



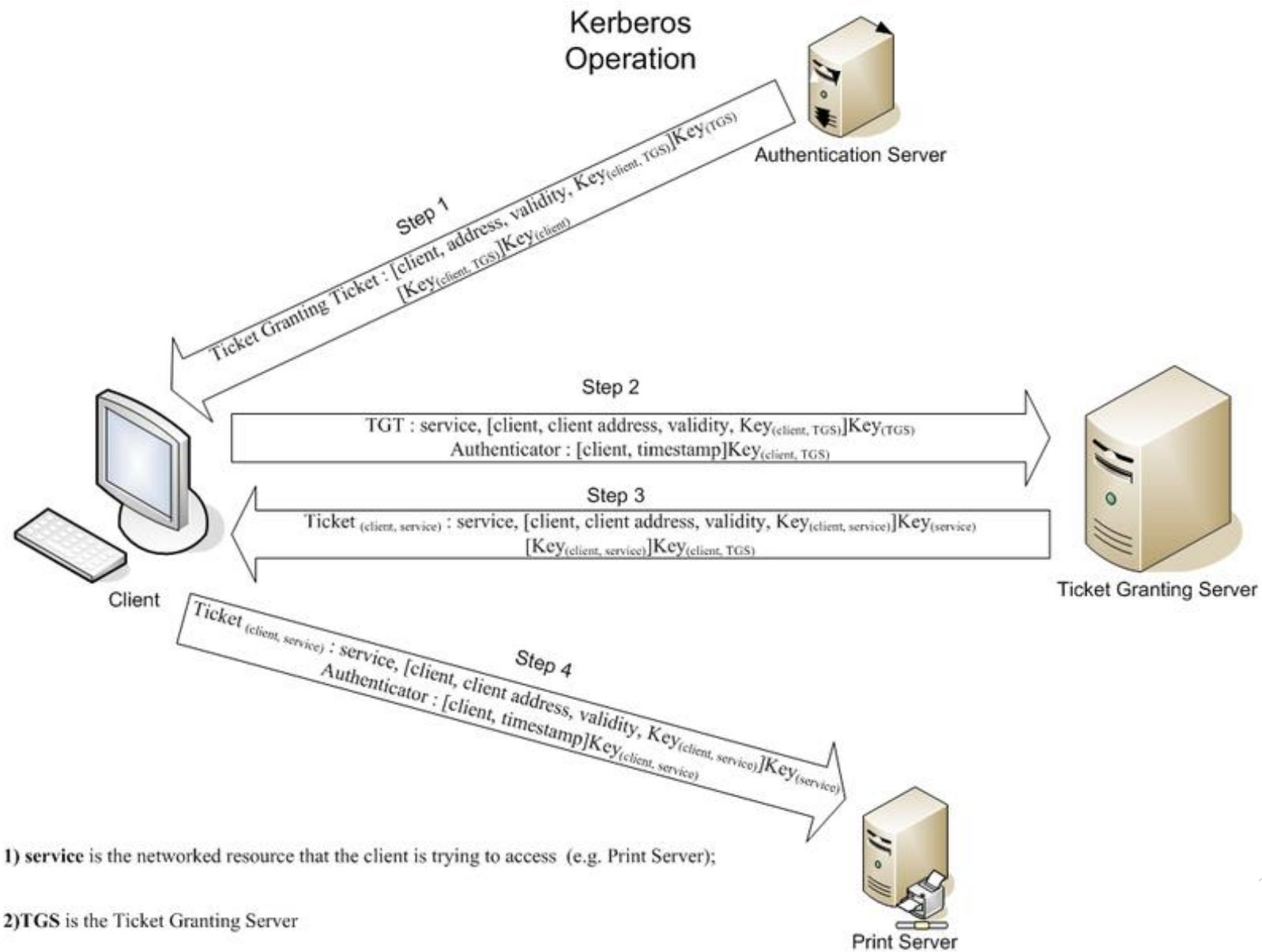
Kerberos

Szolgáltatások védelme Kerberos segítségével

- ▶ Kerberos - Hádész háromfejű kutyája
- ▶ Hálózati autentikációs protokoll
- ▶ Ügyfél és kiszolgáló közötti kapcsolatok titkosított autentikációja
- ▶ Cél: Single Sign On rendszer megvalósításának támogatása
- ▶ Az ügyfél titkosított jelszóval igazolja magát, majd a további kommunikáció is titkosítva történik
- ▶ Védelem belső és külső támadások ellen
- ▶ Biztonságos változatok az rsh, rcp, telnet, ftp kliensek helyett

Fogalmak

- ▶ **Résztvevő (Principal):** minden felhasználó, számítógép és kiszolgálók által biztosított szolgáltatást
- ▶ **Példány (Instance):** szolgáltatás-résztvevők és speciális adminisztratív résztvevők megnevezése
- ▶ **Tartomány (Realm):** a Kerberos rendszer által biztosított egyedi felügyeleti tartomány - a DNS-tartomány nagybetűssé alakítva (KEFO.HU).
- ▶ **Kulcsszolgáltató (KDC):** a résztvevők adatbázisa + a hitelesítési kiszolgáló (AS) + jegymegadási kiszolgáló
- ▶ **Jegybiztosító jegy (TGT):** a hitelesítési kiszolgáló (AS) adja ki, evvel kérhet a felhasználó hozzáférést egy szolgáltatáshoz
- ▶ **Jegykiadó szolgáltatás (TGS)** szolgáltatásjegyeket ad ki a klienseknek
- ▶ **Szolgáltatásjegy:** segítségével férhet hozzá az ügyfél a szolgáltatáshoz. Igazolja a két résztvevő (ügyfél és szolgáltatás) identitását
- ▶ **Kulcstáblafájlok:** egy szolgáltatás vagy gép titkosítási kulcsát tartalmazzák



Autentikáció

1. Bejelentkezéskor automatikusan
2. A felhasználó kezdeményezi kinit-tel

Ez utóbbi menete

- ▶ A Kerberos felhasználónevet elküldi az Authentication Server (AS)-hez
- ▶ Az AS visszaküld egy tikett kiutaló tikettet (Ticket Granting Ticket - TGT), amit a felhasználó nyilvános kulcsával titkosít
- ▶ A kinit bekéri a jelszót, dekódolja a TGT-t

Autentikáció menete

- ▶ A kliens program (pl. levelező ügyfél) elküldi a TGT-t a tikett kiadó szerverhez (Ticket Granting Server - TGS)
- ▶ A TGS generál egy tikettet a levelező szerver szolgáltatás eléréséhez, és titkosítva elküldi az ügyfélhez
- ▶ Az ügyfél ezzel a tikettel igénybe veszi a szolgáltatást
- ▶ Ha a felhasználó egy másik szolgáltatást akar igénybe venni, akkor ugrás a dia első pontjához