

# TLS-SRP draft update

Current version: draft-ietf-tls-srp-03

Ciphersuites:

- TLS\_SRP\_SHA\_WITH\_cipher - password authentication only (mandatory)
- TLS\_SRP\_SHA\_RSA\_WITH\_cipher - password+server authentication
- TLS\_SRP\_SHA\_DSS\_WITH\_cipher - password+server authentication

3DES is required, AES-128 and AES-256 are optional.

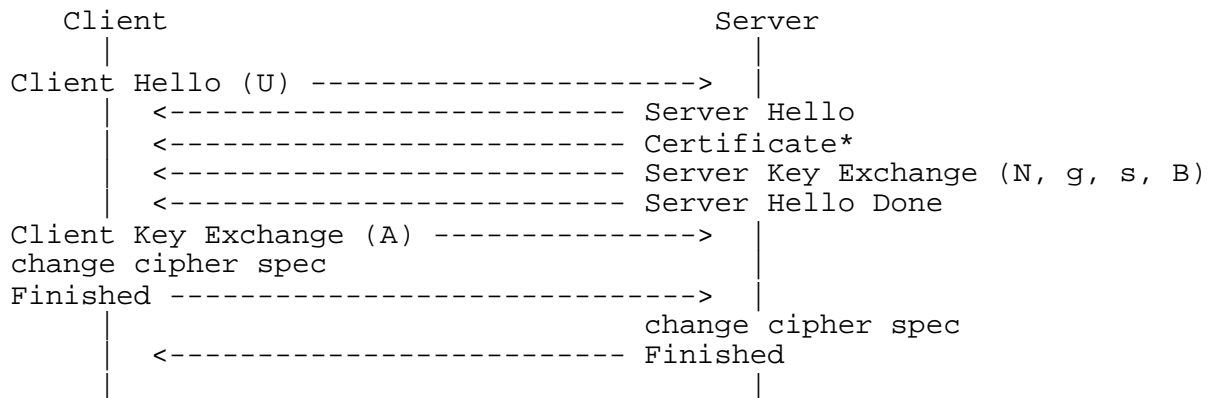
Next revision will incorporate SRP-6.

- <http://srp.stanford.edu/srp6.ps>
- Submitted to IEEE P1363.2 WG

SRP-6 improvements over SRP-3/RFC2945:

- Thwarts "two-for-one" guessing attack.
- Allows more flexibility in key exchange message ordering.

TLS message flow (proposed):



Uses TLS client extension to send username; works with resumption.

Performance of SRP ciphersuites expected to be similar to ADH and EDH.

Work in Progress - Integration with HTTPS: How to negotiate SRP and non-SRP on same server?

- "Missing Username" TLS alert