RFC3279bis and RFC4055bis

draft-ietf-pkix-ecc-subpubkeyinfo-03.txt
draft-ietf-pkix-rfc4055-update-00.txt

Sean Turner
Dan Brown
Kelvin Yiu
Tim Polk
Russ Housley

ECC subpubkeyinfo ID

- 3 versions since last IETF
- d01: Comments from Russ Housley, Dave Kemp, and Bob Moeller
  - Replace verifiably random with verifiably pseudorandomly
  - Remove cRLSign from EE's KU
- d02: Comments from Russ Housley
  - Remove text that went along with EE's KU
- d03: Comments from Alfred Hînes
  - Lots of editorial fixes
  - Make ECPKAlgorithms extensible
  - Refer to FIPS 180-3 instead of 180-2?
- To Do:
  - In 2.2, first byte of key indicates compressed/uncompressed not first two
  - From 2.1.1.2.3, remove note about compressed/uncompressed that does not apply to FieldElements (as suggest by Alfred).
  - Register ECDH and ECMQV family OIDs.
  - Add and compile ASN.1 module.

RFC 4055 ID

- d00 submitted after IETF70
- Makes RSA-OAEP-params MUST NOT as opposed to SHOULD in SubjectPublicKeyInfo
- Changes in two paragraphs: 4 and 4.1
- To Do:
  - Section 3 in RFC4055 incorrectly refers to publicKeyAlgorithms field. It should be SubjectPublicKeyInfo's algorithIdentifier field. Could do it with errata or in this ID?
  - Determine whether PSS-SHA224->SHA512 defaults are fixed at 20 or whether they really are variable as text in 3.1 indicates.

Questions

?