From: David A. Cooper
To: Dang, Quynh H. (Fed); Dworkin, Morris J. (Fed); Miller, Carl A. (Fed); Apon, Daniel C. (Fed); Davidson, Michael S. (Fed)
Subject: Re: Fw: Stateful HBS document by NIST
Date: Tuesday, August 27, 2019 8:47:30 AM

On 8/27/19 8:33 AM, Dang, Quynh (Fed) wrote:

> I just recalled one more thing: our specification does not include HSS, but a 1 or 2 level trees using LMSs. Since this is not compliant with the RFC, we should mention it.

Our specification does include HSS, and it is compliant with the RFC. In the case of a distributed multi-tree implementation, each cryptographic module implements LMS, but an external non-cryptographic device collects the signatures and public keys from these modules and combines them in appropriate ways to create the HSS public key and signatures. Note that unlike XMSS^MT, there are no HSS parameter sets.