7525BIS

YARON SHEFFER, THOMAS FOSSATI & PETER SAINT-ANDRE

IETF-111

RECENT CHANGES

- Added a co-author: Thomas Fossati
- Published draft-ietf-uta-rfc7525bis-01 on 2021-07-07
- We've attempted to address all issues the authors have identified
- We'd appreciate feedback on several of open issues

DOCUMENT UPDATES

- SHOULD-level requirement for forward secrecy in TLS 1.3 session resumption
- Removed TLS 1.2 capabilities: renegotiation, compression
- Specific guidance for multiplexed protocols
- MUST-level requirement for ALPN, more specific SHOULD-level guidance for ALPN / SNI
- SHOULD-level guidance to avoid 0-RTT in TLS 1.3 unless it is documented for the particular protocol
- SHOULD-level guidance on AES-GCM nonce generation in TLS 1.2
- SHOULD NOT use static DH keys or reuse ephemeral DH keys across multiple connections
- 2048-bit DH now a MUST, ECDH minimal curve size is 224, up from 192

OPEN ISSUES

- Specify ChaCha20 / Poly1305 and an ECDSA cipher suite as a SHOULD for TLS 1.2?
  - So far we have NOT made these recommendations because (a) we're trying not to make too many changes to TLS 1.2 (b) if deployments really want these features, they can upgrade to TLS 1.3
- Adopt suggestions from draft-cooley-cnsa-dtls-tls-profile? (3072-bit RSA, 3072-bit DHE, ECDHE with secp384r1)?

CURRENT PLAN

- Incorporate any feedback we receive over the next 2-3 months
- Request WGLC around IETF 112