憑證認證的運作 -相互認證

- 說明如下：（Alice 為發起者，Bob 為回應者）
  - 訊號 (1)：Alice 發送自己的憑證（$Cert_A$，包含公開鑰匙）與一個亂數（N_1）給 Bob。
  - 訊號 (2)：Bob 收到後，送出亂數（N_2）與簽署碼（$Sig_{KRb}[N_1 \| N_2]$）。
  - 訊號 (3)：Bob 將自己的憑證（$Cert_B$，包含公開鑰匙）與產生一個亂數 N_3 一併傳送給 Alice。
  - 訊號 (4)：Alice 確定對方身份無誤之後，將亂數與簽署碼（$Sig_{KRa}[N_3 \| N_4], N_4$）傳送給 Bob。