S/E-Mail 安全郵件標準

- **(A) OpenPGP 規範**
  - **『非常好的隱密』(Pretty Good Privacy, PGP) 由 Phil Zimmermann 教授獨立發展**
  - **RFC 1991, PGP Message Exchange Formats**
  - **RFC 2015, MIME Security with Pretty Good Privacy**
  - **RFC 2440, OpenPGP Message Format**
  - **RFC 3156, MIME Security with Pretty Good Privacy**
- **(B) S/MIME 規範**
  - **Secure/MIME 由 RSA Data Security Inc. 發行**
  - **RFC 2311, S/MIME Version 2 Message Specification**
  - **RFC 2312, S/MIME Version 2 Certification Handling**
  - **RFC 2313, PKCS #1: RSA Encryption Version 1.5**
  - **RFC 2314, PKCS #10: Certification Request Syntax Version 1.5**
  - **RFC 2315, PKCS #7: Cryptographic Message Syntax Version 1.5**
  - **RFC 2268, Description of the RC2 Encryption Algorithm**

S/E-Mail 安全郵件標準

(C) S/MIME 與 OpenPGP 之比較

制定規範	S/MIME v3	OpenPGP
訊息格式	Binary, based on CMS	Binary, based on PGP
憑證格式	Binary, based on X.509v3	Binary, based on PGP、X.509v3
秘密鑰匙系統	Triple DES	Triple DES
簽章演算法	Diffie-Hellman DSS	ELGamal DSS
雜湊演算法	SHA-1	SHA-1
MIME 簽署封裝	multipart/signed 或 CMS	multipart/signed
MIME 加密封裝	application/pkcs7-mime	multipart/encrypted