From: Peralta, Rene (Fed)
To: Alperin-Sheriff, Jacob (Fed)
Subject: Re: PQC Forum content
Date: Monday, May 8, 2017 3:26:13 PM

Thanks Jacob.

Rene.

From: Alperin-Sheriff, Jacob (Fed)
Sent: Monday, May 8, 2017 3:24 PM
To: Bassham, Lawrence E (Fed); Regenscheid, Andrew (Fed); Chen, Lily (Fed); Perlner, Ray (Fed); Liu, Yi-Kai (Fed); Peralta, Rene (Fed); Daniel Smith (b) (6) ; Moody, Dustin (Fed)
Subject: Re: PQC Forum content

So I'm assuming silence = acceptance, and I'll post it at 4pm if there are no objections before then.

From: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Date: Monday, May 8, 2017 at 1:28 PM
To: "Regenscheid, Andrew (Fed)" <andrew.regenscheid@nist.gov>, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, "Peralta, Rene (Fed)" <rene.peralta@nist.gov>, "Daniel Smith (b) (6)
"Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Subject: Re: PQC Forum content

I like the way this is worded. It covers my biggest concern about distributing binaries since we say they should include source code and makefile(s).

On: 08 May 2017 10:10, "Regenscheid, Andrew (Fed)" <andrew.regenscheid@nist.gov> wrote:

I'd like to hear from Larry before we post anything. (I corrected the distribution list- the last email went to Larry Bennett, not Larry Bassham.)

-Andy

From: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Date: Monday, May 8, 2017 at 1:00 PM

To: Lidong Chen <lily.chen@nist.gov>, Ray Perlner <ray.perlner@nist.gov>, "Bennett, Lawrence H. (Assoc)" <lawrence.bennett@nist.gov>, "Regenscheid, Andrew (Fed)" <andrew.regenscheid@nist.gov>, "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, Rene Peralta <rene.peralta@nist.gov>, "Daniel Smith (b) (6)
"Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Subject: Re: PQC Forum content

Do we have any objections on this or can I send it out on the forum this afternoon? (Or do we want to wait a week or whatever for Dustin)

From: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Date: Friday, May 5, 2017 at 1:01 PM
To: "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Bennett, Lawrence H. (Assoc)" <lawrence.bennett@nist.gov>, "Regenscheid, Andrew (Fed)" <andrew.regenscheid@nist.gov>, "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, "Peralta, Rene (Fed)" <rene.peralta@nist.gov>, "Daniel Smith (b) (6)
"Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Subject: PQC Forum content

To send out on the pqc-forum after we've gotten consensus among ourselves:

We would like to make the following clarifications on the use of third-party open source libraries in the reference and/or optimized implementations, and are interested in your thoughts on the subject before we officially add them to the FAQ.

In short, they may be used, with the following caveats.

1) The library source code should be integrated into the submission package in a self-contained manner. This means that the submission package should contain build scripts which will allow for seamless "one-stop" building of the submitter's original code and all dependencies.

For example, on a Linux platform, it should require no more work to build the than running the standard

```
> ./configure [--options]
> make
> make install
```

succession of commands. The build process should not require the installation of any new libraries that are not contained in the submission package.

Separate build scripts should be included for the reference Windows platform and reference Linux platform that work using the GCC Compiler Collection (or ports thereof) and related tools as well as any platform-specific commands required.

2) As part of the written submission, the submitter shall describe in their own words the functionalities provided by any algorithms from third-party open-source libraries that are used in the implementations.
3) The submitter is responsible for ensuring that they abide by all requirements of the license (if any) under which said library has been released.

—Jacob Alperin-Sheriff