6LoWPAN ND Address Protection

Behcet Sarikaya, Pascal Thubert, Mohit Sethi

IETF 100

Singapore
Status of 6LoWPAN ND extensions

• Reviews by Charlie Perkins and Bob Moskowitz
  • Changes applied in 03
  • Editorial clarifications, important rewriting
  • Crypto ID computation clarified

• Reviews by René Struik
  • Changes applied in 04
  • Now reference RFC 8032 for alternate signature using EdDSA curve Ed25519ph (pre hash for consistency)
What’s next?

• Ready for SecDir review and then WGLC