Internet X.509 Public Key Infrastructure - Algorithm Identifiers for Kyber

draft-ietf-lamps-kyber-certificates

Panos Kampanakis, Jake Massimo, Sean Turner, Bas Westerbaan

LAMPS@IETF116 - 20230329

Changes

Revised to only address Kyber: 512, 768, & 1024

Added ASN.1 (2021)

Added “Applicability Statement” section

Question

To avoid extra OCTET STRING Wrappers, is this correct?

```
pk-kyber-* PUBLIC-KEY ::= {
    IDENTIFIER id-alg-kyber-*
    -- KEY no ASN.1 wrapping -
    PARAMS ARE absent
    CERT-KEY-USAGE { keyEncipherment }
    --- PRIVATE-KEY no ASN.1 wrapping --
    }
```

To Do

Add examples

Wait for NIST to finish:

- Polite: Add ref to their module/OIDs
- Impolite: When can we do this? :)

Comments & PRs welcome on mailing list @ GH Repo