Deprecating Obsolete Key Exchange Methods in TLS

Carrick Bartle, Nimrod Aviram

TL;DR

- draft-ietf-tls-deprecate-obsolete-kex-00:
- ❌ RSA Key Exchange
- ❌ Static FFDH
- 👍 FFDHE: Only when fully ephemeral, with group >= 2048 bit.
- 👎 Static ECDH

Open Issue

- FFDHE groups:
  - Client can’t reasonably verify group structure.
  - Group safelist likely impractical.
  - Hence, requirement for client to abort the connection if it can’t verify the group structure - also impractical.

Avenues Forward

1. Non-option: Deprecate FFDHE entirely - no consensus.
2. **Our suggestion: No requirement around group structure.**

- Web clients have already disabled FFDHE.
- Email clients are not going to verify group structure.
- **This single issue is holding the I-D since IETF 113.**

Thanks!