From: Moody, Dustin (Fed)
To: Robinson, Angela Y. (Fed); Dworkin, Morris J. (Fed); internal-pqc
Subject: Re: Terminology
Date: Thursday, June 25, 2020 3:24:07 PM
Attachments: 43A58A1DE3204A1DBF896820C21C63AA.png
A34B0016AA2E4684BE3E4D2C74F4F4C1.png
F399A78DE3D54B758DB97CF4C38C11F5.png

If we call them "alternates", then we could certainly call them "alternate candidates". I think the reverse is true too.

From: Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>
Sent: Thursday, June 25, 2020 3:22 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: Terminology

I thought we discussed this and concluded that we would call them “alternate candidates”.

Sent from Mail for Windows 10

From: Moody, Dustin (Fed)
Sent: Thursday, June 25, 2020 3:21 PM
To: Dworkin, Morris J. (Fed); internal-pqc
Subject: Re: Terminology

I like "secondary candidates", but it doesn't exactly roll off the tongue. It would be helpful if we had something easy that did. This is similar to the fact we don't have a nice simple name for our standardization process. So everybody (including us) often call it a contest or competition, even if it's not exactly correct. For that reason, I think "alternates" is the best I've heard so far.

I like the sports analogy John gave for alternates. I think it mostly conveys what we want about the eight non-finalists. (Or we could keep with the sports theme and do "varsity" and "junior varsity"!)

Dustin

From: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Sent: Thursday, June 25, 2020 3:05 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Re: Terminology

I’m okay with “alternates” but how about “secondary candidates”? The term “finalist” could be introduced as the shorthand for “primary candidates.”

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, June 25, 2020 at 3:03 PM
To: "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>, "Cooper, David A. (Fed)" <david.cooper@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: Re: Terminology

To me, we've called them all candidates because they are in the evaluation phase. Once we think they are strong possibilities of being standardized, we call them finalists. For the eight "alternates", they are just continuing on being candidates.

So, to me its consistent. But we can come up with a better term or phrase.
From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Thursday, June 25, 2020 2:52 PM
To: Cooper, David A. (Fed) <david.cooper@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: Terminology

I don't think "alternate" has a negative connotation. (If you hear that someone was an alternate for the US Olympic gymnastic team, you don't hear it as an insult.) But if it does, we should find some other one-word thing to use in its place. And that word shouldn't include "candidates" since we're using "candidates" to mean all algorithms in the competition, including the ones that didn't make it to the third round at all.

--John

From: "David A. Cooper" <david.cooper@nist.gov>
Date: Thursday, June 25, 2020 at 14:47
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: Re: Terminology

I think using "candidates" to refer specifically to those algorithms advancing to the third round, but not as finalists, is confusing. We've been using the term "candidate" since the CFP to refer to all submissions that are still under consideration. In the current report we say that the process started with "69 candidate algorithms," and say that there are "26 second round candidate algorithms." It would be very confusing to then, when talking about the third round say that "candidate" means algorithms that have not been eliminated but that are not finalists.

Rather than overloading the term "candidate," I think it is much better to separate the algorithms moving on to the third round as finalists and alternates (or alternate candidates). If there is concern that "alternate candidates" has negative connotations, we could replace it with something like "additional candidates." But, trying to use "candidates" to refer to just the alternates will be confusing given all of the other uses in the report of "candidates" to refer to all remaining algorithms.

On 6/25/20 2:32 PM, Moody, Dustin (Fed) wrote:

> John,
>
> I tried to unify this. I put in a couple of sentences that the 7 finalists are called "finalists" and that other 8 advancing on are called "candidates". We often add an adjective to the candidates, such as "additional candidates" or "alternate candidates". Did you find somewhere where "candidates" is being used to apply to the finalists?
>
> Dustin
>
> **From:** Kelsey, John M. (Fed) <john.kelsey@nist.gov>
> **Sent:** Thursday, June 25, 2020 2:22 PM
> **To:** internal-pqc <internal-pqc@nist.gov>
> **Subject:** Terminology
>
> Everyone,
>
> I'm going over the document again after not looking at it for a few days. One problem I keep noticing—we do not have consistent terminology for our track 1 candidates, our track 2 candidates, and for all the stuff in round 2.
>
> The best terminology I've seen in our document for this is:
>
> a. Track 1 candidates are "finalists."
> b. Track 2 candidates are "alternates,"
> c. All the algorithms in the second round are "candidates."
>
> We can always put "algorithm" after that term—"finalist algorithm" or "alternate algorithm" or "candidate algorithm." But I think we'd be much more clear if we tried to stick to this (or some other) consistent terminology for the different algorithms across the whole document. I keep seeing places where we use slightly different terminology for them in different sections (probably because each of us uses slightly different terminology).
>
> Thanks,
>
> --John