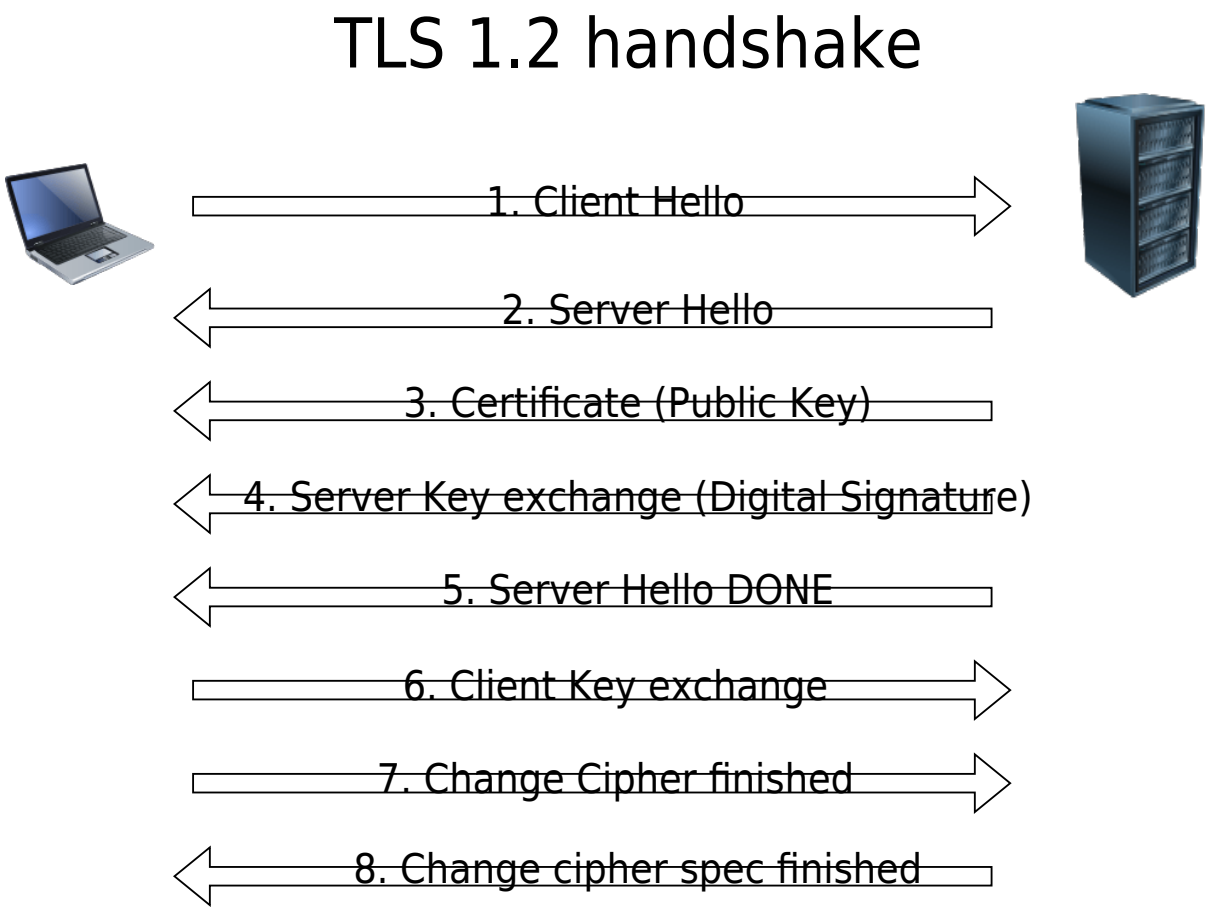
Security: Schemat działania TLS 1.2



Shared Secret (e.g. Elliptic Curve Diffie-Hellman Ephemeral - ECDHE)

Server Authenticity (e.g. Rivest–Shamir–Adleman - RSA)

Mechanism to make sure nobody tampered with the message