

# TLS Handshake Diagrams

TLS 1.2 RSA Handshake:

```
Client                               Server
-----                               -----
ClientHello ----->
<----- ServerHello
<----- Certificate
<----- ServerHelloDone
ClientKeyExchange ----->
ChangeCipherSpec ----->
Finished ----->
<----- ChangeCipherSpec
<----- Finished
```

TLS 1.2 ECDHE Handshake:

```
Client                               Server
-----                               -----
ClientHello ----->
<----- ServerHello
<----- Certificate
<----- ServerKeyExchange
<----- ServerHelloDone
ClientKeyExchange ----->
ChangeCipherSpec ----->
Finished ----->
<----- ChangeCipherSpec
<----- Finished
```

TLS 1.3 ECDHE Handshake:

```
Client                               Server
-----                               -----
ClientHello
+ KeyShare (ECDHE)
+ SupportedVersions (incl. TLS 1.3)
+ CipherSuites
+ Extensions (SNI, ALPN, etc.) ----->

ServerHello
+ KeyShare (ECDHE)
+ ChosenVersion (TLS 1.3)
+ ChosenCipher
{EncryptedExtensions}
{Certificate (if needed)}
{CertificateVerify}
{Finished} <-----

{Finished} ----->

[Application Data ↔ Application Data (encrypted with app keys)]
```

Comparison: TLS 1.2 vs TLS 1.3

TLS 1.2 (RSA/ECDHE)

- Separate ClientKeyExchange
- Separate ServerKeyExchange
- ChangeCipherSpec messages
- Handshake messages in cleartext
- More roundtrips (2-RTT)

TLS 1.3 (ECDHE)

- ClientHello includes KeyShare
- ServerHello includes KeyShare
- No ChangeCipherSpec
- Encrypted after ServerHello
- Faster (1-RTT, 0-RTT possible)