擴展型 Needham-Schroeder 協定

- 加入時間戳記問題：
  - 必須保持時間同步，很難達成。
  - 回應者不知道發起者身分。如果事先通知回應者，可解決重播攻擊的問題。
- 取得回應者同意的亂數 N_B ，取代加入時間戳記。
- 通行票：$Ticket = E_{KB}[ID_A \| K_S \| N_B]$