From: Moody, Dustin (Fed)
To: Perlner, Ray A. (Fed); Chen, Lily (Fed); Liu, Yi-Kai (Fed)
Subject: Re: Tentative changes to address "standardization" comment
Date: Tuesday, July 5, 2016 4:57:46 PM

Sounds good to me. Thanks Ray!

From: Perlner, Ray (Fed)
Sent: Tuesday, July 5, 2016 2:43:11 PM
To: Chen, Lily (Fed); Moody, Dustin (Fed); Liu, Yi-Kai (Fed)
Subject: RE: Tentative changes to address "standardization" comment

For the FAQ, how about the following:

Q: What are NIST's plans regarding stateful hash-based signatures?

A: 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 this 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.

From: Chen, Lily (Fed)
Sent: Tuesday, July 05, 2016 12:47 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Subject: RE: Tentative changes to address "standardization" comment

Dustin:

Ray and I will draft one for hash based signature.

Lily

From: Moody, Dustin (Fed)
Sent: Tuesday, July 05, 2016 12:40 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Subject: Re: Tentative changes to address "standardization" comment

The current version of the FAQ I have doesn't have anything about hash-based signatures

---

From: Chen, Lily (Fed)
Sent: Tuesday, July 5, 2016 12:39:21 PM
To: Moody, Dustin (Fed); Perlner, Ray (Fed); Liu, Yi-Kai (Fed)
Subject: RE: Tentative changes to address "standardization" comment

Yes. Hash based signature is what Ray and I talked about in the FAQ.

Lily

From: Moody, Dustin (Fed)
Sent: Tuesday, July 05, 2016 12:38 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Subject: Re: Tentative changes to address "standardization" comment

Ray,
With Lily's suggested revision for the first section of text, I noticed we don't have anything in our Call saying hash-based signatures are out of scope. Ray, can you add another FAQ question dealing with hash-based signatures? You can say things like they are out of scope for our process, we are coordinating with other standards groups, and they will likely be standardized only for certain applications. Thanks,
Dustin

From: Chen, Lily (Fed)
Sent: Thursday, June 30, 2016 4:56:45 PM
To: Moody, Dustin (Fed); Dustin Moody (b) (6) ; Regenscheid, Andrew (Fed)
Subject: Tentative changes to address "standardization" comment
I tentatively made some changes in two places to address Ajit's comments on the term "standardization". I found one paragraph is just too loose and difficult to follow. I simplify it significantly.
Please take a look and tell me what you think.
Lily