從郵件安全到安全郵件—郵件加密與企業安全訊息管理策略

作者：網擎資訊　行銷團隊

郵件安全 VS 安全郵件

郵件安全(Email Security)一直是這幾年資訊安全市場中非常重要的一項議題，不過單單只講郵件安全已不再能夠完全涵括電子郵件所面臨的資安威脅。Forrester 在 2006 年所作的企業資安採購調查中發現，接近 50%的企業主在新的一年會有訊息安全的建置計畫，除了傳統認知上的垃圾郵件、病毒信件與惡意軟體的防治之外，也有 21%的企業主認為需要加入郵件加密(Email Encryption)的解決方案。郵件加密技術是安全郵件(Secure Email)的基礎，與郵件安全的不同點在於前者強調的是每一封郵件傳輸過程的安全性，後者則泛指電子郵件的內容安全。

郵件加密與資安威脅

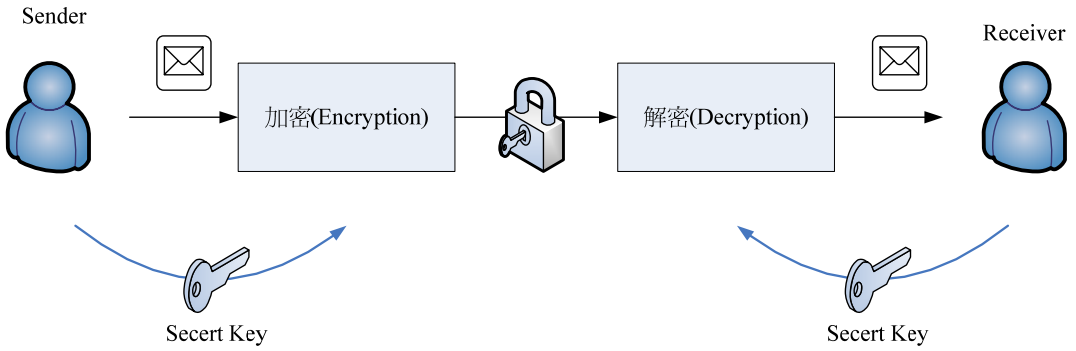
其實在網際網路上傳遞一封電子郵件，就像在實體的郵遞寄送過程中郵寄一張明信片，是沒有任何隱私的，所有這封 email 經過的任何節點與中介伺服器(MTA，Mail Transfer Agent)都有能力與權限看到 email 裡面的內容，並且加以攔截、複製、或刪改，即便收件人的郵件伺服器上已經閱讀過或刪除，這些資訊都還可能保留在上面。這就是如今垃圾郵件與各式各樣的釣魚信件(phishing)興起的主要原因之一，因為要在網際網路上進行身分的隱藏錯置與獲得收件人資訊是十分容易的。

如今的資安威脅已經超越軟體與技術層面，進入企業治理與法規遵循的層次。因為企業不再只是擔心外對內的資安威脅，同時間內對外所產生的資安疑慮，不管是洩密、惡意信件、不當信件等都有可能在轉瞬之間破壞企業的商譽與商機。要真正防制郵件傳輸過程中的安全，郵件加密是唯一可以讓企業免於郵件洩密與被攔截竊聽等等威脅的防治之道。

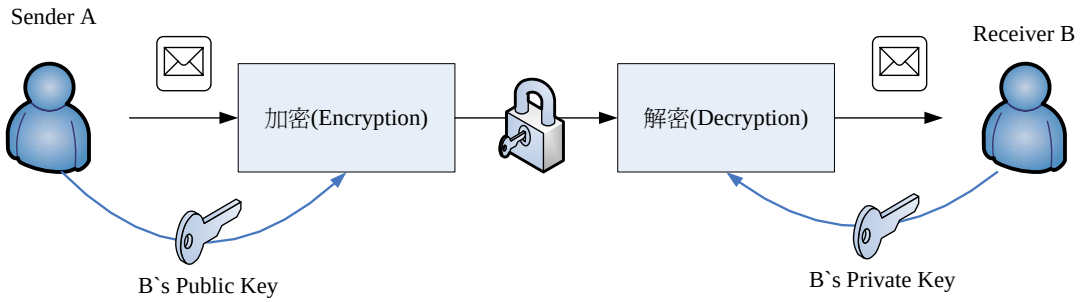
郵件加密的密碼技術簡介

在密碼學(Cryptography)的領域中，主要有兩大類的密碼系統。第一類稱為「對稱金鑰(Symmetric Key) 」密碼系統或稱「秘密金鑰(Secret Key) 」密碼系統，第二類稱為「非對稱金鑰(Asymmetric Key)」密碼系統或稱「公開金鑰(Public Key) 」密碼系統。

前者之所以被稱為對稱式金鑰密碼系統，是因為在加密與解密的過程中是使用同一把金鑰，所以這把金鑰被稱為秘密金鑰，是不能公開的。此類密碼系統的優點為其加解密速度極快，遠高於後者的公開金鑰密碼系統，但在目前網路環境上，通訊各方互相無法見面的的環境下，如何使通訊的各方能夠都獲得此秘密金鑰，讓通訊雙方執行加解密，是此類密碼系統在運用上一大問題。因此，秘密金鑰密碼系統不適合直接應用在大範圍的網際網路上。



非對稱金鑰密碼系統是由 Diffie 與 Hellman 在 1976 年所提出的，這個概念有效的解決了對稱金鑰密碼系統通訊雙方金鑰共享困難的缺點。公開金鑰密碼系統的觀念很簡單，其加密金鑰與解密金鑰是一組相對的金鑰。每一對金鑰(Key Pair)包含兩把相互對應的金鑰，一把為可以公開的金鑰（Public Key，簡稱「公鑰」）用來加密訊息；與一把必須保持秘密的金鑰（Private Key / Secret Key 簡稱「私鑰」或「密鑰」）用來解密，訊息加密傳送的過程如圖示。



非對稱式金鑰技術雖然有傳輸訊息的方便性，但是加密方與解密方還是同時需要公鑰與私鑰才能進行加解密，這需要一個建構完全的「公開金鑰基礎建設(PKI, Public Key Infrastructure)」，才能滿足網際網路隨時隨地要讓任何人都能取得公鑰的需求。PKI 的建構需要由政府或全球具有信譽的憑證管理機構(CA, Certificate Authority)來進行全球性或全國性的認證、註冊與憑證管理，加密郵件所需的電子憑證通常就是依靠 CA 所簽發的電子憑證作為基準。

郵件加密解決方案常見架構

目前的郵件加密解決方案分為兩種架構：客戶端架構(Client-Based)與閘道器架構(Gateway-Based)。這兩種架構分別是從不同的思考邏輯來設計的，分別敘述如下：

- 客戶端架構(Client-Based)

客戶端架構主張者認為終端使用者才是要負責與決定郵件加密的人，因此需要在客戶端電腦上加裝 Client 端軟體或插件(Plug-in)來進行加解密，目前已有許多第三方軟體商設計的套件可以安裝在常用的 Microsoft Outlook、Microsoft Outlook Express 或 Lotus Notes 上，用戶只需要加裝套件在這些常見的客戶端郵件軟體上即可進行加密的動作，不過要注意的是收件方也需要具備同樣的軟體才能解密。

客戶端架構給予使用者那些信件需要加密的設定自由，適合應用在中小型企業或大型企業中的特定族群（例如高層主管），因為使用客戶端架構的郵件加密解決方案，會造成企業郵件政策的不一致與增加管理複雜性，同時也要求使用者具備比較高的能力去了解並滿足法規遵循與企業政策，一般來說，導入客戶端架構的郵件加密解決方案要花費比較多的費用。

- 閘道器架構(Gateway-Based)

閘道器架構的郵件加密解決方案是為了滿足企業在法規遵循與郵件政策上的需求而設計的，閘道器架構主張者認為組織應該是負責維護郵件安全的角色，因此此方案的系統架構需要建構一台置放於企業內部郵件收發流程中的閘道器，此閘道器可以是硬體的 Appliance 也可以是軟體伺服器，目的在統一執行郵件加密的政策，並且不影響收發信的流程。

閘道器架構的解決方案雖然可以統一企業的郵件政策，在建置上會比單獨的客戶端軟體要來的經濟，但是在實用上卻比較不方便，因為收件方的郵件系統架構不一定會有相對應的解密條件，這時候通常的解決方法是請收件方連到特定的網路「安全收件匣」來收取加密信件，收件匣通常是以加密的網頁形式呈現，收件者需要連至指定網頁並鍵入帳號密碼來索取加密信件，這對於使用性來說有些不便。

比較項目	客戶端架構(Client-Based)	閘道器架構(Gateway-Based)
郵件加密負責人	寄件人	組織管理者
企業郵件政策執行	管理困難	統一執行
客戶端部署	需要安裝特定軟體	不需要安裝特定軟體
部署費用	略高	經濟
使用方便性	方便	較不便

主流郵件加密標準

目前主流的郵件加密公開標準大多同時運用上述的加密技術與系統架構，也各自有不同的部署方式，常見的郵件加密標準技術有以下幾種：

- S/MIME

S/MIME (Secure / Multipurpose Internet Mail Extension)標準是建立於公開金鑰密碼系統的技術，最早是由 RSA 所提出的。運用 S/MIME 技術需要具備 PKI，寄件方需要先安裝 CA 提供之個人電子憑證作為私鑰才能進行加密，同時也需要在加密端儲存收件端的解密金鑰才能同時進行加密動作，這需要一個運作良好的 CA 認證網站與 PKI 架構。

- PGP 與 OpenPGP

PGP (Pretty Good Privacy) 與 OpenPGP 是一種公開標準，最早是由 Phil Zimmermann 所設計的。PGP 同時運用了對稱性金鑰與非對稱性金鑰密碼技術，並且需要客戶端軟體或 Plug-in 才能運作。

- IBE

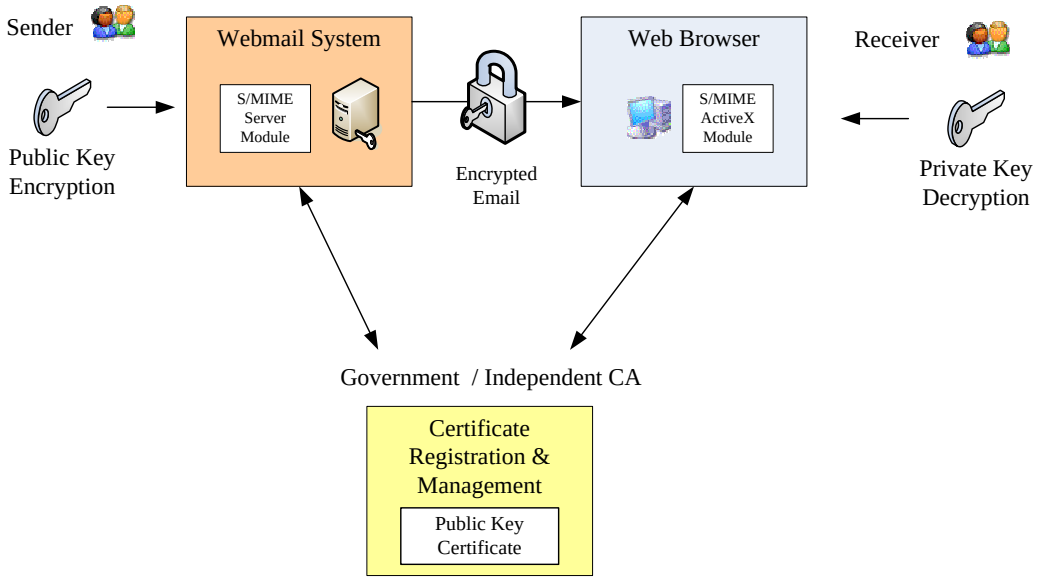
IBE (Identity-Based Encryption) 技術是 1980 年代之後才被提出的最新觀念，利用收件人的電子郵件地址作為加密的公鑰，可以省去 PKI 建置的麻煩。寄件人只需指定收件人郵件地址作為加密公鑰，即可寄出加密信件，收件人只需連上特定的私鑰產生伺服器（Key Server, or Private Key Generator, PKG）即可取得可以解密的私鑰，並且取得私鑰之後就不再需要重新申請。

企業導入郵件加密的應用策略

目前市面可見的郵件加密解決方案都還處在初步階段，實用上都還需要一段時間的印證，部署上也須經過頗為繁複的流程，但是其實通過政府正式立法並行之有

年的各式 PKI 機制，加上適當的 Webmail 郵件加密解決方案，就可以輕鬆的建構企業內部的郵件加密系統。

正如下圖所示，PKI 憑証加上具有郵件加密機制的 Webmail 的郵件平台，可以方便的進行郵件加密，而不需要加裝客戶端軟體，只需在瀏覽器上安裝 ActiveX 的 S/MIME 套件即可進行解密動作，配合已經申請的各式 PKI 系統，諸如內政部核發之自然人憑證或電子工商憑證管理中心核發之公司憑證等等，即可作為公鑰進行加密，傳輸過程中可以透過 OCSP(Online Certificate Status Protocol)或者是 CRL(Certificate Revocation List)等標準協定與 CA 網站進行溝通確認憑證。



傳統上的郵件加密應用大致集中於金融與政府市場，諸如電子憑證簽章之於電子帳單與電子商務，應用電子憑證作為各式政府 E 化申請表單等，但是由於各種企業治理與法規遵循的需求，企業內部稽核與訊息安全控管成為推動郵件加密的新動力，新的郵件加密應用將集中於達成企業郵件政策集中控管，確定訊息安全傳輸過程，應用電子憑證作為簽章郵件以利企業流程管理或企業安全單一登入機制(SSO)等等方面。

在可見的未來，郵件加密市場將會逐漸興起，越來越多的國際大廠漸漸的也會把眼光放在郵件加密這塊領域。在郵件安全成為企業資安管理最重要一環的今天，郵件加密已經是企業維護自身智慧財產與商業機密的最重要手段，缺少了安全郵件的解決方案，郵件安全將缺失穩固的一角，企業應當停下腳步，好好思考建置具備郵件加密功能的安全訊息機制以確保組織競爭力。