From: Moody, Dustin (Fed)
To: Bassham, Lawrence E. (Fed)
Subject: RE: My write-up in the PQC call
Date: Wednesday, March 23, 2016 1:52:54 PM

I'm only asking because later on (in Section 5) there is some text which says:

ii. *Compiler* (Note that the selection of this compiler is for use by NIST in the evaluation phase(s), and does not constitute a direct or implied endorsement by NIST.): The ANSI C compiler in the Microsoft Visual Studio 2005 Professional Edition.

And I want to make sure this is what you want.

From: Bassham, Lawrence E (Fed)
Sent: Wednesday, March 23, 2016 1:51 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: My write-up in the PQC call

I think what I have is correct. Write code in ANSI C that will compile on the reference platform that include GCC compiler (which will compile ANSI C).

Larry

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Wednesday, March 23, 2016 at 1:06 PM
To: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Subject: RE: My write-up in the PQC call

I saw the line

"NIST Reference Platform: Intel x64 running Windows or Linux and supporting the GCC compiler."

So… instead of the ANSI C compiler we will use the GCC compiler? Just want to make sure.

Dustin

From: Bassham, Lawrence E (Fed)
Sent: Wednesday, March 23, 2016 1:05 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: My write-up in the PQC call

There is some text in there that refers to the Reference Platform:

"NIST Reference Platform: Intel x64 running Windows or Linux and supporting the GCC compiler."

Larry

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Wednesday, March 23, 2016 at 12:49 PM
To: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Subject: RE: My write-up in the PQC call

Larry,

Thanks for the write-up. One more question for you. What compiler will you be using? The SHA-3 FRN had:

The ANSI C compiler in the Microsoft Visual Studio 2005 Professional Edition.

Is this still what you want?

Dustin

From: Bassham, Lawrence E (Fed)
Sent: Wednesday, March 23, 2016 11:32 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: My write-up in the PQC call

My sections. Let me know if you need more.

Larry