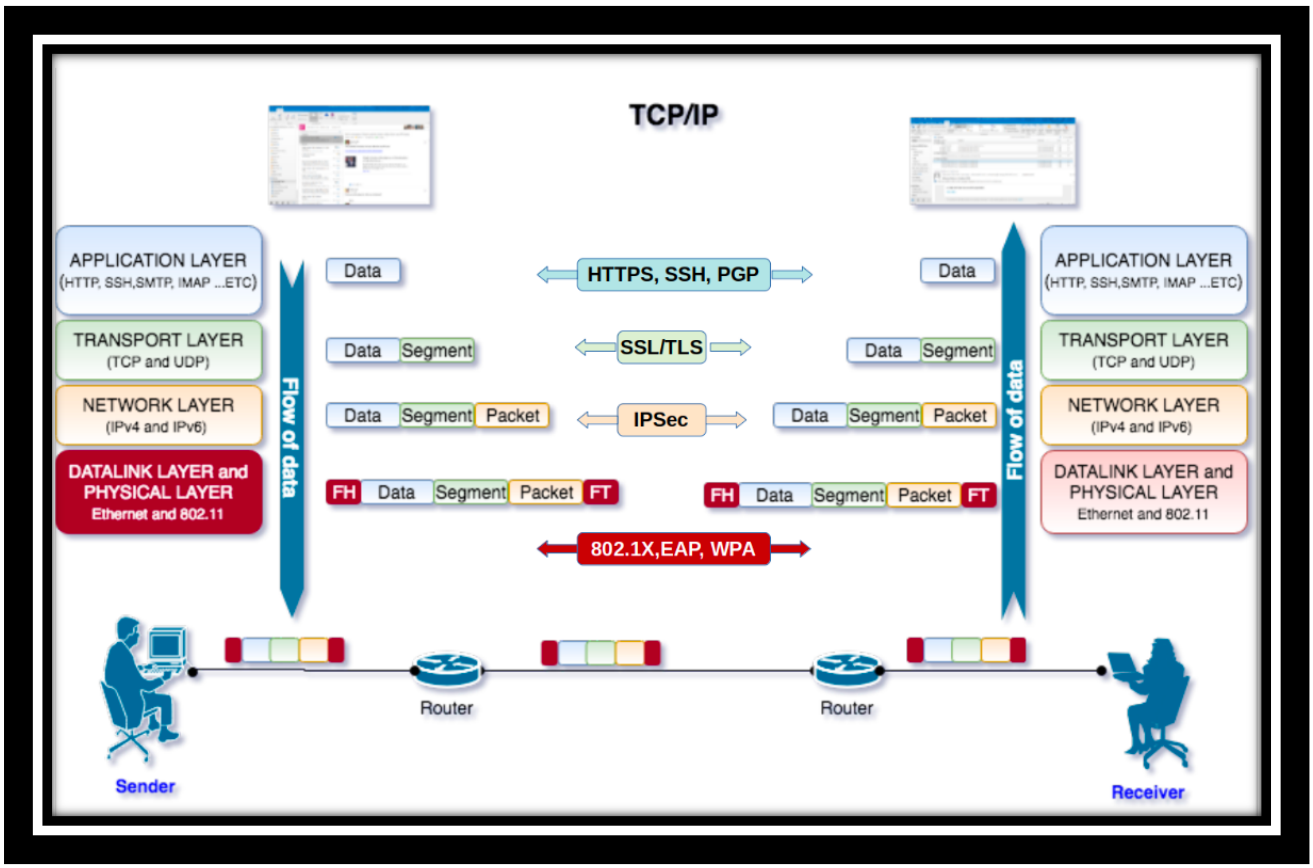
Transport Layer Security (TLS)

Transmission Control Protocol and Internet Protocol (TCP/IP)



SECURITY ISSUES WITH TCP/IP

Med mindre du bruker sikkerhetsprotokollene vi skal dekke i dag, når en enhet mottar et IP-pakke, har den ingen garanti:

Datakonfidensialitet:

- at pakken ikke har blitt inspisert av en tredjepart under transport

Dataautentisitet/dataintegritet:

- om pakken faktisk er sendt av enheten referert til i kildeadressen til pakken
- at pakken inneholder de opprinnelige dataene og ikke har blitt endret under transport
- at den mottakende enheten faktisk er enheten som avsenderen ønsket å sende pakken til.

SIKKERHETSPROBLEMER I IP-NETTVERK:

1. **Avlytting:** Dette refererer til uautorisert overvåking av data mens de overføres over nettverket.
2. **Endring av pakker underveis:** Dette innebærer uønsket modifisering av datapakker mens de er i bevegelse gjennom nettverket.
3. **Identitetsspoofing (forfalskede kilde-IP-adresser):** Dette innebærer å forfalske eller etterligne kilde-IP-adressen for å lure nettverket om opprinnelsen til dataene.

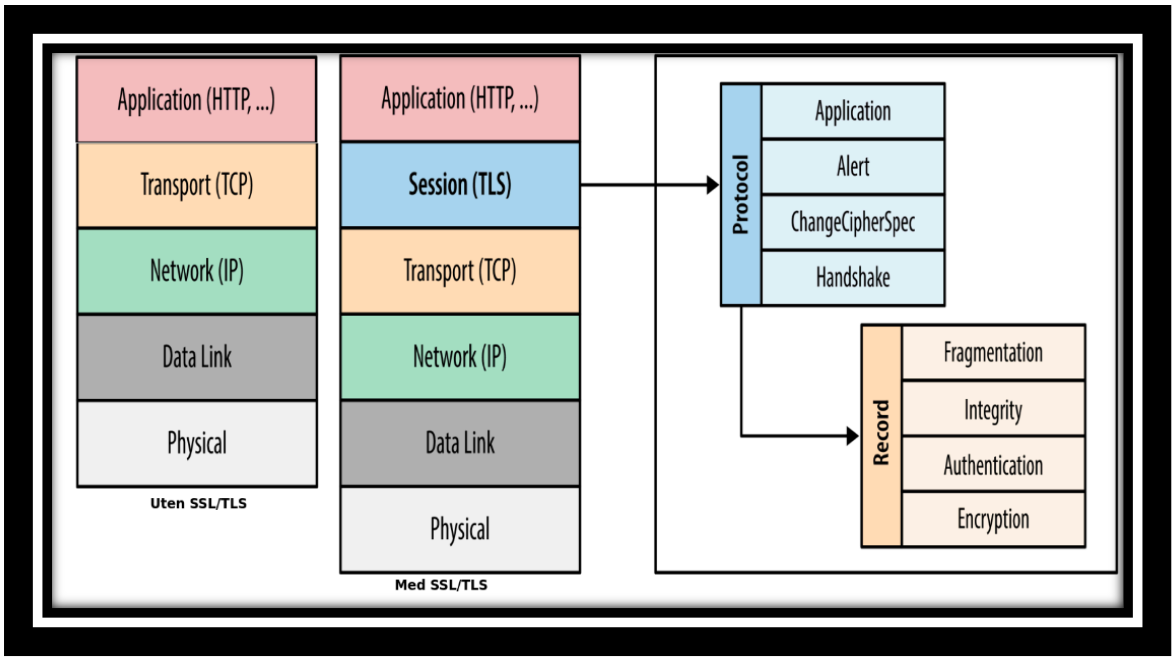
Noen av sikkerhetsprotokollene som kan beskytte data under overføring er:

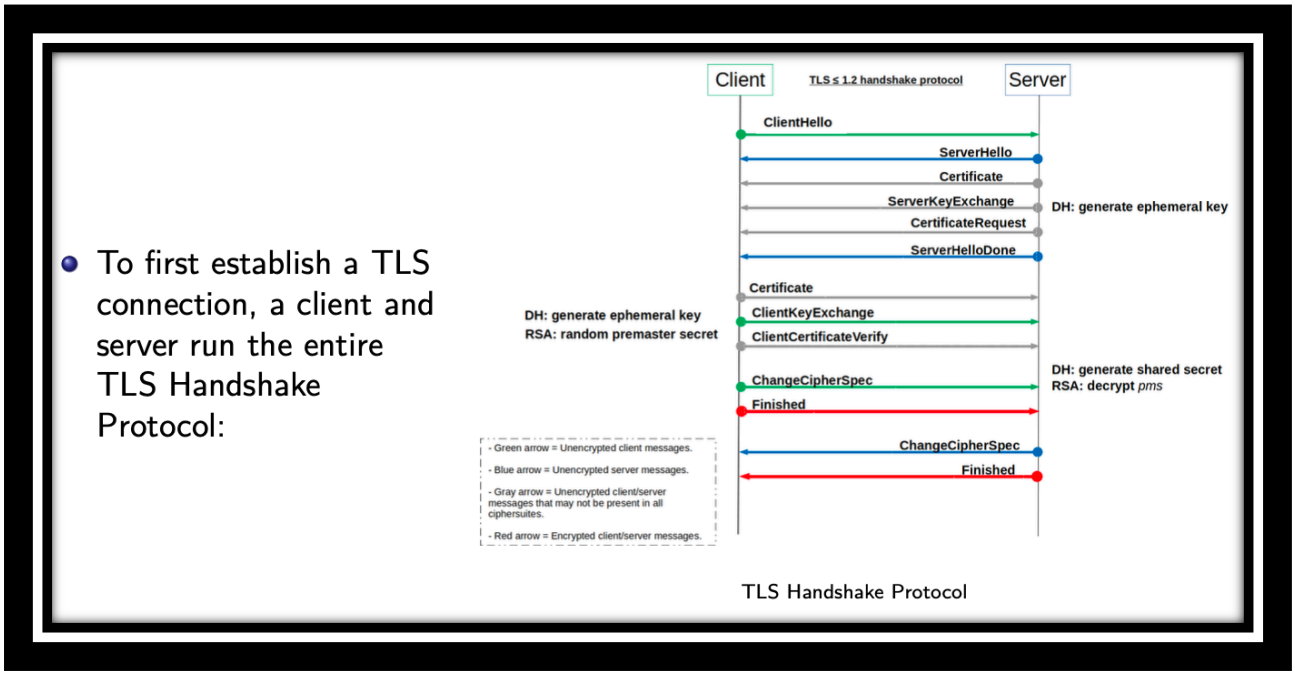
1. **Transport Layer Security (TLS):** Dette er en krypteringsprotokoll som brukes til å sikre dataoverføring over internett, vanligvis i forbindelse med sikre nettleserforbindelser (HTTPS).
2. ~~**Internet Protocol Security (IPsec):** Dette er en omfattende sikkerhetsprotokoll som brukes til å sikre data på IP-nettverk og kan tilby både kryptering og autentisering.~~
3. ~~**Secure Shell (SSH):** Dette er en protokoll som gir sikre fjerninlogging og datatransport, ofte brukt for sikre administrasjon av fjerntliggende datamaskiner.~~

Transport Layer Security(TLS)/Secure Socket Layer (SSL)

Secure Socket Layer (SSL)

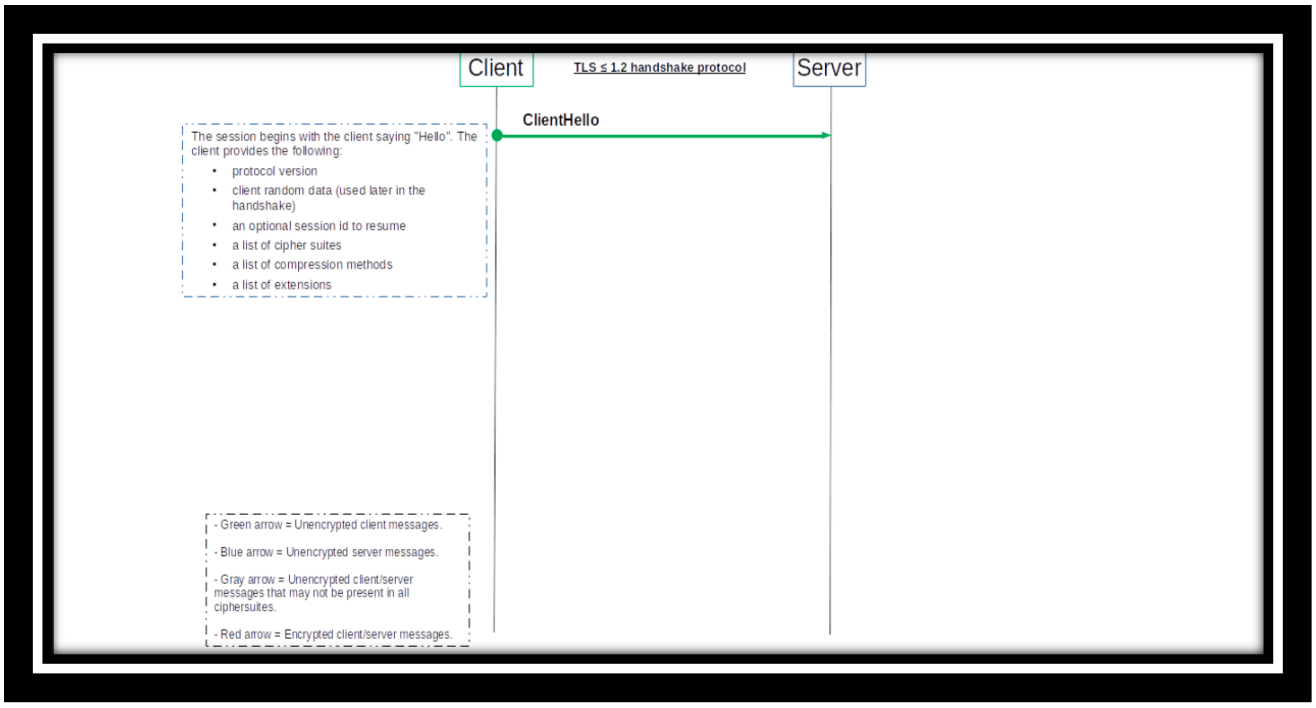
- Secure Socket Layer (SSL) ble utviklet av Netscape og først introdusert i Netscape Navigator 1.1 i 1995.
- SSL er en kryptografisk sikkerhetsprotokoll som beskytter sikkerhetsmålene for ekthet, integritet og konfidensialitet i kommunikasjonen mellom en klient og en server.
- SSL versjon 3 ble utviklet med revisjoner fra offentlige aktører og innspill fra industrien og ble til slutt publisert som et IETF-utkastsdokument
- Bruker TCP for å gi oss sikker ende-til-ende kommunikasjon. Transport Layer Security (TLS) er basert på SSLv3
    - TLS er en IETF-standard
        - ~~RFC 2246 fra januar 1999 - TLS v1.0~~
        - ~~RFC 4346 fra april 2006 - TLS v1.1~~
        - RFC 5246 fra august 2008 - TLS v1.2
        - RFC 8446 fra august 2018 - TLS v1.3





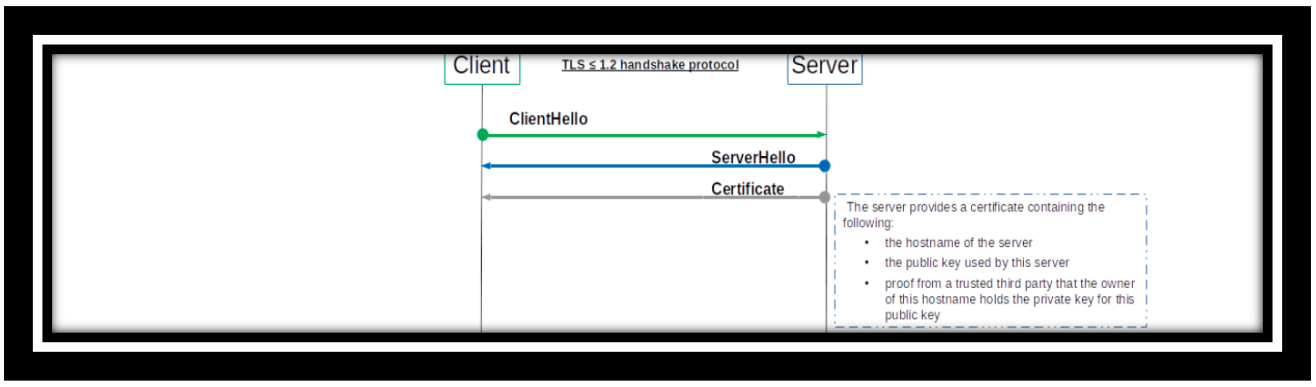
RFC 5246 fra august 2008 - TLS v1.2

KLIENT HALLO

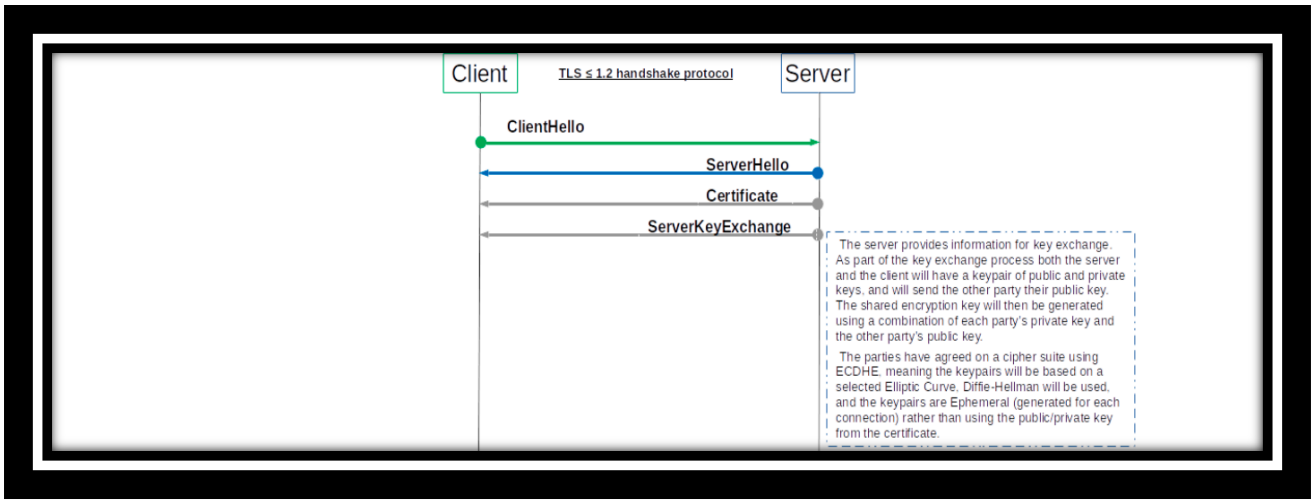


SERVER HALLO

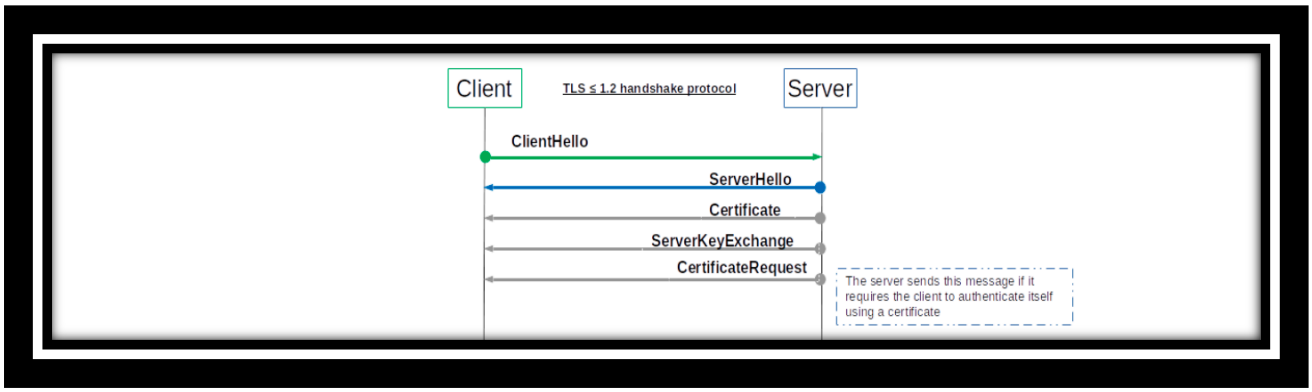
SERTIFIKAT SERVER



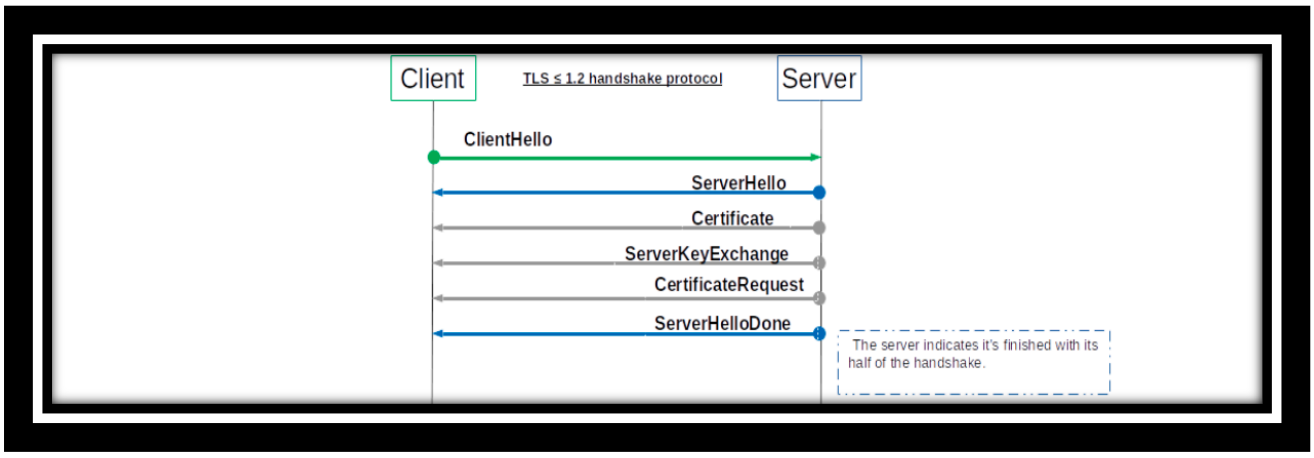
SERVERKEY EXCHANGE



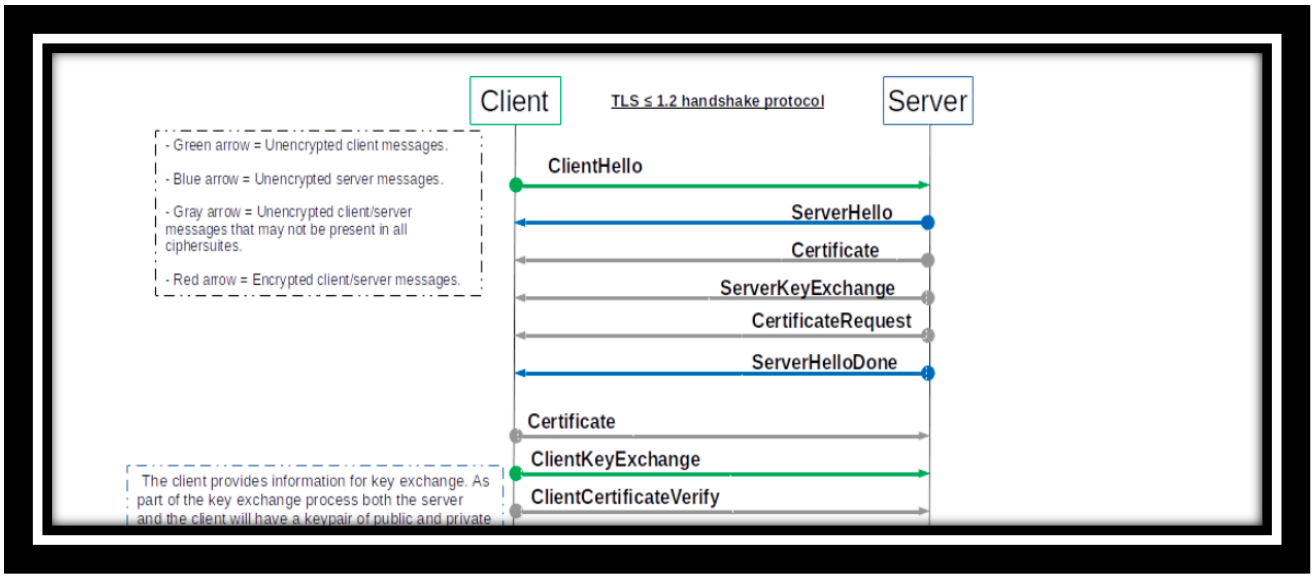
CERTIFICATE REQUEST



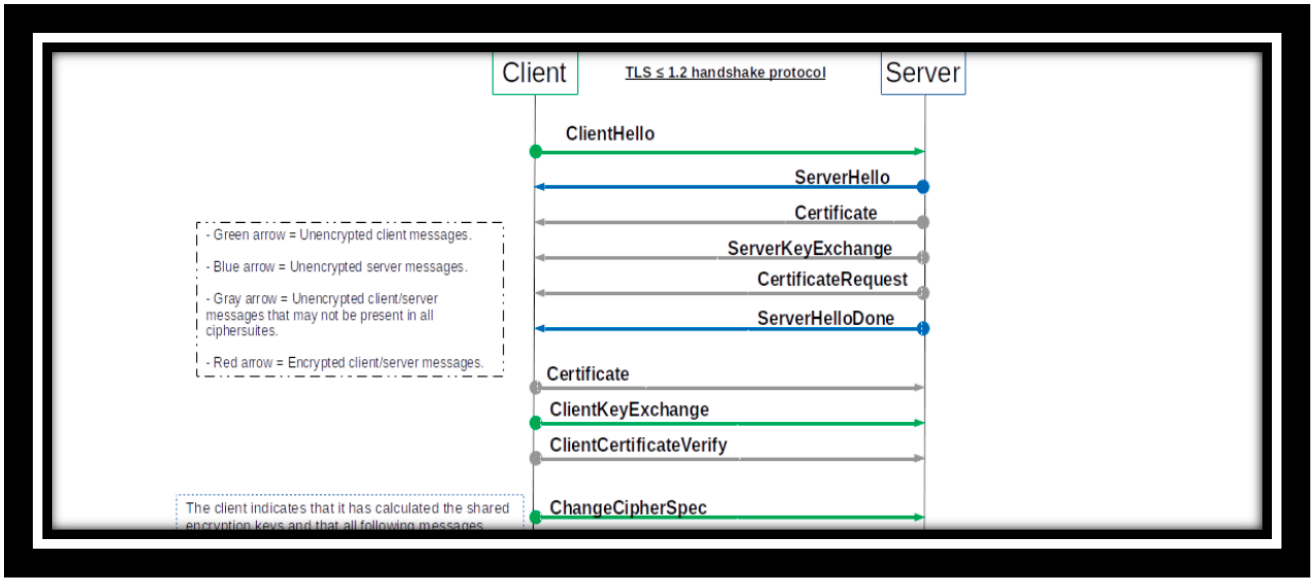
SERVER HALLO DONE



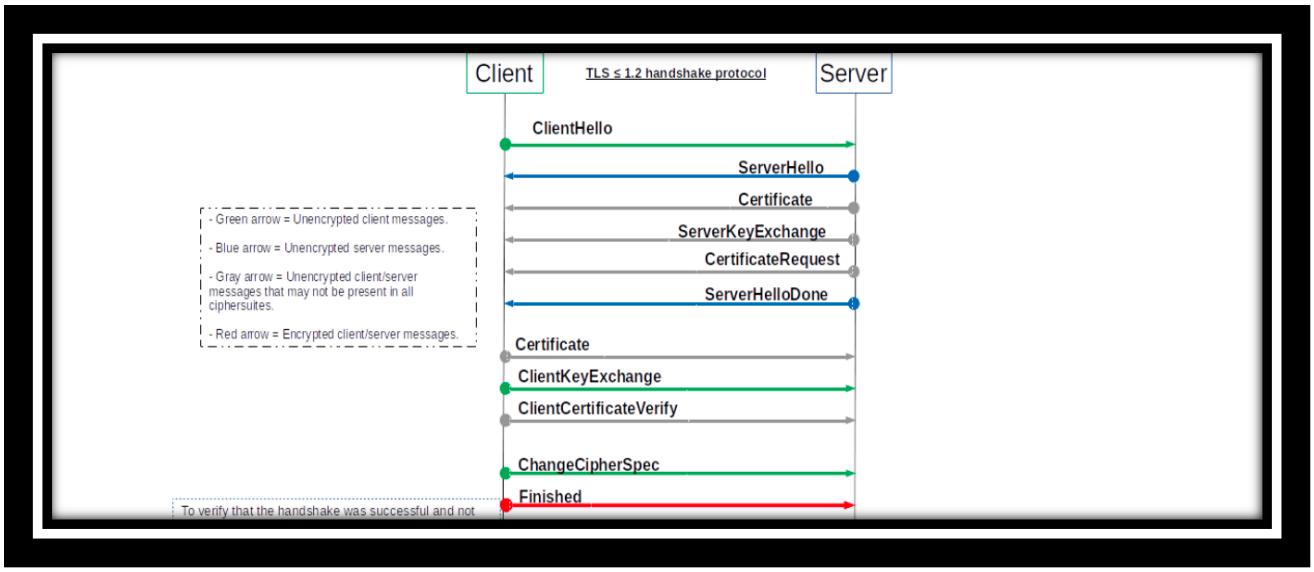
CLIENT KEY EXCHANGE



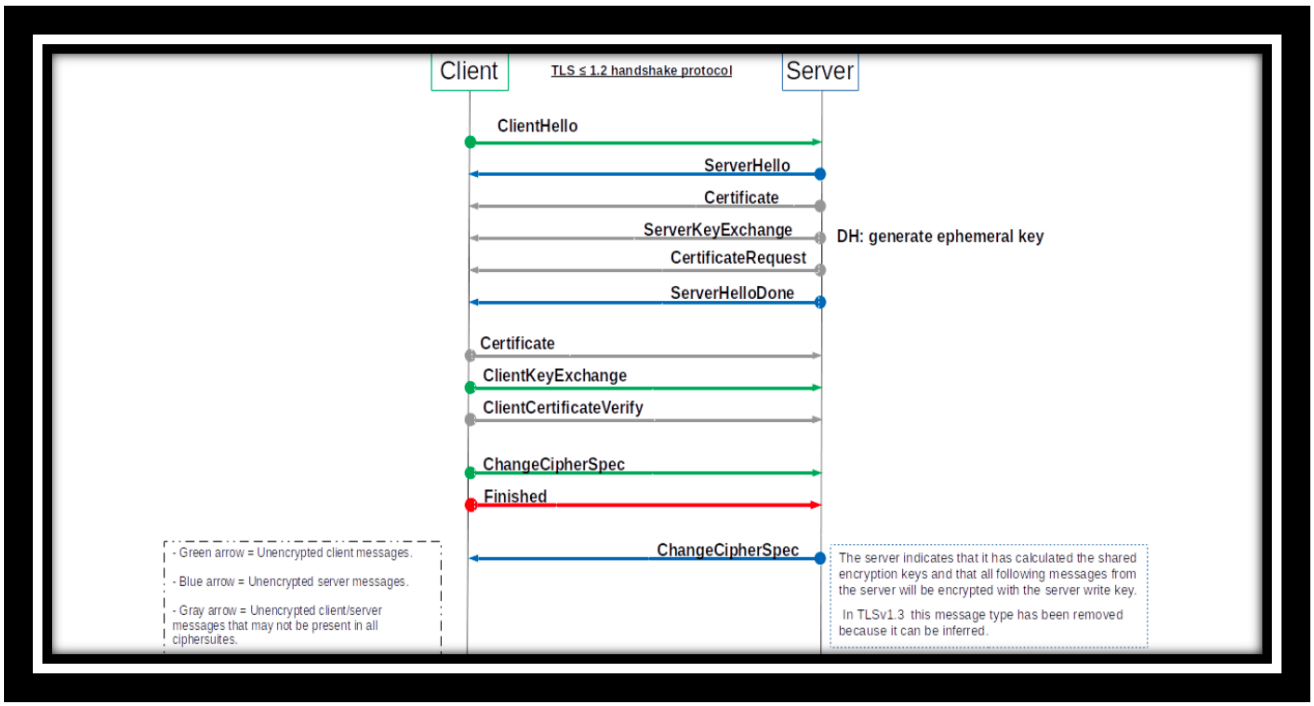
KLIENT CHANGE CIPHER SPEC



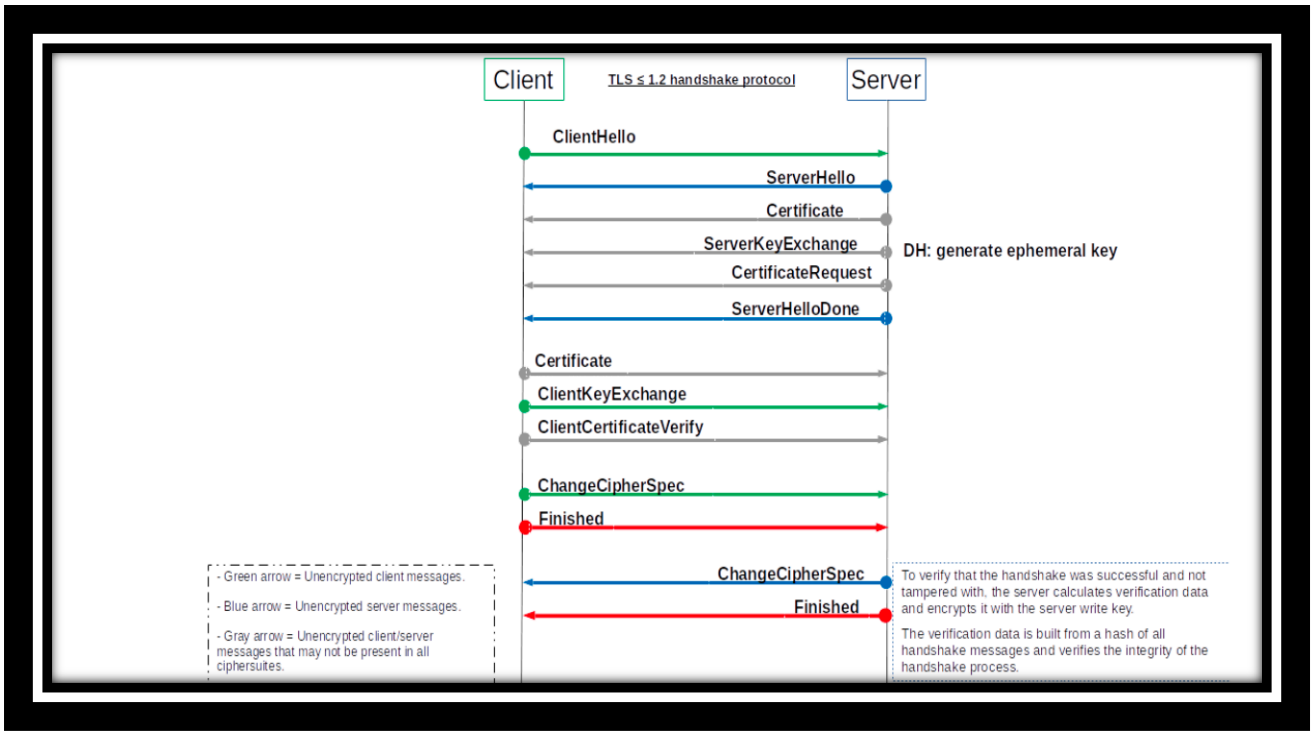
KLIENT FINISH

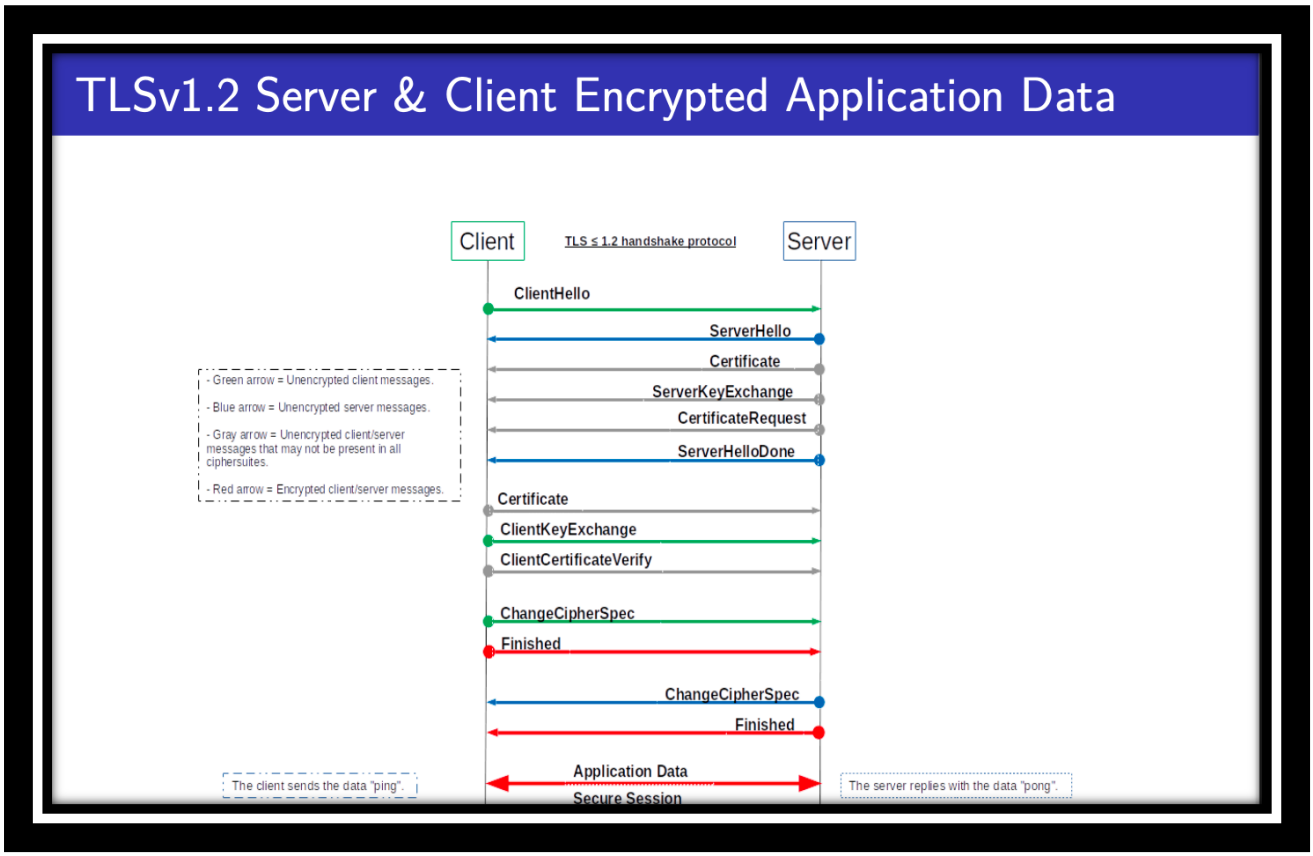


SERVER CHANGE CIPHER SPEC



SERVER FINISH


Client
TLS ≤ 1.2 handshake protocol
Server
ClientHello
ServerHello
Certificate
ServerKeyExchange
DH: generate ephemeral key
CertificateRequest
ServerHelloDone
Certificate
ClientKeyExchange
ClientCertificateVerify
ChangeCipherSpec
Finished
ChangeCipherSpec
Finished
- Green arrow = Unencrypted client messages.
- Blue arrow = Unencrypted server messages.
- Gray arrow = Unencrypted client/server messages that may not be present in all ciphersuites.
To verify that the handshake was successful and not tampered with, the server calculates verification data and encrypts it with the server write key.
The verification data is built from a hash of all handshake messages and verifies the integrity of the handshake process.

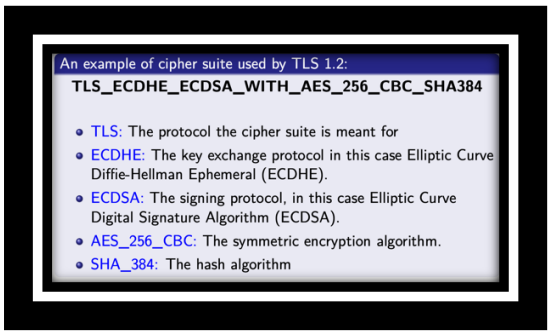

TLSv1.2 Server & Client Encrypted Application Data
Client
TLS ≤ 1.2 handshake protocol
Server
ClientHello
ServerHello
Certificate
ServerKeyExchange
CertificateRequest
ServerHelloDone
Certificate
ClientKeyExchange
ClientCertificateVerify
ChangeCipherSpec
Finished
ChangeCipherSpec
Finished
Application Data
Secure Session
- Green arrow = Unencrypted client messages.
- Blue arrow = Unencrypted server messages.
- Gray arrow = Unencrypted client/server messages that may not be present in all ciphersuites.
- Red arrow = Encrypted client/server messages.
The client sends the data "ping".
The server replies with the data "pong".

HTTPS er en extenxion av HTTP protokollen. Med HTTPS sendes data på en kryptert form med det som heter TLS. Hvis en hacker kommer i mellom og får tak i dataen som sendes ser vedkommende kun jumbo data.

https://www.youtube.com/watch?v=j9QmMEWmcfo&ab_channel=ByteByteGo

TLS-HANDSHAKEPROTOKOLLEN (CIPHERSUITES)

- ClientHello-meldingen må forårsake at klienten og serveren forbereder seg på å kommunisere sikkert ved hjelp av de samme algoritmene og komponentprotokollene
- Klienten sender en liste over kryptografiske algoritmer (CipherSuites) for å indikere alle de ulike måtene den er villig til å kommunisere med serveren
- Deretter velger serveren en i responsen (forutsatt at det er noe overlapp mellom krypteringsalgoritmene de støtter)
- En CipherSuite i TLS inkluderer ett valg for hver av følgende:
    - Algoritme for nøkkelutveksling
    - Algoritme for digital signatur
    - Symmetrisk krypteringsalgoritme
    - Hashfunksjon



CHANGE CIPHER SPEC PROTOCOL (TLS 1.2)

- Denne delprotokollen brukes til å bytte "nøkkelmateriale" som brukes mellom klient og server

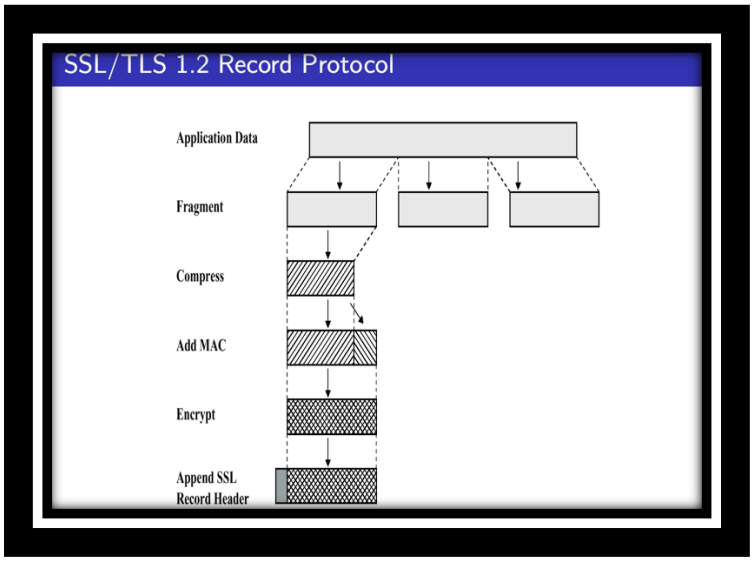
- "Nøkkelmateriale" er rådata som brukes til å lage nøkler for kryptering
- Protokollen består av en enkel melding som forteller den andre parten i SSL/TLS-økten at avsenderen vil bytte til et nytt sett med krypteringsnøkler
- Nøklene genereres fra informasjon som utveksles i "Handshake"-protokollen.

SSL/TLS

SSL, eller Secure Sockets Layer, er en kryptografisk protokoll som brukes til å sikre kommunikasjonen mellom en klient (for eksempel en nettleser) og en server (for eksempel en nettstedsserver). Den sikrer at data som overføres mellom klienten og serveren forblir private og ikke kan avlyttes av uautoriserte parter. SSL brukes ofte til å opprette en sikker tilkobling for nettbaserte transaksjoner, som online kjøp og pålogging på sikre nettsteder. SSL har blitt etterfulgt av Transport Layer Security (TLS), som er den nyere versjonen av protokollen, men begge brukes ofte om hverandre og har lignende formål.

Tilbyr to grunnleggende sikkerhetstjenester/prinsipper

- Konfidensialitet
    - Handshake-protokollen definerer en "felles hemmelighet" som brukes for symmetrisk kryptering av SSL/TLS-nødpakker
- Meldingsintegritet
    - Handshake-protokollen definerer en "felles hemmelighet" som brukes for å generere en meldingsautentiseringskode (MAC)



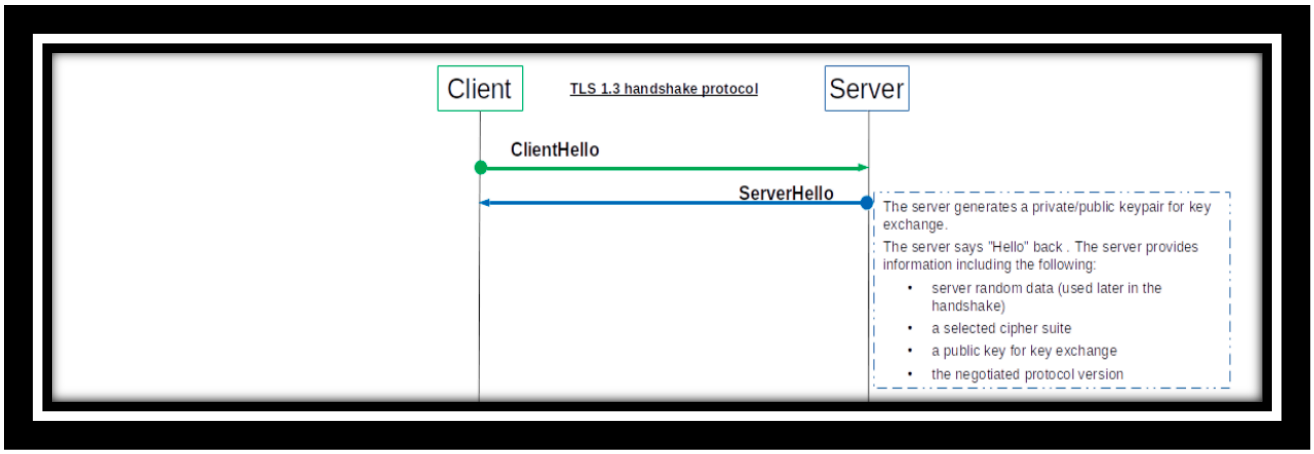
TLS Alert Protocol: Denne sub-protokollen brukes for å sende status meldinger mellom klient og server med for eksempel status endringer og feil meldinger.
katastrofal: uventet melding, dårlig opptaksmac, dekomprimeringssvikt, håndtrykkssvikt, ulovlig parameter
advarsel: lukk varsel, ingen sertifikat, ugyldig sertifikat, ikke-støttet sertifikat, sertifikat tilbakekalt, utløpt sertifikat, ukjent sertifikat

TLSv1.3

- I 2014 begynte Internet engineering task force å utvikle den neste versjonen av TLS 1.3.
- I august 2018 ble TLS standardisert i RFC 8446
- Motivasjonene bak utviklingen av TLS 1.3:
    - Eliminere gamle kryptografidke algoritmer og bytte til moderne algoritmer og ulike moduler av operasjoner
    - Kryptere deler av handshake for å forbedre privacy, i deler av responsen til masse overvåknings bekymringer
    - Redusere forsinkelsen ve då tilby færre runder round trips
    - Generelle endringer i kru´yptografisk og andre operasjoner av protokollen, inkludert froenklingen av protokoll logikk

Klient hallo:

Server hallo:



Kryptert extensions: