From:	Apon, Daniel C. (Fed)
To:	Cooper, David (Fed); Perlner, Ray A. (Fed); Moody, Dustin (Fed); Chen, Lily (Fed); internal-pqc
Subject:	Re: revised FAQ on hybrid mode
Date:	Friday, December 20, 2019 9:06:30 PM

(Of course, feel free to disagree with me about our / NIST's sense of assurance that such schemes will work out well in all facets.. I just want to highlight a concern I have.)

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Friday, December 20, 2019 9:04 PM
To: Cooper, David A. (Fed) <david.cooper@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: revised FAQ on hybrid mode

While I am on vacation, this issue is important to me.. (Apologies for the late reply.)

I would prefer additional language surrounding the "*Does NIST consider the hybrid key establishment mode and dual signatures as a long-term solution?*" answer, aiming to pro-actively absolve us of blame should such hybrid-KEM constructions be mis-managed in future practice by the application engineers.

The previous answer was:

"*NIST leaves the decision to each specific application as to whether it can afford the implementation cost and performance reduction of a hybrid mode for key establishment or the use of dual signatures. Experience will help to decide on whether they can be a useful long-term solution. To assist, NIST will accommodate the use of a hybrid key-establishment mode and dual signatures in FIPS 140 validation when suitably combined with a NIST-approved scheme.*"

My proposed changes are:

NIST leaves the decision to each specific application as to whether it can afford the implementation cost, performance reduction, and engineering complexity (including proper and independent security review) of a hybrid mode for key establishment or the use of dual signatures. While the current situation is not clear, future experience will help to decide on whether they can be a useful long-term solution. To assist external parties who desire such a mechanism, NIST will accommodate the use of a hybrid key-establishment mode and dual signatures in FIPS 140 validation when suitably combined with a NIST-approved scheme.

From: David A. Cooper <david.cooper@nist.gov>
Sent: Wednesday, December 18, 2019 11:20 AM
To: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: revised FAQ on hybrid mode

I'm proposing a few more edits to try to address Philip Lafrance's confusion. It is clear that he is confusing signature validation with FIPS 140 validation, as he says:

> If both parties consider valid signatures to be ones that are FIPS validated, and if a hybrid signature with an approved and a non-approved algorithm is invalid as NIST suggests above....

At the end of his comment, Phillip says: "to accept a hybrid signature as *cryptographically* valid, all constituent signatures must successfully verify under their respective verification algorithms." At the very least I think we should adopt his use of "cryptographically valid" when referring to signature validation in order to help avoid the confusion between FIPS 140 validation and signature validation. This would mean changing:

> The dual signature is valid if and only if both (or all) signatures are valid.

to

> The dual signature is cryptographically valid if and only if both (or all) signatures are cryptographically valid.

The other changes that I propose in the attached may be considered unnecessary, as they are intended to make the text a little more precise with respect to FIPS 140. The changes are based on Section 1.23 of the FIPS 140 Implementation Guidance. To be more precise, I don't think the real question is whether a hybrid-key establishment or dual signature can be validated according to FIPS 140 but whether these operations can be performed in an approved mode of operation. According to IG 3.5. a non-approved cryptographic algorithm may be used in an approved mode of operation if the non-approved algorithm is not needed to support a security claim. This is what the text states -- that the hybrid-key establishment and dual signature are secure even if the post-quantum algorithm is not. So, for the purposes of FIPS 140 validation, the post-quantum algorithm is not a security function and so may be used in an approved mode of operation.

On 12/17/19 4:05 PM, Perlner, Ray A. (Fed) wrote:

> One additional edit.
>
> Changed “The experience will help decide…” to “Experience will help decide…”
>
> Ray
>
> ---
>
> **From:** Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
> **Sent:** Tuesday, December 17, 2019 3:46 PM
> **To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; internal-pqc <internal-pqc@nist.gov>
> **Subject:** RE: revised FAQ on hybrid mode
>
> I put in some additional edits.
>
> Mostly they are minor edits for readability. The most significant edit was that I replaced the statement:

"FIPS 140 validation can only validate a part of the dual signature that is currently approved by NIST. "

With

"Like hybrid key establishment schemes, dual signatures can be accommodated by current standards for use in FIPS mode, provided at least one of the signature methods is a properly implemented and NIST-approved."

I think the meaning of the latter statement is somewhat different, but I felt that the new content is what readers are more likely to be interested in. If we think it's necessary (I don't particularly, but I am open to persuasion) to retain more of the meaning of the original statement, we could add something like:

"FIPS 140 validation only assesses the security protection provided by the NIST Approved part of the dual signature. It does not attest to any additional security benefit that may be provided by the non-NIST approved component."

Ray

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Tuesday, December 17, 2019 3:17 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: revised FAQ on hybrid mode

Some minor edits attached.

We still probably want to try to clarify signature verification/validation and FIPS 140 validation….

Dustin

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Tuesday, December 17, 2019 2:57 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: revised FAQ on hybrid mode

Attached please see some tentative changes. Please feel free to tweak.

Thanks,

Lily

From: Chen, Lily (Fed)
Sent: Monday, December 16, 2019 11:21 AM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Comments received on Draft FAQ for Hybrid mode

Attached please see a few comments received on the draft we sent on October 30th,

2019. Maybe we can use 10-20 minutes to discuss resolutions at tomorrow's meeting.

Thanks,

Lily