# Secure MIME - Multipart/Signed 型態

## (A) Multipart/Signed 型態

- MIME 型態名稱：Multipart/Signed
- 參數：boundary, protocol, micalog

```
Content-Type: multipart/signed; protocol="TYPE/STYPE";
        micalg="MICALG"; boundary="Signed Boundary“
--Signed Boundary
Content-Type: text/plain; charset="us-ascii“
   This is some text to be signed although it could be
   any type of data, labeled accordingly, of course.
--Signed Boundary
Content-Type: TYPE/STYPE
  CONTROL INFORMATION for protocol "TYPE/STYPE" would be here
--Signed Boundary--
```

# Secure MIME - 數位信封包裝

- **(B) Application/pkcs-7-mime**
  - 信件包裝成 CMS (Cryptographic Message Syntax)
  - 數位信封格式
  - PCKS #7 安全套件

```
EnvelopedData ::= SEQUENCE {
    version Version,
    recipientInfos RecipientInfos,
    encryptedContentInfo EncryptedContentInfo }
RecipientInfos ::= SET OF RecipientInfo
EncryptedContentInfo ::= SEQUENCE {
    contentType ContentType,
    contentEncryptionAlgorithm
    ContentEncryptionAlgorithmIdentifier,
    encryptedContent
      [0] IMPLICIT EncryptedContent OPTIONAL }
EncryptedContent ::= OCTET STRING
```

# Secure MIME - 僅信封包裝郵件

- 僅信封包裝格式
  - 包裝成『數位信封』
  - 可加密或明文封送

```
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
        name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m
    rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GhIGfHfYT6
    7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H
    f8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
    0GhIGfHfQbnj756YT64V
```

# Secure MIME - 僅簽署郵件

- 僅簽署郵件
  - 採用 **Application** 型態
  - 採用 **Multipart** 型態

```
Content-Type: multipart/signed;
        protocol="application/pkcs7-signature"; micalg=sha1; boundary=boundary42
--boundary42Content-Type: text/plain
      This is a clear-signed message.
--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s
      ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
      4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbn
      n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
      7GhIGfHfYT64VQbnj756
-boundary42--
```