數位簽章的仲裁機制

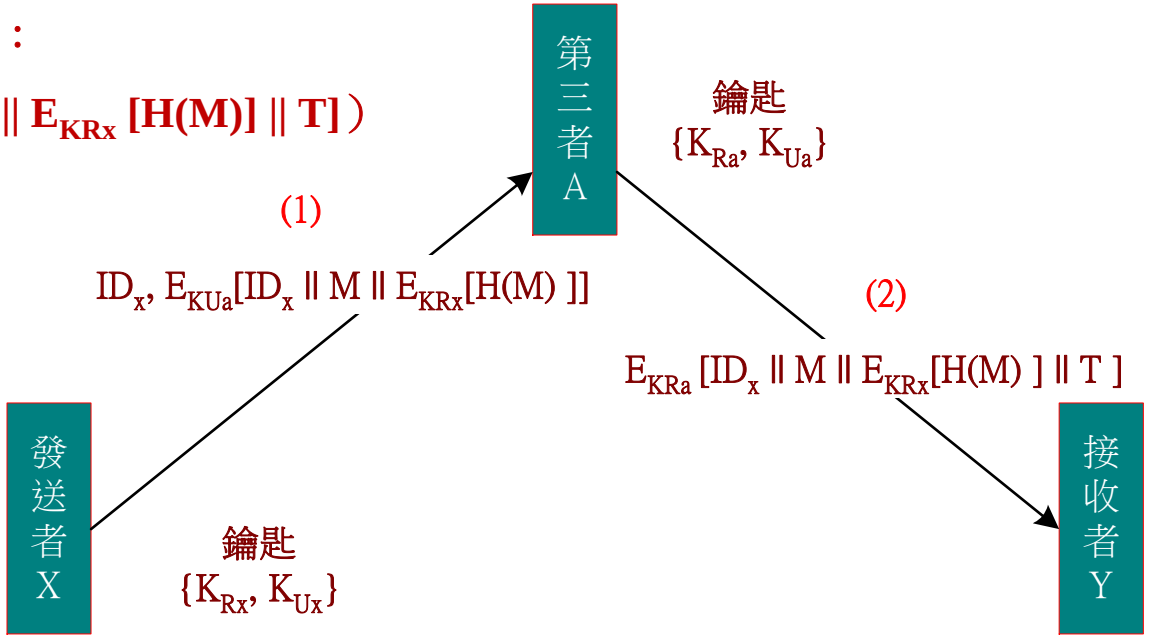
- 數位簽章應具有的特性：
  - 能夠驗證簽章的所有者、日期與時間。
  - 簽章的同時，能夠確認文件的內容。
  - 發生糾紛時，能由第三者驗證此簽章。
- 仲裁機制：
  - 直接仲裁
  - 第三者仲裁

數位簽章的直接仲裁

- 非隱密式直接仲裁
  - 訊息： **M**
  - 發送者的私有鑰匙：
  - 數位簽章：E_{KRx} [H(M)]
- 隱密式直接仲裁
  - 訊息：**M**
  - 發送者的私有鑰匙：K_{Rx}
  - 接收者的公開鑰匙：K_{Uy}
  - 加密後的數位簽章：E_{KUy} [M || E_{KRx} [H(M)]

數位簽章的第三者仲裁

- 類似『存證信函』的功能
- （A）訊息不保密的第三者仲裁
  - 第三者鑰匙：$\{K_{Ra}, K_{Ua}\}$
  - 發信者鑰匙：$\{K_{Rx}, K_{Ux}\}$
  - 填寫存證信函：
    - $(ID_x, E_{KUa}[ID_x \| M \| E_{KRx}[M \| H(M)]])$
  - 時間戳記的存證信函：
    - （$E_{KRa}[ID_x \| M \| E_{KRx}[H(M)] \| T]$）



數位簽章的第三者仲裁

（B）訊息保密的第三者仲裁

- 第三者鑰匙：$\{K_{Ra}, K_{Ua}\}$
- 發信者鑰匙：$\{K_{Rx}, K_{Ux}\}$
- 接收者鑰匙：$\{K_{Ry}, K_{Uy}\}$
- 填寫存證信函：

$(ID_x, E_{KUa}[ID_x \| E_{KUy}[E_{KRx}[M \| H(M)]]])$

- 時間戳記的存證信函：

$(E_{KRa}[ID_x \| M \| E_{KRx}[E_{KRx}[M \| H(M)] \| T])$