From: Chen, Lily (Fed)
To: Mink, Alan; Mink, Alan (Assoc)
Subject: RE: approved crypto
Date: Wednesday, December 18, 2019 4:58:00 PM

Alan,

The needs for certain type of crypto functions, e.g. encryption, authentication, etc. are well justified by applications, for example, block cipher, hash function, signature, etc.

When we determined to develop an FIPS for a given function, for example, a block cipher, we will determine a way to select an algorithm. For example, in case of AES, we determined to have a competition. In the call for proposals, we did have criteria for block cipher. This is also the situation for hash function in SHA-3 competition, for post-quantum cryptography, and for lightweight cryptography. Or we might determine to adopt an algorithm which has been standardized in other standards bodies, for example, RSA signature was first standardized in X9.

It is not like we have a set of general minimum requirements so that people can submit an algorithm. It is also not the case that if it satisfies the minimum requirements, then we are going to develop an FIPS. We have minimum requirements only when we identifies a crypto function which we are going to develop standards. The requirements are for that specific function.

For some crypto functions, we may have determined not to develop standards and therefore no minimum requirements for that "function". For example, we are not going to develop standards on bitcoin, therefore, we do not have minimum requirements for bitcoin.

The level of cost and security benefit will also be judged for each specific function. For example, those for block ciphers and signatures can be different.

I think people asked those questions may have something in their mind. Let them to be specific.

Lily

-----Original Message-----
From: Mink, Alan <amink@nist.gov>
Sent: Wednesday, December 18, 2019 1:17 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Mink, Alan (Assoc) <alan.mink@nist.gov>
Subject: Re: approved crypto

But what are the minimum requirements for NIST to even consider drafting a FIPS for a method/algorithm/protocol ?

For example:
- needs detailed certification method
- needs some level of user demand
- needs some level of cost/security benefit
- needs ???

Thanks,
Alan

On 12/17/2019 3:48 PM, Chen, Lily (Fed) wrote:
> Hi, Alan,
>
> Here is the definition.
>

> "Approved - FIPS-approved or NIST-Recommended. An algorithm or
> technique that is either 1) specified in a FIPS or NIST Recommendation, or 2) adopted in a FIPS or NIST Recommendation and specified either (a) in an appendix to the FIPS or NIST Recommendation, or (b) in a document referenced by the FIPS or NIST Recommendation."
>
> You are correct that AES is approved because it is specified in FIPS 197. We have other crypto standards such as signatures are specified in FIPS 186 and key establishment in SP 800-56A/B/C, hash functions SHA2 and SHA3 in in FIPS 180 and FIPS 202, ...
>
> We do not have a list. But in SP 800-175A/B, you can find most of the algorithms listed there.
>
> I would not be surprised that no one in QKD working group knows NIST crypto standards because they are not crypto users. I would say that in order to be included in NIST standards, a minimum criteria is to publish it in research literature. We have multiple ways to develop crypto standards. For example, AES is selected through a competition. So is SHA3. We are selecting PQC now. We also have a project in developing lightweight crypto standards.
>
> Hope this helps.
>
> Lily
>
> -----Original Message-----
> From: Mink, Alan <amink@nist.gov>
> Sent: Tuesday, December 17, 2019 2:48 PM
> To: Chen, Lily (Fed) <lily.chen@nist.gov>
> Cc: Mink, Alan (Assoc) <alan.mink@nist.gov>
> Subject: approved crypto
>
> What is involved in becoming or what is the min criterion to be considered an approve crypto method/algorithm/protocol ?
> I believe NIST has a list of acceptable methods, like AES, etc ?
> This question recently came up at a QKD stds mtg and no one seemed to know !!!
>
> Thanks,
> Alan
>