Secure E-Mail 安全性功能

- **S/E-Mail 安全性功能**
  - **隱密性 (Privacy)**
  - **確認性 (Authenticity)**
  - **完整性 (Integrity)**
  - **不可否認性 (Non-repudiation)**

S/E-Mail 隱密性功能

隱密性功能

公開鑰匙加密

- 傳送訊息：M
- 加密系統：E
- 訊息加密：E_{KUa} [M]

信件標頭
內文型態：encrypted; public-key
E_{KUa} [M]

會議鑰匙加密

- 訊息加密：E_K [M]
- 會議鑰匙加密：E_K [M]

信件標頭
內文型態：encrypted; session key
Key-info：E_{KUa} [K]
E_K [M]

S/E-Mail 完整性功能

- 完整性功能
  - 雜湊函數：H (如 SHA-1 演算法)
  - 雜湊值：H[M]

信件標頭
內文型態：text
M（明文訊息）
內文型態：MIC，sha-1
H [M]

S/E-Mail 確認性功能

- 確認性功能
  - 僅確認性功能：
    - 雜湊值：H[M]
    - 簽章函數：SIG
      (如 RSA 演算法)
    - 簽章碼：SID_{KRb} [H[M]]

信件標頭
內文型態：text
M（明文訊息）
內文型態：signed
SIG_{KRb} [H[M]]

  - 確認附加隱密性功能：
    - 密文：E_K [M || SIG_{KRb} [H[M]]]
    - 會議鑰匙加密：E_{KUa}[K]

信件標頭
內文型態：encryped
E_K [M || SIG_{KRb} [H[M]]]（密文）
內文型態：
SIG_{KRb}

- 12-2-4 不可否認功能
  - 確認性功能