



# e-Cert 管理軟件

管理智能身份證之內置電子證書

安裝指南

版本 v1.7



版權所有©2003 香港郵政

---

# 目錄

## 說明

關於 e-Cert 管理軟件.....	3
特性.....	3
系統要求.....	4
支援智能卡.....	4
支援應用系統.....	4
安裝概述.....	4
支援.....	5
準備進行保密安裝.....	5
安裝環境的完整性.....	5

## 安裝 e-Cert 管理軟件

接駁智能卡閱讀器.....	6
安裝 e-Cert 管理軟件.....	6
登記你的電子證書.....	7
在微軟視窗註冊香港郵政核證機關根源證書及簽發人證書.....	7
在 Mozilla Firefox 上註冊香港郵政核證機關根源證書及簽發人證書.....	8
設置 Mozilla Firefox 以使用 e-Cert 管理軟件.....	9

## 設置你的電子郵件應用程式

設置微軟 Outlook Express / Windows Mail / Windows Live Mail.....	10
設置 Mozilla Thunderbird.....	12
在 MozillaThunderbird 上註冊香港郵政核證機關根源證書及簽發人證書..	13

## 排解疑難

e-Cert 管理軟件的錯誤訊息.....	15
微軟管理控制台錯誤.....	15

# 第 1 章

## 說明

### 關於 e-Cert 管理軟件

e-Cert 管理軟件是專門管理智能卡上的電子證書。e-Cert 管理軟件保護私人密碼匙，它是在智能卡中最重要數碼身分元件，提供解密和數碼簽署功能，以及與微軟整合，為電子郵件客戶系統、網頁瀏覽器和其他應用系統，提供加密的保安服務。

當應用系統，如：電子郵件程式，需要使用加密的保安服務（例如：簽署電子郵件），e-Cert 管理軟件就會確認及處理指示，使用智能卡執行所要求的簽署和/或解密工作。

如此一來，e-Cert 管理軟件可清晰地把商業操作保密；同時亦把智能卡中最重要數碼身分元件 – 私人密碼匙，於設有防修改及可被鎖上特性的智能卡中加以保密。



註： 如需要更多關於 e-Cert 管理軟件，可參考 e-Cert 管理軟件用戶指南。

### 特性

在智能卡中的 e-Cert 管理軟件和電子證書應用系統提供以下特性。

加密的功能：

- 1024/2048 位元在卡 RSA 數碼簽署。
- 1024/2048 位元在卡 RSA 鑰匙產生。
- 軟件內置 MD5, SHA-1 及 SHA-256 的加密干擾訊息。
- 為傳輸和加密鑰匙作大量的隨機數字產生。

鑰匙管理：

- 為已有密碼保護的智能卡保障存取。
- 支援獨立的簽署鑰匙和加密鑰匙。
- PKCS #12 鑰匙庫的負載支援。
- 自動偵測智能卡和閱讀器種類。
- 在微軟證書庫登記證書。

介面標準：

- PKCS #11 及微軟 CryptoAPI 支援。
- X.509 及 PKCS #12 證書服務支援。

智能卡和閱讀器。

- 支援多種類智能卡。
- PC/SC 智能卡閱讀器支援。

## 系統要求

- Intel Pentium 166 處理器
- 32mb 隨機記憶體
- 10mb 可使用硬碟空間
- 可用作安裝閱讀器的串列、PCMCIA 或 USB 埠
- PC/SC 智能卡閱讀器
- 智能卡閱讀器 PC/SC 驅動程式

## 支援智能卡

- 智能身份證是由香港特別行政區入境事務處簽發。

## 支援應用系統

操作系統：

- 微軟視窗 XP
- 微軟視窗 Vista
- 微軟視窗 7
- 微軟視窗 8

網頁瀏覽器：

- 適用於視窗 XP / Vista / 7 的微軟 Internet Explorer 8
- 適用於 Windows Vista / 7 的微軟 Internet Explorer 9
- 適用於 Windows 8 的微軟 Internet Explorer 10 (傳統型)
- 適用於視窗 XP / Vista / 7 的 Mozilla Firefox 3.6 或以上

電子郵件應用系統：

- 適用於視窗 XP 的微軟 Outlook Express 6.0
- 適用於視窗 Vista 的微軟 Windows Mail 6.0
- 適用於視窗 7 的微軟 Windows Live Mail 2009
- 適用於 Windows 8 的微軟 Windows Live Mail 2012
- 適用於視窗 XP / Vista / 7 / 8 的 Mozilla Thunderbird 3.0 或以上

## 安裝概述

建立 e-Cert 管理軟件的步驟如下：

1. 接駁智能卡閱讀器至個人電腦。
2. 安裝閱讀器驅動程式。
3. 安裝 e-Cert 管理軟件。
4. 設置電子郵件應用系統去使用智能卡。

## 支援

e-Cert 管理軟件是專為用戶自行管理智能身份證上的電子證書而設計，並沒有任何需要管理員知識的特殊功能。如果你在使用時遇到疑難，並需要支援，可參閱本指南尾部 *排解疑難* 章節；亦可向香港郵政核證機關查詢。

電子郵件：[enquiry@hongkongpost.gov.hk](mailto:enquiry@hongkongpost.gov.hk)

服務熱線：2921 6633

## 準備進行保密安裝

為確保 e-Cert 管理軟件在安裝時並無受潛在性安全威脅，或可能存在的保安漏洞而影響保密性，請用戶於安裝時跟隨數個相關指引。

### 安裝環境的完整性

為確保安裝環境不會破壞 e-Cert 管理軟件數據保安機制，安裝時必須確定智能卡閱讀器不會對智能卡與電腦之通訊構成干擾。另外，安裝 e-Cert 管理軟件的電腦，必須是具備保安管理，及定期更新保安批次檔，包括：

- 可由公用網絡〔如互聯網〕存取的電腦，必須有可靠設置及受信任的防火牆。
- 功能變數內容〔如 ActiveX 及 Java〕應由受信任的編碼控制，及容許 e-Cert 管理軟件存取〔要取得關於在功能變數內容保護系統的資訊，請檢視網頁瀏覽器的線上支援〕。電腦必須裝有有效的防病毒保護，及定期更新病毒定義檔。
- 電腦只可執行被信任的服務。
- 用戶檔案必須隔離處理，以免其他用戶修改執行檔的路徑及設置數據。

若果你的電腦受到惡性軟件的破壞，可引致 e-Cert 管理軟件不能正常發揮它的保安功能。



當完成安裝後，可在系統匣中右擊 e-Cert 管理軟件的圖示，然後選擇管理員，去檢視 e-Cert 管理軟件的版本。在檢視 e-Cert 管理軟件應用系統的內容時，可檢查在智能卡的應用系統的版本編號〔要取得更多資料，請參閱 *e-Cert 管理軟件用戶指南*〕。

# 第 2 章

## 安裝 E-CERT 管理軟件

本章會說明安裝 e-Cert 管理軟件的步驟，及如何把智能卡上的電子證書註冊到電腦中。

以下為安裝程序的主要步驟：

1. 從香港郵政核證機關網頁下載 e-Cert 管理軟件 ([www.hongkongpost.gov.hk](http://www.hongkongpost.gov.hk))，
2. 執行 e-Cert 管理軟件，並進行設置，使 e-Cert 管理軟件能使用你的智能卡閱讀器，
3. 插入你的智能卡，並用微軟證書庫登記註冊你的電子證書。

### 接駁智能卡閱讀器

你需要用不同的步驟來安裝不同的智能卡閱讀器，請參照生產商的說明書安裝閱讀器及有關驅動程式。

基本上，安裝新的智能卡閱讀器時，是需要有實體的電線連接著你的閱讀器及電腦，並確定已安裝正確的驅動程式，以便視窗系統辨認及使用你的閱讀器。最新型的智能卡閱讀器支援 PC/SC 介面，微軟視窗已內置 PC/SC 驅動程式，你並不需要另外再安裝，但建議你先向生產商確認這點。

### 安裝 e-Cert 管理軟件

要安裝 e-Cert 管理軟件，步驟如下：

1. 從香港郵政核政機關網頁下載 e-Cert 管理軟件(如果你未曾下載)，
2. 執行 e-Cert 管理軟件，
3. 依照安裝程序，
4. 按**完成**，即完成整個安裝程序，
5. 在安裝完成後重新啟動你的電腦。

如果你需要在其他進階的功能中使用 e-Cert 管理軟件，請先在你的電腦中安裝**微軟管理主控台** (Microsoft Management Console)。這是一個在視窗 2000 及視窗 XP 中內置的程式，但在其他系統中，你必需要另外安裝。有關如何取得**微軟管理主控台**軟件，請參閱本文中的排解疑難篇。

重新啟動電腦後，你需要用微軟證書庫來登記智能卡上的電子證書。證書庫是所有需要使用電子證書之應用系統，如電子郵件系統或瀏覽器的共同存取庫。

## 登記你的電子證書

你需要用微軟證書庫來登記證書，你的電子郵件系統或瀏覽器才可使用你的電子證書。



**注：** 有關微軟證書庫的詳情，請參閱 *e-Cert 管理軟件用戶手冊*。

登記你的電子證書，可確保系統在需要時可以使用你的電子證書。

你可以點擊 e-Cert 管理軟件中的**複製 e-Cert 到 IE 電子證書庫**的按鈕，登記註冊在你的智能身份證中的電子證書。系統可能會要求你輸入私人密碼，在輸入正確密碼後，你會看到確認訊息。

登記你的電子證書，步驟如下：



1. 右擊系統匣中的 e-Cert 管理軟件圖示，並在彈出的功能表中選擇**管理員**，啟動 e-Cert 管理軟件；
2. 點選要登記的電子證書；
3. 在行動功能表中，選擇**複製證書至 IE**；
4. 你已成功登記證書。

如果微軟證書庫中並無香港郵政核證機關證書，你也許需要自行安裝一個。你可從我們的網站：[www.hongkongpost.gov.hk](http://www.hongkongpost.gov.hk) 中，下載及安裝香港郵政核證機關電子證書。

你需要設置你的應用系統，以配合已登記的電子證書，在使用系統時作數碼簽署及加密。

## 在微軟視窗註冊香港郵政核證機關根源證書及簽發人證書

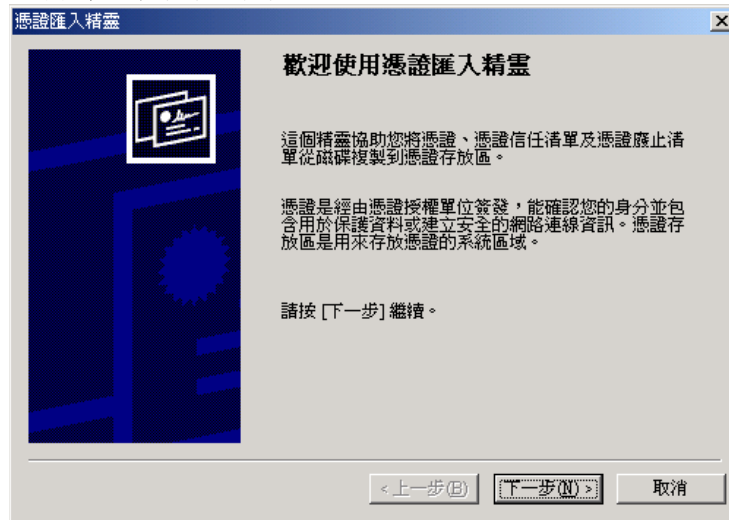
註冊了香港郵政核證機關根源證書後，你就可以肯定其他把訊息加密的用戶是否在使用合法的電子證書。

普通情況下，你只需要在電腦中，把香港郵政核證機關根源證書註冊一次。

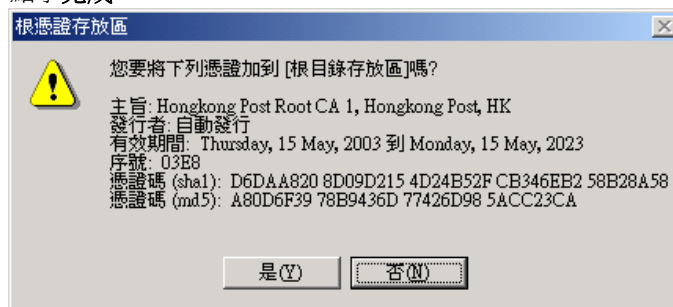
在微軟視窗註冊核證機關根源證書步驟如下：

1. 從香港郵政核證機關網頁下載香港郵政核證機關根源證書 (如果你未曾下載)，
2. 雙擊 smartid\_rt.cer. 證書資料會顯示出來，

3. 點擊**安裝憑證**開啓憑證匯入精靈，



4. 點擊**下一步**，
5. 請確認**按照證書種類自動選擇證書庫**只被點選，然後點擊**下一步**，
6. 點擊**完成**。



要註冊香港郵政核證機關的簽發人證書，請你重複第二至第六個步驟，並使用 smartid\_ca.cer 或 ecert\_ca\_1-10.cer 檔案（你亦可在香港郵政核證機關網站中找到此檔）。

香港郵政核證機關根源證書及簽發人證書已成功註冊到你的電腦中。

## 在 MozillaFirefox 上註冊香港郵政核證機關根源證書及簽發人證書

登記你的電子證書，步驟如下：

1. 啓動 Mozilla Firefox。
2. 在**工具**功能表中，選擇**選項**。
3. 選擇**進階**，再選擇**加密**然後點擊**檢視憑證清單**。
4. 選擇**憑證機構**選項卡，然後點擊**匯入**。
5. 從香港郵政核政機關網頁下載香港郵政核證機關根源證書 (如果你未曾下載)。
6. 選擇香港郵政核證機關根源證書，然後點擊**開啓**。



7. 請確認你已點選所有的空格：



8. 單擊**確定**以註冊證書在 Mozilla Firefox 上使用。

請你重複以上步驟註冊 CA 的中繼證書，並使用 smartid\_ca.cer 或 ecert\_ca\_1 - 10.cer（可從香港郵政核證機關網頁下載）。

## 設置 Mozilla Firefox 以使用 e-Cert 管理軟件

要設置 Mozilla Firefox 以使用 e-Cert 管理軟件，步驟如下：

1. 在**工具**功能表中，選擇**選項**。
2. 選擇**進階**，再選擇**加密**然後點擊**安全裝置**。
3. 點擊**載入**。
4. 在**模組名稱**框中，鍵入“e-Cert Control Manager PKCS#11”。在**模組檔名**框中，鍵入 PKCS#11 文件的完整路徑，再點擊**確定**。

這個文件的默認安裝位置是：

(32 位元) C:\Program Files\Hongkong Post e-Cert\e-Cert Control Manager\tncp11a.dll

(64 位元) C:\Program Files\Hongkong Post e-Cert\e-Cert Control Manager\tncp11a64.dll



# 第 3 章

## 設置你的電子郵件應用程式

本章會說明如何設置電子郵件應用系統的步驟，讓你能使用智能卡上的數碼身分證明來簽署並解讀訊息。下列為將被介紹的電郵系統：

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

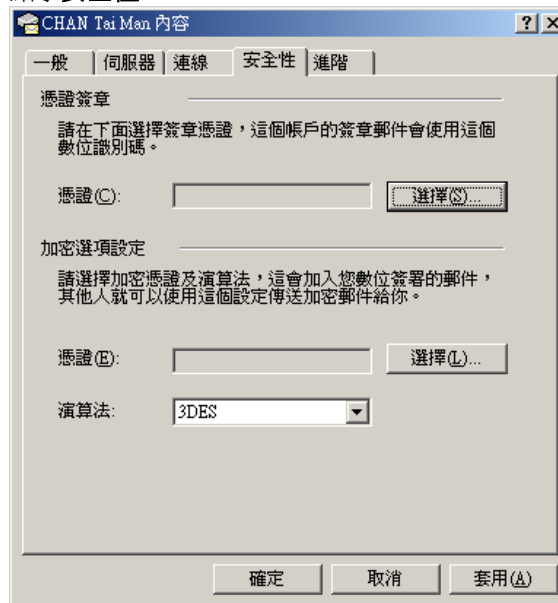
### 設置微軟 Outlook Express / Windows Mail / Windows Live Mail

Outlook Express/ Windows Mail / Windows Live Mail 會把你的安全措施設定儲存為你的電郵帳號設定一部份。

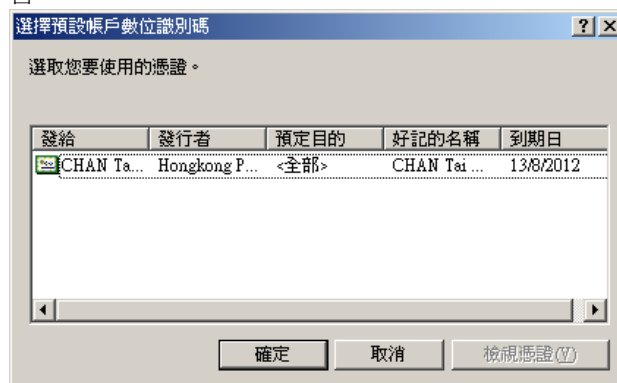
設署 Outlook Express/ Windows Mail / Windows Live Mail 來使用你的智能卡，步驟如下：

1. 啓動 Outlook Express / Windows Mail / Windows Live Mail。
2. 在工具功能表中，選擇**帳號**。
3. 點擊**郵件**。
4. 選擇你現用的電郵帳號，並點擊**內容**按鈕。

## 5. 點擊安全性。



## 6. 在憑證簽章部份中，點選選擇，並在已開啓證書庫中選擇用作簽署的證書。



如果你未能在清單中找到你的證書，請先登記證書—詳情請參考第 7 頁的登記你的電子證書

7. 在加密選項設定部份點擊選擇，即可選擇你想用以加密的證書—此選擇有可能與你的簽署證書相同。
8. 於清單中點選適用的演算法，然後按確定。



注： e-Cert 管理軟件用戶手冊載有有關如何數碼簽署電郵、獲取加密用電子證書、及設定 Outlook 視窗，使工具列顯示簽署及加密的按鈕等之詳情。你在 Outlook Express / Windows Mail / Windows Live Mail 的說明搜尋中，輸入 'Sending Secure Messages' 來查閱詳情。

## 設置 Mozilla Thunderbird

設置 Mozilla Thunderbird 步驟如下：

1. 在工具功能表中，選擇**選項**。
2. 選擇**進階**，再選擇**加密**然後點擊**安全裝置**。
3. 點擊**載入**。
4. 在**模組名稱**框中，鍵入“e-Cert Control Manager PKCS#11”。在**模組檔名**框中，鍵入 PKCS#11 文件的完整路徑，再點擊**確定**。

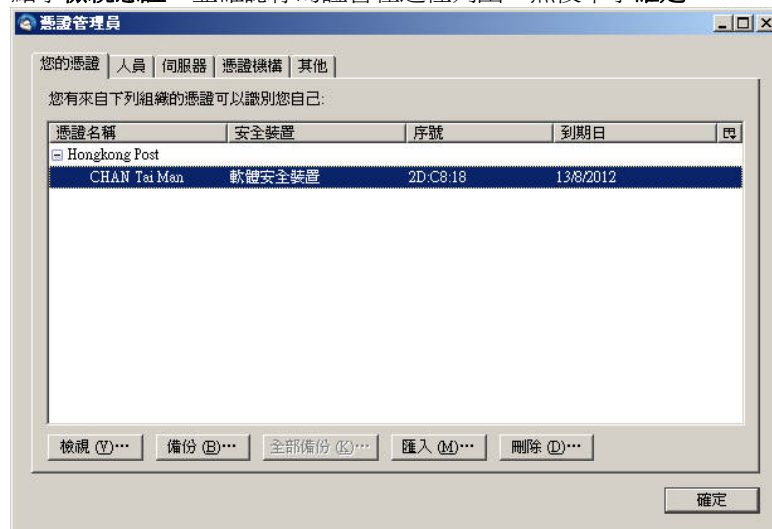
這個文件的默認安裝位置是：

(32 位元) C:\Program Files\Hongkong Post e-Cert\e-Cert Control Manager\tncp11a.dll

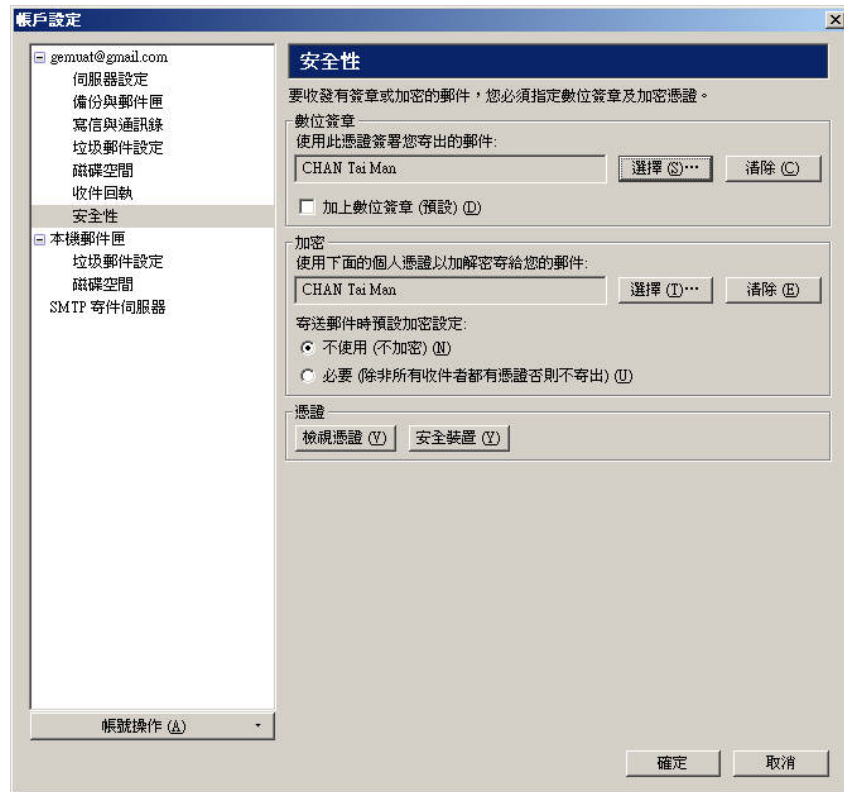
(64 位元) C:\Program Files\Hongkong Post e-Cert\e-Cert Control Manager\tncp11a64.dll



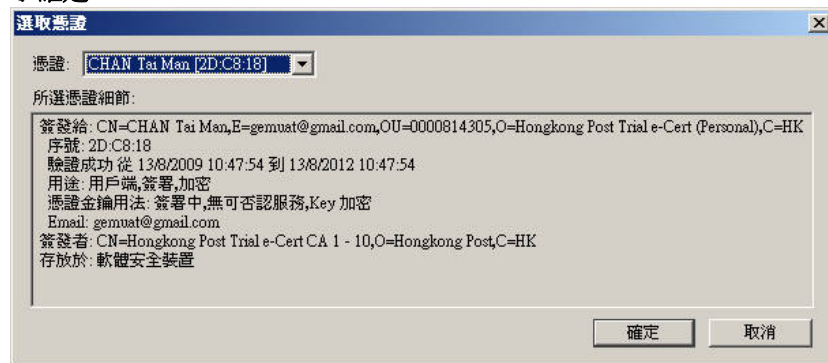
5. 把你的智能卡插入閱讀器中。
6. 點擊**檢視憑證**，並確認你的證書在這裡列出，然後單擊**確定**。



7. 如果你超過一張電子證書，你需要設立預設證書。要設立預設證書，在工具功能表中，選擇**帳戶設定**，再選擇**安全性**。然後點擊**使用此憑證簽署你寄出的郵件**選項旁的**選擇**按鈕。



8. 在下一個畫面，從下拉式清單中選擇用來簽署加密訊息的電子證書，再點擊**確定**。



9. 要進行加密，你須要重複第七及第八個步驟，選擇其他人仕用作加密給你的電子郵件的證書。

### 在 MozillaThunderbird 上註冊香港郵政核證機關根源證書及簽發人證書

香港郵政核證機關根源證書需要在 MozillaThunderbird 上另外註冊。要註冊證書，步驟如下：

1. 啟動 Mozilla Thunderbird。
2. 在工具功能表中，選擇**選項**。
3. 選擇**進階**，再選擇**加密**然後點擊**檢視憑證**。

4. 選擇**憑證機構**選項卡，然後點擊**匯入**。
5. 從香港郵政核政機關網頁下載香港郵政核證機關根源證書 (如果你未曾下載)。
6. 選擇香港郵政核證機關根源證書，然後點擊**開啓**。
7. 系統會要求你匯入證書。請確認你已點選所有的空格：



8. 單擊**確定**以註冊證書在 Mozilla Thunderbird 上使用。

請你重複第二至第八個步驟註冊 CA 的中繼證書，並使用 smartid\_ca.cer 或 ecert\_ca\_1 - 10.cer (可從香港郵政核證機關網頁下載)。

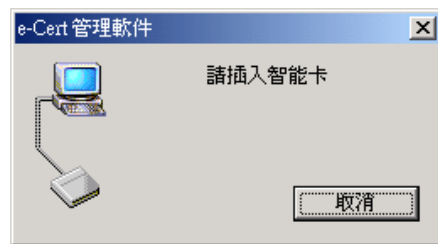
# 第 4 章

## 排解疑難

本章節會列出你在安裝或使用 e-Cert 管理軟件有可能面對的問題及疑難，並提供有關的資訊及解決方案。

### e-Cert 管理軟件的錯誤訊息

#### 智能卡存取錯誤



- 確定所有數據線路及電源線路(如有) 已穩妥地連接閱讀器及你的電腦。
- 確定智能卡閱讀器上的指示燈經常閃亮，並於插入智能卡時，持續亮起。在並非使用 PC/SC 介面的系統時，閱讀器指示燈會於初始時持續閃動，在 e-Cert 管理系統讀取智能卡時持續亮起。
- 確定智能卡已完全插入閱讀器中
- 確定智能卡的正確插入方向及讀取面，並無上下或前後反轉。

#### 於執行‘載入鑰匙庫’指令後，P12 檔未能載入到智能卡中

- 確定已在你的電腦中成功安裝微軟虛擬機器。最新的微軟虛擬機器可於 <http://download.microsoft.com> 下載。
- 確定‘檔名’中已選定正確有效的 P12 檔案。
- 輸入正確的 P12 密碼及智能卡密碼。

### 微軟管理控制台錯誤

在安裝時，e-Cert 管理軟件偵察到一個舊版的管理控制台。



e-Cert 管理軟件需要配合微軟管理控制台版本 1.1 或以上。這版本會於視窗 2000 或 XP 操作系統安裝時自動安裝，如果你的視窗並非上述兩種，請你自行手動安裝。在視窗 NT/98/ME 的環境中，如果你正在使用中文版，請安裝 MMC 版本 1.1，如果你正在使用英文版，請你下載並安裝 MMC 版本 1.2。

你可從微軟的視窗更新網站上免費下載最新版本的微軟管理控制台：  
[windowsupdate.microsoft.com](http://windowsupdate.microsoft.com)

啓動 e-Cert 管理軟件時，系統警告所選用的檔案並非一個管理控制台文件



你所選用的微軟管理控制台版本太舊 — e-Cert 管理軟件需要配合微軟管理控制台版本 1.2 或以上。你可從微軟的視窗更新網站上免費下載最新版本的微軟管理控制台：

[windowsupdate.microsoft.com](http://windowsupdate.microsoft.com)

在視窗 NT/98/ME 的環境中，如果你正在使用中文版，請安裝 MMC 版本 1.1，如果你正在使用英文版，請你下載並安裝 MMC 版本 1.2。