About stateful hash-based signatures

Ahto Truu <ahto.truu@guardtime.com>

Thu 9/15/2016 5:09 AM

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

Hello,

At http://csrc.nist.gov/groups/ST/post-quantum-crypto/faq.html#StatefulSignatures, there's a hint that NIST may be working with IETF towards standardization of stateful hash-based digital signatures. Is there any more detailed information you could share, such as timelines (however tentative), current state of affairs, or perhaps more specific contacts at either NIST or IETF?

With best regards,
Ahto Truu

--
Ahto Truu
Integration Architect
Guardtime | Information Assurance
+372 5175876