From:	Dworkin, Morris J. (Fed)
To:	Kerman, Sara J. (Fed)
Cc:	Cooper, David (Fed); Chen, Lily (Fed); Scholl, Matthew A. (Fed); Foti, James (Fed)
Subject:	Re: Question about 800-208
Date:	Thursday, December 12, 2019 10:01:41 AM

Thanks, Sara.

From: Sara Kerman <sara.kerman@nist.gov>
Date: Thursday, December 12, 2019 at 6:23 AM
To: "Foti, James (Fed)" <james.foti@nist.gov>, "Dworkin, Morris J. (Fed)" <morris.dworkin@nist.gov>
Cc: "Cooper, David A. (Fed)" <david.cooper@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>, Matthew Scholl <matthew.scholl@nist.gov>
Subject: RE: Question about 800-208

The Stateful Hash Based Signature project page has also been updated with the new draft and the new PDF with the Feb 4 Public Comments **with NIST responses** has been uploaded.
https://csrc.nist.gov/Projects/stateful-hash-based-signatures

-Sara

From: Foti, James (Fed) <james.foti@nist.gov>
Sent: Wednesday, December 11, 2019 3:37 PM
To: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Cc: Cooper, David A. (Fed) <david.cooper@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>; Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Subject: RE: Question about 800-208

The draft is now online, along with the CSRC Update. A GovDelivery notice will be sent shortly.

Best,
Jim

From: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Sent: Wednesday, December 11, 2019 10:49 AM
To: Foti, James (Fed) <james.foti@nist.gov>
Cc: Cooper, David A. (Fed) <david.cooper@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: Re: Question about 800-208

Hi, Jim,

No, we decided ***not*** to include that sentence. It's omitted in the latest version on the SharePoint

site, and there's at least one other minor change—the link to the PQC page on csrc is set on the word "standards" instead of the phrase "standards for post-quantum-secure". There's also a placeholder for a link to "publication details."

I'm attaching that version.

MD

From: "Foti, James (Fed)" <james.foti@nist.gov>
Date: Wednesday, December 11, 2019 at 8:38 AM
To: "Dworkin, Morris J. (Fed)" <morris.dworkin@nist.gov>
Cc: "Cooper, David A. (Fed)" <david.cooper@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>, Sara Kerman <sara.kerman@nist.gov>
Subject: Question about 800-208

Hi-

First, it looks like the NIST Library will be able to post the draft (and activate the DOI) around midday or else this afternoon. We'll update CSRC as soon as the PDF is online.

Second, in the announcement text that Dave sent, he included the sentence "The multi-tree variants of LMS and XMSS are approved for use with two levels of trees but not with three or more levels," indicating that the authors were still making a technical decision about whether to include this. From a quick skim of the draft SP, it appears that this is the case. However, can you please confirm that this sentence should remain as-is? I'm attaching the full announcement again, for the sake of completeness and context.

Thanks!
Jim

Jim Foti | IT Security Specialist | Computer Security Division | csrc.nist.gov
P:301.975.8018 | jfoti@nist.gov
NIST | 100 Bureau Drive, Stop 8930 | Bldg. 222, Room B349 | Gaithersburg, MD 20899-8930