Kerberos V5 - 運作程序

- 增加參數：
  - 領域 (Realm)
  - 選項 (Options)
  - 時間參數 (Times)
  - 亂數 (Nonce)
- 運作步驟
  - 認證身份與取得 TGT 門票：

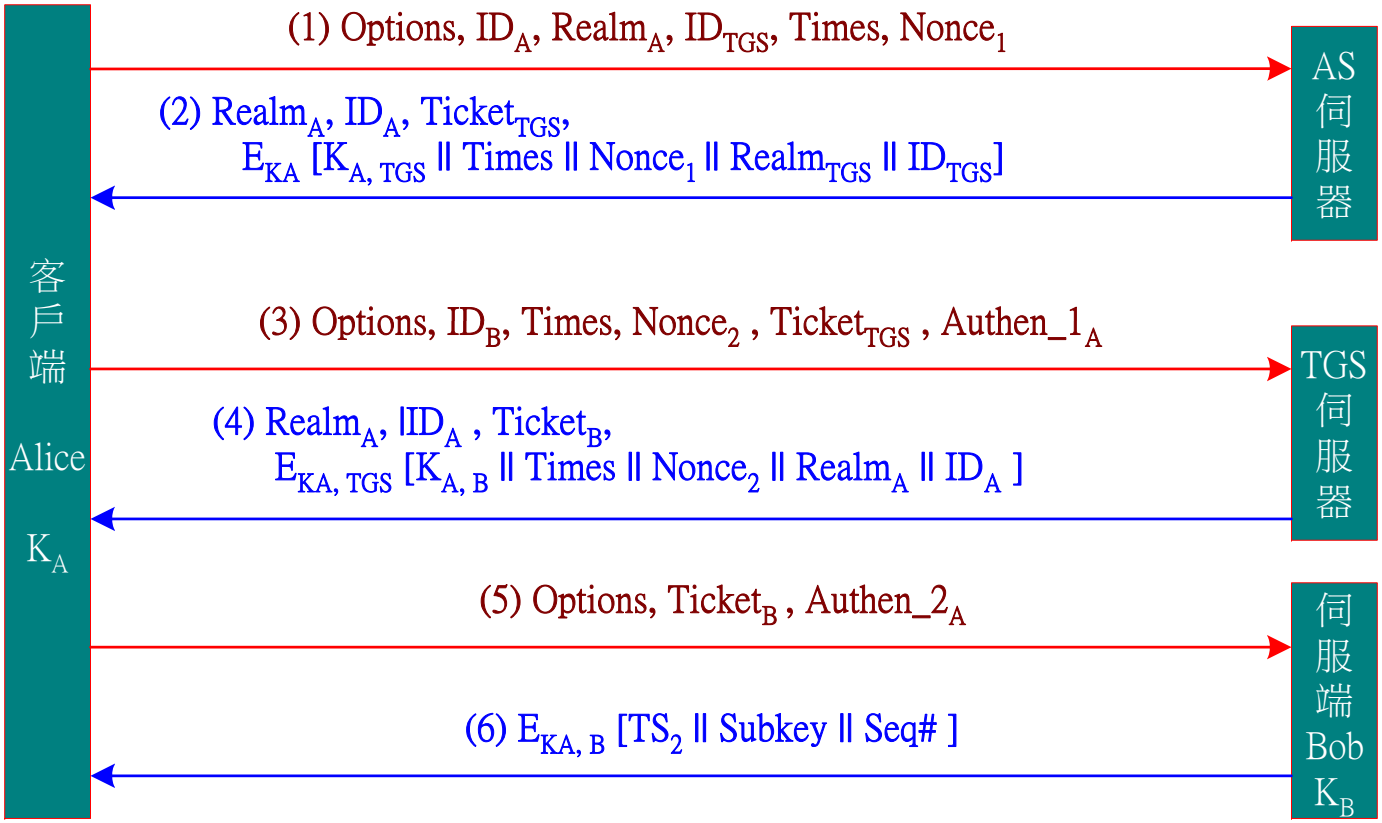
    $Ticket_{TGS} = E_{KTGS}[Flages \| K_{A,TGS} \| Realm_A \| ID_A \| Times \| Authen\_Data]$
  - 索取服務門票：

    $Ticket_B = E_{KB}[Flages \| K_{A,} B \| Realm_A \| ID_A \| AD_A \| Times \| Authen\_Data]$

    $Authen\_1_A = E_{KA,TGS}[ID_A \| Realm_A \| TS_1]$
  - 要求服務：

    $Authen\_1_B = E_{KA,}[ID_A \| Realm_A \| TS_1 \| Subkey \| Seq\#]$

Kerberos V5 - 運作程序



$Ticket_{TGS} = E_{KTGS}$[Flages || $K_{A, TGS}$ || $Realm_A$ || ID_A || AD_A || Times || Authen_Data]

$Ticket_B = E_{KB}$[Flages || $K_{A, B}$ || $Realm_A$ || ID_A || AD_A || Times || Authen_data]

$Authen\_1_A = E_{KA, TGS}$ [ID_A || $Realm_A$ || TS_1]

$Authen\_2_A = E_{KA, B}$ [ID_A || $Realm_A$ || TS_2 || Subkey || Seq#]

Kerberos V5 - Ticket 格式

- **Ticket 格式**
  - **Encryption Key 會議鑰匙**
  - **旗號(flags)：**
    - **INITIAL**
    - **PRE-AUTHENT**
    - **HW-AUTHENT**
    - **RENEWABLE**
    - **….**