From: Bassham, Lawrence E (Fed)
To: Moody, Dustin (Fed)
Subject: Re: Open Quantum Safe
Date: Monday, April 17, 2017 10:44:38 AM

Given your last email about Open Quantum Safe I won't spend too much time looking at what they have now. We can discuss internally the _KAT to _deterministic change.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Monday, April 17, 2017 at 10:04 AM
To: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Subject: Open Quantum Safe

Larry,

I hope what we do is still compatible with the Open Quantum Safe project as well (https://openquantumsafe.org/). It says they use liboqs, which also includes common routines available to all liboqs modules, including a common random number generator and various symmetric primitives such as AES and SHA-3. Do they already have a NIST DRBG can you tell? From my un-expert eyes, it seems they might be using AES Ctr DRBG? See https://github.com/open-quantum-safe/liboqs

Dustin