Kerberos 基本構想

Kerberos 基本構想

- 認證機制：
  - 認證伺服器 (Authentication Server, AS)
  - 門票核准伺服器 (Ticket-Granting Server, TGS)
- 特性：
  - 主密鑰分配
  - 客戶密碼只要輸入一次
  - 防禦偽裝攻擊
  - 防止重播攻擊

- TGS 門票：

$$Ticket_{TGS} = E_{KTGS}\,[ID_A \,||\, AD_A \,||\, ID_{TGS} \,||\, TS_1 \,||\, Lifttime_1]$$

- 伺服器門票：

$$Ticket_B = E_{Kb}\,[ID_A \,||\, AD_A \,||\, ID_B \,||\, TS_2 \,||\, Lifttime_2]$$