From: Peralta, Rene (Fed)
To: (b) (6) ; Perlner, Ray A. (Fed)
Cc: Alperin-Sheriff, Jacob (Fed); Moody, Dustin (Fed); Liu, Yi-Kai (Fed); Bassham, Lawrence E. (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Miller, Carl A. (Fed); Smith-Tone, Daniel C. (Fed); Regenscheid, Andrew R. (Fed)
Subject: Re: Hash-based signatures
Date: Wednesday, January 4, 2017 7:20:14 PM

Thanks to all for the clarifications. There is no contradiction with what I stated.
NIST is interested in hash-based signatures. Stateful hash-based signatures
are out of scope for the PQC CFP but in scope for the PQC project.

I also stated that the names of the people in the project is not a secret (most
are named as authors of the PQC report), and that we would make the list of
names public somehow.

Regards, Rene.

From: Daniel Smith (b) (6)
Sent: Wednesday, January 4, 2017 5:52 PM
To: Perlner, Ray (Fed)
Cc: Alperin-Sheriff, Jacob (Fed); Moody, Dustin (Fed); Peralta, Rene (Fed); Liu, Yi-Kai (Fed); Bassham, Lawrence E (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Miller, Carl A. (Fed); Smith-Tone, Daniel (Fed); Regenscheid, Andrew (Fed)
Subject: Re: Hash-based signatures

Aside from what is written in the CFP and the FAQs, I believe that we specifically addressed stateful hash-based signatures in our Q&A session at PQCRYPTO 2016 last February. There we said that we would likely standardize hash-based signatures in a separate process and would not be considering them for this process. (You can check the YouTube video to see if I am a liar.) I don't think that our plans have ever reneged on this promise, so we should probably stick to that. Now that our document is complete, we can always say that anything fitting the API will receive consideration and leave it at that.

Cheers!

On Wed, Jan 4, 2017 at 2:54 PM, Perlner, Ray (Fed) <ray.perlner@nist.gov> wrote:

> We didn’t say anything explicit, but it is implied by our API that stateful hash-based signatures are out, in terms of the main process. We are likely to standardize them in a separate process, probably earlier than we otherwise would. (assuming the IETF gets its act together and publishes an RFC we can copy.)

From: Alperin-Sheriff, Jacob (Fed)
Sent: Wednesday, January 04, 2017 2:52 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>; Daniel Smith (b) (6); Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Cc: Perlner, Ray (Fed) <ray.perlner@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>; Miller, Carl A. (Fed) <carl.miller@nist.gov>; Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>; Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>
Subject: Re: Hash-based signatures

I believe (apologies for the pun) this means Rene may be a “FAQing liar” since as I emailed earlier in the actual CFP we never made any explicit statements about stateful or stateless.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Wednesday, January 4, 2017 at 2:50 PM
To: "Peralta, Rene (Fed)" <rene.peralta@nist.gov>, Daniel Smith (b) (6), "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>
Cc: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@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>, "Miller, Carl A. (Fed)" <carl.miller@nist.gov>, "Smith-Tone, Daniel (Fed)" <daniel.smith@nist.gov>, "Regenscheid, Andrew (Fed)" <andrew.regenscheid@nist.gov>
Subject: RE: Hash-based signatures

Anything is in scope that fits the API we gave. As stated in our FAQ:

NIST plans to coordinate with other standards organizations, such as the IETF, to develop standards for stateful hash-based signatures. As stateful hash-based signatures do not meet the API requested for signatures, this standardization effort will be a separate process from the one outlined in the call for proposals. It is expected that NIST will only approve a stateful hash-based signature standard for use in a limited range of signature applications, such as code signing, where most implementations will be able to securely deal with the requirement to keep state.

So, stateful hash-based is not going to fit the API and we don’t want it submitted if it doesn’t. We will likely standardize stateful schemes outside of our submission process, within the next year or two.

I don’t know if this makes a liar out of you or not!

From: Peralta, Rene (Fed)
Sent: Wednesday, January 04, 2017 2:47 PM
To: Daniel Smith (b) (6) ; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Cc: Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Perlner, Ray (Fed) <ray.perlner@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>; Miller, Carl A. (Fed) <carl.miller@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>; Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>
Subject: Hash-based signatures

Somebody asked whether I was contradicting the statement that "NIST is not interested in hash-based signatures". I said "yes", hash-based signatures are in scope. Then Dan Boneh asked whether that included stateful hash-based signatures. I answered that we are open to someone making the case that these are useful despite the size of the private keys.

Don't make a liar out of me.

Rene.