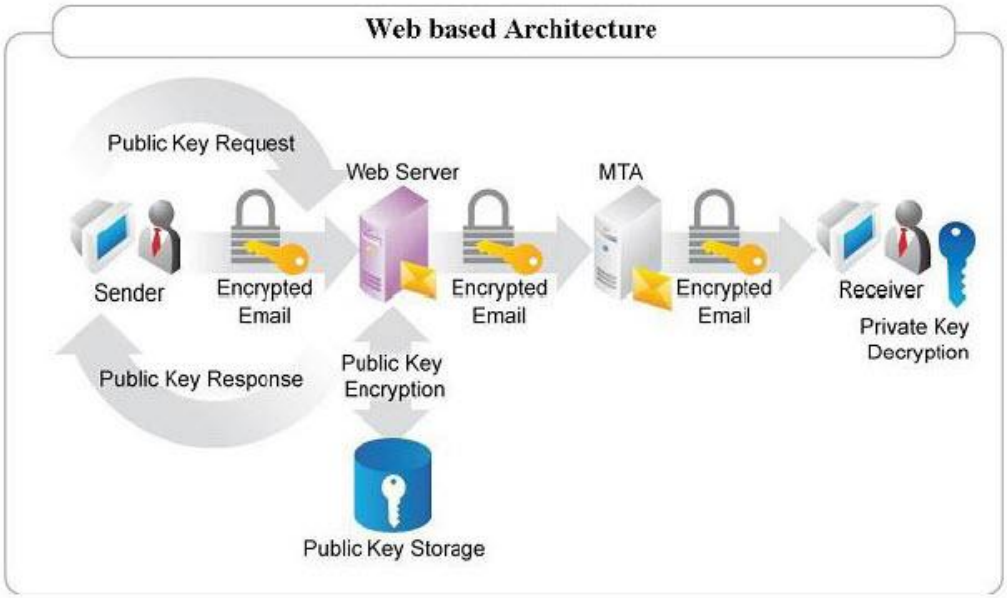
由 **PKI** 數位簽章 探討郵件安全

Openfind Mail2000 PKI 支援政府憑證 GCA、自然人憑證 MOICA、工商憑證 MOEACA 等主流憑證，加上可攜性的使用優勢，將可為政府單位、企業用戶帶來最佳的郵件安全競爭力！

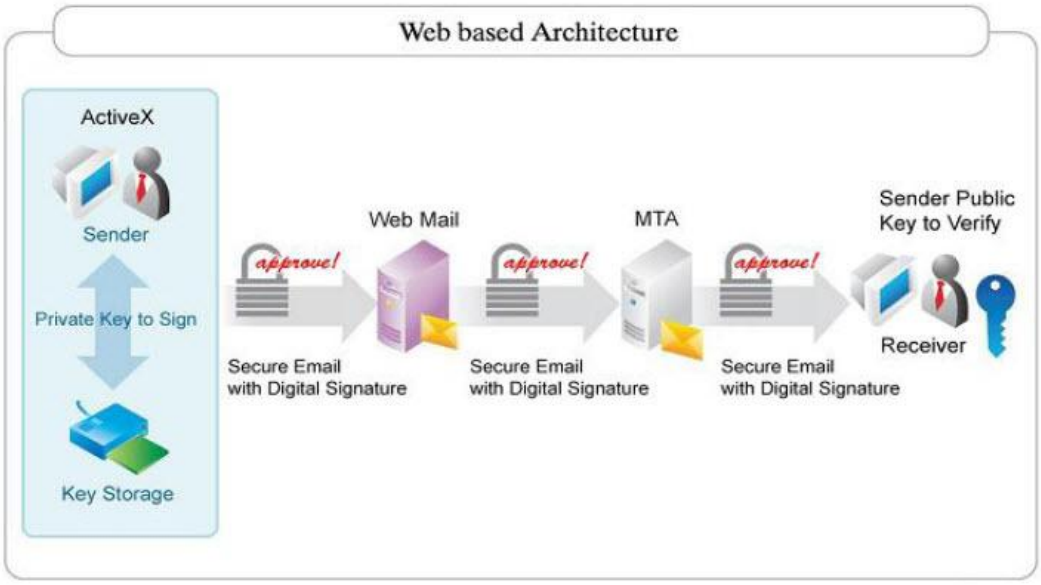
電子郵件近幾年來已成為絕大多數公司不可或缺的重要系統，許多公司行號依賴電子郵件甚深，許多商業書信皆透過 E-mail 傳遞，一旦郵件無法正常運作或郵件內容被駭客竊取，都將直接導致企業營運的立即性損失！所以電子郵件既然作為正式商業往來，當然更要兼顧「機密性」與「不可否認性」，一方面企業不容許自己送出的郵件遭到攔截或篡改；一方面更希望收到的電子郵件能有正式法律效力，同時送信方不能否認自己簽名蓋章過的郵件。為達到這個目的政府於 2002 年 4 月正式頒布電子簽章法，使用法定憑證機構所提供之數位簽章（政府憑證 GCA、自然人憑證 MOICA、工商憑證 MOEACA），在法律上不但防止竄改及冒名頂替，亦可達到簽名蓋章之效果，以防止事後否認傳送。

PKI 是電子郵件的安全機制之一，在嚴格的 PKI 定義中一份郵件只要離開自己的電腦就必須是安全的，而不是到了郵件伺服器才開始進行加密、解密的安全作業，因此在各家提供 PKI 的廠商中，大部分公司會把所需要的 Public Key 以及 Private Key 存放在使用者本機電腦的個人通訊錄中，雖然這種作法可以達到 PKI 的精神，但是只要換台電腦或個人通訊錄損毀等狀況發生，所有辛苦收集回來的收件人 Public Keys 將會通通遺失而無法再傳送加密文件給對方，把需要使用 PKI 的使用者綁死在一台電腦前面，這並不合乎人性！

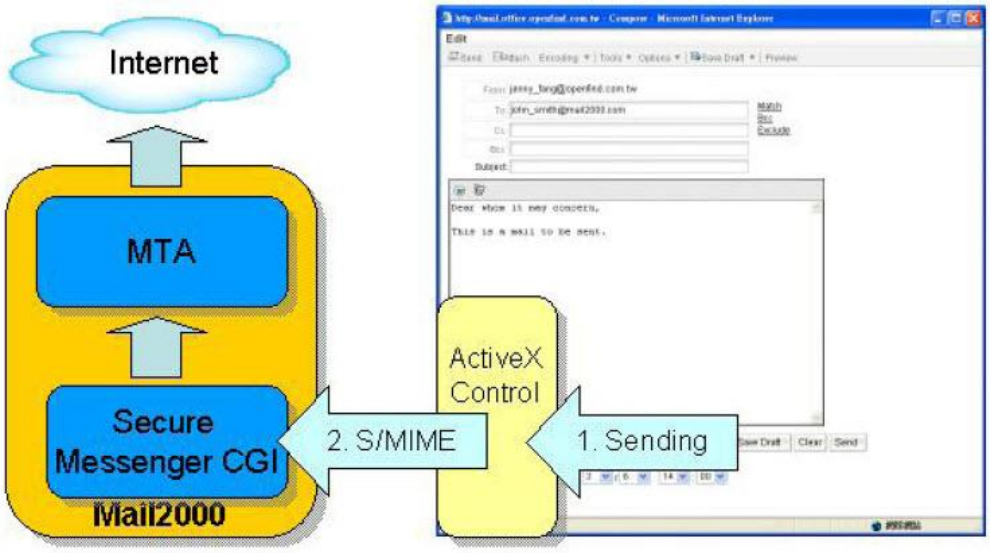
Openfind Mail2000 PKI 的機制把聯絡人的 Public Keys 存放在郵件伺服器上，而使用者自己的 Private Key 則放在卡片裡，因此使用者不論走到世界各地，只要帶著自己的卡片，透過瀏覽器就可輕鬆的收發 PKI 加密郵件。所以就算帳號密碼被偷取，只要沒有卡片進行驗證是無法看到加密郵件；而若是卡片遺失，但沒有 PIN Code 也是無法開啟加密郵件，所以 Mail2000PKI 同時兼顧了方便性以及安全性。使用流程說明如下圖所示：



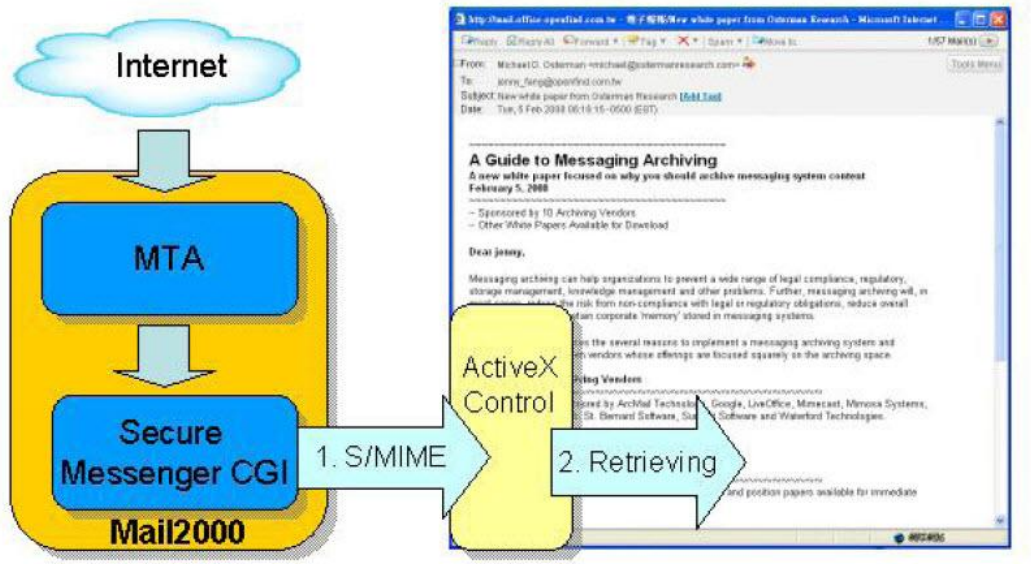

所以當使用者透過瀏覽器要發送加密郵件給對方時，會先於郵件伺服器上讀取接收者的 Public Key 並在瀏覽器端製作成 S/MIME 加密格式，因此只要是離開使用者的電腦郵件必定是加密型態，嚴守 PKI 的安全精神。




此外若使用者送出電子簽章郵件，瀏覽器只需要到卡片上讀取 Private Key 並製作成簽章郵件格式，郵件一旦離開自己的電腦就具備法律上的「不可否認性」，此特性對於商業書信或機密文件的往返十分重要，同等於簽名蓋章，以防止事後否認傳送。建議政府單位、企業敏感性部門（如法務、財務）可先建置第二台安全郵件系統，確保機密安全與郵件法律效力。




如此嚴密的 PKI 機制，對於使用者卻是十分簡單，僅需要在 Web Mail 上勾選郵件加密選項，其他動作皆由瀏覽器端的 ActiveX control 和卡片溝通即可完成加密，完全不需要改變使用者的行為。




而收到加密郵件時也由瀏覽器端的 ActiveX control 去做解密的動作，保證傳輸過程中的安全。

故 Openfind Mail2000 PKI 除提供完整郵件安全的「機密性」與「不可否認性」外，更同時考量「憑證可攜性」、「使用便利性」，再加上支援政府憑證 GCA、自然人憑證 MOICA、工商憑證 MOEACA 等所有主流憑證，是政府單位、企業內部最佳的「第二套郵件伺服器」，專門提供給電子文件需法律效力的單位、或是需高安全性的特定部門、以及高階主管所使用，為政府單位、企業用戶帶來最佳的郵件

安全競爭力。