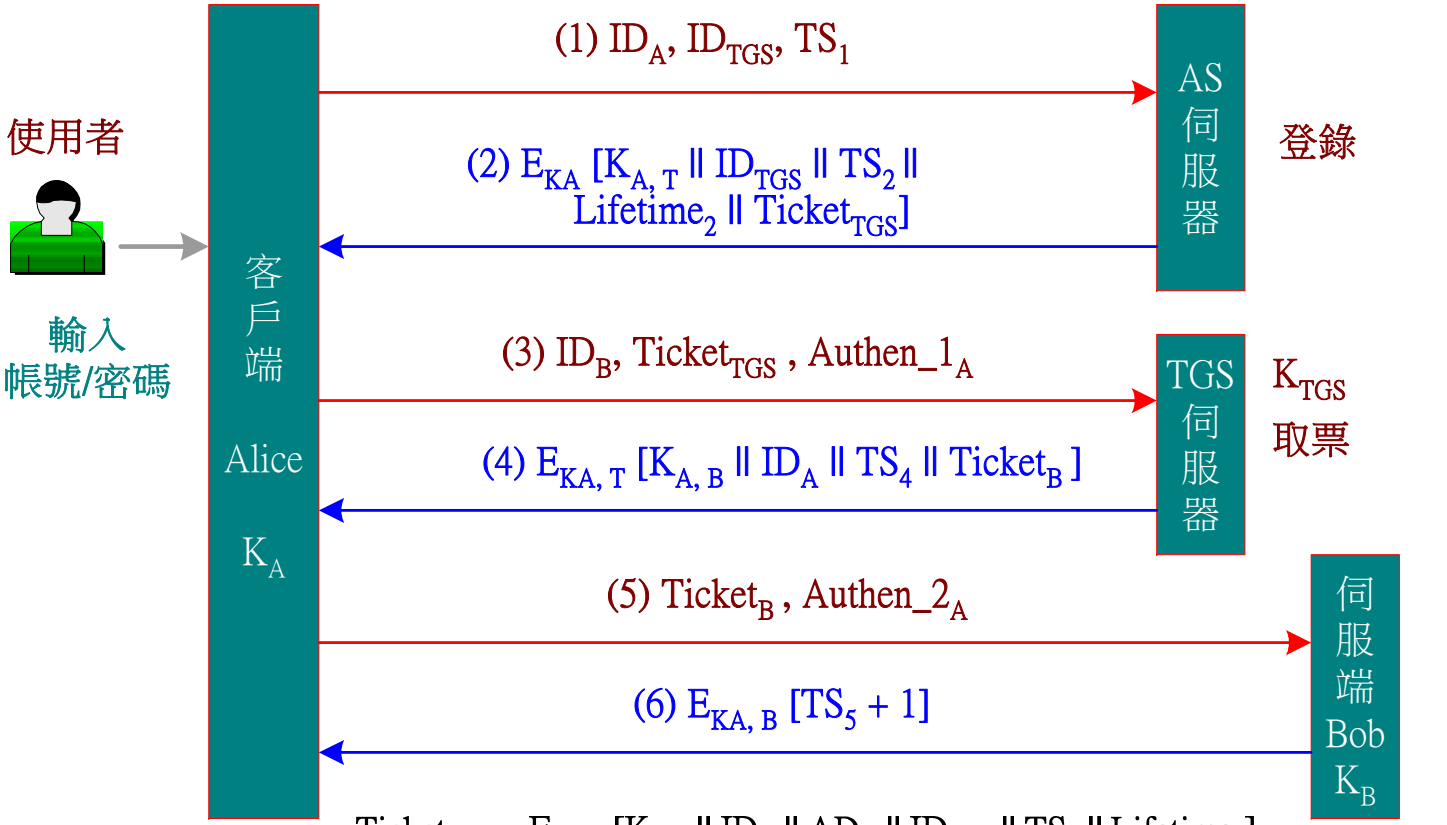
Kerberos V4 認證系統 - 參與運作者

- 參與運作者：
  - 客戶端 (Client) 、伺服端(Server)皆稱為『主角』 (Principal)
  - 每位主角皆有一只主密鑰 (Master Secret)
  - 認證伺服器 (Authentication Server, AS)
    - 認證用戶身分
    - 發給 通往TGS 門票
    - 用戶與 TGS 之間會議鑰匙
  - 門票核准伺服器 (Ticket-Granting Server, TGS)
    - 確認用戶身分
    - 發給 通往伺服器門票
    - 用戶與伺服器之間會議鑰匙
  - 服務伺服器 (Service Server)
    - 確認用戶身分

Kerberos V4 - 認證程序



$Ticket_{TGS} = E_{KTGS}[K_{A,T} \| ID_A \| AD_A \| ID_{TGS} \| TS_1 \| Lifetime_1]$

$Authen\_1_A = E_{KA,T}[ID_A \| AD_A \| TS_3]$

$Ticket_B = E_{KB}[K_{A,B} \| ID_A \| AD_A \| ID_B \| TS_2 \| Lifetime_2]$

$Authen\_2_A = E_{KA,B}[ID_A \| AD_A \| TS_5]$

Kerberos V4 - 認證程序

- 運作程序：
  - 登錄：取得 TGS 門票

    $Ticket_{TGS} = E_{KTGS} [K_{A,T} \| ID_A \| AD_A \| ID_{TGS} \| TS_2 \| Lifetime_1]$
  - 取票：
    - 簽署身分證明：

      $Authen\_1_A = E_{KA,T} [ID_A \| AD_A \| TS_3]$
    - 取得伺服器門票：

      $Ticket_B = E_{KB} [K_{A,B} \| ID_A \| AD_A \| ID_B \| TS_4 \| Lifetime_2]$
  - 要求服務：
    - 簽署身分證明：

      $Authen\_2_A = E_{KA,B} [ID_A \| AD_A \| TS_5]$
  - 達到相互認證的功能。