Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria

Meier Willi <willi.meier@fhnw.ch>

Fri 9/16/2016 7:09 AM

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

Cc: christian.rechberger@tugraz.at <christian.rechberger@tugraz.at>; martin.lauridsen@infosecglobal.com <martin.lauridsen@infosecglobal.com>; Meier Willi <willi.meier@fhnw.ch>;

Dear NIST Team,

we have a comment to your DRAFT Call for Proposals:

For proposals of digital signatures, could you make a more clear separation between a mode vs. a underlying primitive that instantiates this mode?

We believe such separation would be less applicable to other categories like encryption or key-exchange, but a similar distinction came up, e.g., in the CAESAR competition.

Best regards,

Christian, Martin, Willi