

電子郵件安全指引 - 電子郵件加密 / 驗證技術篇

上兩期針對常見的電子郵件攻擊以及相關防備方法做了初步的介紹。由於在網際網路上傳遞一封電子郵件，就像在實體世界中寄送明信片一般，是沒有任何隱私的，所有這封電子郵件經過的任何節點與中介伺服器（MTA，Mail Transfer Agent）都有能力與權限看到電子郵件裡面的內容，並且加以攔截、複製或刪改，要避免郵件洩密與被攔截竊聽，對郵件進行加密與驗證是最好的防治之道，所以本期將針對電子郵件加密與驗證技術來進行說明，並以 Mail2000 電子郵件系的功能作為範例參考。

公開金鑰基礎架構

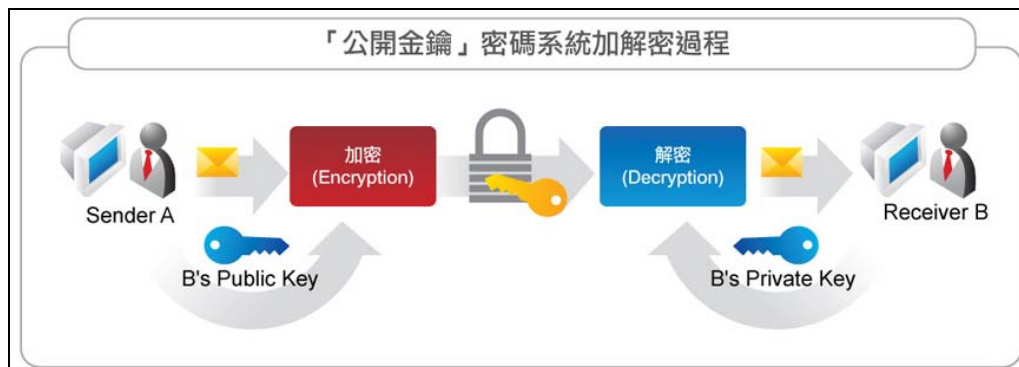
公開金鑰基礎架構（Public Key Infrastructure）是針對網路世界傳輸安全所建構的一個解決方案，目的在達到資料傳輸保密以及對資料傳輸人進行驗證。

公開金鑰基礎架構運用的是公開金鑰的加解密系統來進行資料保密與身分驗證，公開金鑰是利用兩把互相對稱的金鑰，這兩把金鑰分別為公開金鑰（Public Key）以下簡稱為公鑰，與私密金鑰（Private Key / Secret Key）以下簡稱為私鑰，這兩把金鑰的特性在於，公鑰加密的資料只有私鑰能夠解密，私鑰加密過的資料只能夠用公鑰解密，而公鑰可放置於公共區域讓任意人存取，私鑰則是私人保管。

以下利用範例說明公開金鑰的加密流程：

今天 A 要將一份機密資料透過公開金鑰系統加密給 B：

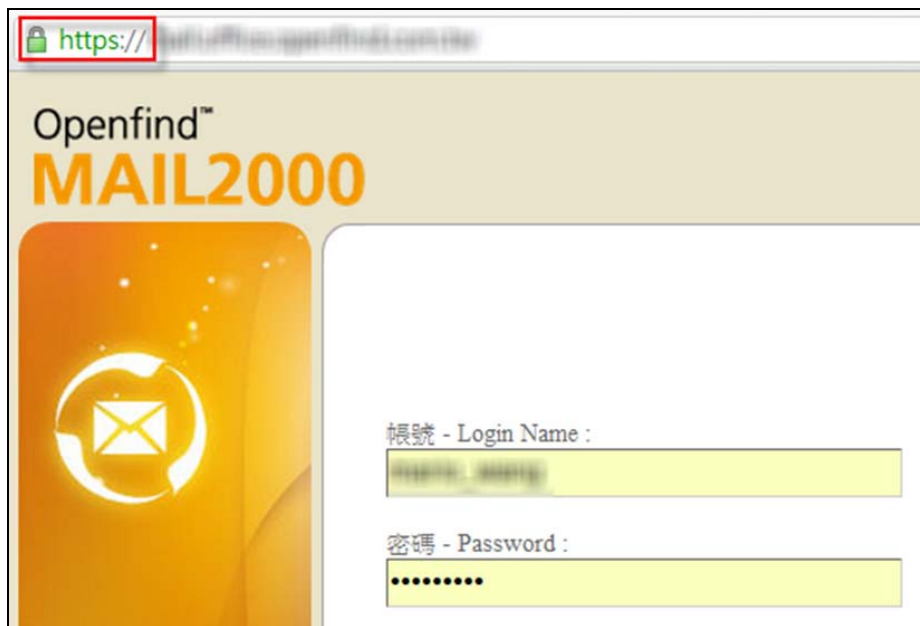
- (1) A 先取得 B 的公開金鑰。
- (2) A 用 B 的公開金鑰將資料加密後傳輸給 B。
- (3) B 收到加密資料後，以自己的私鑰解密取得原始資料。



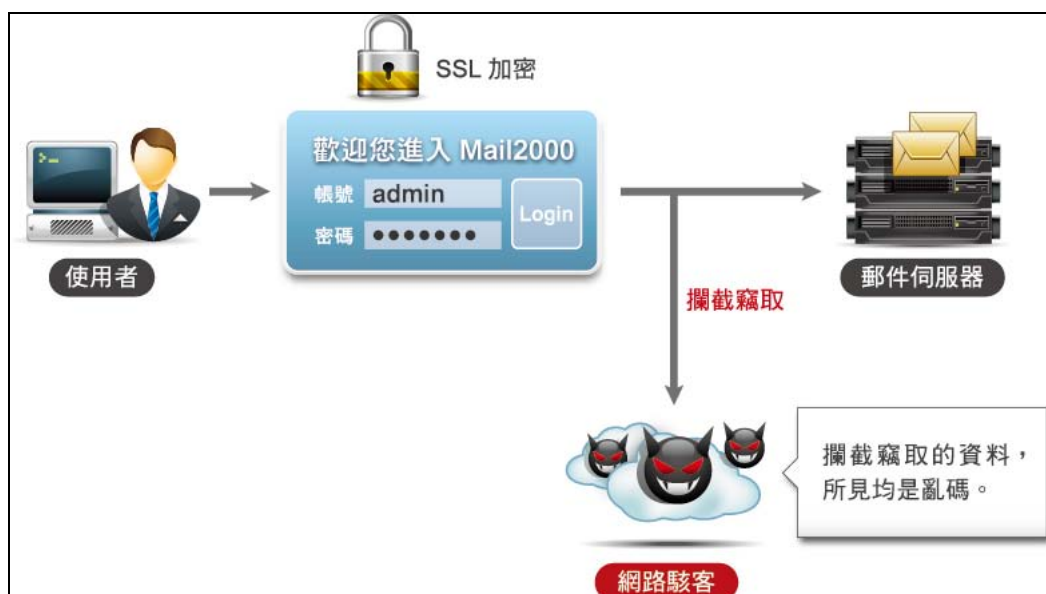
公開金鑰示意圖

SSL 加密技術

SSL 是利用公開金鑰的技術來確保用戶端與主機端在傳送機密資料時的加密通訊協定，目前廣泛的被應用於網路平台上，例如購物網站與各大網站的登入頁面，使用 SSL 技術的網頁可以在網址列中看到「https」作為網址的開頭，若沒有使用 SSL 技術的話只會看到「http」，利用 SSL 技術傳輸資料的情況下，駭客就算從中攔截，也只能看到亂碼無法得知原始訊息內容。



SSL 加密後的網頁範例



SSL 加密技術

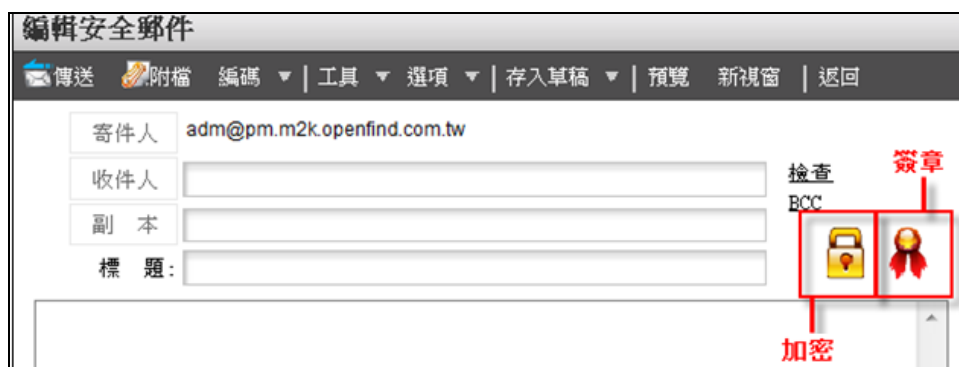
S/MIME 信件加密

電子郵件的標準格式最早為 TXT 格式(文字信件格式)，後來為了滿足電子郵件傳輸圖片、聲音、影像等需求而發展出了 MIME (Multipurpose Internet Mail Extension) 多媒體信件格式。

S/MIME (Secure / Multipurpose Internet Mail Extension) 中文譯為「安全的多媒體信件格式」，是利用公開金鑰基礎架構 (PKI) 來對多媒體信件 (MIME) 進行加密，所發展的電子郵件加密格式。

Mail2000 - S/MIME 信件加密介紹

Mail2000 安裝了 PKI (公開金鑰基礎架構) 模組之後，編輯信件的頁面就會多出了兩個按鈕，分別為「簽章」與「加密」，點擊「加密」按鈕後便可完成信件 S/MIME 加密。



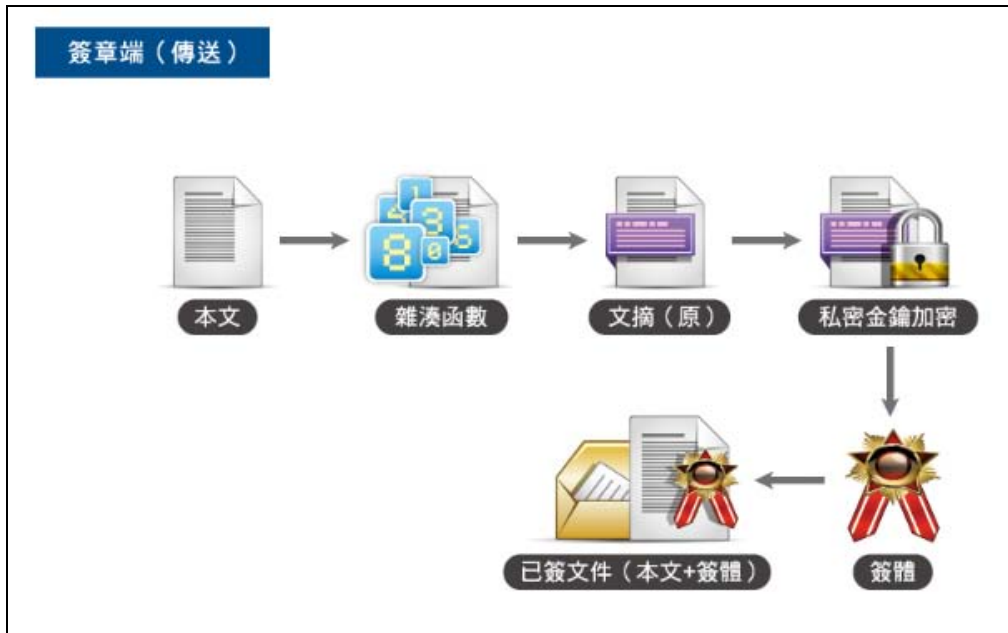
Mail2000 S/MIME 信件加密

數位簽章

數位簽章是一個用來確認寄件人身分以及信件完整性(完整性指的是信件在傳送的過程中沒有遭任何竄改)的工具，我們可以把數位簽章理解成是運用於網路上的電子印鑑，每當你的信件蓋上這個印鑑時，對方可以透過這個印鑑驗證是不是你本人，而且透過公開金鑰基礎架構 (PKI) 加解密的原理驗證信件的完整性。以下針對信件完整性驗證進行說明：

● 簽章端 (傳送)：

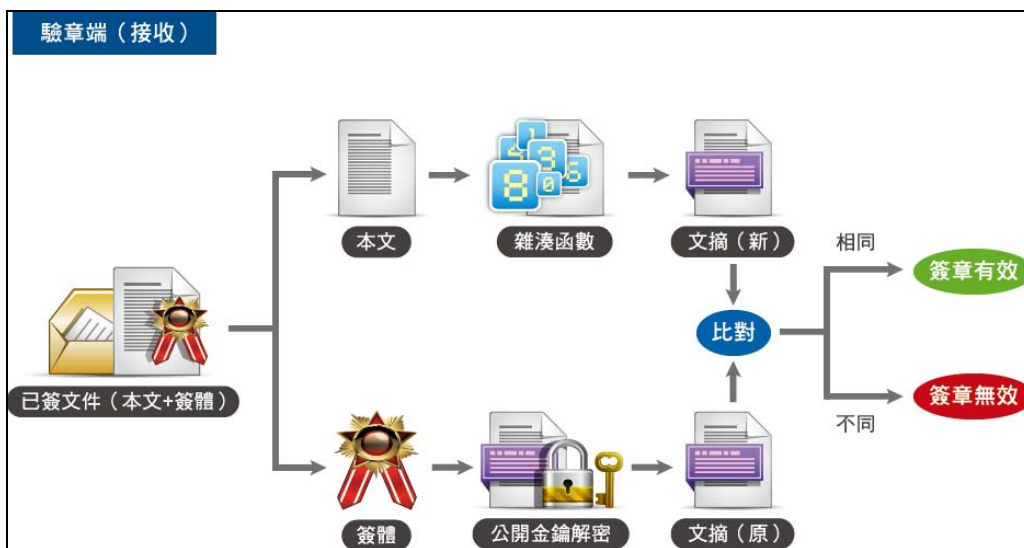
- (1) 傳送者會先將信件本文丟到雜湊函數裡產出文件摘要(雜湊函數是一個不可逆的函數，利用雜湊函數運算後的資料具獨一無二且無法逆向推導的特性)。
- (2) 文件摘要透過傳送者的私密金鑰加密後形成一個簽體。
- (3) 簽體和原來的信件本文一起傳送給接收者。



數位簽章流程圖 (簽章端)

● 驗章端 (接收):

- (1) 接收者收到信件。
- (2) 接收者將信件本文再丟到雜湊函數 (傳送方會告知使用的雜湊函數) 裡面，產出文件摘要 (新)。
- (3) 接收者將簽體透過傳送者的公開金鑰解密後產出文件摘要 (原)。
- (4) 比對兩個文件摘要是否一致，若一致就代表傳送人是正確的而且信件內容沒有被更改。



數位簽章流程 (驗章端)

Mail2000 - 數位簽章介紹





● 編輯簽章信件

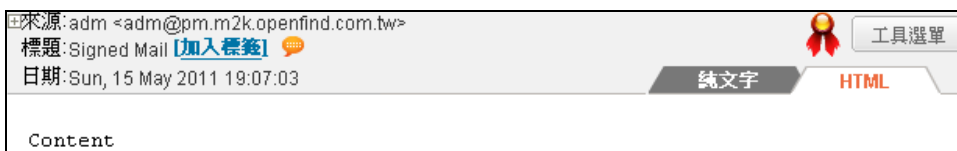
Mail2000 安裝了 PKI（公開金鑰基礎架構）模組之後，編輯郵件時會看到畫面多出了兩個按鈕，分別為「簽章」與「加密」，點擊「簽章」按鈕後便可完成信件簽章。



Mail2000 編輯簽章信件

● 信件簽章驗證

收取的信件若附有數位簽章時，會在信件標題列看到簽章符號 。若此為不合法的簽章，簽章符號會變成 。點選  或  即可查看詳細的簽章資訊。

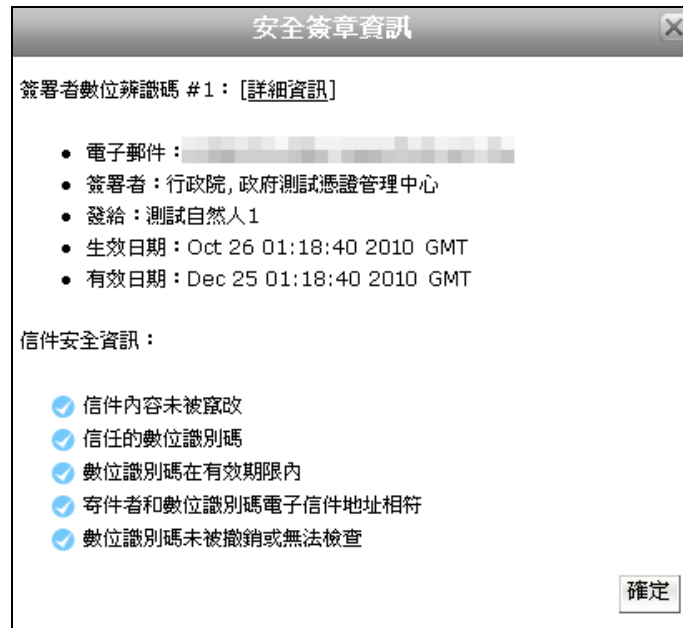


Mail2000 信件簽章驗證

● 合法簽章範例

若此信件簽章為合法簽章，則可在信件安全資訊中看到下列資訊：

- 信件內容未被竄改
- 信任的數位辨識碼
- 數位辨識碼在有效期限內
- 寄件者與數位辨識碼電子信件地址相符
- 數位辨識碼未被撤銷或是無法檢查



Mail2000 合法簽章範例

經過了這一期電子報的說明，大家是不是更瞭解如何在郵件傳遞過程中避免機密資料外洩了呢？下期電子報我們將會繼續介紹，面對不斷進化且數量與日俱增的廣告信件以及釣魚信件，所發展出的常用電子郵件過濾技術與工具。