# Internet X.509 Public Key Infrastructure: Algorithm Identifiers for SLH-DSA

draft-ietf-lamps-x509-slhdsa-02

Kaveh Bashiri, Scott Fluhrer, Stefan Gazdag, Daniel Van Geest, Stavros Kousidis

IETF 121 – LAMPS

# -02

- Aligns with FIPS 205
- Adds private key format
- Adds examples

# WGLC

- Markku's fault attack comments
- 2021 ASN.1
- Fixed certificate example
- nits & minor editorial comments
- Will/did post -03 soon/yesterday

- *draft-ietf-lamps-dilithium-certificates* and pre-hash