From: Ferraiolo, Hildegard (Fed)
To: Regenscheid, Andrew R. (Fed); Chen, Lily (Fed); Moody, Dustin (Fed); Scholl, Matthew A. (Fed)
Subject: RE: FPKI Policy Authority
Date: Wednesday, April 13, 2016 12:04:33 PM

Thanks Dustin. I've added some comments to Andy's notes below in green.
Also: The discussion yesterday at FPKI-PA was also about the PKI shared service providers who have been testing and planning for migrations to either ECC or RSA 3072+ - for the intermediate CAs etc. The End Entity Certificates (PIV and other person and non-person end entity certs) are governed under Common Policy for the federal agencies, which are aligned with NIST specs. They are currently 2K RSA certs. The question they had, as Dustin said to move to 3K or to ECC.
Hildy

From: Regenscheid, Andrew (Fed)
Sent: Wednesday, April 13, 2016 9:26 AM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Scholl, Matthew (Fed) <matthew.scholl@nist.gov>
Cc: Ferraiolo, Hildegard (Fed) <hildegard.ferraiolo@nist.gov>
Subject: Re: FPKI Policy Authority

Re: Mandate
I wonder what they mean, here. Would they consider the SHA-1 -> SHA-2 transition a "mandate," or would they want to see some sort of specific directive from the White House? Or, perhaps they were thinking of ECC, for which there was never a transition mandate. As Lily said, though, it's too early for a transition plan.

Re: Pre-Quantum Guidance
I wonder if this is partially a reaction to the NSA's new CNSA suite, which is billed as transitional "pre-quantum" guidance, to some extent. But we didn't have the same need to update our crypto suite.

//Yes – I think this is the case here. From our side (for PIV), all I can point to is 131A timelines and that RSA 2048, ECC P-256, P-384 are fine until 2030, but that somehow contradicts our quantum computing findings and strategy in NIST IR 8105.

NISTIR 8105 is light on immediate guidance for agencies. We should probably expand on that, even if it is merely to say they don't need to do anything special other than be aware that there could be a big transition in the future (there's a sentence alluding to that at the very end, but maybe we should expand on that).

Re: DH/RSA-4096
In general, I think people are surprised to learn that 4096-bit RSA/DH isn't included in our standards and guidelines. For that reason, I'm not sure something like a Facebook or Twitter post would even be effective, since people wouldn't be looking for it. We mostly just need to make sure that it's allowed within CMVP/CAVP, and that we have something "official" to point people to that ask questions. An IG is probably a good short-term item.
-Andy

From: Chen, Lily (Fed)
Sent: Wednesday, April 13, 2016 9:02 AM

To: Moody, Dustin (Fed); Regenscheid, Andrew (Fed); Scholl, Matthew (Fed)
Cc: Ferraiolo, Hildegard (Fed)
Subject: Re: FPKI Policy Authority

Hi, Dustin:

Thank you for the notes. We will develop transition plan as we did in 800-131A, once new PQC standards are available. But we do not know whether and how we can make the plan clear at this stage. My personal feeling is that it might be a little too early for that.

For RSA-4096, we certainly will include in the next version of 56A and 56B. Maybe it is not soon enough to get the message out. I have always wanted to make our website more accessible through update Q&A or even facebook or twitters. But we may not have the resource right now to handle it.

Lily

From: Moody, Dustin (Fed)
Sent: Wednesday, April 13, 2016 8:15:02 AM
To: Chen, Lily (Fed); Regenscheid, Andrew (Fed)
Cc: Ferraiolo, Hildegard (Fed)
Subject: FPKI Policy Authority

Andy and Lily,

I gave a briefing at the FPKI Policy Authority meeting yesterday on a status update for ECC and PQC. It went well, and I just wanted to report back on a few of the things they seem to want from us.

- They recommended that if we want people to implement our PQC algorithms after they are standardized that there needs to be some kind of mandate with a deadline. Otherwise they can't get their bosses to transition to new algorithms. They thought it a good idea if we could state now that there will be a mandate.
- They wanted specific guidance as to what to use until PQC algorithms are approved. The specific use case asked about was for PIV issuers: "If you are going to rekey in the next 3 years, what should you use?" Same question for PIV-derived systems.
- They asked our stance on using RSA-4096. I told them it's not currently in our standards, but we would be adding it in as we revise our documents. They were glad to hear that, but wanted to know if we had some statement in any of our documents that states we are not opposed to RSA-4096. I think I recall we were going to add something like that to an Implementation Guidance? Do we say this anywhere?

Dustin