From: Moody, Dustin (Fed)
To: Bassham, Lawrence E. (Fed)
Subject: RE: KATs on SIKE
Date: Tuesday, October 17, 2017 1:41:30 PM

Also, Jacob wrote this about SIKE:

Your code should not be targeting a given operating system.

```
#define OS_LINUX     1

#if defined(__LINUX__)        // Linux OS
    #define OS_TARGET OS_LINUX
#else
    #error -- "Unsupported OS"
#endif
```

I realize this isn't a C standard thing, but it is quite annoying to include ".c" files (instead of standard inclusion of .h files), as it kills the automated script we've been using to do testing. We would strongly prefer if you were to put everything included into a single C file directly and/or ensure that each .c file itself includes the proper .h files.

Is this correct?

From: Bassham, Lawrence E (Fed)
Sent: Tuesday, October 17, 2017 1:40 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: KATs on SIKE

You could let them know that the modified version of my file that they are using called "PQCtestKAT.c" needs to be slightly modified. The "../../KAT/PQCkemKAT" is three levels up. It needs to be "../../../KAT/PQCkemKAT".

Larry

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Monday, October 16, 2017 at 3:23 PM
To: "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>
Subject: KATs on SIKE

Larry,

Could you double check something for me? Jacob checked the KATs for SIKE, and the checklist says they didn't match on our end. They have a very experienced team, so I just wanted to double check that we didn't miss anything. Let me know. Thanks,

Dustin