從公開金鑰基礎建設為導向探討現行安全電子郵件使用之普及度

指導教授：韓豐年　老　師
吳幸收　老　師
研究學生：葉家銘　黃彥錫

摘　要

有鑑於二十一世紀網際網路的發達資料傳輸來往頻繁，爲了保護資料的完整性與私密性，大多數的系統會利用加密技術來防止資料遭篡改。因此資料傳送在保護機制運作上以所謂公開金鑰基礎建設(Public Key Infrastructure)，最能提供完善的安全功能。它所衍生出來的一種資訊安全架構乃是利用金鑰的加解密技術，它是透過密碼學原理及數學式求得加解密鑰匙，進而還原資料原貌。這樣的技術目前通用於企業資料通訊傳遞，如：電子公文、電子郵件、自然人憑證等具授權關係的場合。由於各企業組織導入 PKI 機制已日漸普遍。然而政府機關自推行電子化政府制度後亦積極將 PKI 導入組織內部。PKI 包含各層面的應用範圍，安全電子郵件即爲其中一項，爲詳細瞭解政府機關內之資訊人員是否對於資訊安全有足夠的認知，並使用電子郵件時，能妥善將訊息加密的技能與利用上之普遍程度，因而做量化調查與探討。

本研究變項包括「PKI 和安全電子郵件使用知識」、「安全電子郵件使用技能與環境」、「安全電子郵件使用普及度」。工具上使用描述性統計、次數分配、因數分析、單因子變異數分析（含獨立 T 檢定），相關係數分析。

壹、緒論

一、研究背景與動機

隨著網際網路的興起，資料的傳輸與往來頻繁及通訊技術日益成熟進而帶動電子商務及各項網路技術的蓬勃發展，因此現今的「網路安全」及「使用者認證」等議題成爲電子商務發展重點。電子郵件在我們生活中已成爲不可或缺的一項溝通工具，因爲它提供人們信件快速抵達的便利性，傳送快速成本低廉廣受大眾的喜愛。早期的電子郵件系統沒有任何安全機制，第三人士若有心即可偷窺，甚至遭篡改。之後安全電子郵件標準系統如： PGP、PEM、S/MIME 皆是利用加解密技術及認證的方式達到信件的私密性、完整性、可驗證性和寄件人不可否認性。以 Outlook 電子郵件爲例：收信人在收到信件後仍可以將信件內容任意複製、剪貼、列印或轉寄給第三人，或是信件存放於主機內，遭後門程式植入作爲遠端控制被窺視、竊取而破壞使用者的私密性及安全性。

基於以上原因，本次研究將針對現行政府機關自 PKI 導入組織後在各項應用領域裡，例如：安全電子郵件的使用上，是否因

資訊安全認知的提升，而有普遍的趨勢，以及應用的成效做進一步探討及調查分析。

貳、文獻探討與相關理論技術介紹

一、公開金鑰基礎建設

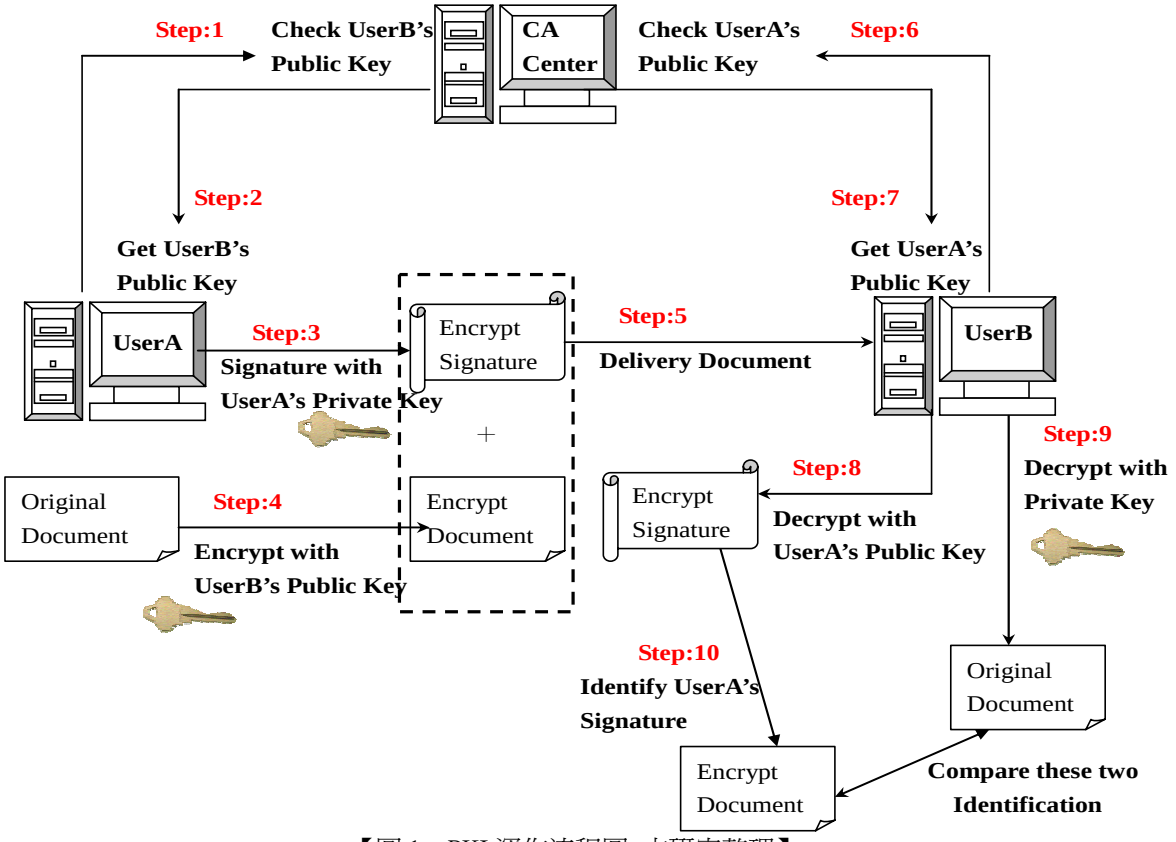
公開金鑰基礎建設(Public Key Infrastructure)是憑證結合密碼學的應用發展，資料在網路傳輸中的一項安全機制，利用一對金鑰(Key-Pair)，即可將資料安全完整傳遞至收信人手中，而不被破壞。最早於1977年由Daffier and Hellman提出，期間經二十多年安全性測試，證實是目前最安全可靠非普通電腦運算能破解的，在此架構下須透過憑證中心將金鑰認證始得發生作用，使用者透過憑證可以辨識對方身份；並確認金鑰爲對方所有，將欲寄送之文件利用金鑰之密碼演算法將其加密簽章來保護文件完整未遭修改，提供資料隱密性。這樣的機制可以應用在電子商務、網路交易和其他複雜的安全驗證作業。

(一)、PKI 定義

PKI (Public Key Infrastructure) 、公開金鑰基礎建設顧名思義就是以公開金鑰密碼技術爲基礎所衍生出的一種資訊安全架構，它必須運用金鑰加解密的技術和憑證管理（Certificate Authority,CA）的認證、即驗證金鑰，來確保網路資料傳輸或交易的安全。透過這個機制，可以在電子訊息的傳遞與執行交換過程中提供身分認證Authentication、來達到資料的完整性Integrity，不可否認性 Non-Repudiation，私密性 Confidentiality。

(二)、PKI 的運作模式

當使用者取得憑證與金鑰後便可以透過的安全機制保護電子訊息機交換的安全及完成身分認證，PKI 安全機制運作方式依下圖表示：使用者持有公鑰與的檔案，公鑰公諸於大眾，私鑰自行保管，公鑰和私鑰間



【圖 1　PKI 運作流程圖 本研究整理】

具有單一之對應關係，在傳遞訊息時，寄件者先以自己的私鑰對訊息摘要做簽章，再用收件者的公鑰對訊息加密，之後進行傳輸，過程裡訊息本身無法輕易由非訊息接收者解讀；只有訊息收件者之私鑰可將寄件者之訊息解密，來獲得原始訊息內容。

二、現代密碼學介紹

（一）對稱性密碼系統

對稱式密碼系統(symmetric cryptography)在進行加解密時所使用的鑰匙均爲同一把。DES（Data Encryption Standard）標準資料加密即爲對稱性加密法。

Des 將明文分爲 64 區塊每個區塊經由調換（transposition）代替（substitution）等運算方式做加密處理，故加解密速度快常被用於較長的資料上。但對稱式密碼最大問題在於加密解密均用同一把鑰匙，傳送過程中易遭竊取。資料私密性將受威脅。

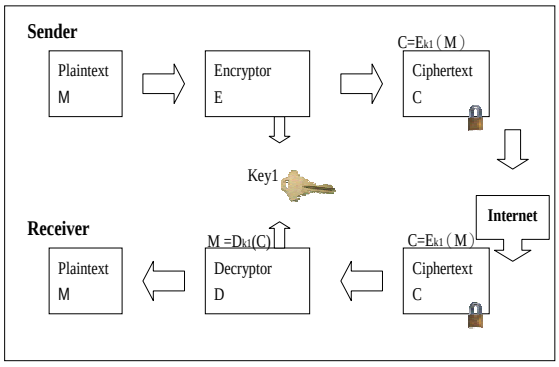


圖 2-3 對稱式密碼圖解

（二）非對稱性密碼系統

非對稱性密碼系統（Asymmetric cryptography），於 1976 年由 Whitfield Diffie Martin Hellman 提出，每一個使用者均有兩把鑰匙：（ P、S ）P 爲公鑰、S 爲私鑰；公鑰與私鑰內容不同；P≠S，也就是公鑰不需保密可對外公開，私鑰需妥善保管，不可被第三人知曉。例如：User A 傳一封信給 User B，User A 先用 User B 的公鑰 P 加密，當 User B 收到信件後，就用自己的私鑰 S 解密。雖然公鑰是公開的，但是要計算出對應的私鑰是很困難，所以非對稱式加解密不必擔心公鑰在 Secure channel 中遺失或遭盜取。

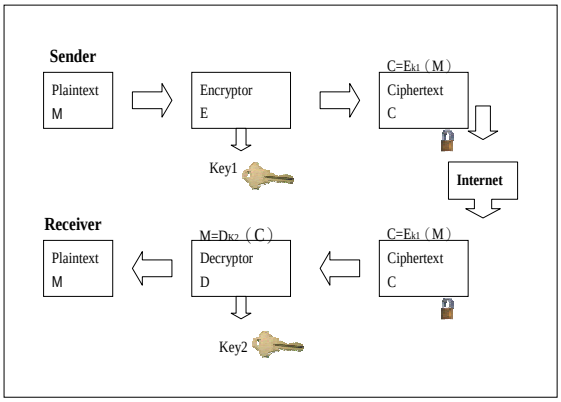


圖 2-4 非對稱式密碼圖解

（三）公鑰與私鑰的產生

RSA 是 Rivest, Shamir 和 Adleman 於 1978 年共同提出的數學演算法，爲目前最普遍的非對稱性公鑰加解密法，它的加解密速度比對稱式加解密法（DES）慢，常被用短訊息加密。例如：對於 DES 秘密鑰匙的加密、數位簽章簽署（信件摘要加密）。

以下以 RSA 爲例說明公鑰與私鑰的產生：

條件：

1. 選擇兩個極大質數 p 和 q，令 n = p × q。
2. 選擇一個滿足與 (p-1) × (q-1) 互質之整數 e，且 e＜(p-1) × (q-1)。
3. 計算 d，d 須滿足(exd) mod [(p-1) × (q-1)] =1，且 d＜(p-1) × (q-1)。
4. 以(e ,n)爲公鑰 (d ,n)爲私鑰。

實例：

1. 選擇兩個質數 p=3，q=11。
2. 計算 n，n=p×q=33。
3. (p-1)×(q-1)=20，選擇與 33 互質之整數 e=3。計算 d，3×d (mod 20)=1，其中 e=3、d=7。
4. 以(3，33)爲公鑰；(7，33)爲私鑰。

（四）加密、解密之運算流程

若 User A 送一訊息 M 給 User B，用 User B 公鑰 P=(3，33)將訊息 M 加密成 C 後公式應爲： C=M mod n，其計算方式爲：

if(m==2)

then(C=2 % 33=8)

當 User B 接到密文後須用自己的私鑰 S=(7，33)解密成明文 M 時公式應爲：

M = C mod n，其計算方式爲：

if(C==8)

then(M=8 % 33=2)

※非對稱性密碼對鑰匙的管理遠比對稱性密碼有效率，且不易被破解、安全性較高；其另一特點則是非對稱性密碼執行運算加密時，不一定要用公鑰 P 加密，私鑰 S 亦可作加密，即一明文 M 若用私鑰 S 加密成 C，解密時則須公鑰 P 將密文 C 解密。

（五）雜湊函式

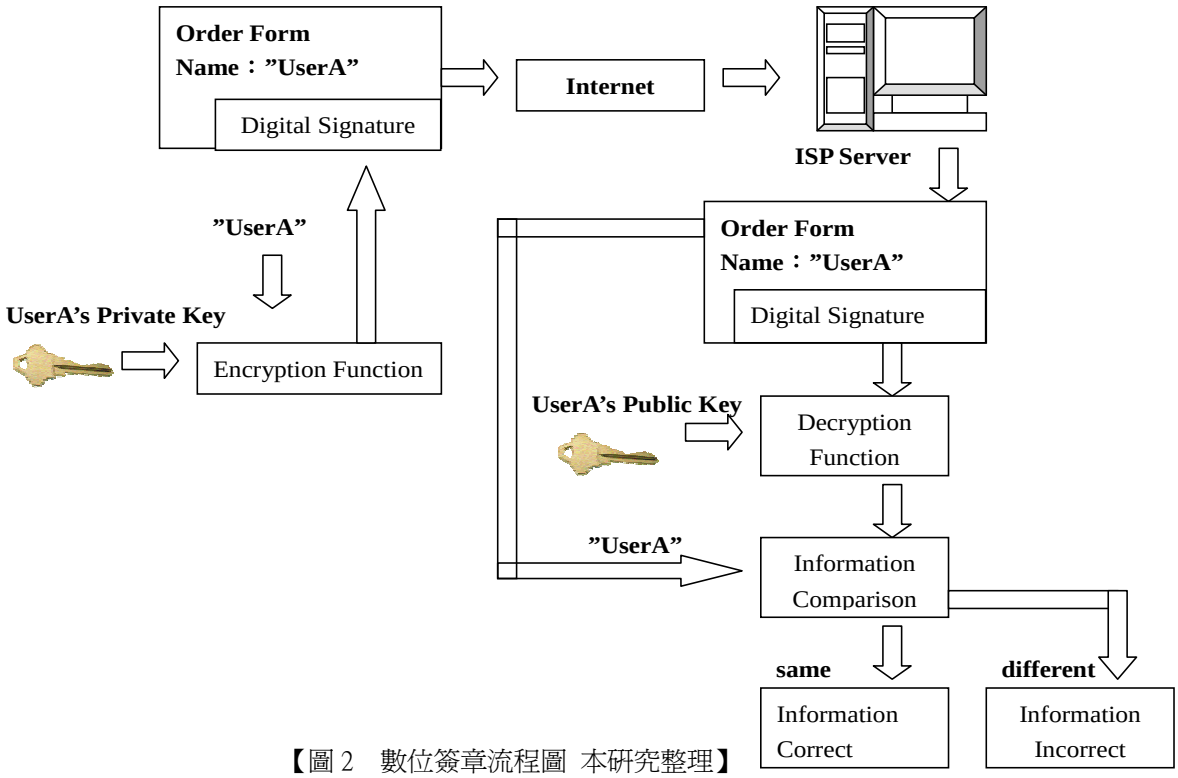
雜湊函式(Hash Function)是一種單向的數學函數，目的是將一個任意的訊息雜湊成一個較短固定長度之數值（Hash Value）。此固定數值就被稱做訊息摘要，在 PKI 的應用上其功能則是讓使用者在網路公開訊息，並阻止有心人士竄改內容。目前較知名的雜湊函式有 MD4、MD5、SHA-1 三種演算法。

（六）數位簽章

數位簽章就是利用 sander 的私鑰去對名字加密，理論上是對發送的文件表示負責。證明是 sander 發出的訊息無誤。至此也保護文件的不可否認性。圖 2-3 爲數位簽章簽署的過程，舉例說明：user A 有一對金鑰（P.S），當 user A 要在網路下訂單時，他先用私鑰 S 對自己的名字 user A 加密，之後再將這份簽名附在訂單上送出。當商店收到訊息後，接收者用 user A 的公鑰 P（P 是公開的），對這份數位簽名作解密的動作，若解出的訊息確定是“user A”則商店即可確認這份訂單是 user A 寄出。

三、數位憑證

網路上傳輸資料若使用公開金鑰加解



【圖 2 數位簽章流程圖 本研究整理】

密，公鑰是必須先認證許可才得以使用。因此使用者需向有權力之機構（Certificate Authority）申請數位憑證，來證明使用者身份的合法性及訊息發送的不可否認性。由一個公正單位確認使用者和他的公開金鑰之間的關係，目的即是查驗憑證申請人資料的正確性和金鑰是否屬於使用者，若是，則憑證管理中心將爲使用者發給證明文件，稱之爲公開金鑰憑證 PKC（Public Key Certificate），亦稱之爲電子證書。

（一）國內 PKI 憑證中心

政府公開金鑰基礎建設(GPKI)採階層式架構，設置政府憑證總管理中心（行政院研考會負責），負責簽發憑證給憑證機構其下設置：

(1)內政部憑證管理中心（內政部負責），負責簽發自然人憑證。

(2)電子工商憑證管理中心（經濟部負責），負責簽發公司行號憑證。

(3)政府憑證管理中心（行政院研考會負責），負責簽發機關（單位）憑證、伺服器應用軟體憑證、社團法人、財團法人及非法人團體憑證及測試憑證。

(4)測試憑證管理中心（行政院研考會負責），負責簽發機關（單位）憑證、伺服器應用軟體憑證、社團法人、財團法人及非法人團體憑證及測試憑證。

四、基本電子郵件系統架構

E-mail 係爲一種電子資料傳遞的工具之一，也是一種非同步的資料傳送方法，它是一種分散式主從架構並由兩個部份所組成：

◆ 郵件使用代理者（Mail User Agent MUA）：一種使用者互動的電子郵件應用程式，可用來編輯、傳送、接收電子郵件的介面。例如：MS Outlook Express、Unix elm、pine。均是 MUA。

◆ 郵件傳送代理者（Mail Transport Agent MTA）：根據所屬之規則來判定這個郵件的處理方式，如果郵件的收信人並非它的收信者，就會把郵件轉送至收信人的郵件伺服器內；若此郵件的收信人是它的使用者，則會將郵件儲存至使用者之信箱等待使用者取信。例如：Unix sendmail、qmail 和 MS Exchange server。

（一）電子郵件系統通訊協定

1. POP3（Post Office Protocol Version 3）：這是一種主從式架構電子郵件收信的通訊協定，它允許使用者連線至郵件伺服器檢查新信件，並下載回客戶端電腦，可供離線（Office）閱讀，並可刪除伺服器上之郵件，避免伺服器容量額滿。

2. SMTP（Sample Mail Transfer Protocol）：以字面上而言、SMTP 係爲一種用來傳送郵件的簡單傳輸協定。SMTP 將郵件由客戶端（MUA）送到伺服器（MTA）上，或是由一台伺服器（MTA）傳送至另一台伺服器（MTA）上。

3. IMTP（Internet Message Access Protocol）：是一種直接對伺服器上的信件作存取操作的通訊協定，不同於 POP3 的是它提供線上直接對伺服器上的信件作存取操作的通訊協定，因爲信件均放置於郵件伺服器上，使用者只需透過網路即可直接閱讀信件，不需先行下載至目的端主機讀取，例如：http://www.police.org.tw-Open Web Mail（網頁式電子郵件）。

（二）傳統電子郵件缺點分析

傳統電子郵件不具有任何安全的措施，因此具有以下缺點：

◆ 訊息易造成外洩：傳統電子郵件在傳送過程前沒做任何簽章及加密動作，極容易遭第三人窺視和訊息外洩。

◆ 信件易遭僞造和冒名寄出：電子郵件工具如：Outlook，若先前收到之信件沒有加密，一般使用者都可使用轉寄信件之功能，可將內文加以修改並以自己名義再行發出，則無法確定信件的完整性。

◆ 無法確認寄信人之身分：在傳統郵件系統沒有寄信人簽名，同時郵件伺服器在執寄信人轉送信件服務時，也未對寄信人的身分作確認，因此有心人士即可僞裝他人寄信。一旦收信人無法對信件來源做驗證，即無法確認該信寄件人之身分。

◆ 寄件人無法限制收件人存取信件的行爲：寄件人若把信件寄出，則無法限制使用者作複製、列印、轉寄、剪貼等動作

◆ 信件無法自動銷毀：當信件傳送至郵件伺服器內，若收信人未至伺服器收取郵件，信件將永久存於伺服器裡，寄信人並無法判定收信人是否確實收到寄信人所寄出之信件，因爲收信人有可能沒收到，或者已收到但否認。

（三）安全電子郵件的優點分析

安全電子郵件利用金鑰加/解密功能，達到以下優點：

◆ 訊息不易遭竄改：使用者透過公/私鑰將訊息加密及簽章後傳送到收件者手中，確保其完整性、私密性，使訊息不易遭有心人士窺視和篡改。

◆ 使用者身份易識別：郵件一經傳送給收件者後，利用對應的私鑰將訊息解密，再核對寄件者的數位簽章是否爲同一人，來達到身份的不可否認性。

◆ 收件者無法任意轉寄：訊息解密後收件者雖可修改其內容，但只限於自行保留無法轉寄給第三人，因爲就算解密之訊息轉寄後、則變成先前的訊息摘要也會隨著訊息一起寄出，與第二次轉寄之寄件人即不相符合，無法達到一致性。

五、密碼系統於電子郵件的應用

（一）PGP（Pretty Good Privacy）

PGP（Pretty Good Privacy）於 1991 年由 PHILIP R.ZIMMRMANN 所開發設計的郵件簽章與加解密程式。可配合 MS Outlook Express 使用，PGP 最初發展之際曾被美國限制其技術輸出國外，如今已被世界廣泛使用，在個人使用者方面 PGP 是免費的軟體，它採用 RSA、DSS 及 Diffie-Hellmann 之加密演算法。

此外PGP擁有自己的金鑰伺服器負責簽發予註銷憑證，只要使用者自行產生公鑰後，上傳至 PGP「公鑰伺服器」；PGP「公鑰伺服器」就會將您的公鑰傳送至其他的「公鑰伺服器」。每一個使用者都可以到「公開金鑰伺服器」去取得某人的公鑰。

（二）PEM（Privacy Enhanced Mail）

安全電子郵件 PEM 是網際網路的一項標準亦是針對傳統電子郵件的缺點所另行改良設計，它主要利用加密技術、雜湊函式及電子證書，來保證信件傳輸過程中的完整性、發信人的身分確認及不可否認性和資料驗證性。因此 PEM 在密碼學的功能上就是身分驗證訊息加密及金鑰交換。

（三）S/MIME

S/MIME（Secure/Multipurpose Internet Mail Extension）是爲了達到安全電子郵件系統所制定的標準規格，並提供私密完整及不可否認性之安全服務。它是已 RSA 加密法爲其基礎，爲了使讀者對 S/MIME 有初步認識，以下大略介紹 RFC 822 和 MIME。

RFC 822 定義安全電子郵件系統所傳送訊息文字格式，在 RFC 822 中訊息被分爲信封與內容兩部份，信封包含傳輸與遞送所需要的訊息，而內容則是要送給收件人的物件。RFC 822 針對內容所訂定標準此內容定義了一組標頭欄位（Head Field），郵件系統

可以利用這些標頭欄位來產生信封，且此標準的設計目的是爲了讓程式可以很簡單擷取這些欄位資訊。

RFC 822 所制定之訊架構從訊息開頭是由一些標頭列所組成，接著就是沒有限制的本文文字部分。標頭與本文之間是用一列空白列來區隔。訊息必須由 ACSII 文字組成，第一行空白列之前的文字列都會被當成標頭列電子系統的 UMA 部分會用到這些標頭列。

一個標頭列是由一個關鍵字、一個冒號與一個參數值所組成的，標頭具有非常高的擴充性可以根據不同需求定義不同關鍵字，最常使用的關鍵字就是 To、Subject、From、以及 Date。以下是一個 RFC 822 的訊息範例：

標頭
```
Message-ID:<20040720010845.9381.qmail@web16913.mail.tpe.yahoo.com>
Received: from [192.83.171.253] by web16913.mail.tpe.yahoo.com via HTTP; Tue, 20 Jul
2004 09:08:45 CST
Date: Tue, 20 Jul 2004 09:08:45 +0800 (CST)
From: =?big5?q?joan4518?= <joan4518 @ yahoo.com.tw>
Subject: 凱達格蘭學校青年領袖班請書會..有興趣可以來聽一聽喔.
To:"Russell" <russell0385@ms93.url.com.tw>
```

本文
```
日期：2004 年 07 月 24 日
講座時間：02 ： 00 PM
講座地點：凱達格蘭學校
全程時間：60 ～ 90 分鐘
主講老師：簡偉斯　導演
```

MIME 是 RFC 822 架構的擴充，它希望能夠解決 SMTP 協定和 RFC 822 所遇到的限制與問題，主要問題爲 SMTP 無法傳送非七位元的 ASCII 字元，例如不同語系是用 8 位元編碼、二進位資料的執行檔、圖片等。

MIME 的衍生是爲了解決 RFC 822 無法傳送日益月增的不同型態資料訊息，並且與存的 RFC 822 架構使能相容。

六、現行安全電子郵件使用狀況

（一）組織企業使用安全電子郵件狀況分析

根據中華民國資訊基礎建設產業發展協進會於 2002 年台灣 PKI 趨勢研究報告結果，其中一項針對組織使用 PKI 應用領域，除了「網路應用（Web Application）」和「交互認證 SSL」爲最被廣泛應用於 PKI 之外，所佔之比例爲 76%和 73%；但超過半數（51%）受訪組織利用 PKI 於安全電子郵件用途。由圖 2-6 顯示在 PKI 導入組織企業後安全電子郵件的使用僅次於上述兩項。

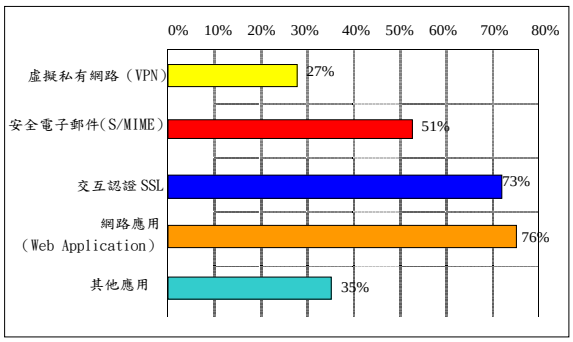


圖 2-6 組織利用 PKI 領域【來源：PKI 趨勢研究報告】

【圖 2-6 組織利用 PKI 領域 來源:PKI 趨勢報告】

此外根據文獻研究調查報告發現 PKI 應用領域依不同產業類別，由圖 2-7 所示由於研究調查之受訪者大部分屬資訊業，因此 PKI 應用均 IT 產業使用者爲最大誤差結果，在虛擬私有網路、安全電子郵件等應用部分尤其明顯。

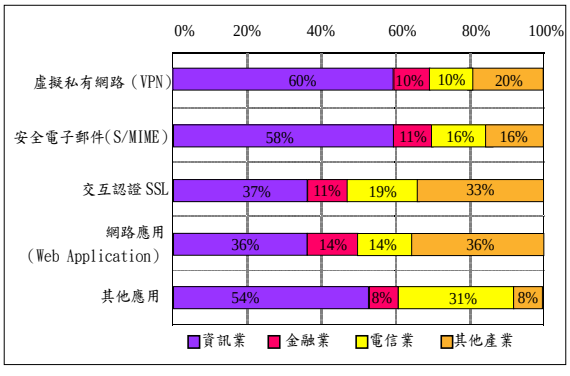


圖 2-7 各產業別所使用 PKI 應用【來源：PKI 趨勢研究報告】

【圖 2-7 產業之 PKI 應用比例圖 PKI 趨勢報告】

（二）PKI 應用於安全電子郵件使用普及度之相關內容

本文依據台灣 PKI 趨勢研究報告[組織應用 PKI 領域相關功能]之數據和內政部自然人憑證中心文獻與學者王旭正、伍麗樵、林宜隆…等人，對資訊安全管理、網路犯罪問題之相關著作、認爲安全電子郵件相關知識與使用技能環境兩個構面，依所示，據以發展設計問卷題目。

叁、研究方法

(一)、研究架構

針對文獻理論所得之資料的分析與歸納，本研究擬對政府機關人員使用安全電子郵件普及度所做的調查項目包括個人背景(年齡、職等學歷電腦使用程度、電腦教育訓練)、工作特性(工作性質、種類、服務單位)及 PKI 應用於安全電子郵件使用(知識、技能、次數)。依據發展概念性研究架構，以了解政府機關人員在整體各層面的 PKI 運用現況和個人背景、工作特性對使用普及度有無影響。

(二)、研究工具

本研究以參考相關文獻後編著之「PKI 導入政府機關於安全電子郵件使用之普及度問卷」作爲抽樣調查工具。

(三)、研究對象

在政府單位 PKI 應用部分，自民國 90 年開始推動至 93 年止， 本次研究係對對政府機關資訊人員作調查，項目包括個人背景（性別、年齡、職等、學歷、電腦使用程度）、工作特性（種類、性質）及公開金鑰基礎建設知識和安全電子郵件傳輸技能。本研究對象以中正國際航空站資訊室及行政院新聞局資訊規畫小組、文建會資訊室之資訊人員爲研究對象，問卷抽樣以 10 個單位各取 15 名，即有 200 個樣本可供研究。

(四)、研究假設

根據文獻探討本研究嘗試探討研究假設如下：

H_1：不同個人背景資的訊人員在使用安全電子郵件之普及度沒有顯著差異。

H_2：不同工作特性的資訊人員在使用安全電子郵件之普及度沒有顯著差異。

H_3：資訊人員的安全電子郵件知識與使用技能與環境沒有顯著相關。

肆、研究結果

（一）樣本蒐集

本研究抽樣調查對象爲行政院以下所屬機關之資訊單位如下：

行政院資訊室各取 6 名；行政院文建會資訊室各取 11 名；內政部資訊中心各取 60 名；經濟部資訊中心各取 10 名；交通部管理資訊中心各取 15 名;內政部警政署資訊室各取 30 名；航空警察局資訊室 5 名；中正國際航空站資料中心各取 12 名； 合計 144 名，有效問卷 120 份。

（二）資料分析

從表 4-2-1 群體描述統計量表中顯示，受測性別之樣本數、平均數、標準差，並以 T 考驗檢測出上述五項因素，發現中性別在 PKI 應用技術因素上有顯著的不同，也就是男性 PKI 應用技術上高於女性。

(三)個人背景與在安全電子郵件使用普及度之關係分析如下：

本研究以個人背景：性別、年齡、學歷電腦使用次數及安全郵件使用次數等五個變數分別以獨立 T 檢定和 ANOVA 方法來檢驗其對安全電子郵件使用普及度之假設。

表 4-2-1 Group Statistics and T-test					
Group Statistics					
	性別	樣本數	平均數	標準差	T 考驗
安全郵件認知	男	67	5.21	1.35	0.86
	女	52	4.99	1.32	
PKI 相關認知	男	68	4.24	1.47	1.71
	女	51	3.75	1.60	
PKI 應用技術	男	68	3.68	1.62	2.10***
	女	51	3.07	1.51	
安全郵件技術	男	67	5.11	1.30	1.15
	女	51	4.83	1.33	
郵件使用環境	男	68	4.23	1.76	1.41
	女	51	3.77	1.72	

1.性別

（1）不同性別的資訊人員在安全電子郵件使用的普及度上差異情形

本研究爲了不同性別的資訊人員在安全電子郵件使用的普及度上差異情形，故建立虛無假設爲：

H1a：不同性別的資訊人員在安全電子郵件的使用普及度上沒有顯著差異。

表 4-3-1 性別對資訊人員在安全電子郵件的普及度檢驗表					
	變異數相等的 Levene 檢定		平均數相等的 T 檢定		
普及度構面	DF	Sig.	T	F	Sig. (2-tailed)
安全郵件認知	.211	.915	1.634	114	.105
PKI 相關認知					
PKI 應用技術					
安全郵件技術					
郵件使用環境					
註：＊＊表示 p＜0.01，＊表示 p＜0.05.。					

經表 4-3-1 顯示，不同性別的資訊人員在安全電子郵件的使用普及度上未達顯著差異標準 ＞.05，亦即，不會因性別不同而有顯著差異，因此接受虛無假設 H5a。

2.年齡

（1）不同年齡的資訊人員在安全電子郵件使用的普及度上差異情形

本研究爲了不同年齡的資訊人員在安全電子郵件使用的普及度上差異情形，故建立虛無假設爲：

H1b：不同年齡的資訊人員在安全電子郵件的使用普及度上沒有顯著差異。

經資料分析後得知，不同年齡的資訊人員在安全電子郵件的使用普及度上未達顯著差異標準，亦即，不會因年齡不同而有顯著差異，因此接受虛無假設 H1b。

3. 職等

（1）不同職等的資訊人員在安全電子郵件使用的普及度上差異情形

本研究爲瞭解不同年齡職等的資訊人員在安全電子郵件使用的普及度上差異情形，故建立虛無假設爲：

H1c：不同職等的資訊人員在安全電子郵件的使用普及度上沒有顯著差異。

經資料分析後得知，不同職等的資訊人員在安全電子郵件的使用普及度上未達顯著差異標準，亦即，不會因職等的不同而有顯著差異，因此接受虛無假設 H1c。

4.學歷

（1）不同學歷的資訊人員在安全電子郵件使用的普及度上差異情形

本研究爲瞭解不同學歷的資訊人員在安全電子郵件使用的普及度上差異情形故建立虛無假設爲：

H1d：不同學歷的資訊人員在安全電子郵件的使用普及度上沒有顯著差異。

由表 4-3-2 顯示：不同學歷的資訊人員在安全電子郵件的使用普及度上未達顯著

表 4-3-2 學歷對資訊人員在安全電子郵件的普及度檢驗表

普及度構面	單因子（ANOVA）變異數分析				
	DF	Mean Square	F	Sig	Scheffee
安全郵件認知	2	3.517	2.397	.096	
PKI 相關認知					
PKI 應用技術					
安全郵件技術					
郵件使用環境					

註：＊＊表示 p<0.01，＊表示 p<0.05.。

差異標準，亦即，不會因學歷的不同而有顯著差異，因此接受虛無假設 H1d 成立。

5. PKI 應用教育訓練

（1）不同 PKI 應用教育訓練的資訊人員在安全電子郵件使用的普及度上差異情形。

本研究爲瞭解不同 PKI 應用教育訓練的資訊人員在安全電子郵件使用的普及度上差異情形，故建立虛無假設爲：

H1e：不同 PKI 應用教育訓練的資訊人員在安全電子郵件的使用普及度上沒有顯著差異。

表 4 -3-5PKI 應用教育訓練對資訊人員在安全電子郵件的普及度之檢驗表

普及度構面	單因子（ANOVA）變異數分析				
	DF	Mean Square	F	Sig	Scheffee
安全郵件認知	2	13.971	10.841	.000	(3)>(1) (2)>(1)
PKI 相關認知					
PKI 應用技術					
安全郵件技術					
郵件使用環境					

註：＊＊表示 p<0.01，＊表示 p<0.05.。

由表 4-3-5 得知，不同 PKI 應用教育訓練的資訊人員在安全電子郵件的使用普及度上有顯著差異，進一步以 Scheffee 檢定後發現結果，不同 PKI 應用教育訓練的資訊人員在安全電子郵件知識和使用普及度上有顯著差異情形，因此拒絕虛無假設 H1e 成立。

6. 安全郵件使用次數

（1）不同安全郵件使用次數的資訊人員在安全電子郵件使用的普及度上差異情形

本研究爲了不同安全郵件使用次數的資訊人員在安全電子郵件使用的普及度上差異情形，故建立虛無假設爲：

H1f：不同安全郵件使用次數的資訊人員在安全電子郵件的使用普及度上沒有顯著差異。

表 4-3-6 安全郵件使用次數對資訊人員在安全電子郵件的普及度之檢驗表

普及度構面	單因子（ANOVA）變異數分析				
	DF	Mean Square	F	Sig	LSD
安全郵件認知	3	4.742	3.349	.022＊＊	(3)>(1) (2)>(4) (3)>(4)
PKI 相關認知					
PKI 應用技術					
安全郵件技術					
郵件使用環境					

註：＊＊表示 p<0.01，＊表示 p<0.05.。

由表 4-3-6 得知，不同安全郵件使用次數的資訊人員在安全電子郵件的使用普及度上有顯著差異，進一步以 LSD 檢定後發現結果，主要差異在於 3-6 次和從未使用之間，每週 3-6 次是遠比從未使用更爲普及，其次差異是 2 次以內和 7-10 次以上之間，每週 2 次是遠比 7-10 次以上更爲普及；由此推斷資訊人員在安全電子郵件的使用普及度上爲中度，因此拒絕虛無假設 H1f 成立。

（四）工作特性與在安全電子郵件使用的普及度之關係

工作特性部分計有：服務單位、工作種類、工作性質等三個因素，試利用 ANOVA

方法來檢驗其對安全電子郵件使用普及度之假設。

1. 服務單位編製

（1）不同服務單位的資訊人員在安全電子郵件使用的普及度上差異情形

本研究為了不同服務單位的資訊人員在安全電子郵件使用的普及度上差異情形，故建立虛無假設為：

H_{2a}：不同服務單位的資訊人員在安全電子郵件的普及度上沒有顯著差異。

經資料分析後得知，不同服務單位的資訊人員在安全電子郵件的使用普及度上沒有顯著差異，亦即，不會因服務單位編製的大小，而有顯著的差異，因此接受虛無假設 **H_{2a}** 成立。

2.工作種類

（1）不同工作種類的資訊人員在安全電子郵件使用的普及度上差異情形

本研究為了不同工作種類的資訊人員在安全電子郵件使用的普及度上差異情形，故建立虛無假設為：

H_{2b}：不同工作種類的資訊人員在安全電子郵件的普及度上沒有顯著差異。

經資料分析後得知，不同工作種類的資訊人員在安全電子郵件的使用普及度上沒有顯著差異，亦即，同為資訊人員不會因從事工作種類的不同，而有顯著的差異，因此接受虛無假設 **H_{2b}**。

3. 業務屬性

（1）不同業務屬性的資訊人員在安全電子郵件使用的普及度上差異情形

本研究為了不同工作種類的資訊人員在安全電子郵件使用的普及度上差異情形故建立虛無假設為：

H_{2c}：不同業務屬性的資訊人員在安全電子郵件的普及度上沒有顯著差異。

經資料分析後得知，不同業務屬性的資訊人員在安全電子郵件的使用普及度上沒有顯著差異，亦即，同為資訊人員不會因從事業務屬性的不同，而有顯著的差異，因此接受虛無假設 **H_{2c}**。

（五）資訊人員在安全電子郵件知識與使用安全電子郵件技能及環境之差異

在此部分，我們最後要探討資訊人員在安全電子郵件知識與使用技能及環境之關係，針對這兩個構面利用相關來探討兩個或兩個以上之連續變相的共變關係，故建立虛無假設為：

H_3：資訊人員的安全電子郵件知識與使用技能與環境沒有顯著相關。

本研究係以 Pearson's r 相關係數檢定來探討安全電子郵件知識與使用技能及環境的相關分析。

表 4-5-1 安全電子郵件知識與使用技能及環境的相關分析。

		安全電子郵件知識	安全電子郵件使用技能與環境
安全電子郵件知識	Pearson Correlation	1	.769**
	Sig. (2-tailed)	.	.004
	N	118	116
安全電子郵件使用技能與環境	Pearson Correlation	.769**	1
	Sig. (2-tailed)	.004	.
	N	116	118

** Correlation is significant at the 0.01 level (2-tailed).

由表 4-5-1 顯示在安全電子郵件知識與安全電子郵件使用技術與環境兩變項之間的相關高達.769(p= .000)，為正相關（正面交

互影響），均達顯著水準，表示安全電子郵件知識與使用技能及環境是具有高度的相關性。因此拒絕虛無假設 **H3**。

伍、結論與建議

（一）研究發現

根據本研究結果發現先將先前研究變項假設驗證結果茲分如下：

資訊人員之個人背景在安全電子郵件使用普及度上分析結果

（1）性別：不同性別的資訊人員在安全電子郵件的使用普及度上沒有顯著的差異。

（2）年齡：不同年齡的資訊人員在安全電子郵件的使用普及度上沒有顯著的差異。

（3）職等：不同職等的資訊人員在安全電子郵件的使用普及度上沒有顯著的差異

（4）學歷：不同學歷的資訊人員在安全電子郵件的使用普及度上沒有顯著的差異

（5）PKI 應用教育訓練：不同 PKI 應用教育訓練的資訊人員在安全電子郵件的使用普及度上有顯著的差異。

（6）安全郵件使用次數：不同安全郵件使用次數的資訊人員在安全電子郵件的普及度上有顯著的差異。

根據 PKI 和安全郵件知識、安全郵件的使用技能與環境中發現，安全郵件使用次數對於安全電子郵件的普及度有顯著差異，由單因子變異數中分析得知，主要差異在 3-6 次和從未使用之間，證明使用安全電子郵件次數愈多者，其組織在推行 PKI 應用安全電子郵件層面越普及。次數分配資料所顯示從未使用之間所佔比例 20.8%，證明 74.2%的資訊人員均有因業務而使用安全電子郵件需求。

柒、結論

一、本研究結論

（一）在 PKI 和安全電子郵件知識方面

個人背景上學歷、PKI 相關教育訓練、安全電子郵件使用次數上有顯著差異，即表示 PKI 相關教育訓練和安全電子郵件使用次數多寡對於 PKI 和安全電子郵件知識有增進的程度。

工作特性上沒有顯著差異，表示對於 PKI 和安全電子郵件知識沒有決定性影響。

（二）在安全電子郵件使用技能與環境方面

個人背景上性別、學歷、PKI 相關教育訓練、安全電子郵件使用次數上有顯著差異，即表示 PKI 相關教育訓練和安全電子郵件使用次數多寡對於 PKI 和安全電子郵件使用技能與環境有進步的程度。

（三）在安全電子郵件使用普及度方面

PKI 應用教育訓練與安全郵件使用次數對於安全郵件使用普及度有增進的影響。

二、建議

（一）提升資訊人員對 PKI 應用領域的建議

茲根據研究結果提出下列三項關於如何提升資訊人員在 PKI 應用領域的知識建議。

一、加強資訊人員對於 PKI 議題的認知

近幾年政府機關部門已經普遍瞭解資訊安全的重要性但是對於 PKI 的認知程度仍有加強的空間，國內 PKI 相關業務服務與應用等狀況亦呈多元化趨勢，例如企業組織採用 SSL 認證、安全電子郵件、VPN 項目外又衍生無線 PKI 等應用，目前企業組織 PKI 應用以 Web Application 最多，未來 PKI 的相關應用會更普遍亦成爲市場的主流。因此在 PKI 導入機關的同時，也建議機關對此議題的重視，讓資訊人員在此領域的各項應用與認知都能更專業，如此才能建構一個優良的資訊環境。

（二）、培養 PKI 相關建置人才

相關人才的培育是極爲重要的，機關導入 PKI 後所花費的經費是龐大且費時，因此經常性的訓練是刻不容緩，從規劃資訊安全教育訓練和 PKI 技術訓練中可培育適當人才，不論機關未來是採行自行管理或是成本考量的委外管理，優秀的 PKI 建置人才可作爲專案管理的溝通橋樑，爲機關節省不必要的花費。

(三)、推廣機關以下各部門對於安全電子郵件的使用

安全電子郵件是具有高度安全性的 PKI 應用項目之一，它可保障訊息傳遞的私密性完整性，並配合憑證中心核發的金鑰憑證，經過數位簽章簽署達到身分的鑑別性與不可否認性。在組織內對於機密性文件和私人信件的保密具有良好的效果。本次研究在探討電子郵件使用普及度，其樣本結果顯示機關內的資訊人員使用已極爲普遍，但日後應逐漸推廣於部門間，使其提升使用率。

陸、參考文獻

一、中文部分

1. 王旭正、高大宇（2003）資訊安全。P.150~P.168 博碩文化圖書

2. 王旭正（2004）密碼學與網路安全--理論實務與應用。 博碩文化圖書

3. 伍麗樵（2002）網路安全與管理。P.2-3~P.2-33 全華科技圖書

4. 林宜隆（2000）網際網路犯罪問題研究。中央警大出版社

巫坤品/曾志光（2001）密碼學與網路安全--原理與實務第二版。碁峰資訊版

5. 廖有祿、李相臣（2003）電腦犯罪:理論與實務。五南圖書

6. 賴溪松、韓亮、張真誠，（1998）近代密碼學及其應用。松崗出版社

7. 洪仲璽、黃宗立（1999/9）網際網路安全與公開金鑰基礎建設。 IICM 第二卷。

8. 胡龍騰、黃瑋瑩、潘中道 合譯（2000）研究方法。學富圖書公司

9. 范紀鍠（2002）安全電子郵件系統公鑰自動取得機制之研究。國立交通大學資訊工程研究所未出版之碩士論文。

10. 林國祥（2001）政府機關網路憑證之研究---以警察機關爲例。P.8~P.15 中央警察大學資訊管理研究所未出版之碩士論文。

李佳隆（1999）安全電子郵件系統設計與實作。P.15~P.19 國立成功大學資訊工程研究所未出版之碩士論文。

11. 武俊麟（2002）公開金鑰基礎建設架構及應用研究---以海巡資訊系統爲例。P.7~P.11； P.20~P.23； P.37~P.38 國防大學國防資訊 研究所未出版之碩士論文。

13. 楊順元（2002）門檻安全電子郵件系統。P.4~P.5 ； P.12~P.17 國立雲林科技大學電子與資訊工程研究所未出版之碩士論文。

14. 2002 年亞洲 PKI 趨勢調查報告。PKI 中華台北推動委員會。

15. 2002 台灣 PKI 趨勢調查結果報告。PKI 中華台北推動委員會

16. *http://moica.nat.gov.tw/html/index.htm*。內政部管理憑證中心

17. *http://grca.nat.gov.tw/cindex.htm*。GRCA

二、西文部份

18. Carlisle Adams & Steve Lloyd, （1999）*Understanding Public-Key Infratructure.*

19. Network Working Group,（1998）*S/MIME Version2Message.Specification*