

From: Moody, Dustin (Fed) <dustin.moody@nist.gov> via pqc-forum <ppc-forum@list.nist.gov>
To: pqc-forum <ppc-forum@list.nist.gov>
Subject: [ppc-forum] Round 4 submissions have been posted
Date: Thursday, October 27, 2022 11:38:16 AM ET

Everyone,

We just wanted to let you know that the Round 4 candidates' submission packages have been posted at:

<https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions>

Each team has included a description of their changes from the 3rd round. Thanks,

Dustin Moody

NIST PQC team

From: Brent Kimberley <brent.kimberley@durham.ca> via pqc-forum <pqc-forum@list.nist.gov>
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>, pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] RE: Round 4 submissions have been posted
Date: Monday, October 31, 2022 11:35:12 AM ET

Hi.

Is the lifecycle diagram for CNSA 1.0 and/or 2.0 publicly available?

To the best of my knowledge, the lifecycle document for CNSA implicitly determines IF hybrid aka "Transitionary" cipher suites are required.

The system lifecycle drives the stage gate model.

The stage gate model drives phase acceptance criteria.

Phase acceptance criteria determines what can be released | commissioned | ... | decommissioned | disposed.

From: 'Moody, Dustin (Fed)' via pqc-forum <pqc-forum@list.nist.gov>
Sent: October 27, 2022 11:38 AM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Round 4 submissions have been posted

Everyone,

We just wanted to let you know that the Round 4 candidates' submission packages have been posted at:

<https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions>

Each team has included a description of their changes from the 3rd round. Thanks,

Dustin Moody

NIST PQC team

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.

To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visit <https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB86696981B067720958F95E6DE5339%40SA1PR09MB8669.namprd09.prod.outlook.com>.

THIS MESSAGE IS FOR THE USE OF THE INTENDED RECIPIENT(S) ONLY AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, PROPRIETARY, CONFIDENTIAL, AND/OR EXEMPT FROM DISCLOSURE UNDER ANY RELEVANT PRIVACY LEGISLATION. No rights to any privilege have been waived. If you are not the intended recipient, you are hereby notified that any review, re-transmission, dissemination, distribution, copying, conversion to hard copy, taking of action in reliance on or other use of this communication is strictly prohibited. If you are not the intended recipient and have received this message in error, please notify me by return e-mail and delete or destroy all copies of this message.