From: Brandao, Luis (IntlAssoc)
To: Dang, Quynh H. (Fed)
Cc: Peralta, Rene C. (Fed)
Subject: Re: Notes on crypto collaboration with IETF ... for a poster.
Date: Monday, October 18, 2021 7:33:47 AM

Thank you Quynh,

After some feedback from Lily, it seems that most of this may become more useful for a subsequent crypto reading club presentation about collaborations between NIST and standards organizations.

I'll followup about it in another email in a few minutes, also with a draft poster (quite summarized ... I still consider some of your answers) for possible feedback or corrections.

Thank you, Luís

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Monday, October 18, 2021 06:26
To: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>
Cc: Peralta, Rene C. (Fed) <rene.peralta@nist.gov>
Subject: Re: Notes on crypto collaboration with IETF ... for a poster.

Hi Luis,

See my comments/responses below in red text.

From: Brandao, Luis (IntlAssoc) <luis.brandao@nist.gov>
Sent: Friday, October 15, 2021 5:01 PM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Cc: Peralta, Rene C. (Fed) <rene.peralta@nist.gov>
Subject: Notes on crypto collaboration with IETF ... for a poster.

Hi Quynh,

Hope you are doing well.

It's a bit tight on time, but I'm now preparing a poster about crypto collaborations with standardization bodies, possibly to present in the ITL Science Day 2021. This is somewhat in sequence to the posters of 2019 and 2020 about crypto standards publications and projects.

Lily mentioned you as a point of contact about "IETF – NIST Crypto standards usage in internet security. [Quynh]"

With respect to this, would you be able to provide some brief notes on any of the following:

- Concrete NIST standards that somehow relate to collaboration (based on; affecting ...) with this standardization body

NIST's AES, GCM, CBC mode, elliptic curves (for DH and signatures) are adopted in all protocols which require security, generally speaking.

- Type of collaboration (e.g., NIST provides feedback about draft; some NIST member acts in some official role in a committee; technical input / leadership / coordination, ...others)

Me: Mainly to discuss NIST's standards and activities including future plans etc...with members at the IETF and to receive their feedback either in official meetings or in persons. Work with others to develop new standards for the IETF such as RFC 5758, RFC 8692, Additional Parameter sets for LMS Hash-Based Signatures (draft-fluhrer-lms-more-parm-sets-05), https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-kangarootwelve-06.

> draft-irtf-cfrg-kangarootwelve-06
>
> Internet-Draft KangarooTwelve August 2021 2.1.Inner function F The inner function F makes use of the permutation Keccak- p[1600,n_r=12], i.e., a version of the permutation Keccak-f[1600] used in SHAKE and SHA-3 instances reduced to its last n_r=12 rounds and specified in FIPS 202, sections 3.3 and 3.4 [].KP denotes this permutation.
>
> datatracker.ietf.org

I am not in any leadership role. I provide technical input when I think I need to do so at various working groups' meetings.

- Relevant past activities

Things have been typical. Nothings un-usual have happened in my view.

- Plans (or vision) about possible future activities

What I have been doing is the best for NIST in my view. Any leadership role would consume a ton of my time for non-technical work, so I have not accepted any role like that.

I have good relationships with various people at different corporations at the IETF.

- Benefits arising from the collaboration (e.g., synergies from the participation of various members)

Being active during the developments of crypto standards and security protocols helps the adoption of NIST's crypto options and helps to avoid technical tensions with NIST's standards and recommendations.

- Any other note you might want to emphasize

Nothing else I can think of to share.

The more specific/concrete the notes are, the better it will be. I will then do some editing (possibly some trimming) for the purpose of elaborating a hopefully good-looking poster, and will then share a draft for feedback/edits.

Thank you, Luís