

以 GPG 及 WinPT 實現數位內容的加密與簽章

游啓勝 國家資通安全會報技術服務中心

最後修改：2004.3.28

【摘要】

提到電子郵件的加密及簽章，多數人都知道 PGP 這套軟體，PGP 藉由加密及簽章達到電子郵件或電腦檔案的機密性、完整性及不可否認性。自由軟體 GPG 與 WinPT 則可提供有成本考量的單位建置大規模的公開金鑰加解密及簽章驗證解決方案。

【前言】

電子郵件已是現代人溝通不可或缺的工具之一。提到電子郵件的加密及簽章，多數人都知道 PGP (Pretty Good Privacy) 這套軟體，PGP 藉由加密及簽章，可達到電子郵件或電腦檔案的機密性 (confidentiality)、完整性 (integrity) 及不可否認性 (non-repudiation)。但 PGP Freeware 版本只允許個人在家中的非營利使用、學生在教育機構的非營利使用，及非營利的慈善機構及組織使用，其他使用皆需購買其他版本的 PGP，若是想多人使用，建置成本將相當可觀。不過，自由軟體界也提供了一套 GPG (Gnu Privacy Guard) 提供與 PGP 類似的功能，從 GPG 的名稱就可不難感受到開發者試圖用它與 PGP 相抗衡的意味。

GPG 原本是一個命令列的程式，但有許多的熱心開發者為它加上許多前端介面及加強程式 (Plugin) 來增加使用的便利性，最常見的有 WinPT (Windows Privacy Tools) 與 GPGShell 兩套，本文將介紹如何用 GPG 加上 WinPT 來達成與 PGP Freeware 相似的公開金鑰加解密及簽章驗證解決方案。

WinPT 提供以下數項功能：

- I 電子郵件加解密、簽章、驗證：提供 Outlook Express 及 Eudora 的

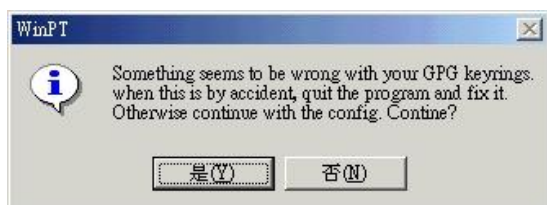
E-mail Plug-in，方便加密電子郵件。

- I 檔案加解密、簽章、驗證、及完全刪除：提供 Explorer Extension，能使用者在檔案總管下直接進行以上功能。
- I 金鑰管理：以 Key Manager 提供介面來管理金鑰。

【安裝 WinPT】

- 一、至 <http://winpt.sf.net/en/download.php>，下載最新版的 WinPT (目前為 1.0rc2)，重要的應用場合請以 md5 檢查檔案是否正確，再進行安裝。選擇安裝元件時，請根據使用的電子郵件軟體，勾選安裝「E-Mail Plugins」中的 Outlook Express Plugins 或 Eudora Plugins。WinPT 也會安裝 GPG，若是需要新版本的 GPG，可自行進行安裝後再複製至 WinPT 安裝目錄即可。
- 二、安裝完成後，WinPT 會警告找不到公開及秘密金鑰 (圖一)，此時可以選擇建立或匯入金鑰 (圖二)。建立時，金鑰資訊儘量以英文為主 (圖三)，若使用中文，接收者若是使用 PGP 時會變成亂碼。金鑰長度愈長，金鑰愈不容易被破解，但簽章或加密時所需的運算時間也愈

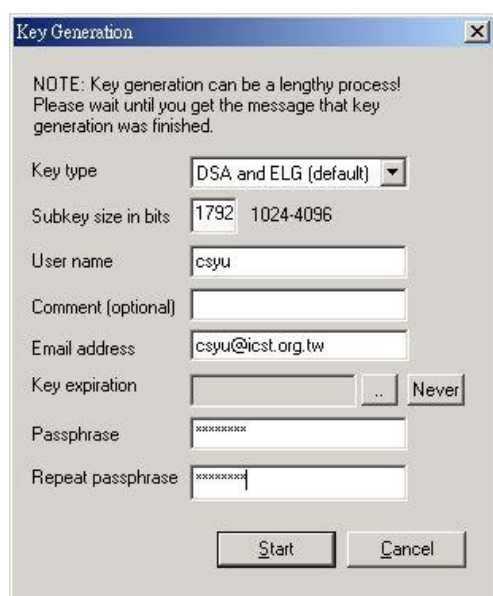
多。建立金鑰時，需要輸入一組密碼（passphrase），將來使用秘密金鑰進行加密及簽章時，會被要求輸入此密碼來做為確認身份的第二防線，降低秘密金鑰失竊時的風險。



(圖一)



(圖二)



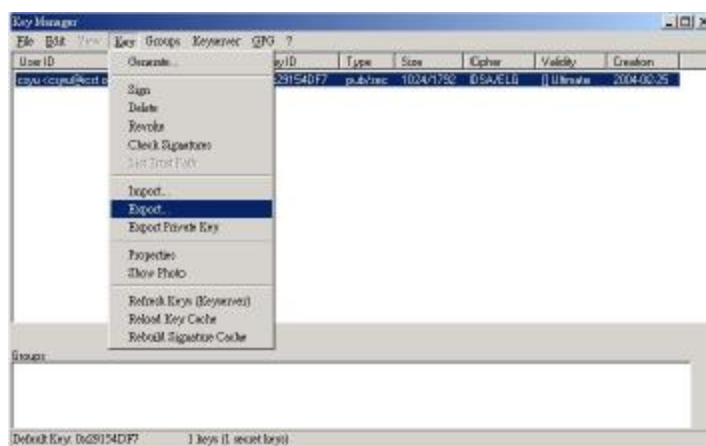
(圖三)

三、在螢幕右下角的 WinPT 圖示上按滑鼠右鍵（圖四），可選擇執行 Key Manager，利用 Key Manager 的匯出（Export）功能將公開金鑰匯出成文字

檔（圖五）放置於網頁上，供需要傳送加密郵件或是驗證簽章的人抓取，也可以考慮將金鑰傳至更安全的 keyserver，供人公開查詢。（例如可傳送至免費的金鑰存放伺服器 www.keyserver.net 上）。秘密金鑰則可存於硬碟，如果要增加安全性，可考慮放置於隨身碟，在需要秘密金鑰時，再將隨身碟插入電腦，可避免電腦被入侵時，秘密金鑰同時遭竊。不論放置於何處，需謹記另存一份備份放置於其他安全處。否則一旦遺失，必須重新產生新的秘密及公開金鑰，用舊有金鑰加密的檔案也會無法解開。



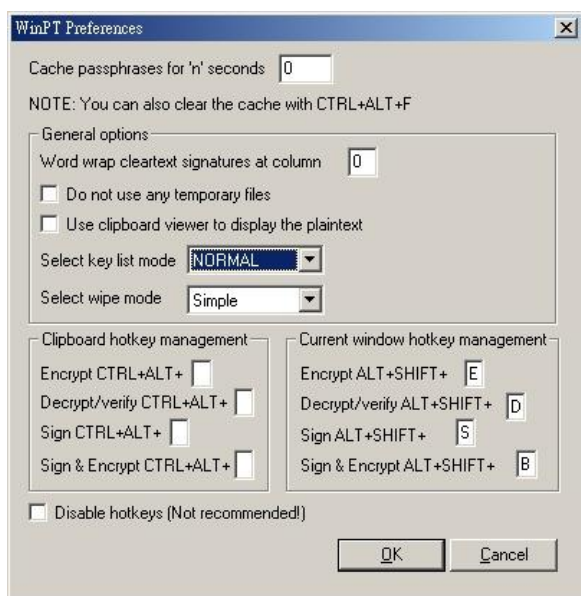
(圖四)



(圖五)

四、在螢幕右下角的 WinPT 圖示上按滑鼠右鍵（圖四），選擇「Preferences」à

「WinPT」可進入設定畫面中設定熱鍵來增加使用的便利性（圖六）。



(圖六)

【GPG 的應用】

GPG 的應用可分為以下數種：

I 電子郵件的簽章及加解密

此為 GPG 最常被使用到的功能，傳送加密郵件及驗證郵件時，需要對方的公開金鑰，傳送簽章郵件及解密郵件時，則需要自己的秘密金鑰（如下表）。**傳送加密或簽章郵件時，附檔不會加密及簽章，需自行先加密。**對方的公開金鑰在使用時必須先行以 Key Manager 匯入（匯入後需 Reload Key Cache，才能看到剛剛匯入的金鑰），當 WinPT 找不到對方金鑰時，程式會發生錯誤而當掉。

	傳送方(A)		接收方(B)	
	公開金鑰	秘密金鑰	公開金鑰	秘密金鑰
加密郵件	√(B)			√(B)
簽章郵件		√(A)	√(A)	
加密與簽章郵件	√(B)	√(A)	√(A)	√(B)

WinPT 所附的 Outlook Express Plugin (OE Plugin) 並不會加入新的按鈕，而是取代現有「加密」及「簽章」的功能（圖七），WinPT 加密或簽章時，有時會發生抓不到現行視窗內的文字，此時之前設的熱鍵就很好用了。舉例來說，若是想要對郵件簽章，只需在郵件本文上按「Alt+A」（選擇全部）、「Alt+Shift+S」（進行簽章）、鍵入密碼後按「Ctrl+v」（貼上）即可。驗證簽章時，OE Plugin 會自行尋找合適的公開金鑰來驗證，並檢視簽章是否正確。



(圖七)

I 檔案的加解密、簽章、及完全刪除

WinPT 提供 Explorer Extension 對一個或多個檔案進行加密、簽章及完全刪除。只要選擇檔案後，按滑鼠右鍵即可以進行各種動作。檔案加密時會進行壓縮，不用 Text Output 會比較省空間，但經測試，Text Output 才能確保相容性，例如：使用 PGP 對檔案加密後，若不以 Text Output 輸出，使用 GPG 解密時會發生錯誤。因此，建議使用 Text Output 來輸出加密及簽章檔案。對整個目錄加密或簽章則需先利用壓縮軟體壓縮成一個檔案，再加以加密或簽章。

完全刪除的功能對銷毀重要的資料特別有用，使用完全刪除功能，會利用密碼學的方法在原來檔案的空間進行資料覆寫，可使檔案無法被救回。在 WinPT 圖示的「File Manager」也提供「Wipe Free Space」可供覆寫目前所有

可用空間。

GPG 和 WinPT 提供了類似 PGP 的公開金鑰加解密及簽章功能，雖然不如 PGP 的功能強大（沒有如 PGPNet 或 PGPDisk 的功能），亦有些小 bug 之外，若是用來作單純的電子郵件加解密簽章之用，也不失為在有限預算下的一個良好解決方案。

【參考資料】

- I PGP(Pretty Good Privacy) :
<http://www.pgp.com/>
- I GPG(GNU Privacy Guard) :
<http://www.gnupg.org/>
- I WinPT : <http://www.winpt.org/>
- I GPGShell :
<http://www.jumaros.de/rsoft/index.html>

• • • • □ • • • • •
• • • □ • • • • •
• □ • • • • •
□ • • • • •
• • • • •
• • • •
• • •
• •
•