ECC to Standards Track/MTI

IETF 90 – tls wg

20140721

Sean Turner – turner@ieca.com

Topics Covered

- Mechanics of moving EC to standards track.
- Whether to MTI it or not.

MECHANICS

Current state of affairs.

- RFC4492 currently at Informational
- Originally because of IPR concerns
- ECC now very widely used
- Also RFC 6090
- Broad support on list for making ECC standards track

How do we pull this off? (options)

- Reclassify 4492?
  - Reality: won't be a straight uplift because there are tweaks to 4492 based on 5246.
  - Tweak list: e.g., add brainpool & 25519, remove ?
- Pull it all into TLS1.3?
- 4492bis for TLS1.2?
- Both 4492bis + pull it into TLS1.3?
- Others?

MTI

What’s the MTI?

- This is JUST a primer!
- Some possible options to consider:
  - DHE only MIT
  - ECDHE only MTI
  - Both MTI