Internet X.509 PKI - Algorithm Identifiers for FrodoKEM

draft-smyslov-lamps-frodokem-certificates-00

Valery Smyslov (svan@elvis.ru)

IETF 125

Motivation

- There is some interest in using FrodoKEM in protocols
- OIDs for FrodoKEM are already allocated
- No specification for public/private key format
- No ASN.1 Module

I-D Content

- Document structure and most of the text were impudently borrowed from draft-ietf-lamps-kyber-certificates
  - many thanks to Sean, Panos, Jake and Bas!
- Existing OIDs (were allocated before)
- Public key and private key formats (simple `OCTET STRING`)
- ASN.1 Module
- No examples (yet?)

Issues

Currently both FrodoKEM and eFrodoKEM are specified. Do we need eFrodoKEM in certificates?

- eFrodoKem (“ephemeral”) keys can only be used < 256 times: effectively we got “one-time” certificates?
- On the other hand, OIDs exist for both, so let eFrodoKEM be in certificates too? Just in case...

Thanks!

Comments?

WG adoption?