From: Dang, Quynh H. (Fed)
To: Moody, Dustin (Fed); Regenscheid, Andrew R. (Fed); Perlner, Ray A. (Fed); Dworkin, Morris J. (Fed); Chen, Lily (Fed)
Subject: 128-bit version for stateful hash-based sigs.
Date: Tuesday, June 9, 2020 9:16:26 AM

Hi all,

I support not approving 128-bit version of LMS and XMSS as I mentioned before.

However, again, the current response text has a clear flaw in its technical justification.

In addition, there would be serious consequences from that response.

That response would imply that AES-128 shall not be used in situations where upgrading to AES-192/256 is not practical. There are a lot of deployments where this is the case I think. So, the people with those deployments would start to panic: they don't know how to handle security compliance because NIST might disapprove AES-128 in a near future. The vendors/manufactures of such devices would have to shuffle their current practices: we got to remove AES-128 and put in AES-256 in our products etc....because NIST might disapprove AES-128 in a near future.

A lot of normal enterprises and vendors would start to worry also: planning to upgrade, planning to removing AES-128 because another implied/perceived consequence is that AES-128 is not secure and strong as originally thought. So, they want to to be proactive in their security compliance issues. Standard bodies would worry as well and would start to revise their requirements and recommendations etc...

Making this huge change with a flaw technical reason would hurt our reputation in a big way.

The PQC community would ask "Hey Dustin, we did not know that level 1 security is not good enough: where upgrading to level 2 or 3 security is not practical, level 1 is not approved."

I called and discussed the issue with Morrie yesterday.

One of the options to handle this that I could think of.

Publish the current draft but change the response to say that we don't have a decision on this option yet. We would like to have an opportunity to discuss this option with the community before we make our decision. Then, we'd send the question to various mailing lists including the PQC one.

After having sufficient amount of discussions, we'll make our decision at that time. This way, we practically avoid the 128-bit version for now (not making Stateful HBS so attractive as one of our goals).

Whether specifying it or not, we would have much better defenses after having such discussions with the community.

If we need to make a decision close to choosing a sig algorithm (Falcon for example), we could have a good reason to not specifying the 128-bit version because Falcon is a better choice.

Quynh.