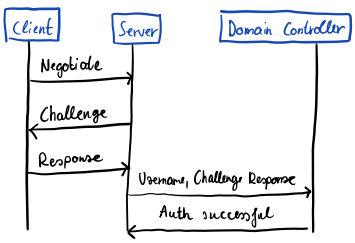
Win OS hitelesítési módok, címlárak, fájlrendsz. bizt.

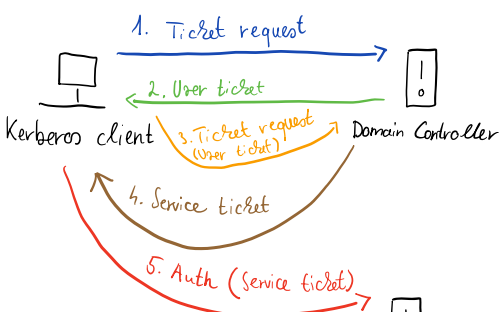
• NTLM

- Microsoft által fejlesztett hitelesítési protokoll, ami Win OS-ba használatos.
- Hitelesítési token szerül használatra, ami az adott munkamenetre vonatkozik.
- Token elkészítéséhez szükség van egy hitelesítési szolgáltatóra, ami felhasználó jelszavával és más azonosító adatok alapján állítja elő.



• Kerberos

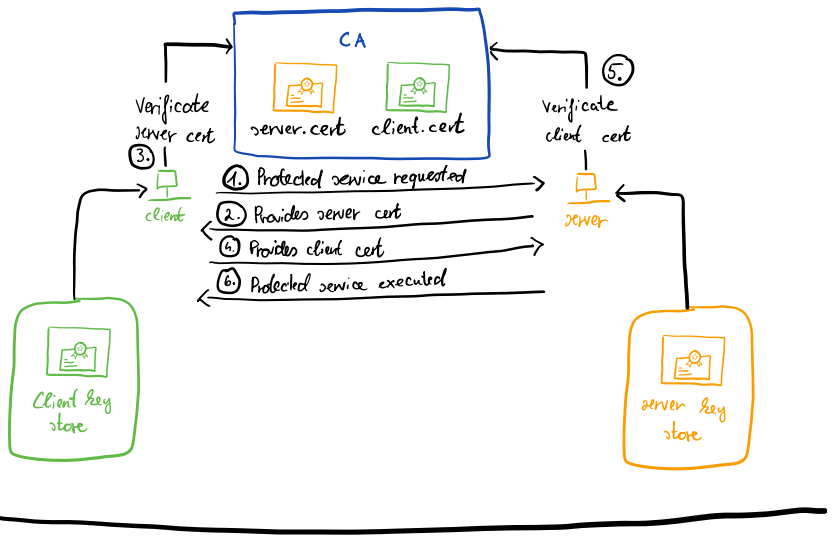
- Nyílt hálózatnál, jelszavas hitelesítés
- Egyszeri regisztráció és a hálózati munkamenet teljes ideje alatt megbízhatóvá válik.
- Szimmetrikus vagy titkos kulcsú kriptográfián alapul.
- Egy adatbázisban tárolja a felhasználóit és a privát kulcsokat.
- Igazolvány
  - Jegy = Session Key -> Tartalmazz ↴
    - A szolgáló és kliens nevét
    - Kliens internetes címét
    - Időbélyegét
    - Életciklusát
    - Egy véletlenszerűen generált kulcsot
  - Hitelesítő -> Tartalmazza ↴
    - Kliens nevét
    - IP címét
    - A munkaállomás aktuális idejét
- Alany = Principal
  - Egy egyedi azonosító, amihez jegy rendelhető.
    - primary -> alany első része, megegyezhet a felh. nevével.
    - instance -> elhagyható, primary jellemzői, "/" karakterrel van elválasztva a primary mezőtől.
    - realm -> domain neve, nagybetűs karakterekkel



6. Service ticket proves client

- Kölcsönös hitelesítés
  - A kliens és a szolgáló megbizonyosodhat a másik azonosságáról.
  - Közös kapcsolati kulcson osztoznak és ezt használják a titkosított kommunikációra.

- Kapcsolati kulcs
  - Ideiglenes privát kulcs
  - A kliens ismeri és ezekkel titkosítja a szolgáló és a munkaállomás közötti kommunikációt.



- Címtár
  - Hálózati objektumok (szolgáltatások, területek, nyomtatók, hálózat felhasználói, gép fiókjai) adatainak tárolására szolgáló hierarchikus struktúra
    - Felhasználók azonosságának, jogosultságainak ellenőrzése.
    - Megkönnyíti a hálózati erőforrások elérését.
    - A címtár és így a hálózat is központi helyről felügyelhető.
    - A hálózat távfelügyelete automatizálható

- Címtár szükségessége
  - Igény -> Sok felhasználó és sok szolgáltatónál is maximális teljesítményi, biztonság
  - Korábban -> Felhasználók nyilvántartása külön-külön.
    - Jogokat mindenhol külön be kellett állítani.
  - Címtárral -> A szolgáltatásokat és a szolgáltatásokat egy adminisztrátor egységbe fogjuk össze.

- AD biztonsági részei
  - Szerver megrongálható
  - Jogosultsági részek kihasználása
  - Bejelentkezési hibák, pl. annak, hogy akár egy támadó próbál belépni.
  - Távolról (RDP)
- Minden felhasználónak joga van munkaállomásokat hozzáadni a tartományhoz
  - Alapértelmezett beállítás
  - Kockázata, hogy a felhasználók csatlakozhatnak a gépekhez, hogy elérjék a vállalati tartományt is és lehet, hogy nem rendelkeznek védelemmel.
  - Rendszergazdai jogosultságot szerez, amikor rácsatlakozik a gépre.
  - Megoldás, hogy limitáljuk a jogosultságokat.
- Túl sok felhasználó egy csoportban
  - Elengedhetetlen csoportok létrehozása csak
- Gyenge jelszó házirend
  - Könnyebben feltörhetőek így a fiókok.
  - Komplex jelszó használata, minimum jelszó hossz beállítása.
- AD biztonságossá tétele
  - Felhasználók és csoportok automatizálása
  - Felhasználói engedélyek elemzése
  - Sebezhetőségek, nem használt fiókok elemzése
  - AD naplózása
  - Biztonsági mentések
  - Naplózás, logolás

- Fájlrendszer biztonsága
  - NTFS
    - Alapból a rendszerkönyvtárak írása tiltva van. (Pl. system32)
      - Ha törlünk valamit a rendszerkönyvtárból, abból bajok is lehetnek.
    - Deny-jog
    - Tulajdon átvétel
    - Jogosultság szimulálása -> Kiz is férhetnek hozzá
    - Fájl szintű titkosítás
    - Jogosultsági szintek
      - Full control -> Teljes hozzáférés és jogok módosítása
      - Modify -> Írás, olvasás, törlés
      - Read & execute -> Megtekintés és alkalmazások futtatása
      - Read -> Megtekintés
      - Write -> Írás