TLS

19 March 2024

draft-ietf-tls-deprecate-obsolete-kex

Internet Engineering Task Force
© 2024 IETF Trust
Production by Meetecho

IETF®

Plan

WGLC completed in 25 July 2023.

Stalled on chairs

Things to address:

- Align with 8447bis “D” (discouraged)
- Update IANA Considerations
- Revise draft

Aligning with 8447-bis

8447bis - Y = Recommended, N = Not Recommended, D = Discouraged

	TLS 1.2	TLS 1.3	Registry Marking (Obs-kex)
RSA	MUST NOT	NA	“D”
FFDH	MUST NOT	NA	“D”
ECDH	SHOULD NOT	NA	“N” ?
FFDHE	MUST NOT	MAY	“D” ?

Static DH Client Certificates

Draft does not currently talk about the use of static DH params in Client Certificates (1.2 Only). Should it say something about them?

	RFC8447bis	Registry Marking (obs-kex)
rsa_fixed_dh	“N”	“D” ?
dss_fixed_dh	“N”	“D” ?
rsa_fixed_ecdh	“N”	“D” ?
ecdsa_fixed_ecdh	“N”	“D” ?