RFC 3279 Update ID

draft-ietf-pkix-ecc-subpubkeyinfo-06.txt

Sean Turner
Dan Brown
Kelvin Yiu
Tim Polk
Russ Housley

ECC subpubkeyinfo ID

- 3 versions since last IETF
  - Comments mostly from: Alfred Hoenes, Russ Housley, Jim Schaad
- d04:
  - Added OIDs (thanks Dan) for the restricted options: id-ecDH and id-ecMQV
  - Added an ’02 ASN.1 module
- d05:
  - Indicated ANSI can extend the SpecifiedCurve version
  - Updated module to be a superset of what’s in RFC 3279
  - Added an ’88 ASN.1 module

ECC subpubkeyinfo ID

- d06:
  - Capitalized keywords
  - Now refer to base point as G (was P)
  - Beefed up security considerations
  - Added normative appendix that address random base generation routines
- To Do:
  - Alignment with PKIX New ASN.1 ID?

Questions

?