simplified and one-way authentication
TLS 1.3 (2018)

N_A, $ECDH_A$


N_B, $ECDH_B$, [$Cert_B$, sign(H(N_A || N_B || $ECDH_A$ || $ECDH_B$ || $Cert_B$))]$_K$

simplified and one-way authentication
TLS 1.3 (2018)

$N_A, ECDH_A$

$N_B, ECDH_B, [Cert_B, sign(H(N_A \| N_B \| ECDH_A \| ECDH_B \| Cert_B))]_K$

TLS 1.3 is much better than TLS 1.2

- ✓ Only one round in the handshake (vs 2 with TLS 1.2)
- ✓ Faster (use of elliptic curves)
- ✓ Certificate is encrypted (better confidentiality)
- ✓ Protocol has been formally proven
  (dos not prevent from implementation bugs)