**From:** Regenscheid, Andrew R. (Fed)
**To:** Moody, Dustin (Fed); Chen, Lily (Fed); Scholl, Matthew A. (Fed)
**Subject:** Re: FIPS vs SP question
**Date:** Tuesday, March 15, 2022 10:48:21 AM

---

So, the original idea of 800-series Special Pubs was that they would support FIPS standards. So, we had AES specified in FIPS 197, which specifically referenced the creation of the 800-38 series on modes.

The key establishment documents in 800-56A and -56B have been strange special cases. My understanding is that their historical connection to ANS X9 standards made FIPS documents practically challenging, and the decision to move forward with Special Pubs was justified on the basis of vaguely similar mathematical techniques being specified in FIPS 186.

If we're trying to be fully in-keeping with past rationale and actions, we'd make all of the PQC algorithm standards FIPS. But the PQC migration is admittedly one of the few opportunities where we could plausibly change paths. That is, we could conceivably create some other parent-level FIPS document to cover crypto algorithm specifications, or consider FIPS 140 a parent-level document. And then we could potentially justify just using SPs moving forward. I'm not convinced that's a good idea, though. Instead I'd say we should just follow our more recent model of keeping the algorithm specifications fairly short, and include additional guidance in companion special pubs.

-Andy

---

**From:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
**Date:** Tuesday, March 15, 2022 at 9:58 AM
**To:** Chen, Lily (Fed) <lily.chen@nist.gov>, Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>, Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
**Subject:** FIPS vs SP question

Matt, Andy, Lily,

I was just thinking about Matt's question, and decided to look at what we'd said about FIPS and SP's before. In section 3 of NISTIR 7977 (https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7977.pdf) it says:

> **Federal Information Processing Standards (FIPS):** By federal statute , FIPS publications are issued by NIST after approval by the Secretary of Commerce and mandatory for non-national security federal systems. They are used by NIST to publish — among other things — standards for fundamental cryptographic primitives, such as block ciphers, digital signature algorithms, and hash functions.
>
> **NIST Special Publications (SP):** NIST SPs document a wide range of research,

> guidelines, and outreach efforts, including computer and information security. Cryptographic guidelines in the 800 series build upon the core cryptographic components specified in FIPS and other publications produced by SDOs and by NIST, sometimes specifying additional cryptographic algorithms, schemes and modes of operation, as well as providing guidance for their use. For example, cryptographic SPs in the 800 series specify random bit generators, block cipher modes of operation, key-establishment schemes, and key-derivation functions. These algorithms and schemes use the block ciphers, hash functions, and mathematical primitives defined in FIPS publications as fundamental building blocks. NIST also issues guidelines on the selection and use of cryptographic algorithms via SPs in the 800 series.

Based on that text, it would seem to suggest that at least Dilithium (and maybe all three signatures) should be a FIPS. The KEMs would be SP's. But it's probably up to us on whatever we want. In my mind, we would create new documents rather than adding to the existing ones. Although, if we hurry we could get Dilithium in FIPS 186-5 maybe!

Dustin