CYBERSECURITY

TLS 1.3 & Post-Quantum Cryptography

Dr. Adrian Stanger, CSD SCA

Commitments

- Standards
  - Security & Performance review
  - Library implementations
  - Transparency for trust-building
  - Interoperability
- Innovation
  - Recognize requirements
  - Seek solutions
- Acceleration
  - Forward-leaning guidance
  - Partnering

TLS

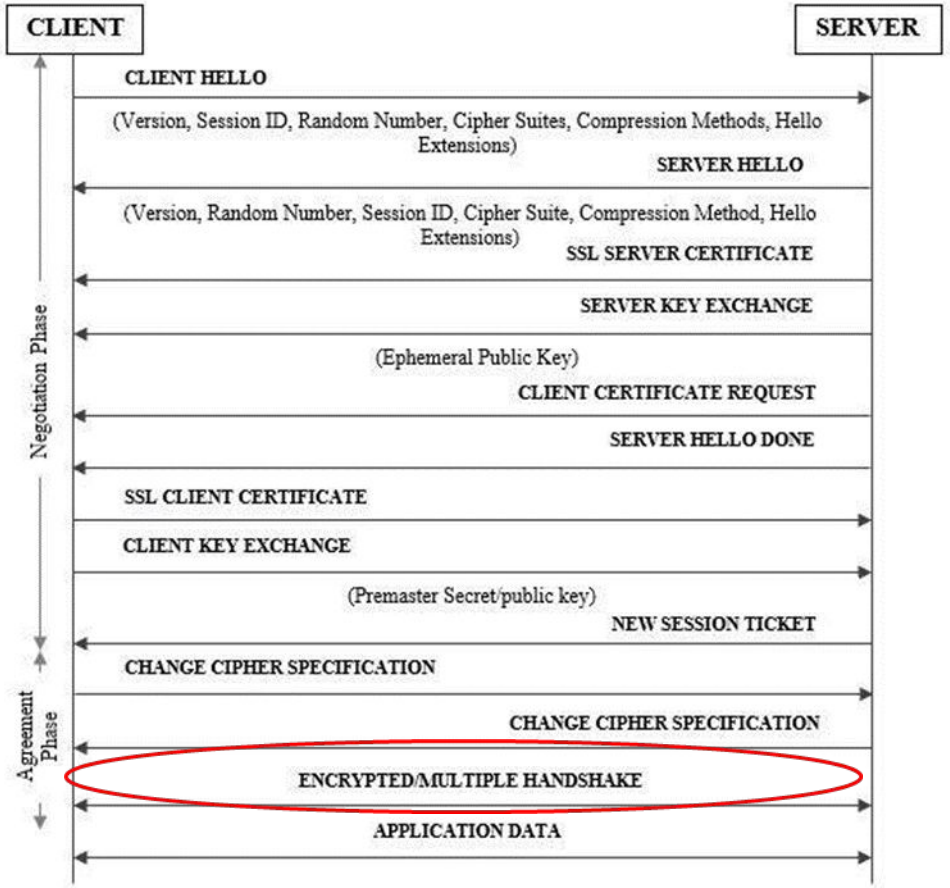
- Transport Layer Security (TLS) -- cryptographic protocol securing Internet communication
- Goals: confidentiality, privacy, integrity, and authenticity
- Widely used in web browsing, email, some VPN applications, Ethernet encryption, enterprise applications, and VOIP
- Current version: TLS 1.3
- Previous versions: SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2.
    - All frozen

TLS version 1.3

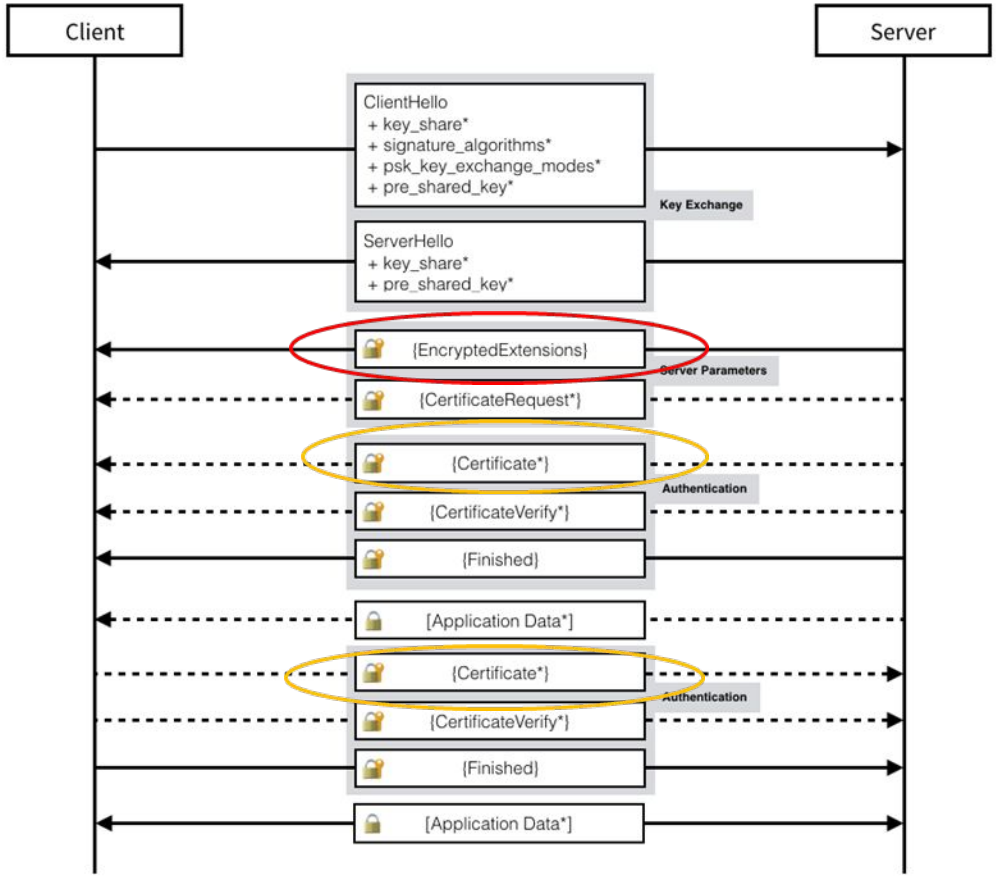
- Published August 2018 (RFC 8446)
- Improvements continue (dozens of RFCs)
- Improves security*, performance, and usability
- Simplified and more robust protocol
- Removed support for: RSA key exchange (RSA ok for signing), CBC mode, SHA-1, non-standard Diffie-Hellman groups
- **No previous versions will have PQC.**

TLS FLOW

1.2



1.3



IETF Standards

- TLS 1.3 (RFC 8446?)
- CNSA 1.0 Profile for TLS (RFC 9151)
- CNSA 2.0 Profile for TLS (Draft)
- ML-KEM (Draft)
- ML-DSA (Draft)

TLS 1.3 Adoption

- Widespread adoption
- 87% of TLS 1.3 adopters changed architecture to accommodate the update
- **Start planning, budgeting, and transitioning now**

EO 14306 & NMM-2025-005

- EO 14306:
  - **TLS 1.3 mandatory to *support* by 2 Jan 2030**
  - Further guidance to come from DOD (for NSS) and OMB (for non-NSS)
- Further guidance (NMM):
  - Enable TLS 1.3, activate CNSA 2.0 certificates
  - Deprecate earlier TLS versions
  - TLS 1.3 with CNSA 2.0 mandatory (lines up with CNSSP-15)
  - Recommendations
    - Architecture considerations
    - Ensure smooth rollover
    - Block earlier TLS versions

TLS 1.3 and monitoring

- TLS 1.3 poses challenges for monitoring
- TLS WG resists enterprise monitoring accommodations
  - Static keys
  - Attack surface
- Questions to ask:
  - Is monitoring needed?
  - How to best limit risks?
- NIST SP 1800-37
- **Goal: Monitoring shouldn’t weaken cryptographic security**

The end

- Questions?

- Contact info:

Adrian Stanger

adstang@nsa.gov