From: Moody, Dustin (Fed)
To: Alperin-Sheriff, Jacob (Fed)
Subject: RE: ramstake checklist
Date: Tuesday, October 17, 2017 10:15:00 AM

The CFP says:

"Both the reference implementation and the optimized implementation shall adhere to the provided API. Separate source code for implementing the KATs shall also be included and shall adhere to the provided API."

To me, this seems to want code for the KATs that follows our instructions. On the other hand, if we can easily verify everything, then that's probably what is what counts? So, in that regard, Ramstake is fine, right?

Dustin

From: Alperin-Sheriff, Jacob (Fed)
Sent: Tuesday, October 17, 2017 10:08 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: ramstake checklist

What did separate source code mean then? I assumed it meant special source code just for the KATs in a separate directory from the Referenced and Optimized.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Tuesday, October 17, 2017 at 10:07 AM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Subject: ramstake checklist

Jacob,

It says:

__N__ Separate source code included for required KATs

But then the checklist seems to indicate the KATs are good. So what's the problem exactly?

Dustin