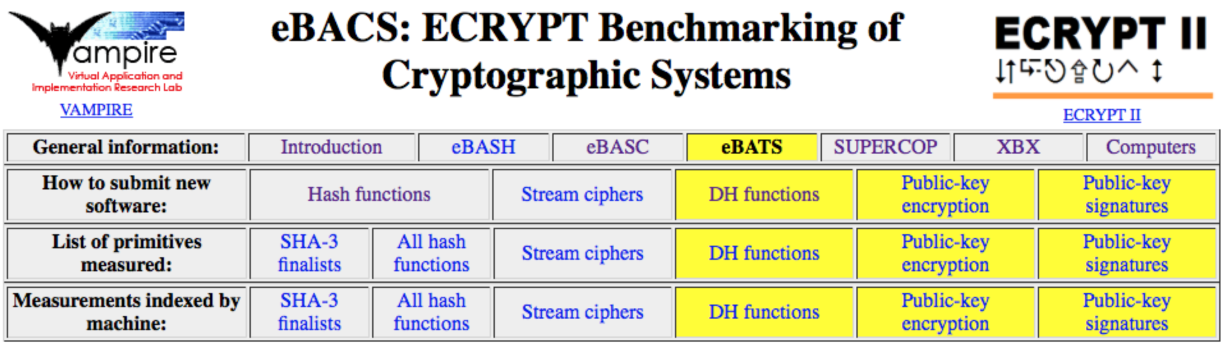
From: Moody, Dustin (Fed)
To: Bassham, Lawrence E. (Fed); Perlner, Ray A. (Fed)
Subject: Re: PQC API
Date: Thursday, May 26, 2016 10:28:09 AM
Attachments: image001.png

Yes, that is correct. Signatures, Encryption, and Key-exchange (for which DH is an example). Ray, correct me if I'm wrong.

From: Bassham, Lawrence E (Fed)
Sent: Thursday, May 26, 2016 10:25:52 AM
To: Moody, Dustin (Fed)
Subject: PQC API

Just verifying what I need API stuff for… I know we are asking for Public-Key signatures. Which of the others should I include? Is here anything we are asking for that is not covered below? I think we are looking at the DH functions, Pub-key encryption, and Pub-Key signature, but I just want to verify.

Larry



Vampire Virtual Application and Implementation Research Lab

VAMPIRE

eBACS: ECRYPT Benchmarking of Cryptographic Systems

ECRYPT II

ECRYPT II

General information:	Introduction	eBASH	eBASC	**eBATS**	SUPERCOP	XBX	Computers

How to submit new software:	Hash functions		Stream ciphers	DH functions	Public-key encryption	Public-key signatures
List of primitives measured:	SHA-3 finalists	All hash functions	Stream ciphers	DH functions	Public-key encryption	Public-key signatures
Measurements indexed by machine:	SHA-3 finalists	All hash functions	Stream ciphers	DH functions	Public-key encryption	Public-key signatures