From: Bassham, Lawrence E (Fed)
To: Moody, Dustin (Fed)
Subject: API doc
Date: Wednesday, August 9, 2017 11:12:24 AM
Attachments: API_080917.rtf

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