From:	Scholl, Matthew (Fed)
To:	Cichonski, Jeffrey A. (Fed); Frankel, Sheila E. (Fed)
Cc:	Hastings, Nelson E. (Fed); Stine, Kevin M. (Fed)
Subject:	Re: A Crypto paper on 5G PQC.
Date:	Thursday, April 4, 2019 10:23:28 AM

Thanks Jeff
These are all good comments. Let me know if its ok to send them on to Lily or if you want Nelson to send them.

From: "Cichonski, Jeffrey A. (Fed)" <jeffrey.cichonski@nist.gov>
Date: Thursday, April 4, 2019 at 10:20 AM
To: "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>, "Frankel, Sheila E. (Fed)" <sheila.frankel@nist.gov>
Cc: Nelson Hastings <nelson.hastings@nist.gov>, "Stine, Kevin (Fed)" <kevin.stine@nist.gov>
Subject: Re: A Crypto paper on 5G PQC.

Matt,

Nelson asked me to give it a once over. I haven't given him feedback yet but here it is;

- it seems to sensationalize the deployment model of 5g jumping right to a pretty advanced microservices deployment discussion.
- It definitively states that devices will no longer require a UICC/SIM. While this might be possible for a standalone network it is a hot topic and still a bit fuzzy.
- The whole notion of networks going 'All In on PKI' is over stated and once again sensationalized. Most likely if an operator already has a PKI they will utilize it to enable network functions (nfs) to use something like tls to securely communicate. Just as the case with LTE there is a broad cop out in the specification saying none of that is needed if these NFs reside in a trusted environment with adequate physical security.
- PKI exists in today's cellular networks and is used heavily by many operators from an operational perspective to manage their networks securely.
- It might make sense to include a note in this paper that the group responsible for specifying 5G security is very aware of and closely following the NIST PQC project.

Jeff

From: "Scholl, Matthew (Fed)" <matthew.scholl@nist.gov>
Date: Thursday, April 4, 2019 at 10:07 AM
To: "Frankel, Sheila E. (Fed)" <sheila.frankel@nist.gov>, Jeffrey Cichonski <jeffrey.cichonski@nist.gov>
Cc: "Stine, Kevin (Fed)" <kevin.stine@nist.gov>
Subject: A Crypto paper on 5G PQC.

This is a paper for QCrypt submission.
I want to be sure you have seen it before I hit the werb button
Thanks
Matt