A Year in the TLS Registries

Rich Salz*, Sabrina Tanamal (IANA)
IETF 118

Miscellany

- Experts: Yoav Nir, Rich Salz, Nick Sullivan; two of three needed
- Few to zero rejections
- May 2023: TLS ContentType: Replaced references to RFC 7983 with references to RFC9443
- September 2023: DES and IDEA cipher suites to historic (RFC 8996)

Cipher Suites, Signatures, Groups

- November 2022: Add Gost cipher suites and signature schemes
- November 2022: Add AEGIS
- May, June 2023: X25519Kyber768Draft0, SecP256r1Kyber768Draft0

Extensions

- October 2022: delegated credentials
- April 2023: sequence number encryption algorithm (Pismeny draft for DTLS)
- In progress: Hybrid X509 from ASC X9.146 (ANSI, ISO to follow); allows client and server to pick which key in a hybrid cert to use, or both

ALPN and Exporters

- Nov 2022: “tds/8.0” Microsoft Tabular Data Stream Protocol (database communication)

- February 2022: TEAP session key seed, session key generating function, inner method key, methods, teapbindkey@ietf.org; see RFC 9427

- June 2023: “dicom” https://www.dicomstandard.org/current (medical information transfer)