From: Bassham, Lawrence E (Fed)
To: Moody, Dustin (Fed)
Subject: Re: meeting recap
Date: Friday, April 14, 2017 8:04:45 AM

Should have something done next week. We really don't need it for quite awhile, but it will be better to get it out of the way.

On: 14 April 2017 07:55, "Moody, Dustin (Fed)" <dustin.moody@nist.gov> wrote:

Great. Any idea of how long that will take? We don't have any rush on this, but don't want it to be forever either....

From: Bassham, Lawrence E (Fed)
Sent: Friday, April 14, 2017 7:38:35 AM
To: Moody, Dustin (Fed)
Subject: Re: meeting recap

In OpenSSL there is an implementation from the AES/Rijndael team. Pretty sure we can use that. That gives us the AES. Still need to wrap CTR_DRBG around it and make it do the things John wants.

On: 14 April 2017 06:45, "Moody, Dustin (Fed)" <dustin.moody@nist.gov> wrote:

I asked John about side-channel protection. He said that at this point in the game, we shouldn't worry about it in regards to an implementation that we provide. Although I think you're right - Dan will probably complain.

Where did you get the implementation?

Thanks,

Dustin

From: Bassham, Lawrence E (Fed)
Sent: Thursday, April 13, 2017 8:49:08 PM
To: Moody, Dustin (Fed)
Subject: Re: meeting recap

Thanks. Sorry I couldn't be there. I think I have something (not using AES-NI), but it will use lookup tables (not resistant to cache-timing attacks). Dan will complain about that probably. It's his axe to grind.

On: 13 April 2017 15:05, "Moody, Dustin (Fed)" <dustin.moody@nist.gov> wrote:

Larry,

So, after our meeting I just wanted to summarize it for you. John is going to write up a response to Dan, incorporating what we discussed, and he'll send that around to all of us to read before sending it to Dan. But basically, we agree that the best solution is to have randombytes call a NIST DRBG, and that we provide the implementation and get Dan to put it in Supercop. So, we want you to keep looking for an implementation that we can use for one of our DRBG's.

Dustin