From: Dworkin, Morris J. (Fed)
To: Cooper, David (Fed)
Subject: Re: Draft summary for PQC team
Date: Tuesday, June 9, 2020 10:11:00 AM

Thanks

MD

From: "David A. Cooper" <david.cooper@nist.gov>
Date: Tuesday, June 9, 2020 at 10:08 AM
To: "Dworkin, Morris J. (Fed)" <morris.dworkin@nist.gov>
Subject: Re: Draft summary for PQC team

Hi Morrie,

I just looked and for some reason you weren't listed as a member of the HBS SharePoint site, so I added you back in.

Dave

On 6/9/20 9:54 AM, Dworkin, Morris J. (Fed) wrote:

> Sorry, I totally missed this message last week. We'll discuss your question at 1:00.
>
> An unrelated issue…recently I had Dustin add me to the Sharepoint for the whole PQC, and today hash-based signatures are no longer listed in Outlook as one of my Sharepoint groups. Is there a simple way to get it back?
>
> Morrie
>
> ---
>
> **From:** "David A. Cooper" <david.cooper@nist.gov>
> **Date:** Thursday, June 4, 2020 at 4:36 PM
> **To:** "Dworkin, Morris J. (Fed)" <morris.dworkin@nist.gov>
> **Cc:** "Dang, Quynh H. (Fed)" <quynh.dang@nist.gov>, "Davidson, Michael S. (Fed)" <michael.davidson@nist.gov>, Carl Miller <carl.miller@nist.gov>, Daniel Apon (b) (6)
> **Subject:** Re: FW: Draft summary for PQC team
>
> Hi Morrie,
>
> Thanks for forwarding Lily's comments. You can count me as one who didn't notice the message in SharePoint.

Based on Lily's comments I made a small change in Sections 5.1, 5.2, 5.3, and 5.4. Where the functions F, H, H_msg, PRF, and PRF_{keygen} are defined I changed the definitions to include the inputs, for example, "F: ..." became "F(KEY, M): ...." That wasn't done in RFC 8391, but it seem logical.

We can discuss the rest of Lily's comments on Tuesday.

One question: At the moment the document is still formatted as a draft. If we are 100% certain that this will be the final version, and that we won't be posting a second draft for public comment, then I'll go ahead and change the front matter to be consistent with a final document.

Thanks,

Dave

On 6/4/20 3:09 PM, Dworkin, Morris J. (Fed) wrote:

> I used the Sharepoint interface to send Lily's comments (below, and in the attachedfile) yesterday, forgetting that you might not see it that way.
>
> So let's not meet tomorrow, but plan to check in Tuesday at 1:00. I sent a calendar invitation.
>
> Morrie
>
> ---
>
> **From:** "Dworkin, Morris J. (Fed)" <morris.dworkin@nist.gov>
> **Date:** Wednesday, June 3, 2020 at 10:04 AM
> **To:** Stateful Hash-Based Signatures <StatefulHash-BasedSignatures@nistgov.onmicrosoft.com>
> **Subject:** FW: Draft summary for PQC team
>
> Good morning,
>
> FYI, here are Lily's comments. John has told me that he's still working on his.
>
> Since there's no full team meeting, I'm thinking we can check in with a teleconference at 10 on Friday?
>
> Morrie
>
> ---
>
> **From:** "Chen, Lily (Fed)" <lily.chen@nist.gov>

Date: Tuesday, June 2, 2020 at 4:07 PM
To: "Dworkin, Morris J. (Fed)" <morris.dworkin@nist.gov>
Subject: Re: Draft summary for PQC team

Hi, Morrie,

The document is well written. I agree with the resolutions the WG proposed on the public comments. I have a few very minor editorial comments as attached. It is not an easy task to have a Recommendation based on IETF RFCs w.r.t. what should be included in this Recommendation. Most of my comments are on whether to refer or to give a short explanation in this document. If you have question, please let me know.

Thanks,
Lily