From: Regenscheid, Andrew (Fed)
To: Moody, Dustin (Fed)
Subject: Re: German PQC Candidates
Date: Wednesday, February 27, 2019 8:33:31 AM

No problem. I have access to the sharepoint site, and noticed there was already something that covered some of the candidates. I just had to spot-check a handful of them.

-Andy

On 2/27/19, 7:55 AM, "Moody, Dustin (Fed)" <dustin.moody@nist.gov> wrote:

Andy,
Thanks for doing this. I was going to come in first thing this morning and find the info, but it looks like you already did it. Sorry that it probably took a little bit of time!

Dustin

-----Original Message-----
From: Souppaya, Murugiah (Fed)
Sent: Tuesday, February 26, 2019 6:31 PM
To: Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>
Cc: Stine, Kevin (Fed) <kevin.stine@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: German PQC Candidates

Thanks Andy so much for the information. It is greatly appreciated and we will include it in Dr. Copan's NAV.

Murugiah

____
From: Regenscheid, Andrew (Fed)
Sent: Tuesday, February 26, 2019 4:30 PM
To: Souppaya, Murugiah (Fed)
Cc: Stine, Kevin (Fed); Moody, Dustin (Fed)
Subject: German PQC Candidates

Murugiah,

Here's the background information you requested for the Director Copan's meeting with BSI.

As you know, the PQC standardization process continues to have broad international participation. We had 82 total submissions, 69 accepted into the first round, and 26 advancing to the 2nd round. There were a total of 278 people who formed part of the submission teams, from 6 continents, including 26 countries and 16 states.

Of the 26 submissions moving into the 2nd round, 6 have team members from Germany research institutions and industry. These organizations included:

* Ruhr-University Bochum

·   Fraunhofer SIT

* Technische Universität Darmstadt (TU Darmstadt)
* Infineon Technologies

In addition, NIST is looking at emerging standards for quantum-resistant, stateful hash-based signatures. One of the two major proposals is XMSS, which has team members from TU Darmstadt and a German IT security company called genua GmbH.

Regards,
Andy