Hongkong Post e-Cert
香港郵政電子核證

e-Cert 管理軟件

管理智能式身份證之內置數碼證書

用戶指南

版本 v1.4

Hongkong Post
香港郵政

目錄

說明

使用 e-Cert 管理軟件

使用證書庫

用 e-Cert 管理軟件爲電子郵件加密

使用 e-Cert 管理軟件來瀏覽受保護的網站

安全運作的要求

排解疑難

第 1 章

說明

智能卡是什麼，它們有何用途？

本用戶指南內所說明的“智能卡”，是指發給香港市民的“智能身份證”。

隨著智能卡越見普及，代表智能卡的小金屬晶片亦廣爲人所熟悉。這金屬晶片稱爲*接觸片* – 是嵌入在智能卡內的微晶片的存取介面，以及與可由微晶片往來傳送數據〔經由電子化信號〕的連接器接觸。

有兩類不同性質的智能卡：

- **記憶卡**只在晶片儲存數據，像一張小型磁片。
- **處理器卡**除了可儲存數據，還可以執行程式，像一部小型電腦。**智能身份證**就是處理器卡。

智能卡的晶片容量很小，所以可儲存的數據及可執行的應用系統是有限，但仍有相當足夠的容量來發揮它的功能。這是因爲智能卡是具高度的可攜性，而它的晶片可儲存和操作電腦數據，這是很適合需要流動數據的應用系統，例如：

- 儲存金額〔如：儲值電話卡〕
- 泊車繳費〔戶口資訊〕
- 存取控制識別〔透過設有保安系統的出入口〕
- 數碼簽署及解密

最後的那一項用途 – 數碼簽署及解密 – 就是 e-Cert 管理軟件在智能身份證應用電子證書。

由於以上所提及很多的智能卡用途是需一定程度的保護〔閣下當然不希望其他人可讀取儲存在晶片上的資訊〕，智能卡已有內建的保安功能，如：防止未獲授

權修改、以密碼保護卡內資訊、以及晶片只儲存只有它能讀取的數據〔即是不可由晶片傳送的數據〕。

使用智能卡管理“數碼身份”

e-Cert 管理軟件把智能卡當作可把私人密碼匙及電子證書解鎖成*數碼身份*的一套鑰匙，來簽署事項及電子郵件，及閱讀只供閣下讀取的保安信息。隨著*互*聯網冒起，以及數碼通訊滲透，人們在廣泛而鬆散地聯繫的公開網絡頻密通訊，沒有任何保證來證明信息是不受干擾〔和可能被修改〕，或假冒信息是不以真實姓名發出。

這樣便提出了兩個問題：如何確定給閣下的信息沒有未經許何而被讀取，以及如何確定收到的信息是真正由寄件者發出？幸運地，Whitfield Diffie 和 Martin Hellman 在 1976 年發表一份創新的文章“加密法的新方向”，啓動了一系列可正確處理這些問題的技術發展：公開密碼匙基礎建設。

公開密碼匙基礎建設(PKI)說明

公開密碼匙基礎建設(PKI)的核心是一套特別的加密技術。把信息加密 – 從遠古已存在，是轉變信息的方法；人們不熟悉某些秘密資訊，通常稱爲*鑰匙*，信息變得難於理解。其中一個問題是加密和解密信息也需要相同的鑰匙，這使加密技術變得繁複。這樣寄件者便需要秘密地把加密信息的鑰匙傳送給收件者來解密信息；需要另尋方法來保密鑰匙傳送過程，引證了傳統加密方式的缺點。

Diffie 和 Hellman 在 1976 年建議的改革中，是有*兩條*獨有而*互*相關連的鑰匙 – 一條是用來加密，另一條是用來解密。因爲兩條鑰匙具備特殊的數理關聯，加密匙能隨意地對外發佈，而鑰匙擁有者就必須謹慎地保管解密匙。這個數理關聯確保鑰匙是不可能由另一條鑰匙計算出來。因此，加密匙就稱爲公開密碼匙，而解密匙就稱爲私人密碼匙。要發出信息給收件者，便向收件者索取公開密碼匙〔可隨意地對外發佈的密碼匙〕，再加密信息。然後收件者便使用私人密碼匙來復修原來的信息。

當這個被稱爲*公開密碼匙加密法*的新技術 – 說明了秘密傳送解密匙給信息收件者的需要，這引發一個新問題：如何確定用來加密信息的公開密碼匙，當真是屬於意屬的收件者？假如可與收件者直接面對面交收公開密碼匙，這就不會有問題。但假如不可面見收件者，而又要由其他地方取得公開密碼匙，便有需要確定公開密碼匙沒有被未獲授權使用，或被其他可容許非意屬收件者解密信息的公開密碼匙取代。

證書

數碼證書是一個可解決辨認公開密碼匙擁有者問題的方法。

獨立地建立數碼證書的概念，可爲公用密碼匙一定程度的可信性。這是透過利用一個獨立的第三者機關：*核證機關* 來達到。核證機關被委託實施一套可確實辨認個人身份的要求〔如：提供護照〕。當個人身份被清楚地辨認，核證機關便以數碼方式，簽發個人的*識別名字*及公開密碼匙 – 這些簽發的資料組成了一張數碼證書。

香港郵政是第一個在香港被認可的核證機關，遵照電子交易條例〔第 553 條〕，簽發被認可的數碼證書〔“電子證書”〕。

證書列明公開密碼匙擁有者符合核證機關的身份證明要求。假如閣下信任該核證機關，就可引申到閣下同樣信任由該核證機關所簽發的證書。這樣閣下就可獲得一個受高度信任的公開密碼匙 – 假如它是由閣下所信任的核證機關簽發。

如何信任一個核證機關？假如閣下對核證機關的身份辨認程序有信心，可以聲明閣下信任該核證機關的公開密碼匙，以及信任其發出的所有證書。

數碼身份證明是由一*配對密碼匙*〔一條公開密碼匙和它的私人密碼匙的結合〕和證書〔由核證機關簽發的公開密碼匙和鑰匙擁有者的識別名字〕組成。e-Cert 管理軟件使用智能卡的內建保安功能，保護私人密碼匙，和執行卡內的程式去簽發及解密信息。這樣，私人密碼匙由卡內的私人密碼保護，及永不離開智能卡。

數碼簽署

數碼身份證明的其中一個重要功能是可產生數碼簽署。使用簽名去批核文件是多個世紀商業傳統，代表文件已被接納，而簽名是個人的特徵和難於假冒。數碼簽署是建基於公開密碼匙加密法，同樣假設個人擁有一個其他人不可存取的獨立私人密碼匙。

根據電子交易條例〔第 553 條〕，數碼簽署是由香港郵政電子證書支援，與真實簽署具有同樣法律地位。

在訊息通常會在被數碼簽署前， 先被縮小成一個固定長的數據形式，稱之爲*亂碼訊息*。 各個亂碼訊息會以特別形式儲存訊息 – 訊息只要相差一個字母，所產生的亂碼訊息都會不同。由於系統需要很長時間才可數碼簽署一個訊息〔尤其是長訊息〕，把訊息轉變爲載有特定訊息的亂碼訊息，然後才加以數碼簽署會更爲快捷。 已簽署的訊息包含原本訊息、已簽署的亂碼訊息、及爲作者驗證簽署的電子證書。

收件者使用作者的證書 來驗證公開密碼匙，並還原由作者編制的亂碼訊息。另一方面，收件者亦會爲原文製作另一套的亂碼，如果兩套亂碼相符，收件者就可以肯定原文爲作者原出，而並無被篡改。

已作數碼簽署的亂碼訊息實爲確保電子訊息在傳送途中並無被篡改的上策，然而，公開密碼匙加密方法卻非常依賴公開密碼匙的可信性。如果收件者使用一套僞造的數碼證書 〔雖然可行性極低〕 來還原亂碼訊息及驗證訊息，亦會有機會誤以爲由僞造者發出的訊息是可信的。現今解決這問題的最佳辦法就是對核證機關基本信任。

深入公開密碼匙基礎建設(PKI)

你並不需要在使用 e-Cert 管理軟件前閱讀本節， 但本節會深入地探討前章所提及的公開密碼匙基礎，其背後的概念，及用戶要留意的*警告*。

加密演算法

其中一種最流行的公開密碼匙加密演算法叫 RSA，取名自它的創造者〔Rivest、Shamin 和 Adleman〕。由於使用 RSA 演算法來加密及解密冗長的訊息時，可能需要很長時間，一種更新、更快的演算法因此應運而生。

其中一種比 RSA 快很多的方法，是使用 RSA，再加上*相對稱方法*來爲訊息加密〔加密及解密都使用同一組密碼匙〕。 比正常訊息短很多的*對稱密碼匙*，會和收件者的公開密碼匙同步加密 到訊息中， 而整個由已加密訊息、RSA 及已加密的對稱密碼匙數據包，會直接送到收件人手上。

當收件人收到加密包，對稱密碼匙會由私人密碼匙解密，然後對稱密碼匙會被用作訊息解密。這方法既有對稱演算法的速度，同時，對稱密碼匙又可以因爲每個不同訊息的 RSA 加密而更改。然而， 這加密法要小心地選擇對稱演算法， 如果這演算法可以被輕易還原，不需要把對稱匙解密就可以還原加密訊息。 對稱演算法 優點，一定要配合數據保密的要求。

簽署演算法

正如前文所述， 亂碼訊息是用作改善加密冗長訊息的最流行方法之一。由於亂碼訊息在加密後會比原訊息短，而且暫時並無方法單憑加密訊息還原爲原訊息，故此亦稱爲*單向加密法*。單向加密法其中一個基本屬性爲由結果反向計算時有*計算性困難*，無可能把煮熟的食物還原爲原材料一般；另一基本屬性是爲兩組不同訊息計算出相同亂碼訊息有*計算性困難*。

當簽署冗長的訊息時， 先產生了比原訊息短很多的亂碼訊息〔單向加密法的結果〕， 然後才應用數碼簽署， 時間就會縮短很多。被簽署的亂碼訊息會連同原訊息一同發給收件人，要驗證訊息，收件人要先用發件人的公開密碼匙復原亂碼訊息，再用同一組匙爲原訊息進行單向加密，檢查結果是否和收到的亂碼訊息一樣。假使兩者相同， 收件人就知到訊息並未被篡改。

最普遍的單向加密法爲： SHA-1 〔Secure Hash 演算法版本 1〕，SHA-256 (Secure Hash 演算法 256 位元) 及 MD5 〔Message Digest 版本 5〕。 e-Cert 管理軟件完全支援上述三種單向加密法。

密碼匙長度

個別演算法的*密碼匙長度* 〔形成密碼匙的二元編碼數量〕會影響該種演算法的*保護能力*〔成功地防禦侵襲〕，這是由於較短的密碼匙可以被*徹底地搜尋*—簡單的一個電腦程式就可以嘗試所有可行的組合，輕易地就可以試到正確的密碼匙。所以最重要的基本原則就是越長的密碼匙，就會越保險的，要謹記會有超過一種的方法來反向還原加密演算法.

例如 RSA 演算法，使用了大額質數的積〔若爲 310 位數〕作爲計算基數。 較大的 RSA 基數會較爲安全， 因爲即使運用現今科技，仍然在回復運算基數時會有*不可能計算*的情況出現。要作此計算，你需要不斷地找出用以乘出基數的大額質數，而這類因數分解會被認作爲*計算性困難*。香港郵政電子證書現正使用 1024/2048-位元的 RSA 運算基數。

‘計算性困難’ 及 ‘不可能計算’

當在保安上使用公開密碼匙基礎建設時，必需要留意現今日新月異的電腦科技界中，並無絕對的數學運算。 PKI 的強處在於所牽涉的數學運算令破解方法*極度*困難〔有如不可能〕。 從 PKI 誕生至今，每年 RSA 數據保安公司都會斥資舉辦比賽，邀請世界頂級的數學家來參加破解 RSA 演算法 的比賽，但至今仍未有人可以成功。 當然，從*不可能程度及困難性*來看， PKI 有可能永遠都是無法破解的加密演算法。

e-Cert 管理軟件如何使用 PKI

e-Cert 管理軟件是由兩組獨特的元件組合而成： 智能身份證中的電子證書應用程式、及電腦上，專爲管理香港郵政電子證書及智能身份證中的私人密碼匙的界面軟件[1] 。電子證書應用程式負責管理你智能卡上的私人密碼匙，及提供解密及簽署的演算法。 e-Cert 管理軟件軟件結合操作系統 ，以提供系統層面的加密服務。當其他應用系統，如：電子郵件客戶端需要使用加密服務〔如簽署電子郵件〕時，證書操作管理員會自動處理和子郵件客戶端溝通，並使用你的私人密碼匙來簽署，免你操心。

e-Cert 管理軟件從而提供端對端簽署及解密服務，亦同時把你的私人密碼匙保存在防篡改、可上鎖的智能卡中。

[1] 根據由 SecureNet 有限公司 開發的 TrustedNet Connect 產品

第 2 章

使用 e-Cert 管理軟件

概覽

e-Cert 管理軟件的設計是爲了與視窗結合，提供視窗操作系統基本以外的服務。e-Cert 管理軟件，作爲一套*副系統*，使你能更容易地操控你的智能卡，及卡內的資料，而並非一般的獨立操作系統。 每當一個視窗應用系統，如電郵客戶端或瀏覽器，需要使用智能卡上的數碼身分， e-Cert 管理軟件就會自動運作，成爲應用系統及智能卡資料中間的連接橋樑。

使用 e-Cert 管理軟件

e-Cert 管理軟件是一套檢視你的智能卡上的電子證書、並可複製電子證書至 Internet Explorer 憑證存放區，及更改密碼的管理工具。同時，e-Cert 管理軟件亦提供了進階模式，讓你能更有效地管理智能卡，閱讀器及所有電子證書及其相對密碼匙。

啓動 e-Cert 管理軟件的步驟如下：

- 雙擊系統匣中的 e-Cert 管理軟件圖示，

e-Cert 管理軟件

檢視你的智能卡電子證書

你可以透過 e-Cert 管理軟件檢視證書，而得到更多有關在智能卡上的電子證書資料， 如：發行的核證機關名稱 ，及有效日期。

檢視電子證書的步驟如下：

- 點擊在 e-Cert 管理軟中的**檢視智能卡電子證書** 按鈕

檢視電子證書

證書視窗有三個標籤：

- **一般**標籤介紹證書的用途、證書持有人、發行人、及有效期。
- **詳細資料** 標籤提供證書中所有欄位的完整資料，包括所使用的簽署演算法、公開密碼匙、及系統識別名稱 〔**主題**〕。
- **憑證路徑** 追踪由此證書到核證機關源頭的路徑， 顯示當中所有有關驗證此證書的*中介核證機關*。

你亦可以點擊**一般**標籤中的**安裝證書**，把證書安裝到微軟證書庫中，步驟和點擊**複製證書至 IE 憑證存放區**相同。

你的 e-Cert 密碼

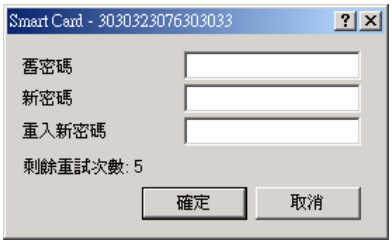
你的智能卡上的資料是由一組解鎖號碼，或稱密碼，所保護。 每次當你需要使用如配對密碼匙或電子證書等之機密資料時，你必需要輸入解鎖密碼，或稱爲*登入*智能卡。

登入一張智能卡

每次當你輸入錯誤的密碼時，系統會自動扣減**剩餘重試次數**。當這號碼變爲零時，你的智能卡會被*封鎖*。你將不可使用你的卡，直至你接觸香港郵政，並請代爲解封。

提示： 要立即鎖上所有的配對密碼匙，你可由閱讀器中取走你的智能卡。就算把卡重新插入閱讀器中，所有的密碼匙都依然鎖上。你亦可右擊系統匣中的圖示，並選擇在捷徑功能單中的**鎖上密碼**。

你可更改用以登入智能卡的密碼，只要右擊電子證書的圖示 ，並在捷徑功能單中選取**更改智能卡電子證書密碼**，然後輸入你現在的密碼，再輸入新密碼兩次以作確認。



更改智能卡密碼

把你的 e-Cert 複製到 Internet Explorer 中

在使用證書簽署電子郵件，或在瀏器中驗證你的身分前， 你的證書必須在 微軟 Internet Explorer 證書庫中註冊。

注： 有關使用微軟證書庫的詳細資料，請參考第 3 章。

透過註冊你的電子證書至 IE 證書庫，步驟如下：

- 在 e-Cert 管理軟件中，點擊 **複製證書至 IE 憑證存放區** 按鈕

你的證書就會自動複製到 IE 證書庫中，並立即可供使用。

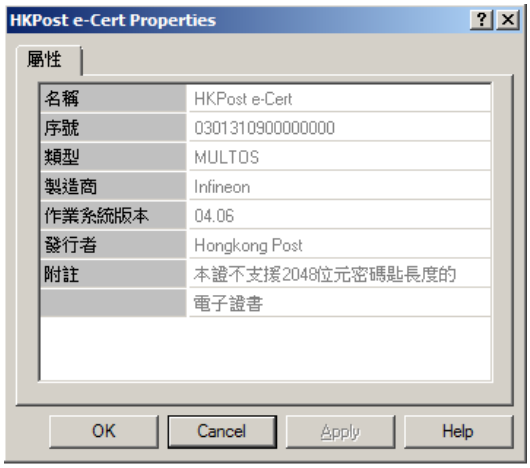
檢查智能身份證的版本以支援 2048 位元的電子證書

你可使用 e-Cert 管理軟件來檢視智能卡版本能否支援 2048 位元密碼匙長度的電子證書。

檢視智能卡版本的步驟如下：

1. 由主要 樹狀表窗格， 點選**智能卡** 文件夾，

2. 右擊智能卡圖示 並點選**屬性**。



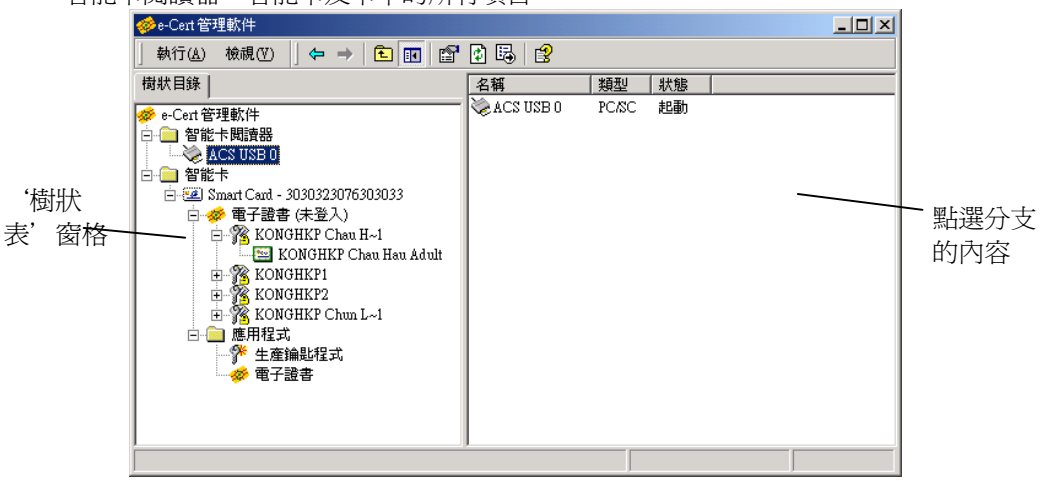
智能卡 屬性

若「作業系統版本」顯示「04.06」，表示此智能身份證不支援 2048 位元 RSA 密碼匙長度的電子證書。但若「作業系統版本」顯示「04.20」或以上版本(如下)，表示此智能身份證支援 2048 位元 RSA 密碼匙長度的電子證書，而附註也會提示你是否須攜同本證親身到指定郵政局辦理電子證書申請。

智能卡 屬性

進階模式

在進階模式中，你可透過 e-Cert 管理軟件提供的‘樹狀檢視’結構來檢視所有智能卡閱讀器、智能卡及卡中的所有項目。



e-Cert 管理軟件

在 e-Cert 管理軟件樹狀分枝下， 所有連到電腦的智能卡閱讀器，及閱讀器中的智能卡都會被顯示出來。e-Cert 管理軟件會自動偵測閱讀器中，智能卡的插入及移走，並更新檢視窗。

微軟管理主控台

要使用 e-Cert 管理軟件的進階模式，你需要微軟管理主控台。 一般來說，這管理主控台都會內置於視窗中。 如果你發現視窗中並無此程式，你亦可在微軟視窗更新的網址中：
http://windowsupdate.microsoft.com
免費下載。

如果你不需要使用 e-Cert 管理軟件的進階模式，你就不需要安裝微軟管理主控台 (Microsoft Management Console)。

起始及停止伺服器

當系統匣中顯示了 e-Cert 管理軟件的圖示，表示 e-Cert 管理軟件伺服器正在背景執行，並等待操作系統的加密要求。

停止伺服器的步驟如下：

- 右擊 系統匣中的圖示，並從捷徑功能單中點擊**關閉**。你亦可右擊管理員中的 e-Cert 管理軟件 圖示，並從捷徑功能單中點選**關閉程式**。

如果操作系統在伺服器被停止後要求 e-Cert 管理軟件進行加密〔如：簽署電子郵件〕，操作系統會自動起始伺服器， 然後處理加密。

起始服務的步驟如下：

- 右擊管理員中的 e-Cert 管理軟件圖示 ，並從捷徑功能單中點選 **啓動程式**。

智能卡閱讀器

由於 e-Cert 管理軟件會顯示所有連到你電腦中的智能卡閱讀器，你必須安裝最少一個智能卡閱讀器 ，以確保 e-Cert 管理軟件正常運作。

檢視 或更改智能卡閱讀器屬性的步驟如下：

1. 點擊 e-Cert 管理軟件中，樹狀表窗格中的 **智能卡閱讀器** 文件夾，
2. 右擊智能卡閱讀器 圖示，並從捷徑功能單中點選 **屬性**，

智能卡閱讀器屬性

智能卡閱讀器屬性如下：

- **名稱：** 智能卡閱讀器顯示的名稱。
- **種類：** 是智能卡閱讀器與電腦通訊所用的*界面*，只包括 **PC / SC**。
- **PCSC 名稱：** 閱讀器自動在視窗註冊爲 PC/SC 兼容閱讀器的名稱。

設置新的智能卡閱讀器

當 PC/SC 兼容的智能卡閱讀器連接到你的電腦時，e-Cert 管理軟件在不必另加配置的情況下，會自動識別閱讀器。

智能卡

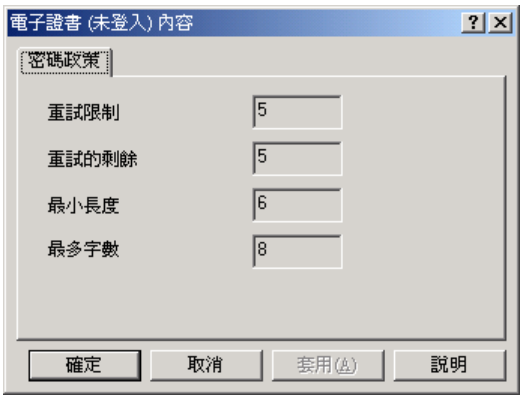
e-Cert 管理軟件靠辨認序號來識別智能卡〔即你的智能身份證〕。當把智能卡插入閱讀器時，e-Cert 管理軟件會自動重新整理，並顯示智能卡的內容。

智能卡內的資料共分爲三大類：

- **電子證書：** 電子證書 是由*香港郵政核證機關簽發*的*公開密碼匙*
- **配對密碼匙：** 是用來簽署及加密資訊的*公開及私人密碼匙*。
- **應用程式:**智能卡上用以處理資訊的應用程式。配合智能身份證及 e-Cert 管理軟件，就能達到最低限度的**電子證書程式**應用。

密碼政策

你的智能卡存取保密，只可以在電子證書*密碼政策*下，以密碼加以保護。你可以右擊 電子證書 圖示並從捷徑功能單中點選 **屬性**，來檢視政策。



電子證書密碼政策

密碼的政策選項如下：

- **重試次數限制：** 在*封鎖*智能卡前，可容許的錯誤密碼輸入次數。
- **重試剩餘次數：**若是在配對密碼匙封鎖前，這設定爲重試密碼輸入的次數，若是在配對密碼匙封鎖後，這設定則爲解封重試次數。
- **最少字數：** 密碼字組的最少字數。
- **最多字數：** 密碼字組的最多字數。

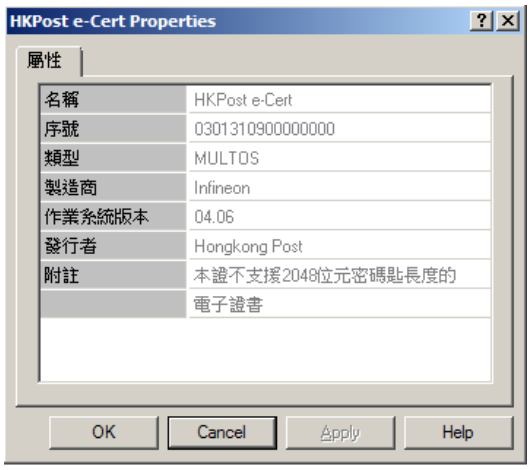
警告： 當你在嘗試自行解封智能卡時，錯入密碼的次數超過**重試次數限制**，你的智能卡會被封鎖而不能再使用，繼而，配對密碼匙 亦會示爲**封鎖**，你將不能**登入**到你的智能卡中。 在此情況下， **重試剩餘次數**爲智能卡可被解封的次數。要解封智能卡，你必須要聯絡香港郵政。

智能卡屬性

你可使用 e-Cert 管理軟件來檢視智能卡中內置的個別屬性。

檢視智能卡屬性的步驟如下：

3. 由主要 樹狀表窗格， 點選**智能卡** 文件夾，
4. 右擊智能卡圖示 並點選**屬性**。



智能卡 屬性

智能卡的屬性如下：

- **名稱** 爲智能卡的通用名稱。
- **序號** 爲智能卡的序列號碼。
- **類型** 爲智能卡的種類。
- **製造商** 爲智能卡的製造商名稱 。
- **作業系業版本** 爲智能卡用以執行應用程式的操作系統版本。
- **發行商** 爲發行智能卡的機構名稱。
- **附註** 爲智能卡支援 2048 位元密碼匙長度的附加資料。

更改智能卡的名稱

你可以透過 e-Cert 管理軟件來爲你的智能卡命名，使它更易於被辨認。管理員的樹狀檢視中會顯示智能卡的名稱。

已命名的智能卡

如果智能卡尚未命名，e-Cert 管理軟件會用智能卡序號作爲該卡的名稱。

要命名智能卡的步驟如下：

1. 右擊 e-Cert 管理軟件中的智能卡，並從捷徑功能單中點選 **重新命名**.
2. 輸入智能卡的新名稱 。智能卡名稱應爲該卡擁有者所易於辨認。

智能卡名稱會被儲於卡中， 就算在其他電腦上使用亦會保持不變。

清除智能卡的所有電子證書內容

你可以輕易地清除所有智能卡上的密碼匙及電子證書， 亦可分開清除。

清除所有智能卡內容的步驟如下：

1. 右擊 e-Cert 管理軟件中的智能卡，並從捷徑功能單中點選 **清除所有電子證書**。
2. 你被要求輸入你的電子證書密碼。 輸入密碼後就能完成清除智能卡的過程。

電子證書

電子證書是根據 CA 政策，因應你的證書發行要求，由核證機關發行，用以清晰地辨別你的身分。香港郵政所採用，以發行電子證書的政策及程序詳列於香港郵政電子核證作業準則〔CPS〕。 CPS 可於香港郵政 CA 網頁中瀏覽及下載，網址爲 http://www.hongkongpost.gov.hk

將一張電子證書〔e-Cert〕載入到你的智能卡中，就能配合其相關配對密碼匙的使用。

Bob Smith 的電子證書

把電子證書載入到你的智能卡中

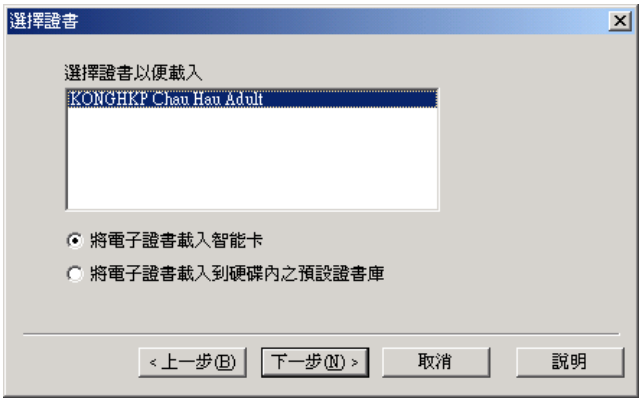
你可以透過 e-Cert 管理軟件，把證書載入到你的智能卡中。

把證書載入到智能卡中的步驟如下：

1. 右擊 e-Cert 管理軟件的 電子證書 圖示，並從捷徑功能單中點選 **載入電子證書**。
2. 基本上， 電子證書是以檔案形式儲存， 你需要用電子證書密碼來解鎖。電子證書密碼會透過密碼信封獨立地派發給你。點擊**瀏覽**，找出證書檔案的位置，如果需要，輸入密碼，然後點擊 **下一步**。

3. 點選要載入的證書， 再揀選證書位置。你可以把電子證書載入到智能卡或離線證書庫。離線證書庫詳情可參閱第 3 章“使用證書庫”。 選

好證書及載入位置後， 點擊 **下一步**。



4. 如果證書已被載入到智能卡中，相對應的密碼匙就會成爲*現用密碼匙*，並會用於將來的所有數碼簽署及解密功能上。

當載入電子證書後，e-Cert 管理軟件會檢查證書是否在卡中已有想對應的公開密碼匙，而智能卡上的姓名亦符合證書上的名稱。 如果證書未有相符的公開密碼匙，或智能卡上的姓名並不符合，證書便不能被載入智卡中，e-Cert 管理軟件亦會報告有關錯誤訊息。

提示： 配對密碼匙〔及相關的證書〕亦可由檔案載入到你的智能卡中。如果你已有被核實的配對密碼匙，這會是一個非常方便的方法。以上的步驟亦可應用到從檔案載入配對密碼匙，及其相關證書。 配對密碼匙會被載入到最先找到的可用位置， 或系統要求你 所選擇的覆蓋位置。卡上的證書 則會被移到離線證書庫。

把電子證書滙出到檔案

若你的朋友希望發送加密資料給你， 或檢核你的數碼簽署， 他們會需要你的數碼證書。 藉著滙出證書，你就可以把電子證書製成一個可自由地電郵或發送給朋友的檔案 。

滙出證書的步驟如下：

1. 右擊顯示在 e-Cert 管理軟件中，你希望滙出的證書，並從捷徑功能單中點選 **輸出證書**。
2. 輸入檔案名稱 並把證書儲存到檔案中。

電子證書 會滙出成 X.509 DER 加密的檔案， 並可兼容微軟證書庫。

刪除電子證書

如果你的證書已經過期， 或希望以新的證書取代智能卡中的舊證書， 你需要由智能卡中刪除證書。

刪除證書的步驟如下：

1. 在樹狀表窗格， 右擊你想刪除的證書，並從捷徑功能單中點選 **刪除**，
2. 點擊 **是** 以確定操作，

3. 輸入你的電子證書密碼 以確認你有權從智能卡中刪除證書。

除非證書已經過期， 否則你應該在永久刪除證書前，先滙出到檔案中作備份。

證書 屬性

除了檢視證書， 你亦可以在 e-Cert 管理軟件中快速地檢查你的證書屬性。

檢視證書屬性的步驟如下：

1. 在樹狀表窗格中， 點選證書，即可檢視。
2. 右擊證書，並從捷徑功能單中點選 **屬性**。

證書 屬性

電子證書屬性如下：

- **名稱：** 證書持有人的通用名稱 〔系統識別名稱的相反〕。
- **鑰匙庫：** 儲存證書的智能卡名稱 。
- **類型：** 智能卡的物件種類。
- **序號：** 證書 的個別單一序號。
- **用途：**相對應的配對密碼匙可以如何使用。
- **過期日：**證書到期日。
- **證書位置：** 顯示證書的儲存位置，在智能卡或在離線證書庫內。
- **鑰匙位置：** 顯示鑰匙的儲存位置，應在智能卡內。

配對密碼匙

數碼身分的關鍵在於你的配對密碼匙，如第 1 章所言，配對密碼匙中包括負責用來爲你收到的訊息簽署及解密的你*私人密碼匙*， 和負責替你的訊息收件人驗證你所送出的訊息中的簽署 ，及替訊息加密的*公開密碼匙*。

在使用你的 e-Cert 配對密碼匙前，你需要先登入你的智能身份證。 你可以右擊在 e-Cert 管理軟件，樹狀檢視中的 電子證書 圖示，然後選擇**登入**或**登出**來開始及停止使用你的智能卡。

配對密碼匙 屬性

檢視配對密碼匙屬性的步驟如下：

- 右擊 e-Cert 管理軟件內，樹狀表窗格中的配對密碼匙，並從捷徑功能單中點選 **屬性**。

配對密碼匙 屬性

配對密碼匙屬性如下：

- **名稱** 是配對密碼匙產生時制定的名稱。
- **鑰匙庫** 儲存配對密碼匙中私人密碼匙的智能卡名稱。如果庫中是空的，密碼匙仍能儲於智能卡中，但智能卡並未被命名 〔詳情請參閱第 17 頁的*更改智能卡的名稱*〕。
- **類型** 是智能卡的類別。

刪除配對密碼匙

如果某個配對密碼匙已不再被你使用、或不再安全， 你可以從智能卡中刪除 該配對密碼匙，以騰出多餘空間並容納新的配對密碼匙。

刪除配對密碼匙的步驟如下：

1. 右擊樹狀表窗格中，你希望刪除的配對密碼匙，並從捷徑功能單中點選 **刪除鑰匙**，
2. 點擊 **確定**確認操作，
3. 要清除配對密碼匙，你必須輸入電子證書密碼。

更改智能卡上電子證書及現用配對密碼匙

智能卡上的電子證書及現用配對密碼匙是用來處理所有數碼簽署及文件解碼，並會同時載入一張相關的證書。如果更改現用配對密碼匙， 你必須同時由離線證書庫載入其相關證書。

指定另一個配對密碼匙爲現用配對密碼匙的步驟如下：

1. 右擊樹狀表窗格中，你 想指定爲現用的配對密碼匙，並從捷徑功能單中. 點擊 **從離線證書庫載入電子證書**
2. 輸入你的電子密碼，由離線證書庫中滙入相關的證書。

應用程式

所有配合 e-Cert 管理軟件的智能卡都儲有電子證書應用程式。

e-Cert 管理軟件中的應用程式文件夾顯示智能卡上有哪些程式。所有應用程式都可獨立操作，不需更改或設置 e-Cert 管理軟件。

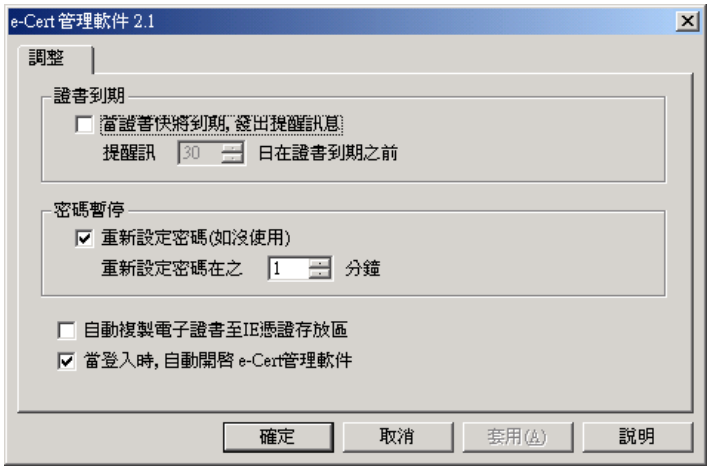
e-Cert 管理軟件設定

正如 e-Cert 管理軟件內置的設定般， 你可以指定下列選項：

- 證書到期警告。
- 密碼有效時限。
- 自動複製電子證書至 IE 憑證存放區。
- 自動啓動 e-Cert 管理軟件。

設置 e-Cert 管理軟件選項的步驟如下：

- 點選 “行動”功能單中的“設置”



證書到期日

每張證書 都有一段*有效時期*， 過了這時期證書就會過期失效，而你 亦需要重新向核證機關 申請一張新的證書。

e-Cert 管理軟件可以在證書快將到期時提醒你，以便你聯絡核證機關 ，在現有證書過期前取得新的一張。要啓動到期警告，請勾劃**證書到期**的匣及揀選你所要求的警告日數。

密碼有效時限

已開鎖的密碼匙會這時限內開放，時限過後，密碼匙會自動鎖上，你需要重新輸入電子證書密碼，才可再使用該配對密碼匙。

要立即鎖上所有配對密碼匙，你可由閱讀器中抽走智能卡，這樣做後，就算重新把智能卡插入閱讀器，卡中的配對密碼匙依然會被鎖上。你亦可以右擊系統匣中的圖示 ，並從捷徑功能單中點選**密碼上鎖**，鎖上所有配對密碼匙。

自動化選項

其他選項包括：

- **自動複製電子證書：** e-Cert 管理軟件會在你 把智能卡 插入閱讀器時， 檢查卡中的電子證書是否已複製到微軟 IE 證書庫，否則，e-Cert 管理軟件便立即進行自動複製。
- **自動啓動：** 當這選項被點選後，系統會在每次你登入電腦時自動啓動 e-Cert 管理軟件。

注： 如果你設定了證書 過期警告 及 自動複製電子證書 的選項後，你每次插入智能卡時，系統都會要求你輸入密碼。

第 3 章

使用證書庫

概覽

使用 e-Cert 管理軟件來維護及加強數碼保安時，管理電子證書是非常重要的一環。 在加密電子郵件、或驗證數碼簽署的可信性時， 你必需知道如何取得、區分及檢視電子證書。

微軟證書庫是爲方便不同用戶透過不同應用系統管理電子證書而設的特別軟件。如：無論任何時候，當電子郵件 程式需要驗證一個數碼簽署時， 程式可以由證書庫查取核證機關的公開密碼匙複件，但密碼匙必需已經於微軟證書庫註冊。

同樣地，你要簽署電子郵件時，電子郵件程式亦要把你的證書附加到內文中以便收件者驗證你的簽署。在這情況下，電子郵件 程式亦會由證書庫中查取你的證書。

離線證書庫

e-Cert 管理軟件可以在你的智能卡中儲存最多四組鑰匙及一張電子證書，而智能卡中的證書會相對應現用的密碼鑰匙。對應非活躍鑰匙的證書會儲存到離線證書庫位於在 e-Cert 管理軟件被安裝的目錄下。

注： 在 Windows Vista/ 7 上，離線證書庫都被移至 Windows 環境變數 ALLUSERPROFILE 所設定的使用者目錄下（在大多數情況下是 C:\ProgramData）。

如果把智能卡帶到另一台電腦中使用，除非你把離線證書庫都一併轉存到新電腦中，否則你將不能再使用在離線證書庫中的電子證書 。 要轉移你的離線證書庫，

1. 把離線證書庫目錄資料夾下的證書複製到新機器的離線證書庫，
2. 重新啓動 e-Cert 管理軟件（詳情可參考 15 頁中起始及停止伺服器）。

當你插入智能卡時， e-Cert 管理軟件會檢查離線證書庫 ，及偵測相對於你智能卡上的密碼鑰匙的電子證書，使所有程式都能應用到證書及密碼匙。

注： 要把你的電子證書附加到電子郵件，並營造一個安全的網上連接，你要先確認證書已存在於智能卡上或在微軟證書庫中註冊。離線證書庫 只儲存相對於智能卡中，並未設爲現用密碼匙的電子證書。

此章餘下部份會討論如何使用微軟 Internet Explorer 證書庫。

IE 證書庫

微軟證書庫以四種不同形式來安排電子證書：

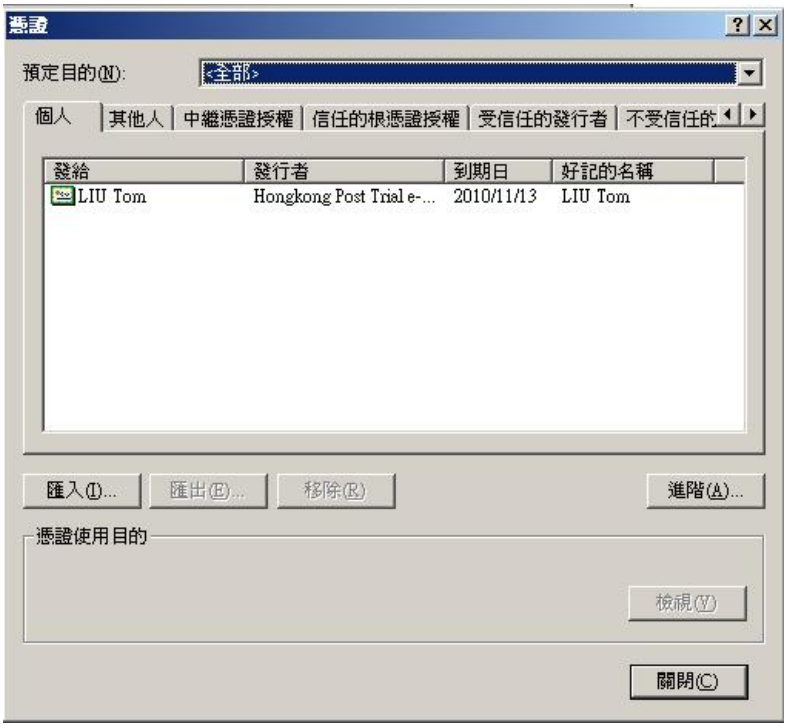
- **個人：** 可以證實你身分的電子證書， 亦包括已被核證機關簽署的公開密碼匙。
- **其他人：** 可證實其他人身分的電子證書， 亦可用以爲訊息加密。
- **中繼憑證授權：** 屬於架構內的核證機關的電子證書， 亦受可信及的源核證機關簽署。
- **信任的根目錄憑證授權：** 由你所信任的核證機關所自我簽署的電子證書 。

開啓證書庫

證書庫是在控制台中，網際網路選項的其中一部份。

開啓證書庫的步驟如下：

1. 在開始功能單中， 點選 設定中的控制台，
2. 雙擊 **網際網路選項**，
3. 點擊 **內容**，
4. 點擊 **憑證** 按鈕。



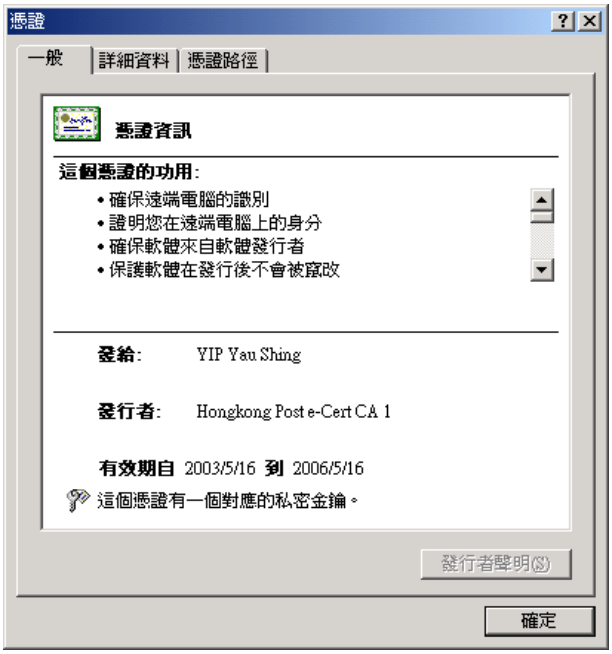
微軟證書庫

檢視電子證書

所有證書庫內的電子證書均按照不同類別而區分。

檢視證書的步驟如下：

- 在類別中找出證書，然後雙擊該證書。



個人證書

證書資料

證書檢視中，你可看到：

- 證書的一般概覽及用途目的。
- 證書內的欄位及屬性的詳細總覽。
- 證書路徑。

一般

一般檢視提供以下資料：

- 證書用途目的， 如：電子郵件保護， 交換鑰匙， 及遙距認證。
- 證書持有人名稱 。
- 發行證書之核證機關名稱。
- 證書有效期限。
- 是否有該證書的私人密碼匙， 及可否使用該證書來簽署電子郵件 及解密。

詳細資料

詳細資料檢視提供證書中的所有欄位資料及其屬性 ，包括：

- **版本：** 證書種類的版本。
- **序號：** 核證機關所應用的證書序列號。
- **簽章演算法**：核證機關 用以簽署證書的演算法，如： `md5RSA` ，即用 RSA 簽署，並應用到 MD5 digest 的證書。

- **發行者：** 簽署證書的核證機關 。
- **有效起始：** 有效時限開始日。
- **有效到：** 有效時限到期日。
- **主旨：** 可單一地辨識證書持有人的系統識別名稱，系統識別比通用名稱更能準確地識別用戶，核證機關亦因此能夠識別兩位同名同姓的用戶。
- **公開金鑰：** 證書持有人的公開密碼匙。
- **拇指紋演算法：** 每張證書都載有一個公開密碼匙的‘指模’，以確定證書並未經篡改。指摸演算法就是用來產生指模的方法。
- **拇指紋：** 獨特編排方式的密碼，用以驗證公開密碼匙有否被更改。
- **名稱：** 簡短又有意義的證書顯示名稱 。

憑證路徑

憑證路徑物件是你所信任的核證機關及證書之間的信任基線，藉著追蹤證書和可信任的核證機關之間的路徑，提供證書的可信任程度。

如果證書並未能追蹤至一個可信任的核證機關，你應該謹慎處理所有以這證書處理的訊息。

滙入及滙出證書檔案

證書檔案有三大格式：

- **DER encoded Binary X.509**. 這是由 X.509 標準定義的格式， 並使用直接加密法則(Direct Encoding Rules)加密。
- **Base-64 encoded X.509**. 這是由 X.509 標準定義的格式， 並使用 Base-64 〔亦稱爲 MIME〕加密。
- **PKCS #7 電子證書**. 這是由公開密碼匙加密標準第七號(Public Key Cryptography Standard number 7)定義的格式。

證書庫可以辨識所有檔案格式，你亦可以任何上述格式滙出 及滙入電子證書 。

滙入證書檔案

你可以兩種方法滙入證書：

- 雙擊證書檔案 ，並在證書檢視視窗中點擊 **安裝證書**。
- 啓動證書庫 並點擊 **滙入**。

當你 選擇滙入證書時，證書庫會啓動證書滙入精靈，以三個步驟助你滙入證書：

1. 首先介紹滙入證書的程序， 點擊 **下一步**，
2. 然後定義你想把證書放入的證書庫〔個人， 其他人仕， 中間核證機關或可信任根源核證機關〕 。證書滙入精靈可以嘗試測試該證書應屬於那個證書庫，你亦可以指定某個證書庫。
3. 最後，會列出你的選項總滙。 檢視無誤後，點擊 **完成** 即可滙入證書。

注： 你只需直接滙入其他人及核證機關的電子證書到微軟證書庫，而你自己的電子證書已在註冊時滙入到證書庫中。詳情可參考第 12 頁。

滙入香港郵政核證機關根源證書及簽發人證書

要令你的網頁瀏覽器信任所有由香港郵政簽發的電子證書，你必須先滙入香港郵政核證機關根源證書及簽發人證書。 所有的香港郵政核證機關根源證書及簽發人證書都可在 http://www.hongkongpost.gov.hk. 網站中下載。

你只需要在電腦中滙入一次根源證書及簽發人證書，但如果你正在使用 Mozilla Thunderbird 或 Mozilla Firefox，則請獨立地在這些軟件中註冊證書一次。

有關滙入證書的詳細資料，請參閱安裝手冊。

滙出證書檔案

你有兩種方法把證書發給其他人，使他們發已加密電子郵件給你：

1. 簽署並發出電子郵件給他們，你的證書便會附在電郵中，
2. 由證書庫中，把你的證書抽取爲檔案，然後把檔案發給他們。

你用兩種不同方法從證書庫滙出證書：

- 雙擊證書 ，並在**詳細資料**標籤中點擊 **複製到檔案** ，
- 在證書庫中點選證書，並點擊 **滙出**。

當你選擇了滙出證書後，證書庫會啓動證書滙出精靈， 以三個步驟完成指令：

1. 首先，介紹滙出步驟， 點擊 **下一步**。
2. 如果你有這證書的私人密碼匙〔即你是證書持有人〕， 請你 連同私人密碼匙一同滙出。 要保障私人密碼匙的安全， 在智能卡中，受保護的私人密碼匙將*不能*被滙出。 點擊 **下一步**。
3. 請點選檔案格式。 接受這證書的另一方會滙入這證書到證書庫，你可以 使用任何可選擇的格式，否則，請先與對方確認可辨識的格式。點擊 **下一步**。
4. 請輸入檔案名稱，點擊 **下一步**。
5. 最後，系統會顯示操作詳情，並請你確認，點擊 **完成**即可滙出證書。

第 4 章

用 e-Cert 管理軟件爲電子郵件加密

概覽

e-Cert 管理軟件其中一個最重要的工作，是保護及認證敏感內容的電子郵件。e-Cert 管理軟件會結合到你的電子郵件應用系統，爲你寄出的電子郵件自動提供加密及進行數碼簽署。

本章會說明如何設置及配合下列各電子郵件應用系統，使用 e-Cert 管理軟件中的簽署及加密功能：

- 微軟 Outlook Express / Windows Mail / Windows Live Mail
- Mozilla Thunderbird

提示： 關於設置你的電子郵件應用系統來使用電子證書數碼身分的詳細資料，請參閱可以安裝手冊

以 Outlook Express / Windows Mail / Windows Live Mail 爲電子郵件加密

簽署電子郵件

爲訊息作數碼簽署的步驟如下：

1. 在檔案 功能單中， 點選 **新郵件**，
2. 撰寫你的內容，
3. 從工具功能單中， 點選 **數碼簽署**。 證書圖示會在你的電郵地址旁出現，
4. 準備可發送郵件後，你可點擊 **寄送**。 e-Cert 管理軟件會要求你輸入智能卡的解鎖密碼， 以便使用私人密碼匙來簽署訊息。

5. 訊息即被簽署及寄送。

爲電子郵件加密

Outlook Express/ Windows Mail / Windows Live Mail 會要求所有用以加密訊息的電子證書都存到你的通訊錄中。你可以用以下其中一個方法來新增載有證書的通訊連絡人：

- 自動 在你收到已簽署的電子郵件時自動新增。
- 手動 當你收到檔案格式，或以附件形式收到的證書時適用。

儲存證書

如果你收到附加在電子郵件中的證書，你可以自動把證書儲存到你的通訊錄，步驟如下：

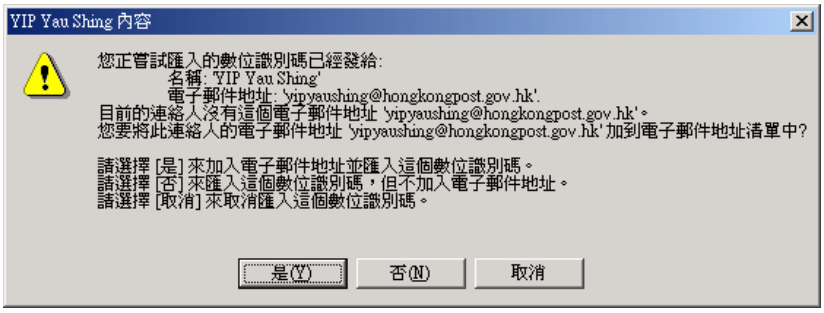
1. 雙擊開啓郵件，
2. 右擊在電子郵件標題中，**寄件人**欄的寄件人地址，並從捷徑功能單中點擊 **新增至通訊錄**，
3. 證書會被到入到通訊錄中，寄件者的紀錄中。

如果收到檔案格式的證書，你需要新增通訊錄紀錄及把證書附加到紀錄中。

把證書連結到通訊錄的步驟如下：

1. 在工具功能單中，點選**通訊錄**，以開啓訊錄，
2. 如果證書持有人並未加入到通訊錄，可在檔案中點選**新連絡人**，
3. 點擊 **數位識別碼**，
4. 在**選擇電子郵件地址**清單， 點選證書持有人電郵地址，
5. 點擊 **滙入**，
6. 找出證書檔案位置並點擊**開啓**。

證書已被加入通訊錄，如果你所選擇的證書持有人電郵地址和證書上所紀錄的不相符， 你會見到以下訊息：



新增證書

如果見到此錯誤，切勿繼續滙入證書。如果你點擊**否**並繼續滙入證書， 你將不能使用該證書來爲電子郵件加密。 請你聯絡證書持有人，以獲得正確的證書。

爲電子郵件加密

要用你已存於通訊錄中的收件人證書爲電子郵件加密，步驟如下：

1. 撰寫你的電子郵件，
2. 要準備發送時， 點選工具功能單中的**加密**。收件人電郵地址旁就會出現一個小鎖圖示，顯示該電子郵件在送出前已被加密。

3. 點擊 **寄出**，發送已加密郵件。 由於並不需要使用你的數碼身分來爲電子郵件加密，你並不需要使用智能卡。

爲電子郵件解密

當你的郵箱收到已加密的電子郵件， 系統會顯示一個有藍色小鎖的圖示 。

讀取已加密郵件的步驟如下：

1. 雙擊電子郵件項目，
2. 你會被要求輸入私人密碼匙的解鎖密碼，然後爲郵件解密。

當你輸入正確的解鎖密碼後，電子郵件會被解密及顯示。

以 Mozilla Thunderbird 爲電子郵件加密

Mozilla Thunderbird 版本 3

簽署電子郵件

數碼簽署的步驟如下：

1. 開啓 Mozilla Thunderbird 並點擊工具列上的**寫信**按鈕，以編寫新郵件，
2. 撰寫你的內容，
3. 點擊工具列上的**安全性**，並選取**對此郵件加上數碼簽章**，
4. 點擊**寄送**，寄出郵件。e-Cert 管理軟件需要使用你的數碼身分來爲訊息加密，所以系統會要求你輸入智能卡密碼。

5. 輸入你的密碼，簽署訊息。

驗證數碼簽署

當你收到一個由非法簽署加密的電子郵件時，Mozilla Thunderbird 會顯示一個說明證書未被信任的圖示。請勿信任任何非法簽署加密的訊息。

有關個別電子郵件加密保安的詳細資料，請於**檢視**功能單中選擇**訊息保安資料**。

爲電子郵件加密

用 Mozilla Thunderbird， 你只可以發送簽署或已加密郵件給已把證書發送給你的收件人，你亦不可以由檔案形式滙入證書。

當你收到一個已簽署的訊息〔有簽署圖示顯示〕，證書會自動被滙入至保安管理員中。你可點選證書管理員，檢視所有已註冊的電子證書，步驟如下：

1. 在**工具**功能單中，點選**選項**，
2. 點選在瀏覽列中的**進階** ，
3. 點選**憑證**，然後點擊**檢視憑證**。

Mozilla Thunderbird 會列出所有已註冊的電子證書， 點擊**人員**可觀看你可以發加密訊息的人仕〔和驗證他們的數碼簽署〕。

要發送已加密的電子郵件給已發證書給你的收件者，步驟如下：

1. 點擊**寫信**按鈕來編寫電子郵件.
2. 輸入或從通訊錄中找出收件人地址，
3. 點擊工具列上的**安全性**，然後點選**加密此郵件**，
4. 點擊**寄送**爲訊息加密及把郵件寄出。

解密電子郵件

當你點擊收件匣中一個已加密的電子郵件時， e-Cert 管理軟件自動要求你輸入配對密碼匙的解鎖密碼來爲訊息解密。

在輸入正確密碼後，私人密碼匙會立即爲訊息解密，完成後系統會顯示圖示，標明訊息爲已加密、簽署、或兩者都有。 已解密的訊息並非會被永遠解密－稍後當你再檢視該已加密訊息時，系統會再要求你輸入密碼 〔如果已超過密碼有效期〕來解密及檢視訊息。

第 5 章

使用 E-CERT 管理軟件來瀏覽受保護的網站

概覽

就像你可以用私人密碼匙來簽署加密訊息，把你的證書寄給其他人來證明你的數碼身分， 你亦可以證書及私人密碼匙來向網站驗證你的數碼身分。

網站是透過一種叫 Transport Layer Security，或 TLS， 亦有人稱爲 Secure Sockets Layer 〔SSL〕的特別 *通訊協定* 來驗證你的數碼身分。 通訊協定是電腦之間互相溝通的特定語言， TLS 協定可爲你的電腦及網站間建立已加密的溝通渠道，從而使你轉送到網站的所有〔可能機密〕 資料，在轉送到互聯網時均已加密。

TLS 如何運作?

Transport Layer Security 通常會被稱爲*握手協定*，因爲在 TLS 連接開始時，網站伺服器〔簡稱‘伺服器’〕 及要連接伺服器的電腦(簡稱‘客戶端’)會互相確認身分，並協議如何保護要建立的連接。

通常會有兩種 TLS， 每種都有各自的保安要求：

- **伺服器端認證**即伺服器會把自己的證書發給客戶端，以確認自己的身分。客戶端會驗證證書是否由已認知的核證機關簽發及是否合法等， 然後用伺服器的公開密碼匙爲所有要傳送的資料加密。香港郵政亦有簽發伺服器電子證書〔即電子證書〔伺服器〕〕來切合伺服器認證要求。
- **客戶端認證**更進一步地驗證客戶的身分。當伺服器已通過伺服器端認證，客戶端會發送自己的證書 〔如電子證書〕給伺服器。伺服器會立即驗證客戶端證書，及檢查合法性，然後使用客戶端的公開密碼匙來建立安全溝通渠道。

TLS 連接

一個 Transport Layer Security 連接握手〔客戶端和伺服器協議加密連接方法的部份〕的步驟如下：

1. 客戶端要求使用伺服器上的一種保密的資源〔如：網頁〕 ，
2. 伺服器把自己的證書發給客戶端。
3. 客戶端使用可信任的根源核證機關，驗證伺服器的證書，如果證書不能被驗證，連接就會就此中斷。
4. 如果證書通過驗證並合法，客戶端和伺服器會磋商一個應用 TLS 連接的加密層面。

5. 客戶端產生一個一次性、獨特的*連接匙*〔一對相稱的鑰匙，可以爲所有伺服器和客戶端間的傳輸加密〕， 用伺服器的公開密碼匙爲連接匙加密，並把已加密的數據包發到伺服器中。
6. 如果伺服器中的資料是極爲機密，又需要客戶端的驗證，伺服器會要求客戶端提供電子證書。客戶需要簽署一份只爲此次握手而設的加密數據包，並連同自己的證書和連接匙發送到伺服器端。
7. 伺服器會爲數據包解密，並用連接匙和客戶端溝通。如果使用客戶端驗證，伺服器會在和客戶端溝通前，先檢查已簽署的數據，並驗證客戶端證書及其合法性。

爲何需要連接匙?

如果伺服器及客戶端在交換電子證書，爲何不直接使用公開密碼匙加密來爲連接加密，反而要再產生一對相稱的連接匙？ 這是由於公開密碼匙加密法比較耗時，使用更快的對稱演算法來爲溝通渠道加密，然後使用公開密匙加密法來傳送連接匙會比較化算。

一般的 TLS 加密演算法包括： RC2， RC4， IDEA， DES 及 3DES。 所有演算法的演算速度都遠勝公開密碼匙加密法。

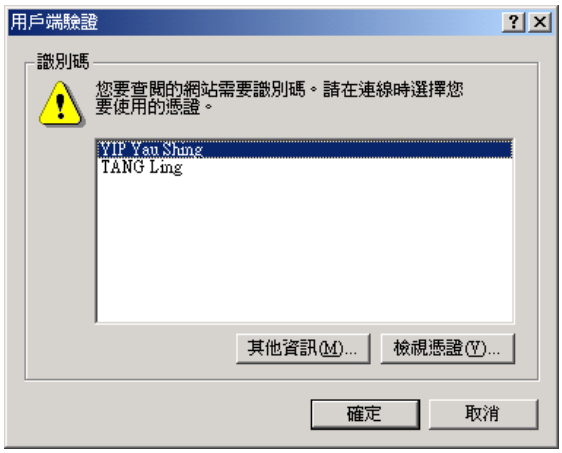
e-Cert 管理軟件和 TLS

透過伺服器上的 TLS， 只需要用你的證書庫中已被承認的核證機關來驗證伺服器的證書。 當證書通過驗證後，你可以用伺服器的公開密碼匙來防衛轉送時的連接匙(session key)。 透過伺服器上的 TLS，你不再需要爲任何訊息作加密，或轉送自己的證書， 所以你亦不需要使用 e-Cert 管理軟件。

如果使用客戶端 TLS， 你需要在 TSL 做握手協議(handshake)時簽署一個特定的數據，並輸送你的證書。 當伺服器向你要求證書，e-Cert 管理軟件會自動要求你選擇證書，和輸入電子證書密碼，以便使用私人密碼匙簽署數據。

要用客戶端 TLS 驗證你的身分，步驟如下：

1. 請確認你已把證書複製至 IE 證書庫中。詳情請參閱第 12 頁的把你的 e-Cert 複製到 Internet Explorer 中，
2. 在瀏覽器上輸入網站的網址，
3. 當有證書要求，瀏覽器會要求你從證書庫中選擇證書：



4. 點選相關的證書並點擊 **確認**，
5. e-Cert 管理軟件會要求你輸入電子證書密碼來簽署送往伺服器的數據：

6. 如果認證通過，而你亦有權使用該項資源，你就可以使用該網站。

第 6 章

安全運作的要求

e-Cert 管理軟件是專爲高度保障用戶數據而設計，但這些保安措施仍會有機會被不法之徒濫用。 *警惕性*在使用 e-Cert 管理軟件來維持安全性是最重要的一環，用戶必需要謹慎處理所有可能是不法入侵的可疑舉動。

本章會介紹如何偵測計對 e-Cert 管理軟件保安的侵襲，並向用戶提供指引，使 e-Cert 管理軟件任何時間都會發揮最強功能來保護用戶的機密資料。

留意你的智能卡

智能卡中存有珍貴的資料，你可使用這些資料簽署及爲資料解密，你必需要謹慎保管你的智能卡，並經常肯定只有你能控制這卡。 只要有任何一個入侵者可以同時使用你的智能卡和密碼，他就可以隨時使用你的私人密碼匙，取用你的私人資料或冒認你。

當你在使用 e-Cert 管理軟件中途離開電腦，請確認已抽走你的智能卡—尤其是當電腦有機會在你離開時被其他人使用。 你應該從閱讀器中移走智能卡，或把卡鎖上，以保證要取用資料時，必須入密碼。

你應該只在使用 e-Cert 管理軟件才把自己的智能卡插入閱讀器。 如果 e-Cert 管理軟件沒有顯示某個指定的閱讀器， 該閱讀器則非由 e-Cert 管理軟件所操控而不應被使用。把智能卡插入不可信任或非經驗證的閱讀器，有機會導致卡上的資料被人盜取或毀壞。同時， e-Cert 管理軟件必需要按照指定程序安裝，詳細資料請參閱 *e-Cert 管理軟件安裝手冊*，並確定所安裝的軟件爲被認可及正確的版本。 否則，e-Cert 管理軟件將會輕易地受到病毒入侵，被他人篡改，或甚至被不法份子冒認你的身分來簽署或爲數據解碼。

使用 e-Cert 管理軟件前， 你要檢查在電腦和智能卡之間並無其他不明的中介設備。

當你遺失或被人偷了智能卡，你必需要立即向你的智能卡發行機構或核證機關報失，以便取消卡上所有電子證書 的效用。

你只可以容許 e-Cert 管理軟件和有需要溝通的應用系統建立信任介面，否則不知名的程式便會乘虛而入，刪除你的密碼匙或在你不知情下取代你的密碼匙。除非你非常肯定正確版本的 e-Cert 管理軟件已被正確地安裝。

留意你的解鎖密碼

用來爲你的私人密碼匙解鎖的密碼是智能卡的最基本的保護機制，你應該選擇一個無人知道的私人密碼。密碼絕對不可以是某個節日的日期或電話號碼，儘可能由隨意抽取的字元組成，小心選擇密碼，使其他人不能輕易地猜中。

在某些情況下，你的發卡機構需要爲你的智能卡進行個人化，使卡只在你所知道的密碼下操作。你必需要小心保管此密碼，絕不能被其他人知道。當你收到智能卡後，要馬上把密碼更改爲更難猜測，但你又可以容易記憶的新密碼。

你必需要把密碼 **保密。** 所有的密碼均需被小心保護！ 請把密碼和智能卡分開保存〔**不要**把你的密碼寫在智能卡上〕。輸入密碼時，請小心留意週遭有沒有其他正留意並猜測你的輸入模式，從而猜出你的密碼。請只在 e-Cert 管理軟件要求時才輸入你的密碼。

如果你發覺某個程式在輸入密碼後，e-Cert 管理軟件並無執行操作或依舊向你求取密碼，該個程式有可能已在盜取你的密碼，請立即使用 e-Cert 管理軟件更改你的密碼。當某個程式透過 e-Cert 管理軟件要求你輸入密碼時，對話應該爲的 e-Cert 管理軟件密碼對話匣，在輸入後，你的要求會被立即執行，否則，你的密碼已有機會被人盜用，你必須立即使用 e-Cert 管理軟件更改你的密碼。

每次當 e-Cert 管理軟件透過視窗要求你輸入密碼時，同時亦會顯示密碼重試剩餘次數，這個顯示的重要性是讓用戶知到錯誤輸入密碼的次數。每次當你輸入正確密碼後，這個數值就會重設到最大值，而錯誤的輸入就會扣減這數值。如果 這數值和你的輸入次數不相符，即代表有人〔或程式〕正不斷嘗試猜測你的密碼。你應確定智能卡並無他人使用，你的電腦中亦無其他不明的程式執行。

隨著時間增長， 密碼的‘老化’使它越來越容易被其他人猜中。 所有密碼 **一定要**定時更改 – 最少每三個月一次。 另外， 當你懷疑有人嘗試猜測你的密碼時〔即所顯示的重試次數和實際次數不符合〕，一定要立即更改你的密碼。

小心你的敏感數據

e-Cert 管理軟件一定要安裝在你的電腦上，以確保其他人不能干擾你所使用的產品，但沒有軟件可以避免被人干擾。e-Cert 管理軟件的安全措施,要求你可以相信任何有權開啓並使用你的電腦，或更改 e-Cert 管理軟件甚至高度保安的操作系統檔案的人。

在 e-Cert 管理軟件的監控下，管理員會全面承擔你的資料的保安。要保護機密數據，所有使用 e-Cert 管理軟件的電腦及程式必需都可以向你的數據提供統一的保安層面。你的電腦亦要可以保護曾被 e-Cert 管理軟件解密的檔案，令其他人不能在未經你同意前取用那些檔案，同樣地，已加密的數據及其他機密數據，亦要受到同樣的保護。

e-Cert 管理軟件的數碼簽署功能可以向其他人驗證你的身分。 你的電腦環境必需可以控制所有對外的溝通都是在你所知道的情況下發生。Transport Layer Security 〔亦稱爲 Secure Sockets Layer 或 SSL〕 使用數碼簽署來驗證連接匙，其他人亦因此肯定只有你可以進行溝通。你的電腦必需要保護機密資料， 並防止有未經許可的訊息外傳。

你必需只可使用 e-Cert 管理軟件和你所信任的應用程式，以防止不被信任的應用程式在你不知情的情況下簽署或解密資料。同時，你亦要留意密碼匙的保管，當你遺失了曾用以加密的密碼匙後，曾用該密碼匙加密，卻又未被解碼的檔案是永不能被回復。遺失智能卡即等如遺失密碼匙，解鎖密碼失效亦會使密碼匙失效，等同遺失密碼匙。

棄置你的智能卡

在棄置智能卡前， 你應該刪除卡上的所有鑰匙〔請參考第 21 頁的*刪除配對密碼匙*〕。這樣做可以確保其他人撿拾到你的棄卡時，不能讀取到卡上的資料或嘗試破解卡內的保護機制，尤其在日後，科技更發達時，入侵者會更容易破解到保密機制，刪除鑰匙的重要性將會更高。

如果你並未刪除所有鑰匙， 你應聯絡香港郵政，刪除智能卡上的電子證書應用程式。

第 7 章

排解疑難

本章會說明有機會在使用 e-Cert 管理軟件時出現的錯誤、可能的原因、及補救方法。

智能卡閱讀器錯誤

閱讀器作業超時

起因： 當你的智能卡閱讀器不再回應由 e-Cert 管理軟件發出的訊息時，就會出現閱讀器作業超時 錯誤。 原因有可能是智能卡閱讀器的技術或硬件出錯，又或者視窗內部錯誤。

補救方法： 重新啓動視窗。 如果問題持續發生， 請聯絡你的智能卡閱讀器供應商。

閱讀器埠的錯誤

起因： 閱讀器埠的錯誤是由於智能卡閱讀器所連接的埠並未正確地配置。有可能是由於兩個智能卡閱讀器 驅動程式同時嘗試使用同一個埠。

補救方法： 移除所有已安裝的智能卡閱讀器驅動程式， 再重新安裝你現正使用智能卡閱讀器驅動程式。

閱讀器讀取錯誤

起因： 閱讀器讀取錯誤是由於所讀取的資料已損壞或不完整。 有可能是因爲智能卡閱讀器的技術問題，或電腦與閱讀器之間的連接問題。

補救方法： 重新啓動視窗並檢查電腦與閱讀器之間的連接。如果問題依然存在， 請聯絡智能卡閱讀器供應商。

閱讀器寫入錯誤

起因： 閱讀器寫入錯誤 和**閱讀器讀取錯誤** 的原因很類似，通常是在閱讀器未能寫入資料時發生。 起因可能是閱讀器的技術問題， 電腦問題，或電腦與閱讀器之間的連接問題。

補救方法： 重新啓動視窗並檢查電腦與閱讀器之間的連接。如果問題依然存在， 請聯絡智能卡閱讀器供應商。

閱讀器 失效

起因： 未明的閱讀器問題，會引致閱讀器失效。起因可能是當 e-Cert 管理軟件遇到和智能卡閱讀器有關的問題，但未能識別出是哪種問題 。

補救方法： 一般起因都是閱讀器的硬件問題。可重新啓動視窗，如果問題依然存在， 請聯絡智能卡閱讀器供應商。

智能卡保安錯誤

密碼不正確

起因： 用作開啓智能卡的密碼不正確。此錯誤會減低你的*重試次數*，若果密碼重試次數減低至零，智能咭將被立即封鎖。

補救方法： 在重開你的智能卡前，請先確認你的密碼。

密碼被封鎖

起因： 當智能卡密碼被錯誤地輸入超過指定次數〔*重試次數*〕，密碼 會被立即封鎖。這極有可能是你的密碼被人強行入侵。

補救方法： 要爲你的智能卡解封，你必需聯絡香港郵政。

密碼長度問題

起因： 你所提供的密碼字數太長或比最低字數少。當你改變智能卡密碼時，系統都會檢查密碼長度。

補救方法： 請確定密碼字數符合字數規格要求。

密碼不夠牢固

起因： 你的密碼太容易被人猜中。不牢固的密碼包括連續字元〔如：‘123456’〕或重覆字元〔如：‘222222’〕。

補救方法： 修改你的密碼 ，使密碼更強抵禦黑客的猜測程序。

智能卡應用系統錯誤

未能支援的指令

起因： e-Cert 管理軟件系統正嘗試執行一個智能卡未能支援的功能。

補救方法： 請確保智能卡閱讀器正插著正確的智能卡。 如果智能卡是正確的， 該智能卡的有限功能未能執行該指令要求。

未經許可的指令

起因： 卡上的安全權限不批准你所要求的指令執行。

補救方法： 你不能挑戰智能卡上的安全權限。

智能卡並不存在

起因： 智能卡並不存在於閱讀器中、或閱讀器中的智能卡在操作過程中被移走。

補救方法： 把智能卡插入或重新插入閱讀器中。

智能卡已滿

起因： 卡上沒有足夠的空間來通過你所要求的功能操作。

補救方法： 刪除智能卡中沒用或不需要的內容〔如：不再需要的電子證書〕便可產生更多空間。

鑰匙庫錯誤

項目已存在

起因： 你正嘗試載入證書或配對密碼匙到智能卡時， 系統發現卡上有另一組相同標籤的項目存在。

補救方法： 取消操作〔你 的卡上已有該項目〕，或刪除已存在的項目後，再重新載入證書或配對密碼匙。

項目並不存在

起因： 你正嘗試存取不存在於智能卡上的證書或配對密碼匙。

補救方法： 檢查是否插入正確的智能卡，或移除並再插入智能卡後，再重試操作。

項目被鎖上

起因： 你正嘗試存取被密碼鎖上的證書或配對密碼匙 。

補救方法： 要存取項目， 你必需鍵入解鎖密碼。

配對密碼不存在

起因： 你正嘗試把證書載入到智能卡上，但其相關之配對密碼匙 並不存在。

補救方法： 在載入證書前，先載入其相關的配對密碼匙 。

檔案格式不正確

起因： 你正嘗試把檔案，如電子證書或加密用的配對密碼匙載入到智能卡中，但系統卻未能識別檔案格式。該檔案可能已經損毀、曾被人試圖篡改。

補救方法： 請檢查你正嘗試載入的檔案，並重新嘗試該操作。如果問題依然存在，請聯絡香港郵政。