**From:** Bassham, Lawrence E (Fed)
**To:** Moody, Dustin (Fed); Perlner, Ray A. (Fed)
**Subject:** Re: draft PQC-Forum post: Planned API change to eliminate separate KAT calls
**Date:** Friday, August 11, 2017 10:01:02 AM

---

I agree

---

On: 11 August 2017 09:34, "Moody, Dustin (Fed)" <dustin.moody@nist.gov> wrote:
Fine by me. Larry?

---

**From:** Perlner, Ray (Fed)
**Sent:** Friday, August 11, 2017 9:32 AM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
**Subject:** RE: draft PQC-Forum post: Planned API change to eliminate separate KAT calls

If the new API guidance and scripts will be a while, can I post the following to the forum?:

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 and scripts for generating KAT calls 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 (dustin.moody@nist.gov) <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