Algorithm Identifiers for NIST's PQC Algorithms for Use in the Internet X.509 Public Key Infrastructure abbrev: PQC KEM for Certificates

draft-turner-lamps-nist-pqc-kem-certificates-00

Sean Turner, Panos Kampanakis, Jake Massimo, Bas Westerbaan

LAMPS@IETF113 — 20220325

What's in this I-D?

Think of this as RFC 3279 for NIST's PQ KEM algorithm(s); the I-D provides the conventions and syntax for putting the algorithm identifiers and parameters into certificates. Think *AlgorithmIdentifier* in the *SubjectPublicKeyInfo* field, how to set the key usage extension, etc.

OIDs? Defined by NIST; will be added when we get them.

Parameters? None! The OID tells you all need to know.

Key Format? BIT STRING (any internal formatting left to crypto engine).

Key Usages? keyEncipherment.

Key/Certificate? One. (not a non-composite/hybrid certificate)

What's left to do?

How many algorithms? Right now just one PQ KEM "CANDIDATE TBD1"

Prohibit key usages? Seems okay to prohibit all signature related key usages.

> If we picked keyEncipherment we should probably MUST NOT keyAgreement, encipherOnly, decipherOnly.
>
> In other words, you set keyEncipherment that's the ONLY key usage you set.

What's left to do?

Keep private key format? Right now it is in there but not wed to it being in this I-D.

Add more security considerations? Right now it's a place holder for side channels.

> How far down this rabbit hole do we need to go?
>
> Shouldn't most of the security considerations be in the NIST documents that specify the algorithms?

What do we want?

WG Adoption