From:	Chen, Lily (Fed)
To:	Perlner, Ray (Fed); Moody, Dustin (Fed)
Subject:	RE: Check slides
Date:	Tuesday, August 14, 2018 4:26:00 PM
Attachments:	QsCI2018-Prepost-08142018.pptx

Changed slide 8 again after talked with Ray.

Thanks,
Lily

From: Chen, Lily (Fed)
Sent: Tuesday, August 14, 2018 4:00 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Check slides

Hi, Dustin and Ray,

Thank you for the comments. Attached version incorporated your comments. Please check the following.

Slide 8, I think some "general applications" include using hash based signature to authenticate message in the handshaking protocol. Then I changed the statement to limit it for code signing and root/intermediate certificates or general applications (incl. code signing, root/intermediate certificates, message/entity authentication, and more). Please check

Slide 10, I include Kerberos as another example. Please check whether the statement can be improved.

Slide 10, I added challenges on QKD, please check. There are many challenges to think QKD can replace today's public key cryptography.

Slide 11, I used "essential" crypto primitives, it seems that Dustin likes "basic" crypto primitives, please tell if we should use "basic" instead of "essential".

Lily

From: Perlner, Ray (Fed)
Sent: Tuesday, August 14, 2018 2:14 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Check slides

Slide 3: The spacing on the timeline seems a little odd. E.g. the ~6 months between round 2 candidates and round 2 conference looks much smaller than the in reality much smaller intervals between submission due date, 1st round candidates, and 1st round conference. Also, have we

rd

committed to having a 3 round?

Slide 4: The diagonal box that says “post-quantum cryptography” is covered up.

Slide 6: “Include larger module” should be “include larger modulus”

Slide 8: Last bullet: I think we are settled that we are going to limit stateful hash-based signatures to certain applications. The question is how much. I think code-signing is definitely in. We’ve also seen requests to allow root and intermediate certificates. Any other applications?

Slide 9: “Quantum resistance schemes” should be “quantum resistant schemes”

Slide 10: I assume “pre-distributed key” is meant to include things like Kerberos. Right?

Slide 11: “As foreseeing” should just be “Foreseeing”

From: Chen, Lily (Fed)
Sent: Tuesday, August 14, 2018 1:24 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Check slides

Hi, Dustin and Ray,

Can you please help me to check the slides for the presentation I am going to give Saturday at the Quantum-Safe cryptography for Industry? Please let me know your comments.

Thanks,

Lily