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 safe & well-known group >= 2048 bit.
- 👎 Static ECDH

Which WG?

- IETF 113: Make sure this falls under TLS WG (as opposed to UTA WG).
- Done, TLS Chairs checked with Paul Wouters, Security AD.

Open Issue(s)

- FFDHE only with safe, well-known groups:
  - Treat group that ships with Postfix as safe & well-known?
    - Our suggestion: Yes, and any other reasonably safe, widely-used group.

- FFDHE with a not-well-known group >= 2048 bits:
  - Client MAY verify group structure and connect?
  - If Client is unwilling to verify group structure: Client SHOULD/MUST abort the connection?

Thanks!