Kerberos

- **Centrální autentizační systém**
- **Klient** – má své heslo, prokazuje se lístky, které dostane od Ticket Granting Service (TGS), neboli Key Distribution Center (KDC).
- **Služba** – má také své heslo (klíč). TGS je také služba.
- **TGT** – ticket-granting ticket (bez nutnosti pokaždé psát heslo).
- **Lístky** – pro každý přístup ke službě.

Získání TGT

- **Žádost o TGT** – uživatel, adresa, jméno služby (TGT).
- **Odpověď** – Lístek, (session key, jméno klienta, jméno serveru) zašifrováno heslem uživatele.
- **Uživatel** – zadáním hesla získá session key a TGT.
- **TGT** – (session key, uživatel, adresa, jméno služby, čas vydání, doba platnosti) zašifrováno klíčem služby (TGS).

Přístup ke službě

- **Žádost o lístek** – použije TGT a *autentizátor*.
- **Autentizátor** – jméno a adresa odesílatele, zašifrovaná pomocí session key.
- **TGS** – rozšifruje lístek, získá session key, ověří autentizátor, platnost lístku, provede autorizaci.
- **Vydání lístku** – Lístek pro novou službu, (jméno klienta, jméno serveru, session key pro novou službu) zašifrováno session key z TGT.
- **Použití lístku vůči službě** – podobné jako použití TGT vůči TGS.

Další vlastnosti

- **Replay cache** – proti odposlechnutí.
- **Autentizace služby vůči klientovi.**
- **Forwardovatelné lístky** – nejsou vázané na adresu.
- **Proxy lístky** – delegace části pravomocí na službu.
- **Různé domény** (realms), interakce mezi nimi.
- **Záložní KDC**

Implementace

- **MIT implementace** – referenční. Většina UNIXů, MacOS X, BeOS.
- **Heimdal** – evropská implementace.
- **Klientské aplikace** – nutnost kerberizace.
- **Kerberizované systémy** – Red Hat Linux, OpenBSD. Na některých jiných – nutnost instalace vlastních aplikací.

Literatura

- **Designing an Authentication System** (rozhovor ve čtyřech scénách) – *http://web.mit.edu/kerberos/www/dialogue.html*.
- **Kerberos v5 Installation Guide** – kompilace systému, základní administrativní rozhodnutí.
- **Kerberos v5 Administrator's Guide** – konfigurační soubory, administrace databáze uživatelů.
- **Kerberos v5 User's Guide** – základní informace pro uživatele.