Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria.

Mike Brown <Mike.Brown@isara.com>

Tue 9/13/2016 3:24 PM

To: pqc-comments <pqc-comments@nist.gov>;

Cc: Atsushi Yamada <Atsushi.Yamada@isara.com>;

Please find enclosed comments from us on the proposed submission and evaluation criteria for the Post-Quantum Cryptography Standardization Process.

Thanks,

Mike and Atsushi.

Page 3, first paragraph of Section 2.

The current submission process has a single deadline. Given the current state of post-quantum cryptography, it may be preferable to separate submissions into several generations to allow for new findings to be accommodated.

Page 7, first paragraph of Section 2.C.1

It is unclear the reason to include optimized source code within the submission package. Typically, optimizations are a way for industry to differentiate product offerings from each other and as such should be considered out of scope for the standardization process.

In addition, optimized code will often contain assembly which goes against the specification requirement of “written in ANSI C”.

Page 7, second paragraph of Section 2.C.1

Perhaps add encryption, decryption and shared secret generation for completeness.

Page 8, first paragraph of Section 2.C.3

Typically source code is also considered to be “written material”. To avoid ambiguity, perhaps reword as “supported documents.”

Page 10, last paragraph of Section 2.D.1

The first sentence says “the quantum-resistant algorithm evaluation process.” For consistency we think you mean “the post-quantum algorithm evaluation process.”

Page 12, first paragraph of Section 2.E

The list includes “source code”. The reference to English is ambiguous then since source code would be written in ANSI C. Instead do you mean that comments in source code should be written in English?

Page 14, Section 4.A.1

Instead of saying “IPSec” perhaps instead use “IPSec/IKE” is IKE is where the public key cryptography is. You may also consider adding S/MIME.