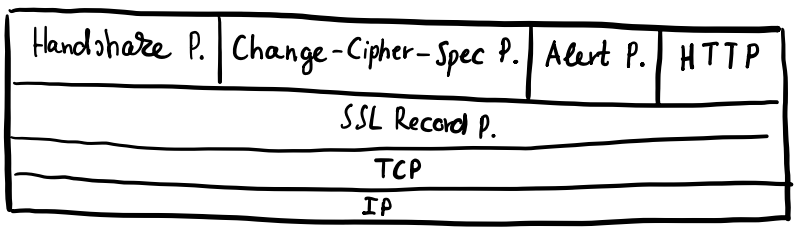
SSL

- **SSL célja**
  - Titkosított kommunikációt biztosító protokoll, ami nyílt hálózatokban, kapcsolatorientált kommunikációban nyújt védelmet.
  - Csak egy-egy kommunikációs csatornát biztosít.
  - Weboldalak titkosítása
- **SSL szerkezeti felépítése**
  - Minden egyes kapcsolat egyedi kulccsal titkosít.
  - Tanúsítvány igazolja a szervert.
  - Biztosítja az adatintegritást (MD5, SHA-1)



• SSL működése

1. Kliens csatlakozik a kiszolgálóhoz.
2. Kiszolgáló elküldi a hitelesíti a tanúsítványt a kliensnek.
3. Kliens ellenőrzi a tanúsítvány hitelességét, majd létrehozza a titkosított kapcsolatot a kiszolgálóval.
4. Kliens és kiszolgáló között így már biztonságosan lehet adatokat cserélni.
5. Ha az SSL kapcsolat megszakad, akkor a kliens és a kiszolgáló kapcsolata is megszakad.

• SSL alprotokolljai

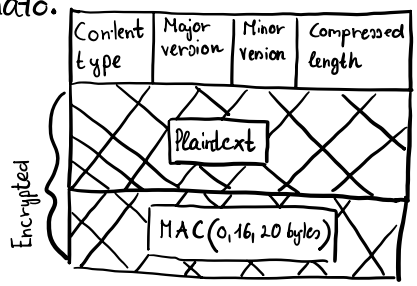
- Rekord protokoll -> Feladata a kliens és a szerver és a felsőbb SSL protokoll entitások védelme
  - Titkosítás, integritásvédelem, üzenet-visszajátszás elleni védelem
- Handshake protokoll -> Rekord protokollban használt kriptográfiai algoritmusok és paramétereik egyeztetése.
  - Kulcscsere és hitelesítés
- Change-Cipher-Spec protokoll -> Egyetlen üzenetből áll, ami a Handshake protokoll kulcscsere részének végét jelzi.
  - Ezt az üzenetet elküldi, utána az adott fél az új algoritmusokat és kulcsokat kezdi használni a küldésre.
- Alert protokoll -> Figyelmeztető és hibaüzenetek továbbítása.

• Rekord protokoll működése

- A felsőbb protokoll rétegétől érkező üzenetekkel:
  1. Fragmentálja, ha szükséges
  2. Fragmenseket tömöríti
  3. Tömörített fragmenseket fejléccel látja el
  4. Fejléccel ellátott, tömörített fragmensre üzenethitelesítő kódot (MAC) és azt a fragmenshez csatolja.
  5. Az üzenethitelesítő kóddal ellátott fragmenst rejtjelezi.

• Rekord üzenetei

- type → Rekord üzenetben melyik felsőbb protokoll található.
- version → SSL verzió
- length → Fragmens hosszát tartalmazza bájtban mérve.
- MAC → Üzenethitelesítő kód generálása.



• Handshake protokoll működése

1. Kliens és szerver elküldi a tulajdonságait, megállapodnak.
2. Szerver elküldi a tanúsítványát és kéri a kliens tanúsítványát (Kulcscseremódszertől függ).
3. Tanúsítvány ellenőrzés és kulcscsere folytatása.
4. Kulcscsere életbelépése, befejezése

• Handshake üzenetei

1. KliensHello
   - Kliens küldi ezt az üzenetet az SSL Handshake kezdeményezésére.
   - Kliens verzió, véletlenszám, viszonyazonosító, biztonsági algoritmusok, tömörítő algoritmusok
2. SzerverHello
   - Kiszolgáló küldi a KliensHello üzenetre válaszul.
   - Szerver verzió, véletlenszám, viszonyazonosító, biztonsági algoritmusok, tömörítő algoritmusok
3. Szerver kulcscsere üzenet
4. Tanúsítvány kérés
5. Kliens tanúsítvány
6. Kliens kulcscsere üzenet
7. Kész üzenet
   - Első olyan üzenet, ami már az új algoritmusokat használva, új kulcsokkal van kódolva.