From: Moody, Dustin (Fed) <dustin.moody@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-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

--