From: Moody, Dustin (Fed)
To: Chen, Lily (Fed)
Subject: FW: hash-based signatures
Date: Wednesday, February 8, 2017 9:49:00 AM

Here's what Quynh said. Do we need to do anything, or just wait for the IETF?

From: Dang, Quynh (Fed)
Sent: Wednesday, February 08, 2017 9:49 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: hash-based signatures

The XMSS scheme is getting through its final steps to become an RFC. I hope it will be done in a 2 or 3 months.

The other scheme is still under reviews/development step by the working group.

Quynh.

From: Moody, Dustin (Fed)
Sent: Wednesday, February 8, 2017 9:25:30 AM
To: Dang, Quynh (Fed)
Subject: hash-based signatures

Quynh,
Has there been anything new with hash-based signatures in the IETF? What's the current status?

Dustin