**From:** Alperin-Sheriff, Jacob (Fed)
**To:** Moody, Dustin (Fed)
**Subject:** Re: Minor Change trying to Clarify the issues raised about key exchange versus KEM
**Date:** Tuesday, November 1, 2016 11:37:48 AM

Sure

**From:** "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
**Date:** Tuesday, November 1, 2016 at 7:47 AM
**To:** "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
**Subject:** Re: Minor Change trying to Clarify the issues raised about key exchange versus KEM

Jacob,

Do you want to turn it into a question on our FAQ? Combine what you wrote with some of what Ray discussed in his email response. Thanks,

Dustin

**From:** Alperin-Sheriff, Jacob (Fed)
**Sent:** Monday, October 31, 2016 4:39:48 PM
**To:** Perlner, Ray (Fed)
**Cc:** Moody, Dustin (Fed); Daniel C Smith (daniel-c.smith@louisville.edu); Perlner, Ray (Fed); Liu, Yi-Kai (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Peralta, Rene (Fed); Miller, Carl A. (Fed); Bassham, Lawrence E (Fed)
**Subject:** Re: Minor Change trying to Clarify the issues raised about key exchange versus KEM

For some reason it did a BCC (I tried to use Outlook to make it easier to send it to everyone but apparently I screwed that up). Hopefully it works right now

I think I agree, though, let's put it in the FAQ.

**From:** "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
**Date:** Monday, October 31, 2016 at 4:33 PM
**To:** "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
**Subject:** RE: Minor Change trying to Clarify the issues raised about key exchange versus KEM

Did you mean to send this to the whole pqc-team, or just me? It looks like you sent it to just me.

Regarding the added paragraph, I'm nervous about the last sentence: In particular, implicitly authenticated key exchange schemes like https://eprint.iacr.org/2014/589.pdf , don't seem to fit too naturally into the KEM framework. (Although technically you should be able to turn it into a KEM by putting in a dummy value for the authentication key, I think, it's probably a stretch to say IAKE schemes are "built around KEMs".)

Also, I think a better place to put this sort of material, might be the FAQ, where we could specify why we didn't provide APIs and security definitions for anything other than PKE, KEM and digital signature. The particular things that have been suggested but were left out were:

1) (what Dan Bernstein calls) DH functions, which were not supported because:
    a. They fit reasonably well into the KEM framework. (although we did explicitly mention that we would consider additional properties of DH functions, like asynchronous key exchange in section 4.C.1 of our CFP)
    b. There is no widely accepted security definition. (that we know of)

   c. Plausible security requirements (e.g. secure static-static key exchange) have not been met by any postquantum DH-like scheme that we know of.

2) IAKE (actually I'm not sure anyone suggested this as opposed to regular old AKE) which were not supported because

   a. The security model is complicated, and the stronger versions like extended Canetti-Krawczyck may be too hard to meet (the scheme I linked above was only proved secure in the Bellare-Rogaway model.)

   b. IAKE specifically is kind of a niche application. In most cases AKE is good enough, in which case it can be met by combining a KEM with a Digital signature algorithm, (and possibly a few other simple primitives like a PRF). We want to leave open the possibility that the signature algorithm and KEM will be provided by different submitters.

   c. While it's not quite natural, you can demonstrate some of the functionality of an IAKE scheme in the KEM framework. (We explicitly considered this possibility in section 4.C.1 of our CFP.)

3) I guess there's also stuff in the, "why would anyone ever want that?" category like undeniable signatures and multiround key exchange, …, I guess the point is that we have to draw the line somewhere if we're ever going to be able to manage this process.

**From:** Alperin-Sheriff, Jacob (Fed)
**Sent:** Monday, October 31, 2016 3:31 PM
**Subject:** Minor Change trying to Clarify the issues raised about key exchange versus KEM

I added a paragraph in Section 2.B.1, pursuant to a discussion Ray and I had today.

—Jacob Alperin-Sheriff