憑證認證的運作 -單向認證

- 用戶端運作
  - (1) 發起者產生 N1，並對 N1 簽署。
  - (2) 送出N1、簽署碼與憑證給對方
  - 認證訊息：$Sig_{KRa}[N_1] \| N_1 \| Cert_A$
- 伺服端運作
  - (1) 由憑證內取出公開鑰匙。
  - (2) 對簽署碼解密(如 RSA)
  - (3)計算 N1 雜湊碼
  - 驗證雜湊碼是否正確
  - 則確認身分。