Minor Update for RFC 5480?!?

• • •

draft-turner-5480-ku-clarifications | repo

Sean Turner & Tadahiko Ito
201907XX

Why are we here?

RFC 5480 Section 3 provides requirements for the Key Usage extension when SPKI includes: id-ecPublicKey, id-ecMQV, and id-ecDH.

But, only 7 of 9 values are included.

We are here to fix that!

What's on offer?

3 pages total!

Provide requirements for keyEncipherment and dataEncipherment.

MUST NOT be set for:

- id-ecPublicKey
    - i.e., unrestricted and ECDSA
- id-ecMQV
- id-ecDH

———

What do we want?

A pony or …

WG adoption* quickly followed by WGLC!

* Whether the draft's name is changed after WG adoption to draft-ietf-lamps is entirely up to you.

———