draft-ietf-lamps-x509-shbs-03

• Since 119
  • Adopted
  • Refer to rfc8708bis
  • No extra ASN.1 wrapping of public key
  • Received IANA OIDs for id-alg-xmss-hashsig and id-alg-xmssmt-hashsig
  • Certificate examples

• Next
  • Fix certificate examples
  • (Private Key wrapping?)
  • WGLC?
draft-ietf-lamps-x509-slhdsa-01

• Since 119
  • Adopted
  • Added sha2/shake/fast/small to intro
  • Refer to draft-ietf-lamps-cms-sphincs-plus for (most) ASN.1
    • Expand SignatureAlgorithms and PublicKeyAlgorithms from RFC 5912
  • Try to be super explicit about raw public key encoding
  • Remove private key encoding text (handled in cms-sphincs-plus)
  • Security Considerations
  • Fill security strengths table

• Next
  • Wait for NIST (OIDs, pure vs prehash, signed context)
  • John Mattson requested it to cover PKCS#10, CMP, OCSP
    • Is there anything that precludes it being used in these? Text is heavily based on existing RFCs