Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria

Morgner, Frank <Frank.Morgner@BDR.de>

Sat 9/17/2016 4:04 AM

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

Cc: Fumy, Walter <Walter.Fumy@BDR.de>; Nguyen Dr., Kim <Kim.Nguyen@bdr.de>;

Dear Sir or Madam,

the Bundesdruckerei is producing ID documents and runs a trust center for various use cases. We are currently involved in the EU project PQCRYPTO, the ISO SC27 WG2 efforts for Post-Quantum-secure algorithms and we are working on post quantum secure implementations with our subsideary company Genua. We are very excited that NIST is moving forward in standardization of PQC.

Unfortunately, standardization committees in general have suffered from a decline in credebility in the past years. Many people think that the standardization process can be manipulated by powerful industry lobbying and governmental intrests. We think, that a modern standardization should include the maximum amount of transparency possible. NIST has done a great job with the AES and the SHA-3 competition. We hope that this success can also be achieved with the standardization of Post-Quantum-Cryptography.

PQC will most likely be used for applications with long term security. Those applications are already in danger today, because encrypted communication can be stored forever and could be analyzed later with a quantum computing. We see a big need for PQC as of today. But of course, new algorithms should be evaluated well from many aspects. The mandatory criteria you have outlined are certainly necessary. Though we are looking at many of your optional features as mandatory.

One of the main problems is that PQC should receive a good amount of cryptanalytic attention before standardization. Therefor, we need to measure the confidence in an algorithm somehow. Means to create this confidence may, for example, be a proof of security, the number of scientific citations/reviews or
simply the time an algorithm has been out there for public review. With the urge today, this effectively means that we should concentrate the standardization efforts on algorithms that are known for a longer time. There are some promising algorithms that have been developed in the past years, but evaluation still needs some time.

An other essential part in the process of establishing thisconfidence is exposing a detailed and well-supported design rationale. This rationale can be used by experts to verify that the design indeed follows the design strategy (recall the curves that were not generated according to the public procedures), and verify whether the security margins offered by the design are consistent with the design strategy and target.

We hope this helps you refining your evaluation critarias. We are looking forward hearing your feedback.

Best regards,

Frank Morgner.