From:	Perlner, Ray A. (Fed)
To:	Chen, Lily (Fed)
Subject:	RE: Public key chapter
Date:	Wednesday, March 2, 2022 1:24:00 PM

I talked to the other authors. We can switch the title to “first generation public key algorithms”

Thanks,
Ray

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Wednesday, March 2, 2022 8:45 AM
To: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Subject: Public key chapter

Hi, Ray,

Please don’t consider this as an official REB comment. I understand that you have 3 authors for the book and must have well considered the word used for the title. Just a curious question about the title “Legacy Public Key Algorithms”. I also understand “Legacy” is relative to “post-quantum”. But legacy also mean “denoting or relating to [software or hardware] that has been superseded but is difficult to replace because of its wide use.” Actually, RSA and ECC are still widely in use. The real replacement may not happen in another 3-5 years. I usually try to avoid to call them legacy. I call them PK systems [currently] in use, or PK systems without considering Quantum, or first generation PK algorithms. Of course, this is a chapter title. You surely do not want it long.

Please explain to me. Thanks,
Lily