Suite B Certificate and Certificate Revocation List (CRL) Profile <draft-solinas-suiteb-cert-profile-01.txt>

Sam Ashmore, NSA
on behalf of

Jerry Solinas, NSA
jasolin@orion.ncsc.mil
Lydia Zieglar, NSA
llziegl@tycho.ncsc.mil

Suite B Certificate & CRL Profile

- Profile of RFC5280
- Relies on RFC5480
- OIDs for Suite B ECC
- Examples (please check)
  - ECDSA signatureValue
  - Elliptic curve point
  - Subject public key
  - AlgorithmIdentifier
  - subjectPublicKeyInfo
- Certificate Types:
  - Self-Signed CA
  - Non-Self-Signed CA
  - End Entity Signature and Key Establishment