From: Regenscheid, Andrew (Fed)
To: Moody, Dustin (Fed); Chen, Lily (Fed)
Subject: Re: authority for hash-based
Date: Tuesday, July 17, 2018 12:48:16 PM

I think that's really a non-issue. SP's were a lot less common when we started the modes of operation work. Now no one seems to question SP vs. FIPS unless we were specifically instructed by law/executive order to do a "standard."

That being said, I don't have a problem with including that sentence in the explanation section. It's easy enough to do.

-Andy

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Tuesday, July 17, 2018 at 12:12 PM
To: "Regenscheid, Andrew (Fed)" <andrew.regenscheid@nist.gov>, Lidong Chen <lily.chen@nist.gov>
Subject: authority for hash-based

Morrie suggested that we add something into FIPS 186, since it's still open, about authority to standardize other signature schemes (to cover stateful hash-based signatures).

Here's what the similar text in FIPS 202 said (in the Explanation section in the preface):

"The KECCAK-p permutations were designed to be suitable as the main components for a variety of cryptographic functions, including keyed functions for authentication and/or encryption. The six SHA-3 functions can be considered as modes of operation (modes) of the KECCAKp[1600,24] permutation. In the future, additional modes of this permutation or other KECCAK-p permutations may be specified and approved in FIPS publications or in NIST Special Publications."

We could add a similar statement at the end of the Explanation section:

"In the future, additional digital signature schemes may be specified and approved in FIPS publications or in NIST Special Publications."

Does that sound fine?

Dustin