From: Moody, Dustin (Fed)
To: Perlner, Ray A. (Fed); Bassham, Lawrence E. (Fed)
Subject: RE: draft PQC-Forum post: Planned API change to eliminate separate KAT calls
Date: Tuesday, August 8, 2017 12:47:25 PM

Larry,
I made a few minor edits. How does it read to you?

We have received a number of comments about the necessity of having separate "KAT calls" in our API (See http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/example-files/api-notes.pdf). In response, we plan to use the "eBATS calls" from our API for both performance testing and known answer tests.

Submitters have been previously instructed in our FAQ (see http://csrc.nist.gov/groups/ST/post-quantum-crypto/faq.html#Q15) to use the function randombytes() where secure randomness is required. In the test environment, we expect this function to point to the AES-256 CTR DRBG generate function specified in section 10.2.1.5.1 of SP 800-90A revision 1 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf). To provide KAT vectors, Submitters will then be asked to provide inputs to the Instantiate function (specified in section 10.2.1.3.1 of SP 800-90A revision 1), that result in the specified test outputs.

We plan to have updated API guidance ready by September 1st.

Does this plan seem sensible?
Thanks,
Ray Perlner

From: Perlner, Ray (Fed)
Sent: Tuesday, August 08, 2017 12:29 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
Subject: draft PQC-Forum post: Planned API change to eliminate separate KAT calls

We have received a number of questioning about the necessity of having separate KAT calls in our API (See http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/example-files/api-notes.pdf). In response, we plan to use the eBATS API for both performance testing and known answer tests.

Submitters have been previously instructed in our FAQ (see http://csrc.nist.gov/groups/ST/post-quantum-crypto/faq.html#Q15) to use the function randombytes() where secure randomness is required. In the test environment, we expect this function to point to the AES-256 CTR DRBG generate function specified in section 10.2.1.5.1 of SP 800-90A revision 1 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf). To provide KAT

vectors, Submitters will then be asked to provide inputs to the Instantiate function (specified in section 10.2.1.3.1 of SP 800-90A revision 1), that result in the specified test outputs, when the appropriate eBATS call immediately follows the specified instantiation of the AES-256 CTR DRBG instance called by randombytes().

We plan to have updated API guidance by September 1st.

Does this plan seem sensible?
Thanks,
Ray Perlner