Clarifications for Ed25519, Ed448, X25519, and X448 Algorithm Identifiers

draft-ietf-lamps-8410-ku-clarifications-00

Sean Turner, Simon Josefson, Daniel McCarney, Tadahiko Ito

LAMPS@IETF113 — 20220325

What's in this I-D?

Text that ought to look very familiar if you read any of the version of draft-ietf-lamps-5480-ku-clarifications or RFC 8813.

The only difference is that this I-D is clarifying the key usages for Ed25519, Ed448, X25519, and X448 that were defined in RFC 8410.

The key usages for X25519 and X448 only referred to keyAgreement, encipherOnly, and decipherOnly.

The key usagess for Ed25519 and Ed448 only referred to nonRepudiation, digitalSignature, keyCertSign, and cRLSign.

All certificates with id-X25519 & id-X448

keyAgreement	-> MUST contain
encipherOnly or decipherOnly	-> MAY
digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyCertSign, and cRLSign	-> MUST NOT

EE certificates with id-Ed25519 or id-Ed448

nonRepudiation and digitalSignature	-> MUST contain one or both
cRLSign	-> MAY
keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, encipherOnly, and decipherOnly	-> MUST NOT

CA certificates with id-Ed25519 or id-Ed448

keyCertSign	-> MUST contain
nonRepudiation, digitalSignature, cRLSign	-> Zero or more
keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, and decipherOnly	-> MUST NOT

What do we want?

WGLC!