From:	David A. Cooper
To:	Dang, Quynh H. (Fed); Dworkin, Morris J. (Fed); Miller, Carl A. (Fed); Apon, Daniel C. (Fed); Davidson, Michael S. (Fed)
Subject:	Re: Allowing multi-level HSS and XMSS^MT
Date:	Tuesday, December 3, 2019 4:49:59 PM

All,

I realized earlier today that some of our responses to the public comments mentioned that we are restricting HSS and XMSS^MT to at most two levels. So, I went through all of our responses and modified any of them that mentioned that restriction. The revision version is on the SharePoint site.

The SharePoint site also includes the current version of the SP, which includes the edits made by Jim Foti and Isabel Van Wyk, in addition to the changes need to allow for more than two levels of trees. I looked through the edits that Isabel made and was willing to accept almost all of them, but there were a couple that I thought were incorrect, and so I undid those two changes.

Jim and Isabel are looking at the draft announcement text now, and I'll upload that to the SharePoint site once they are done with their review.

Dave

On 11/20/19 11:19 AM, David A. Cooper wrote:

> All,
>
> Based on the outcome of yesterday's meeting, which seemed to be leaning towards removing the restriction of at most 2 levels for a multi-level tree, I created a version of the SP that does not include the two-level limit. I made as few changes as possible. So, Section 3.3 only describes two-level trees and the section on creating backups also only describes two-level trees. The text does, however, make clear that more levels are allowed.
>
> It turned out that very little text needed to be changed. The biggest effort in creating this revised version was adding in the additional XMSS^MT parameter sets.
>
> The revised document is on the SharePoint site as "NIST SP on stateful HBS no level limits.docx". I started with a clean copy of the document and used track changes. So, this version has no comments and the only tracked changes are those that I made to remove the two-level restriction.
>
> Dave
>
> On 11/15/19 4:55 PM, Dworkin, Morris J. (Fed) wrote:
>
> > During Tuesday’s PQ meeting, I would like for the team to take some time discuss John’s comment on the draft special pub on stateful hash-based signatures, namely, that we should not limit the number of levels of

the Merkle trees to two. Next week, we'll also send out the latest revision of the draft, along with a summary of the changes in response to internal comments. The working group would like to post the draft soon for public comment, along with our responses to the previous public comments asking for input on how to best address the potential for misuse.

Morrie