From: Bassham, Lawrence E (Fed)
To: Moody, Dustin (Fed)
Subject: Re: API doc
Date: Wednesday, August 9, 2017 12:09:14 PM

Ok

On: 09 August 2017 11:49, "Moody, Dustin (Fed)" <dustin.moody@nist.gov> wrote:
Ok, sounds good. By the way, Ray is working a response to the API, because he doesn't think it does what we discussed.

-----Original Message-----
From: Bassham, Lawrence E (Fed)
Sent: Wednesday, August 09, 2017 11:39 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: API doc

It could be added it to the API doc. Then they don't have to go to multiple places. We can see if some of John's stuff can be pasted in with maybe a bit of tweaking.

On 8/9/17, 11:24 AM, "Moody, Dustin (Fed)" <dustin.moody@nist.gov> wrote:

Larry,
Sorry I sent an older version. Thanks for fixing it - I'll take a look. It'd be great if we could get a doc on the randomness stuff as you describe. We want to let people know as soon as we are able to. It makes sense to either add it to the API doc, or just have it be a separate doc alongside it. Any preference?

Dustin

-----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