PQC Standardization

Standard	Overall Range	Pure PQ conf	Hybrid PQ conf	Pure PQ auth	Hybrid PQ auth
SSH	3 to 7	3	7	3	3
TLS 1.2[1]	0 to 0	0	0	0	0
TLS 1.3[2]	3 to 6	4	6	4	3
X.509[3]	5 to 7	7	5	7	6
S/MIME / CMS	5 to 7	7	5	7	6
OpenPGP	2 to 6	2	6	6	6
IKE / IPSec	3 to 6	6	6	5	3
MLS	4 to 4	4	4	4	4
TPM	2 to 7	7	2	7	2
DNSSec	1 to 1	-	-	1	1

1: DTLS 1.2, FIDO inherit from TLS 1.2

2: DTLS 1.3, MACSEC, FIDO/FIDO2 inherit from TLS 1.3

3: UEFI inherits from X.509

Transport Issues in Standards	Status
TCP Initial Congestion Window	3
QUIC amplification protection	2
Merkle Tree Certs	4

Key

0	Consensus Against Inclusion
1	Blocked / Stalled
2	In Progress / Chartered
3	Unofficial Draft(s)
4	Official Draft(s)
5	Progress to Finalization
6	Near-Finalized
7	Finalized / Approved
-	Unknown / NA

MITRE

Post Quantum Cryptography Coalition