Status Since IETF 93

- Submitted version -04
- Removed some cruft
  - Explicit curve ECCurveTypes
- Added Simon and Manuel’s text on Curve25519 and Curve448.
- Added section on validation.
New Curves

- I copied part of the text from the old “Curve25519 and Curve448” draft.
- Still needs review – I might have missed a bunch of stuff.
- The CFRG document is in the RFC Editor’s queue, so this should not slow us down.
Pull Requests
PR #10

- Remove restrictions on signature algorithms in certificates.
- RFC 4492 required certificates with ECDSA keys to be signed with ECDSA.
  - This was in line with text in TLS 1.1
  - TLS 1.2 removed this restriction.
- Propose to remove this from our document.
  - Old implementation may not accept an ECDSA certificate signed with RSA
  - Some evidence that they don’t mind.
PR #11

• Add EdDSA Signature Support.
• Text by Ilari.
• Note that CFRG has not finalized the EdDSA document.
• This *could* introduce delays.
PR #13

- Modify IANA Policies
- Suggested by Sean
- Make the registries for NamedCurve, ECPointFormat and ECCurveType “Specification Require” rather than “IETF Review”.
PR #14

- Remove RC4 ciphersuites.
  - TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
  - TLS_ECDHE_RSA_WITH_RC4_128_SHA
  - TLS_ECDH_anon_WITH_RC4_128_SHA
  - TLS_ECDH_RSA_WITH_AES_256_CBC_SHA

- We’re not going to explicitly deprecate them – that has already been done elsewhere – just fail to mention them.

- Should we do the same with the corresponding NULL ciphersuites?
  - Does anyone really use NULL encryption in TLS?
Please review and send pull requests