ECC Algorithms for MIKEY

<draft-ietf-msec-mikey-ecc-01>

Andrew Milne
Mitch Blaser
Daniel R. L. Brown
Eugene Chin
Lakshminath Dondeti
Presented By: Brian Minard

MIKEY-DHSIGN with ECDSA

- New Method
- Efficient alternative to MIKEY-DHSIGN with RSA
- Uses Signature Payload defined in RFC 3830

MIKEY-ECIES

- Use of symmetric ciphers tied to key sizes
- ECIES options now just X9.63-KDF [SEC1] and HMAC-SHA-1-160
- ECDH Primitive must be standard not cofactor

Editorial Changes

- Renamed methods as MIKEY-DHSIGN with ECDH and MIKEY-ECMQV
- MIKEY-DHSIGN with ECDH, added one more ECC curve (Group 6)
- MIKEY-ECMQV reference X9.63 2001 for ECMQV schemes

Questions?