**From:** Alperin-Sheriff, Jacob (Fed)
**To:** Moody, Dustin (Fed); Chen, Lily (Fed); Bassham, Lawrence E. (Fed); Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed); Miller, Carl A. (Fed); Peralta, Rene C. (Fed); Perlner, Ray A. (Fed); Smith-Tone, Daniel C. (Fed); Kelsey, John M. (Fed)
**Subject:** Re: Here"s text summarizing what we said in our meeting. Note that John will need to expand on his advice regarding "seed expander"
**Date:** Wednesday, July 19, 2017 9:05:12 AM

Okay.

**From:** "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
**Date:** Wednesday, July 19, 2017 at 9:00 AM
**To:** "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>, "Jordan, Stephen P (Fed)" <stephen.jordan@nist.gov>, "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, "Miller, Carl A. (Fed)" <carl.miller@nist.gov>, "Peralta, Rene (Fed)" <rene.peralta@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Smith-Tone, Daniel (Fed)" <daniel.smith@nist.gov>, "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>
**Subject:** RE: Here's text summarizing what we said in our meeting. Note that John will need to expand on his advice regarding "seed expander"

We can include the phrase already in the CFP:

“If the scheme uses a cryptographic primitive that has not been approved by NIST, the submitter shall provide an explanation for why a NIST-approved primitive would not be suitable.”

**From:** Alperin-Sheriff, Jacob (Fed)
**Sent:** Wednesday, July 19, 2017 8:58 AM
**To:** Chen, Lily (Fed) <lily.chen@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Miller, Carl A. (Fed) <carl.miller@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>
**Subject:** Re: Here's text summarizing what we said in our meeting. Note that John will need to expand on his advice regarding "seed expander"

Did we decide that we are precluding the use of non-NIST approved hash functions for hash-based signature schemes? The statement sort of reads that way …

**From:** "Chen, Lily (Fed)" <lily.chen@nist.gov>
**Date:** Wednesday, July 19, 2017 at 8:43 AM
**To:** "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>, "Jordan, Stephen P (Fed)" <stephen.jordan@nist.gov>, "Liu,

Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, "Miller, Carl A. (Fed)" <carl.miller@nist.gov>, "Peralta, Rene (Fed)" <rene.peralta@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Smith-Tone, Daniel (Fed)" <daniel.smith@nist.gov>, "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>
**Subject:** RE: Here's text summarizing what we said in our meeting. Note that John will need to expand on his advice regarding "seed expander"

Please notice that we haven't included in KMAC based KDF in NIST recommendations. We will introduce KMAC based key derivation in the next version of 56A for one-step key derivation. The draft will release for public comments in August. However, using KMAC hasn't introduced in 800-108 yet, which is used as an expansion function in the two-step key derivation.

For authenticated encryption, GCM is not quite misuse resistance with regarding to IV selection. Do we know the potential use scenario?

Maybe all the issues have been discussed yesterday. Sorry that I cannot attend the meeting for a conflict.

Lily

---

**From:** Moody, Dustin (Fed)
**Sent:** Wednesday, July 19, 2017 8:35 AM
**To:** Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Miller, Carl A. (Fed) <carl.miller@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>
**Subject:** FW: Here's text summarizing what we said in our meeting. Note that John will need to expand on his advice regarding "seed expander"

Everyone okay with Ray's write-up?  We probably need John's write-up explaining his AES seed-expander before we post this…

Dustin

---

**From:** Perlner, Ray (Fed)
**Sent:** Tuesday, July 18, 2017 5:17 PM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
**Subject:** Here's text summarizing what we said in our meeting. Note that John will need to expand on his advice regarding "seed expander"

Q: How should submitters choose symmetric algorithms for their submissions?

A: While NIST will permit submitters to choose any NIST approved cryptographic algorithm for their submission if they feel it is necessary to achieve the desired security and performance, a number of potential submitters have asked us to offer default options for common symmetric cryptographic primitives. As such, here are our suggestions:

1. Hash functions: SHA512 is likely sufficient to meet the requirements of any of our five security strength categories and gives good performance in software, especially for 64 bit architectures. Submitters seeking a variable length output or good performance in hardware may instead prefer to use SHAKE256.
2. Authenticated encryption: We'd suggest AES256-GCM with a random IV.
3. KDFs: Where security proofs can accommodate something that is not indifferentiable from a random oracle, John's AES-based seed-expander will offer excellent performance. Otherwise, KMAC256 will be a good choice.