From:	Chen, Lily
To:	Scholl, Matthew A. (Fed); Dodson, Donna F; Regenscheid, Andrew R. (Fed); Dworkin, Morris J. (Fed)
Cc:	Moody, Dustin (Fed); Liu, Yi-Kai (Fed)
Subject:	Hash based signatures
Date:	Tuesday, February 16, 2016 4:13:01 PM

We may not have to make a decision right away. But we probably need to start to look into more details. Here is a high level summary for thinking. Any opinions and comments are welcome.

Some hash-based signature schemes are relatively mature in the sense of algorithm security and based on well-understood assumptions. Shall we go ahead to standardize those schemes (without waiting to go through 5-7 year procedure)?

The reasons to start standardizing some hash-based signature schemes:

- It is a good exercise for post quantum cryptography standardization.
- IETF has initiated some drafts for hash-based signature, McGrew and XMSS.
- Hash-based signatures are good for code signing, which may need more than ten years signature lifetime.

Some concerns/questions

- There are some new key management challenges for hash based signatures because they are essentially one time signatures. (We may consider stateless signatures, but different issues.)
- Hash-based signatures may not serve well for entity authentication in many-to-many protocols such as IKE. Other signature schemes (not hash based) are needed in the future. Will supporting completely different signature schemes (hash-based and non-hash-based) become a challenge?
- Some optimized hash based signatures are under the development. The improved versions may turn out to be more suitable.
- Compared with encryption/key establishment, signatures in general are less urgent in preparing quantum time for backward secrecy. Do we really have the urgency to standardize hash-based signature, other than code signing?

It is likely that we will try to draft a “pseudo-SP” to see how it looks like. From there, we can have more solid ideas. We will keep everyone posted.

Lily