

From: [Moody, Dustin \(Fed\)](#)
To: [Kerman, Sara J. \(Fed\)](#)
Subject: RE: some small PQC updates
Date: Wednesday, March 29, 2017 12:34:32 PM

I think it is probably v5, if that matters.

From: Kerman, Sara J. (Fed)
Sent: Wednesday, March 29, 2017 12:29 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: some small PQC updates

I can start with dates now.... We went from V1 to V4 last time, so I'm not sure if there this is v5 or maybe v8. From here on out can use the dates.

From: Moody, Dustin (Fed)
Sent: Wednesday, March 29, 2017 12:27 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: RE: some small PQC updates

Hmmm. Maybe dates is the best way? I don't really mind either way, if you have a preference you can go with whatever you want.

Dustin

From: Kerman, Sara J. (Fed)
Sent: Wednesday, March 29, 2017 12:25 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: some small PQC updates

Also, you've been giving me the API files with versions (v1, v4) is this v5? I'm referencing the version number on the "archive" page (so when this latest gets replaced, I want to know what version to call it). Or I can start using dates.

Sara

From: Moody, Dustin (Fed)
Sent: Wednesday, March 29, 2017 12:13 PM
To: Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Subject: some small PQC updates

Sara,

Can you add a new question to our PQC FAQ? It's contained in the attachment called FAQ-

randomness. Also, can you update our API document to the one attached? You can put them in whatever format/font etc. that you want to. Thanks,

Dustin