made something like that available during the SHA3 competition (or AES - I forget which).

On: 09 August 2017 14:00, "Perlner, Ray (Fed)" <ray.perlner@nist.gov> wrote:

As a side note, is there any way we could convince Dan and/or the open quantum safe guys to write a script to generate KATs automatically, or write one ourselves?

From: Bassham, Lawrence E (Fed)
Sent: Wednesday, August 09, 2017 1:22 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: API doc

I'll tweak it some more.

On: 09 August 2017 12:59, "Perlner, Ray (Fed)" <ray.perlner@nist.gov> wrote:

In addition to adding enough info on randomness stuff that the submitters can generate their own KAT files, there are a couple of other changes that still need to be made:

1) The API should not contain any references to CRYPTO_RANDOMBYTES. We want to allow unrestricted API calls to AES-DRBG, and we don't want the instantiation of the AES-DRBG to be inside the submitted code. We would instead want to instantiate AES-DRBG with some constant input at the beginning of benchmarking scripts, and for KAT testing, we would want to instantiate AES-DRBG at the beginning of every test entry, using the inputs

given in the KAT.

2) I don't think we want to specify the flow of entropy from randombytes -> CTR DRBG -> Seed expander. The first step seems unnecessary. I assumed there would be some flag you could set in the test environment that would cause randombytes() to call AES-DRBG-Generate directly. Any calls to seed expander are meant to be part of the submitted code, and strictly optional, if the submitter doesn't like the performance they are going to get from AES-CTR-DRBG due to the backtracking resistance feature.

-----Original Message-----
From: Moody, Dustin (Fed)
Sent: Wednesday, August 09, 2017 11:22 AM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: FW: API doc

-----Original Message-----
From: Bassham, Lawrence E (Fed)
Sent: Wednesday, August 09, 2017 11:12 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: API doc

Dustin,

The version you sent me was older. I had the most recent (they have dates in the name now). Take a look at this. In particular I changed the opening paragraph (deleted all the KAT stuff), tried to change the names on the KEM stuff (is everything correct?), and changed/added stuff at the bottom for Additional Functions for randomness.

We need to put a document up that describes the randomness stuff. I'll get working on that. Basically some pseudocode like John did and something that shows/describes the sequence of calls (entropy from randombytes -> CTR_DRBG -> SeedExpander). Do you think that should be added to the API doc directly?

Larry