

網路安全的理論與實務

楊中皇 著

第十八章 **PGP**

<http://crypto.nknu.edu.tw/textbook/>

金 禾 圖 書

伴 您 學 習 成 長 的 每 一 天



第十八章 PGP

- PGP簡介
- PGP的安裝方法
- PGP的使用



PGP發展歷史

- PGP (Pretty Good Privacy) 是由Philip R. Zimmermann 開發並於1991年發表的一套公開金鑰密碼技術工具，其運作背後，涉及一些密碼學的觀念與技術，如對稱式加密演算法、公開金鑰加密演算法及數位簽章等。
- PGP的用途廣泛，能對任何種類的檔案進行加密保存，或結合其他軟體加強安全功能，是目前應用最普遍的安全電子郵件系統
- IETF特別成立OpenPGP工作小組，致力於PGP的標準規範研究與制定，且PGP本身業已成為專業的網路安全軟體
- PGP產品分為兩支，一為需付費使用的商業PGP (<http://www.pgp.com/>)，另為非商業用途而功能較少的免費PGPi (<http://www.pgpi.org/>)，其PGP商業版本是發展主流，有提供視窗及命令列兩種操作模式的版本，而免費的PGPi幾乎已經停止系統更新



PGP的主要功能

- 訊息加密
 - 採用混合加密方式，亦即同時使用對稱式加密演算法及公開金鑰加密演算法；對稱式加密演算法是將須傳送的訊息加密，而加密用的金鑰則用公開金鑰加密演算法再行加密
- 數位簽章
- 檔案壓縮
 - PGP在對訊息進行加密之前，通常會先將其檔案壓縮，這樣不僅可以節省磁碟儲存空間及網路傳輸時間，更重要的是，有些密碼分析技術是專門針對純文字檔進行攻擊，而檔案壓縮能夠強化純文字檔保密程度，提高對這類攻擊的抵抗



PGP的主要功能(續)

- 訊息編碼
 - 可使用Radix-64轉換法，將加密過後的訊息轉換成ASCII編碼，以相容於電子郵件應用程式中存取
- 訊息分段與重組
 - 由於某些電子郵件系統會限制單一訊息的最大長度，因此PGP在傳送電子郵件時會先將訊息分段，每個區段以一個郵件傳送，而接收方再將所有區段重組成原來的單一電子郵件



操作平台

- 免費PGPi版本可在大多數的作業系統安裝使用
- 不過在PGP成爲商業軟體之後，已不再全力支援PGPi的發展，故PGPi在各種作業系統的支援版本不一，與PGP的商業版本也不一致



作業系統	支援的最新版本
Amiga	PGP 5.0i
Atari	PGP 5.0i
BeOS	PGP 5.0i
MacOS X	PGP 8.0 (已更改連結到PGP商業版網站)
MS-DOS	PGP 5.0i
OS/2	PGP 5.0i
Palm OS	PGP wireless for Palm 1.5 (評估版)
Unix/Linux	PGP 6.5.8 (不再於版本編號後附加"i")
Windows 98/ME/NT/2000/XP	PGP 8.0 (已更改連結到PGP商業版網站)

視窗版（PGP Desktop）	命令列版（PGP Command Line）
Windows XP SP1或SP2	Windows 2003
Windows Server 2003	Windows XP SP1
Windows 2000 Professional SP3或SP4	Windows 2000 SP4
Mac OS X 10.3.9、10.4.0及10.4.1版	HP-UX 11i以上版本（PA-RISC）
	IBM AIX 5.2以上版本
	Red Hat Enterprise Linux 3.0以上版本（x86）
	Solaris 8以上版本（SPARC）
	Mac OS X 10.3以上版本



PGP安裝-Linux

- PGP商業版的命令列版雖然支援Linux，但須付費購買才能使用，而且已經不提供試用版下載
- 因此在Fedora Core 4使用PGPi官方網站所提供的RPM套件安裝，但由於支援Unix/Linux的PGP 6.5.8版不能直接在FC4上安裝，需先將libstdc++.so.2.8複製到/usr/lib目錄下並設為可執行，才能安裝，其相關指令如下：
 - tar xvfz lib.tar.gz（解出libstdc++.so.2.8檔）
 - cp libstdc++.so.2.8 /usr/lib
 - chmod 755 /usr/lib/libstdc++.so.2.8
 - rpm -ivh --nodeps PGPcmdln_6.5.8_Lnx_FW.rpm



在FC4下執行PGP（不指定參數）顯示版本資訊

金禾資訊

伴

您

學

習

成

長

的

每

一

天

Pretty Good Privacy(tm) Version 6.5.8

(c) 1999 Network Associates Inc.

Uses the RSAREF(tm) Toolkit, which is copyright RSA Data Security, Inc.

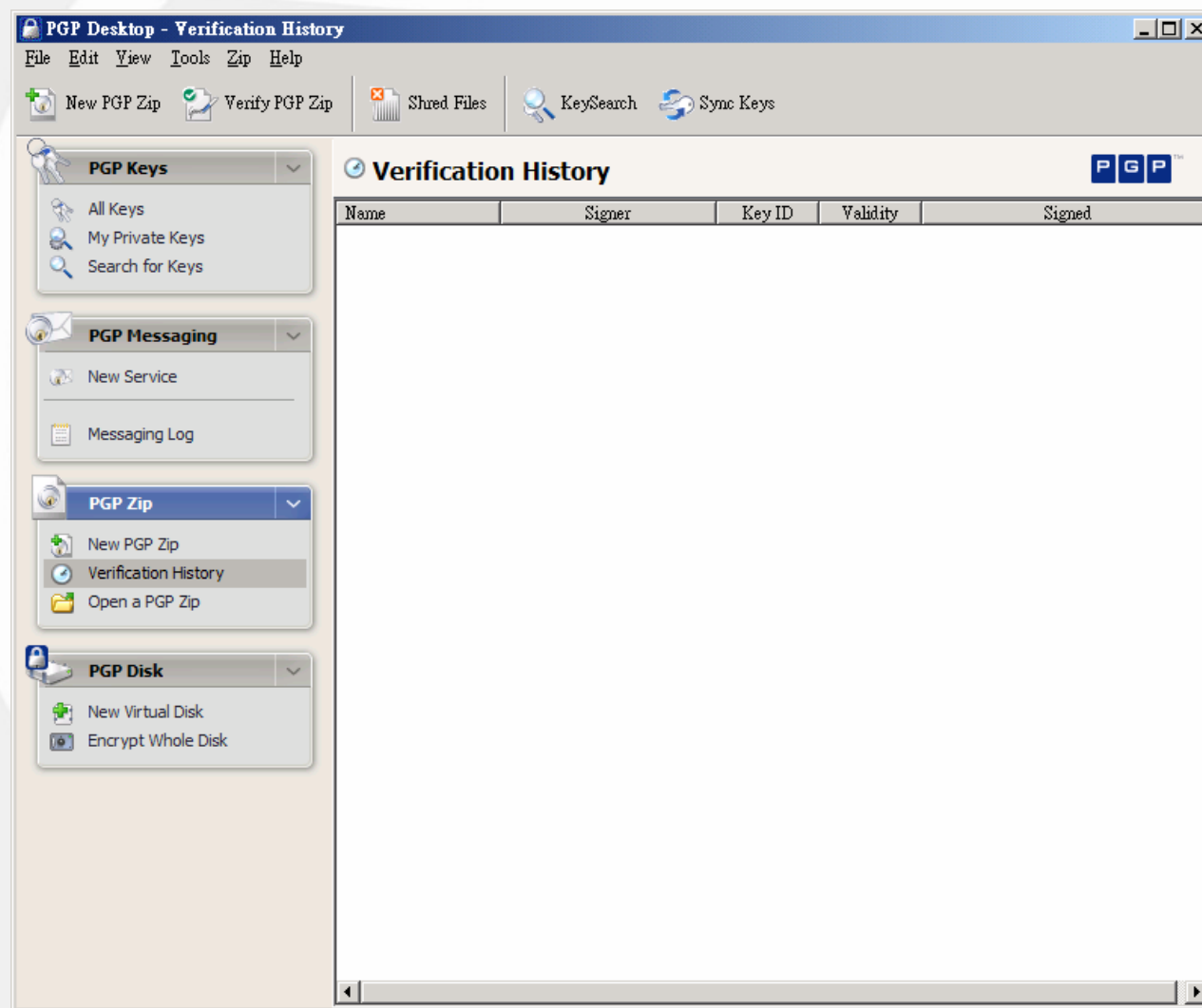
Export of this software may be restricted by the U.S. government.

For a usage summary, type: `pgp -h`



PGP安裝-Windows

- 雖然PGPi官方網站提供支援Windows系統的下載版本，但自8.0版以後，網站上的Windows版本均已連結至PGP的商業版網站
- 要安裝最新PGP for Windows版本，必須到<http://www.pgp.com/>下載。目前最新的版本為PGP Desktop 9.0，其試用版有三十天的評估期
- 讀者可以自行到PGP商業版網站填寫基本資料，以便下載試用版。在安裝完畢之後請先重新開機，PGP服務預設會在開機時自動啟動





PGP的使用-Linux

- 本節介紹在Linux下使用PGP，主要以PGP基本功能為主
- 以下會說明
 - 如何使用金鑰
 - 檔案加解密
 - 數位簽章



建立金鑰對

Pretty Good Privacy(tm) Version 6.5.8

(c) 1999 Network Associates Inc.

Uses the RSAREF(tm) Toolkit, which is copyright RSA Data Security, Inc.

Export of this software may be restricted by the U.S. government.

Choose the public-key algorithm to use with your new key

1) DSS/DH (a.k.a. DSA/ElGamal) (default)

2) RSA

Choose 1 or 2: 1

- 對於第一次使用**PGP**，必須先產生金鑰對（公開金鑰/私密金鑰），所以請在命令提示符號輸入『**pgp -kg**』
- 首先請選擇金鑰要使用的公開金鑰演算法，預設是**DSS/DH（DSA/ElGamal）**，亦可選擇**RSA**，如上圖



設定數位簽章用的主金鑰

Choose the type of key you want to generate

- 1) Generate a new signing key (default)
- 2) Generate an encryption key for an existing signing key

Choose 1 or 2: 1

Pick your DSS ``master key" size:

- 1) 1024 bits- Maximum size (Recommended)

Choose 1 or enter desired number of bits: 1024

Generating a 1024-bit DSS key.

You need a user ID for your public key. The desired form for this user ID is your name, followed by your E-mail address enclosed in <angle brackets>, if you have an E-mail address.

For example: John Q. Smith <jqsmith@nai.com>

Enter a user ID for your public key: Chung-Huang Yang <chyang@nknucc.nknu.edu.tw>

Enter the validity period of your signing key in days from 0 - 10950

0 is forever (the default is 0): 0

You need a pass phrase to protect your DSS secret key.

Your pass phrase can be any sentence or phrase and may have many words, spaces, punctuation, or any other printable characters.

Enter pass phrase:

Enter same pass phrase again:



- 若選擇**DSS/DH**的話，數位簽章用的金鑰與加解密用的金鑰，則必須分別產生
- 主金鑰亦即數位簽章簽署及驗證用的金鑰，需要設定金鑰長度、公開金鑰的辨識資訊（通常是使用者姓名加上電子郵件帳號）及金鑰的有效期限（**0**表示永久有效）等
- 最後設定一組存取私密金鑰通行密語（**Pass Phrase**），它的作用就像通行碼（**Password**）一樣，主要是爲了保護私密金鑰安全，因此最好設定不易遭破解的字串，例如任何單字夾雜空白字元、標點符號或是其他字元。



設定加解密用的子金鑰

PGP will generate a signing key. Do you also require an encryption key? (Y/n) Y

Pick your DH key size:

- 1) 1024 bits- High commercial grade, secure for many years
- 2) 2048 bits- "Military" grade, secure for foreseeable future
- 3) 3072 bits- Archival grade, slow, highest security

Choose 1, 2, 3, or enter desired number of bits: 1024

Enter the validity period of your encryption key in days from 0 - 10950

0 is forever (the default is 0): 0

- 接著設定加解密用的金鑰（如上圖），其金鑰的長度有三種選擇，長度愈長當然愈安全，但相對處理速度會較慢。



執行建立金鑰對

Note that key generation is a lengthy process.

PGP needs to generate some random data. This is done by measuring the time intervals between your keystrokes. Please enter some random text on your keyboard until the indicator reaches 100%.

Press ^D to cancel

42% of required data

100% of required data

Enough, thank you.

.*****

..***** .

Make this the default signing key? (Y/n) Y

....*****

.....***

*** Key generation completed.



執行建立金鑰對(說明)

- 金鑰在設定完畢後，便是執行建立金鑰，而PGP在執行此設定之前，必須產生一些亂數資料，並依據此亂數建立金鑰，而它會標示出目前所需亂數資料的百分比（**XX% of required data**），使用者得任意敲擊鍵盤上任何字元，促使其百分比達到**100%**，以順利建立金鑰對
- 上述步驟執行時，PGP會在使用者目錄底下產生隱藏的.pgp目錄，以便存放建立完畢的金鑰對，公開金鑰和私密金鑰會分別儲存在pubring.pkr及secring.skr兩個鑰匙環（Keyring）檔案中



PGP憑證格式

- PGP憑證格式至少包括以下內容：
 - PGP版本編號
 - 憑證擁有者的公開金鑰
 - 憑證擁有者的基本資料，如名字或使用者ID等
 - 憑證擁有者的數位簽章
 - 憑證的有效期限
 - 憑證的公開金鑰偏好使用的加密演算法，如CAST、IDEA或3DES等



匯出入PGP憑證

- 交換憑證，可透過電子郵件將憑證匯出檔傳送給欲通訊的對方
- 在匯出時要指定自己的ID，通常是原先建立金鑰時輸入的電子郵件帳號
- 另外還要指定匯出的憑證檔名，檔案內容將會是經過編碼並以ASCII字元呈現的純文字檔（如右圖）
- 匯出的指令格式如『pgp -kx <使用者ID> <匯出檔名>』，其範例為『pgp -kx chyang@nknucc.nknu.edu.tw chyang_pk.asc』

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: PGP 6.5.8

```

mQGiBELwfUQRBADCD4dqkvxzkTEWnDO7By2yZ3QuGIBQFJ04R6MPKAUfWrRCCTb
RELMzcEy4Tmbr3F0rtds5oyqTyUFTtJvpRORvtcCMvxtZ+KLMwVV/e+rkajFnkLe
cqLIOysYGMVrXjrjvBo3IzXnoXBHyc6PGmCzosQcVKgxz0D4ipwpzrd51QCg/+R6
UGycWnQFJgqEmGdbMHQeCPMD/3aVQsWpZpUdQnDb5XTCE4eNBk9mHI9YI+MKo2M
Ryc56PF08GyqWo2WEOMMioW9XyASxsQWxEdzXR9oyZPMStoAGBZM3p1s9Hx+WB4
E+j28ctUZVlj1qCXcqkk3Hq/klRgV36LU1wHPu+AVWeaGzGtufuJc711C/k4iz7U
69nVBACq5Yf49D7vFxGauc73fsiyWanSOquPrtd+jDFzYVzznI43T+k2sJgNjrb
SAq8AQqReClGknA2OOwozNliDS44OybhdoqQmQnFg6ArtGg5njsiqvumFZcsaNh5
r2s+edt5VVj+/tKY8j4llyHsqPPVeMui52phYLHIZk/QsB9SYkAPwMFIELwicfT
64mFYNocbBECahQAoJ/NhkCuKa/gZDo82lQOSyfQXjjDAJ9QphHuZ1Vw4clVFUq8
1eK8RNIkw7QjV2VpLVRzdW5nIENoYW5nIDx3dGNlbUBob3RtYWlsLmNvbT6JAE4E
EBECAA4FAkLwfUQECwMBAgiZAAQAKCRDT64mFYNocbAUWAKCikPhUE9iiPEwEs14a
ngVSzv+OEACglxQiH0iPPizrYiEk/a0mgBDPpNe5AQ0EQvB9ShAEAN8UZ68udu6Q
wHH5HHFrSKnKxZahrgbfrD/ZySmt20jjB614wJ4oFuhwazr+LfrYvp+qzKtBqvdl
CpggojeyWcwpoQnXRk/dimN/+DgULEE3WjlOhJhgR6zSdL1gFPglwG2bdqfpaL1C
7zBHLduR9xlrwaYOxNnl4rQNur4lPwY1AAICA/9BorOkQ7VeVqQv/9LHVlaDWwpS
s4r/UGswpninc9vRQU/7e1eRlebMKxOfHXgzen6Xgq7csuqmNPVE2TWhudIGV+W
MdxLXuU1HXSxykxv4TgjLJwREQiUVu1pjG+eEbf9sZHHc+EdL8O0prVVkPlgCDUO
sgWq1/KQ7QR3gZqgfokARgQYEQIABgUCQvB9SgAKCRDT64mFYNocbH29AJ4nesRP
jVM48S7YA1TRhKUpCzXjkWcdEXRYj9Ldzel5W5QhvYxtwOkWMJo=
=Kbnz

```

-----END PGP PUBLIC KEY BLOCK-----



匯出入PGP憑證(續)

- 另一種方式是將憑證匯到金鑰伺服器（Key Server），而金鑰伺服器通常是位於網際網路上（如<ldap://keyserver.pgp.com>）的某個LDAP伺服器，主要用以儲存PGP使用者憑證，任何人都可在金鑰伺服器上搜尋並下載其他人的公開金鑰，其匯出指令格式如下：
 - `pgp -kx <使用者ID> <匯出檔名> <金鑰伺服器的URL位址>`



匯出入PGP憑證(續)

- 若匯入他人憑證，可到金鑰伺服器搜尋欲通訊對方的憑證，並下載存成檔案，再將該檔案匯入自己的公開鑰匙環中，並搜尋下載指令如同將自己的憑證匯出到金鑰伺服器一樣，只是使用者ID必須指定對方的ID，指令格式如『pgp -kx <對方的使用者ID> <儲存檔名> <金鑰伺服器的URL位址>』，再用此指令將對方的憑證匯入『pgp -ka <對方的憑證>』
- 如果要從自己的鑰匙環中移除一把公開金鑰，或是將自己的公開金鑰（憑證）從金鑰伺服器中移除，請使用此指令『pgp -kr <使用者ID> <金鑰伺服器的URL位址>』，而要將一把公開金鑰設定為無效，則使用指令為『pgp -kd <使用者ID>』



檔案加密

Recipients' public key(s) will be used to encrypt.

Key for user ID: Chung-Huang Yang <chyang@nknucc.nknu.edu.tw>

1024-bit DSS key, Key ID 0x6792C4C2, created 2005/08/04

Key can sign.

Ciphertext file: testfile.pgp

- 將檔案以對方的公開金鑰加密後傳送給他（她），對方收到該檔案後便能以自己的私密金鑰解開，加密時可以指定多個接收者的ID，其指令格式如下：
 - `pgp -e <欲加密的原始檔案> <接收者1的ID> <接收者2的ID>...`，其使用範例命令為『`pgp -e testfile chyang@nknucc.nknu.edu.tw`』
- 結果如上圖所示，加密過後的檔案為原始檔案附加.pgp副檔名



檔案解密

File is encrypted. Secret key is required to read it.

Key for user ID: Chung-Huang Yang <chyang@nknucc.nknu.edu.tw>

1024-bit DSS key, Key ID 0x6792C4C2, created 2005/08/04

Key can sign.

You need a pass phrase to unlock your secret key.

Enter pass phrase:

Plaintext filename: testfile

- 如果要解密對方傳送來的檔案，只要設定解密參數-p加上密文檔案即可，命令為『**pgp -p testfile.pgp**』
- 解密時，會使用到私密金鑰，因此必須輸入通行密語取得私密金鑰，才能順利執行解密
- 上圖是解密後的結果，會將原始檔案解出另行儲存。



產生分離式數位簽章

```
A secret key is required to make a signature.  
You need a pass phrase to unlock your secret key.  
Key for user ID "Chung-Huang Yang <chyang@nknucc.nknu.edu.tw>"  
  
Enter pass phrase:  
  
Passphrase is good  
  
Signature file: testfile.sig
```

- 數位簽章的用法是以**-s**參數指定欲產生數位簽章的檔案，及以**-u**指定自己的使用者ID（如果本身只有一對金鑰，則可省略），命令如『**pgp -s testfile -u chyang@nknucc.nknu.edu.tw**』，產生的檔案名稱仍為原始檔名附加.pgp副檔名
- 如果要同時對檔案做數位簽章及加密的話，則使用此命令『**pgp -es <原始檔案> -u <使用者本身ID> <接收者1的ID> <接收者2的ID>...**』
- 上述兩種數位簽章的做法都是簽章的內容依附於原始檔案或加密後的檔案中，如果要將簽章分離產生，則可使用此命令『**pgp -sb testfile -u chyang@nknucc.nknu.edu.tw**』，則分離式數位簽章的執行與產生結果如上圖，檔名則是原始檔名附加.sig副檔名，有別於之前的方式



檢核數位簽章的完整性

File 'testfile.sig' has signature, but with no text.
Text is assumed to be in file 'testfile'.
Good signature from user "Chung-Huang Yang <chyang@nknucc.nknu.edu.tw>".
Signature made 2005/08/04 12:08 GMT

- 而要檢驗檔案的數位簽章，只要輸入pgp命令加上檔名即可『**pgp** <簽章或加密過後的檔案>』，不需要加任何參數，只要指定檔名，**PGP**便會自動驗證數位簽章或對檔案解密
- 上圖是檢驗分離式數位簽章的測試結果，顯示其為完整良好的簽章



撤銷公開金鑰

- 假設
 - － 忘記密碼
 - － 懷疑公開金鑰被破解
 - － 私密金鑰遺失或遭竊取
 - － 及認為有其他危害系統安全的情況時
- 就可以撤銷公開金鑰，其撤銷的命令格式如『pgp -kr <使用者ID> <鑰匙環檔案>』



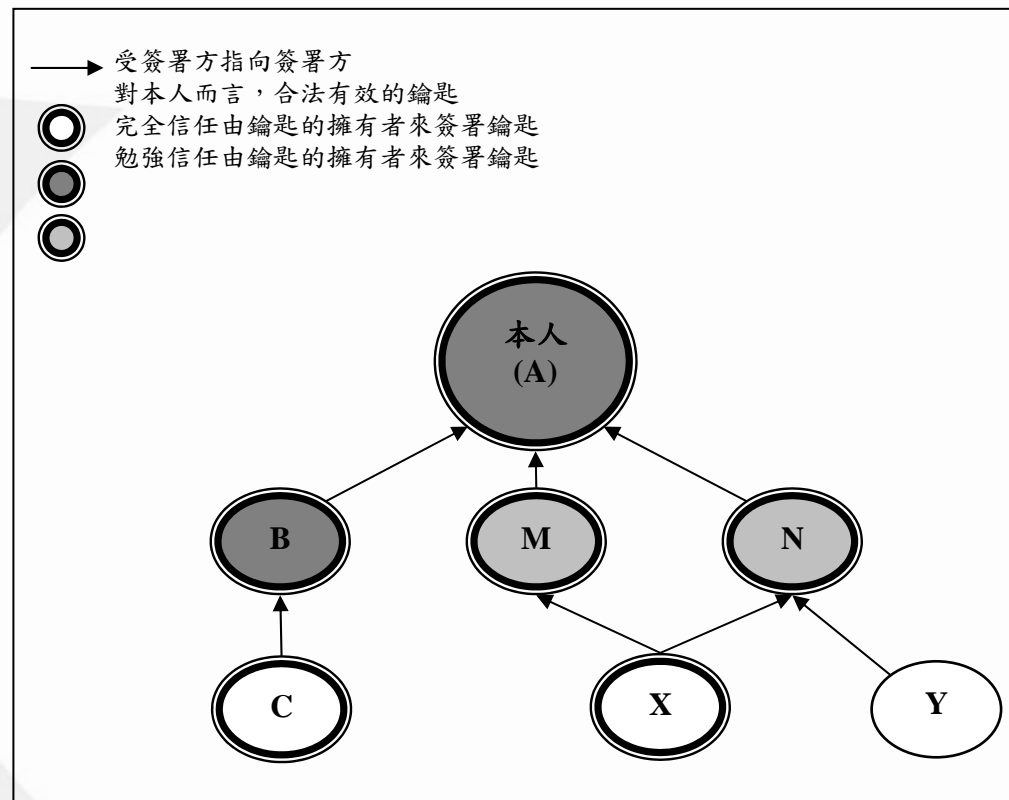
驗證與信任

- 驗證目的是在於讓使用者確實將某把公開金鑰憑證無誤傳送給它的主人，而非假冒第三者
- 在公開金鑰的使用環境中，無法完全避免會有不懷好意的第三者，利用偽造公開金鑰假冒使用者，實際與對方進行通訊，因此驗證步驟是必須的
- 驗證的方式有許多種
 - 使用者可要求通訊對方將他的公開金鑰複製到磁碟片之後，親自面交，這是最安全的做法，但其實既不方便又無效率
 - 另一個可靠方式是核對公開金鑰憑證的指紋，因為每一個公開金鑰都有獨一無二的指紋，這種指紋是以雜湊函數演算法運算得出的訊息摘要，它會成為金鑰的屬性，若想要驗證對方的公開金鑰憑證，使用者可以主動致電對方，請他（她）讀出其公開金鑰指紋。PGP檢視金鑰指紋的指令如『pgp -kvc <使用者ID> <鑰匙環檔案>』



驗證與信任(續)

- 就驗證機制而言，PGP主要是採取信任網（Web of Trust）的信任模式
- 此外由於PGP已經支援X.509憑證，因此亦可採用如同CA（Certification Authority）的階層式信任模式
- 本章僅對信任網作介紹
- 信任網就像人際關係網（如右圖）一樣，使用者A信任使用者B，而使用者B信任使用者C，則A只要請B引薦，他（她）就可以信任C





設定信任他人的程度等級

- 在信任網的環境中，任何使用者都可以驗證其他使用者的公開金鑰憑證，但只有在第三方同時認為驗證者是可信任的引薦者時，才會被信任
- 使用者**A**若要信任使用者**B**所認為有效的金鑰，得先認定**B**是可被信任的引薦者，不然的話**B**對於使用者**C**的公開金鑰驗證對**A**來說是不具任何意義的
- 使用者可為別人的公開金鑰設定**4**種不同等級
 - 不確定（I don't know）
 - 不信任（No）
 - 勉強信任（Usually）
 - 完全信任（Yes, always）

Current trust for this key's owner is: **untrusted**

Make a determination in your own mind whether this key actually belongs to the person whom you think it belongs to, based on available evidence. If you think it does, then based on your estimate of that person's integrity and competence in key management, answer the following question:

Would you trust "Chung-Huang Yang <chyang@nknucc.nknu.edu.tw>" to act as an introducer and certify other people's public keys to you? (1=I don't know (default). 2=No. 3=Usually. 4=Yes, always.) ? 4

- PGP至少需要一個完全信任的簽署或兩個勉強信任的簽署，才能將一把金鑰視為有效，其命令如『**pgp -ke** <使用者ID>』
- 上圖是執行**pgp -ke** 設定對使用者ID為chyang@nknucc.nknu.edu.tw的信任程度
- 此外，**-ke**參數還有另一個用法，在此提出補充，如果**-ke**後面加的使用者ID是本身的ID而非他人，則作用就並非設定信任程度，而是編輯自己的金鑰資訊，如使用者基本資料或是更改通行密語等

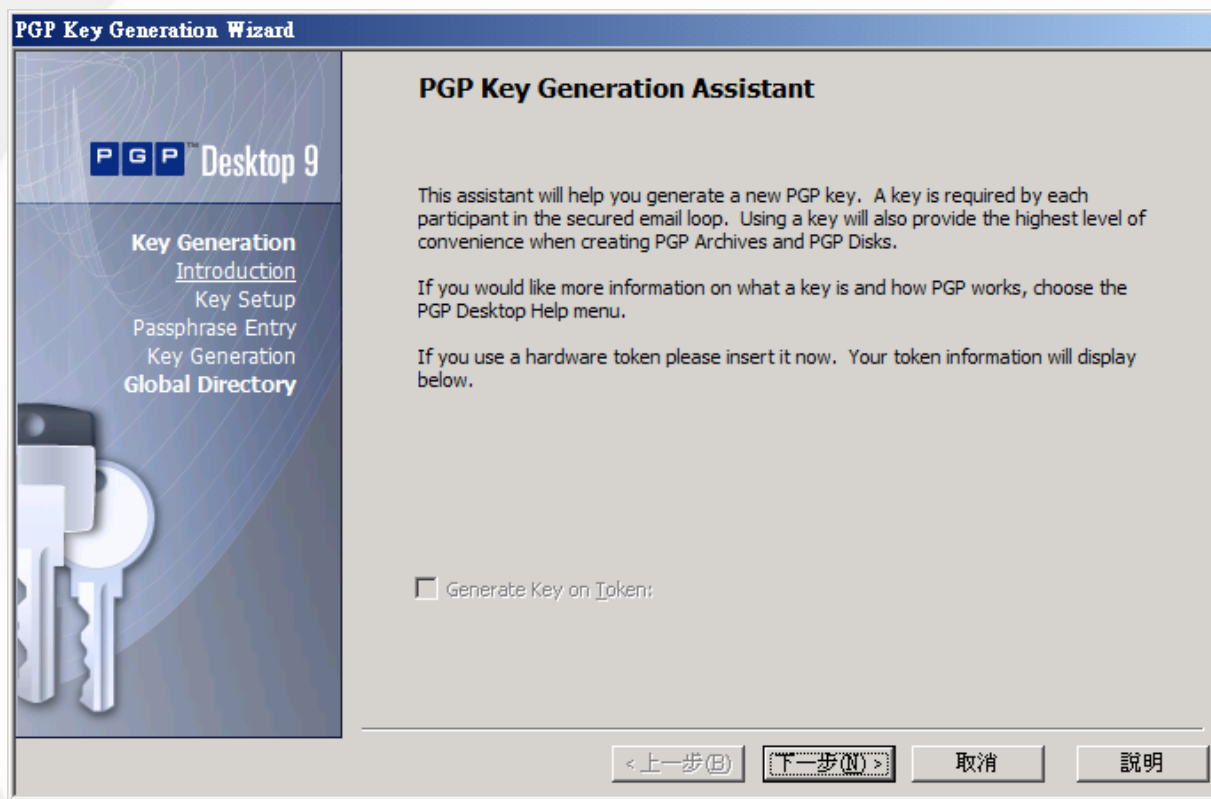


PGP的使用-Windows

- PGP的視窗版介面十分美觀，且功能完整，對於Windows系統的使用者而言，不啻是最佳的選擇
- 本節僅就試用版的功能提出介紹
- 讀者若想進一步瞭解**PGP Desktop**視窗版本的全部功能，除了付費購買取得正式版序號外，還可以參考試用版所提供的使用手冊，其內容亦包含所有**PGP Desktop**功能
- 試用版提供功能主要就是金鑰的使用與管理，以及**PGP Zip**壓縮檔的應用，下面就來說明在Windows XP安裝**PGP Desktop**後如何使用這些功能。



建立金鑰對



- 從主選單的[File]中選取[New PGP Key...]開啓建立金鑰之精靈程式
- 上圖即是建立金鑰對的啓始畫面



輸入金鑰的基本資料

PGP Key Generation Wizard

PGP™ Desktop 9

Key Generation
Introduction
Key Setup
Passphrase Entry
Key Generation
Global Directory

Name and Email Assignment

Every key pair must have a name associated with it. The name and email address let your correspondents know that the public key they are using belongs to you.

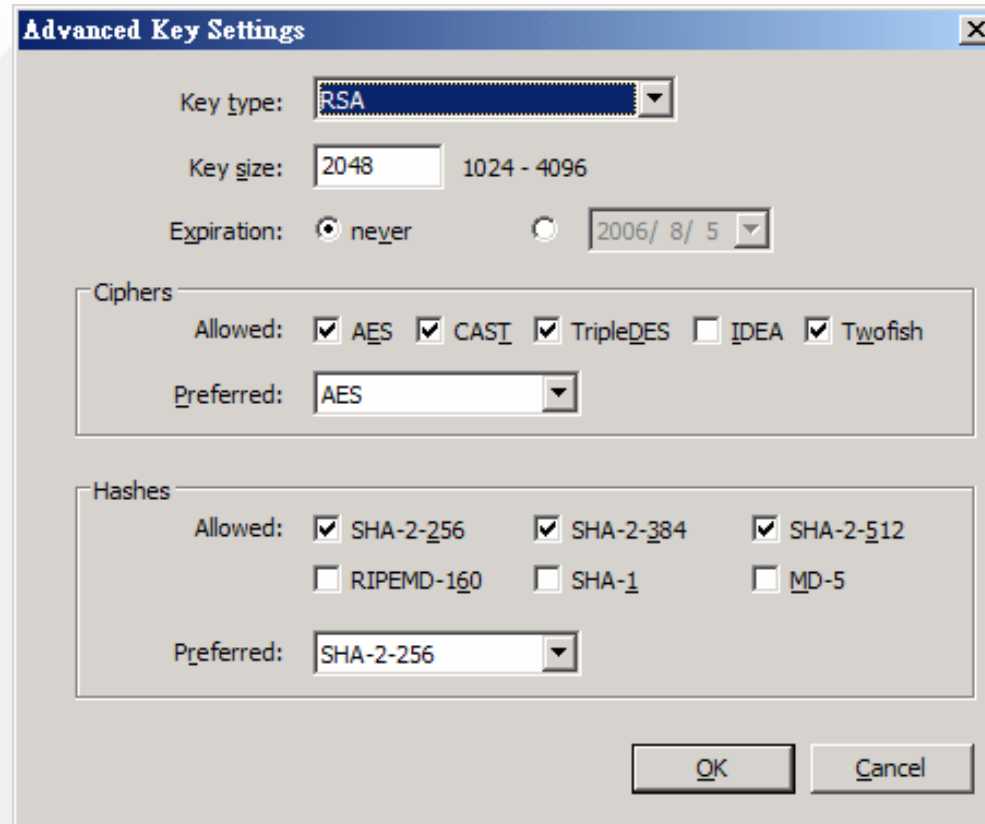
Full Name:

Primary Email:

Click Advanced for more key settings.

< 上一步(B) 下一步(N) > 取消 說明

- 上圖是讓使用者輸入基本資料，包括全名及電子郵件帳號，以作為識別金鑰ID之用

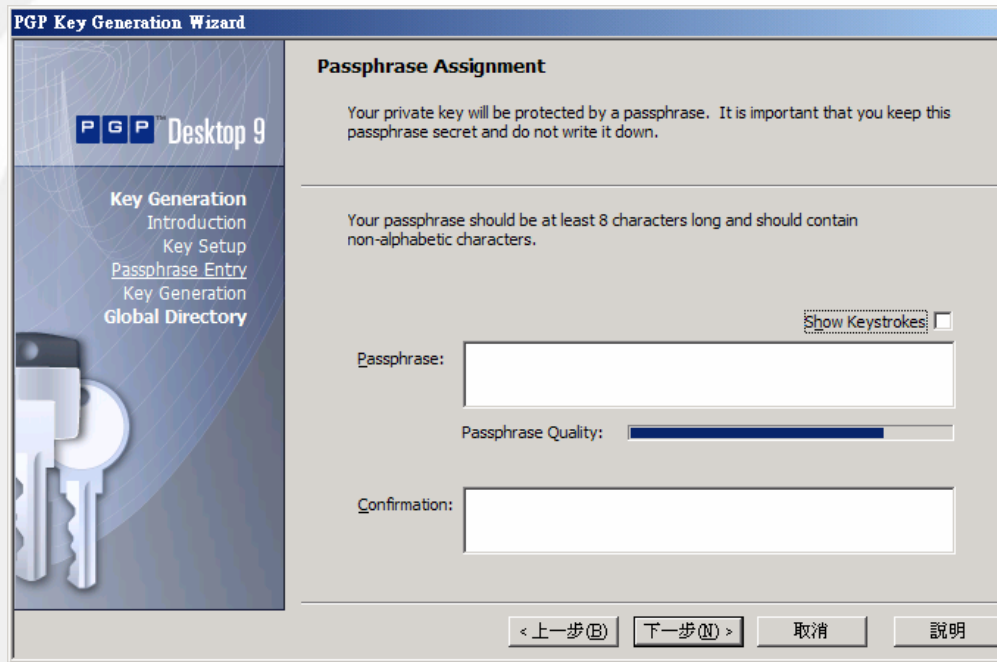


The image shows a screenshot of the 'Advanced Key Settings' dialog box. It contains the following settings:

- Key type:** RSA (selected from a dropdown menu)
- Key size:** 2048 (selected from a dropdown menu, with a range of 1024 - 4096 shown)
- Expiration:** ☒ never (selected), ☐ 2006/ 8/ 5 (available)
- Ciphers:**
 - Allowed:** ☒ AES, ☒ CAST, ☒ TripleDES, ☐ IDEA, ☒ Twofish
 - Preferred:** AES (selected from a dropdown menu)
- Hashes:**
 - Allowed:** ☒ SHA-2-256, ☒ SHA-2-384, ☒ SHA-2-512, ☐ RIPEMD-160, ☐ SHA-1, ☐ MD-5
 - Preferred:** SHA-2-256 (selected from a dropdown menu)

At the bottom right, there are 'OK' and 'Cancel' buttons.

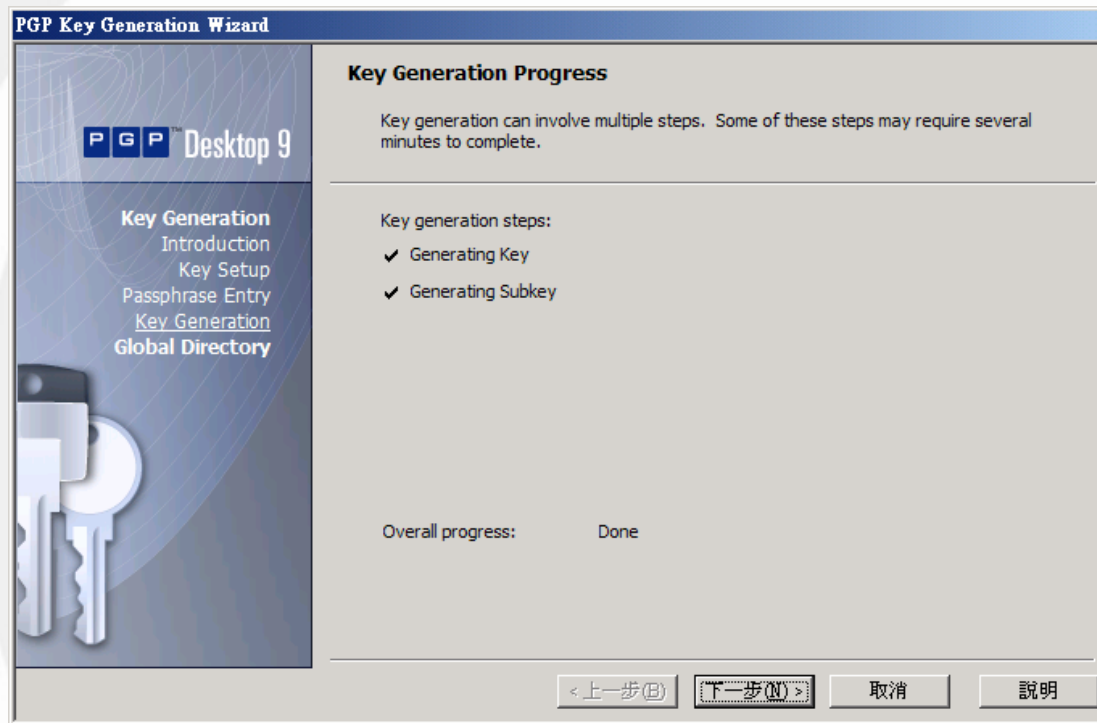
- **[Advanced...]**可設定進階選項，包括金鑰使用的演算法、金鑰長度、有效日期、偏好使用的對稱式加密演算法及雜湊函數演算法等
- 設定畫面如上圖



- 接著是設定存取私密金鑰的通行密語（如上圖），在畫面中間的**[Passphrase Quality:]**列會顯示使用者所設定的密語品質比例，換言之，就是密語的安全程度，品質愈高表示愈安全愈不易遭到破解
- 這個部分使用者應審慎設定，建議至少達到評估比例的一半以上。另外在**[Passphrase:]**密語輸入欄位的右上方有個**[Show Keystrokes]**選項，勾選之後便會顯示使用者所輸入的密語字串以方便檢視



成功建立金鑰對



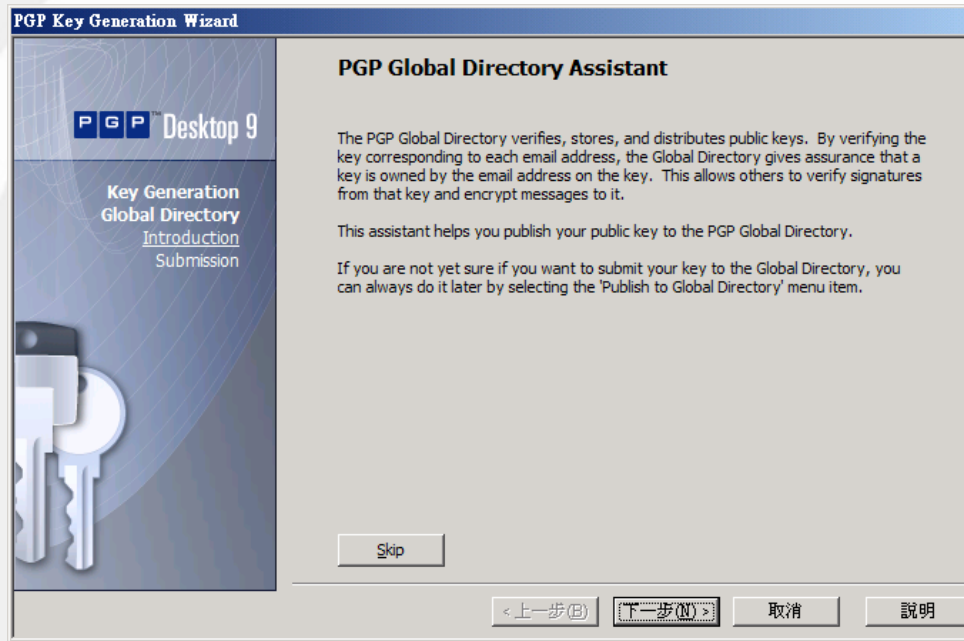
- 完成所有設定後，下一步便是產生金鑰對，而金鑰對建立成功如圖上所示
- 由於這次建立金鑰所使用的公開金鑰演算法設定為**RSA**，因此數位簽章用的金鑰及加解密用的金鑰會接續產生



將公開金鑰發佈到PGP Global Directory的設定畫面

金禾資訊

伴 您 學 習 成 長 的 每 一 天



- 上圖是在完成金鑰對後所呈現的畫面，此功能主要是讓使用者將自己的公開金鑰發佈到PGP Global Directory，其作用在於驗證、儲存及發佈所有人的PGP公開金鑰
- 在此先將它省略。如果讀者以後考慮要將自己的公開金鑰經由PGP Global Directory與他人交換，可從主選單的[Keys]子選單執行[Publish to Global Directory]功能

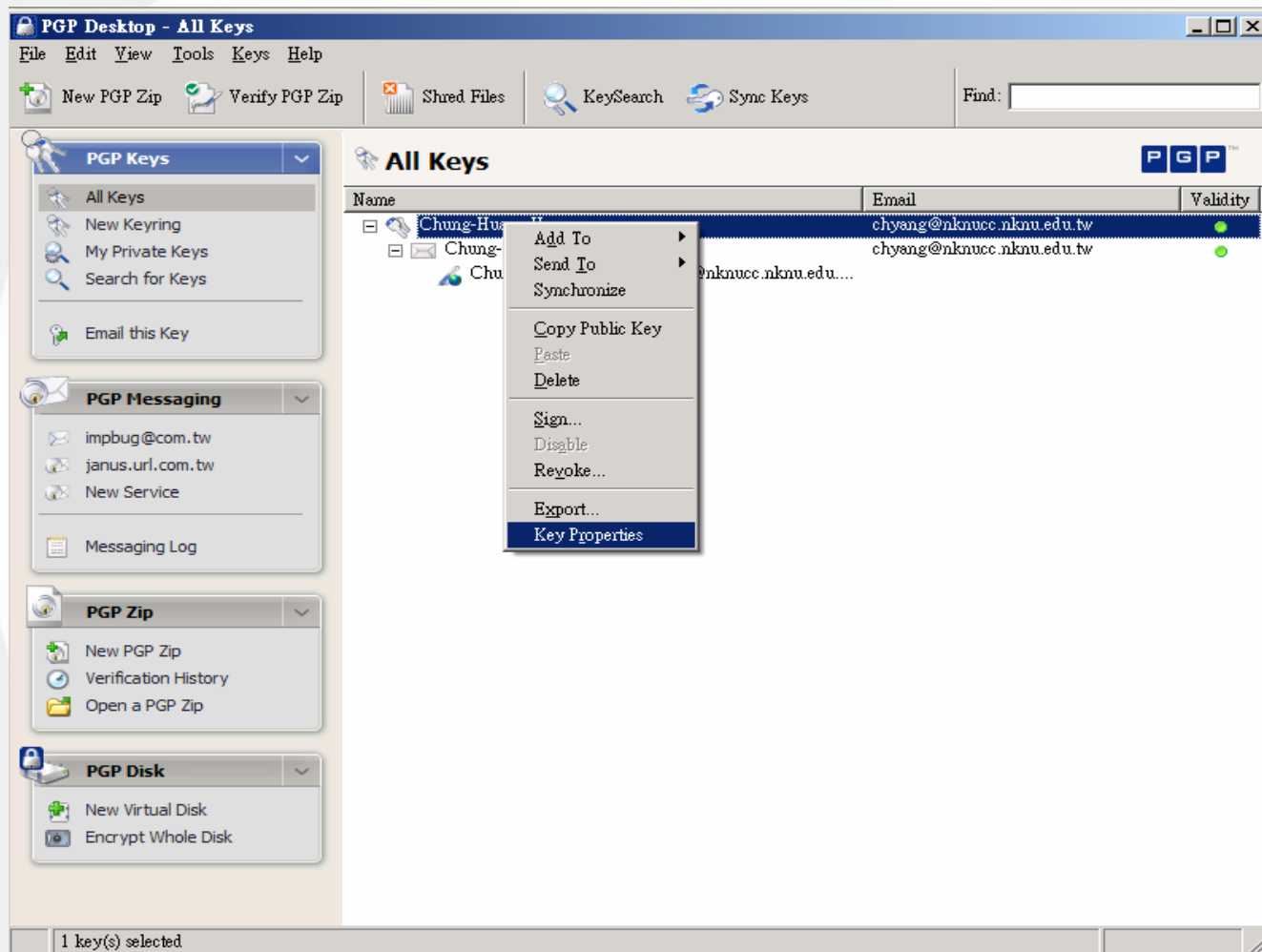


金鑰的儲存

- 若以Administrator身份建立完畢後，鑰匙環檔會儲存在
 - C:\Documents and Settings\Administrator\Application Data\PGP Corporation\PGP目錄底下



檢視金鑰內容




- 金鑰對成功建立後，則可檢視金鑰之屬性，如上圖




檢視金鑰的屬性

Chung-Huang Yang <chyang@nknuc.nknu.edu.tw>

Add Email Address Request Certificate Change Passphrase




 Chung-Huang Yang chyang@nknuc.nknu.edu.tw


ID	0x97D12725	Created	2005/8/8
Type	RSA	Expires	Never
Size	2048/2048	Group	No
Trust	Implicit	Cipher	AES-256
Validity	Valid	Hash	SHA-2 256
Enabled	Yes	Compression	ZLIB
Keyserver	None		




Fingerprint  Copy




Hexadecimal Biometric

0E46 B9C4 DFA9 D77F AC6C
BB65 D027 4A2C 97D1 2725

Subkeys  Revoke  Remove  Add

Valid from	Expires	Size	ID
 2005/8/8	Never	2048	0xC81B5F...

ADK  Update  Remove  Add

Revokers  Update  Remove  Add



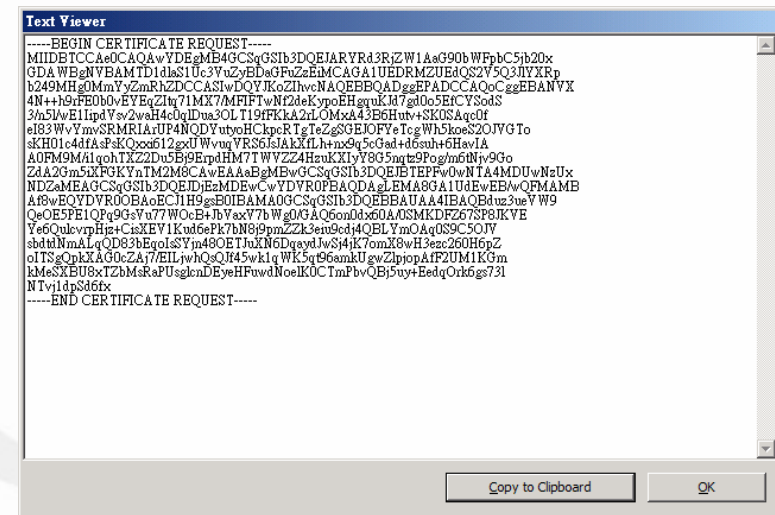
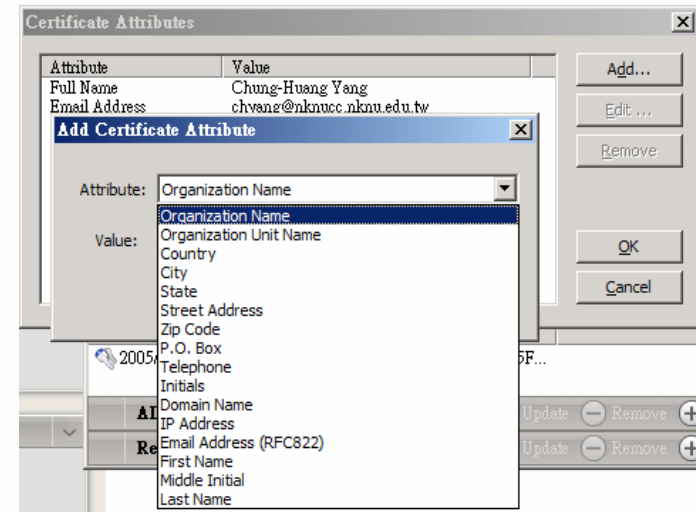
金鑰屬性

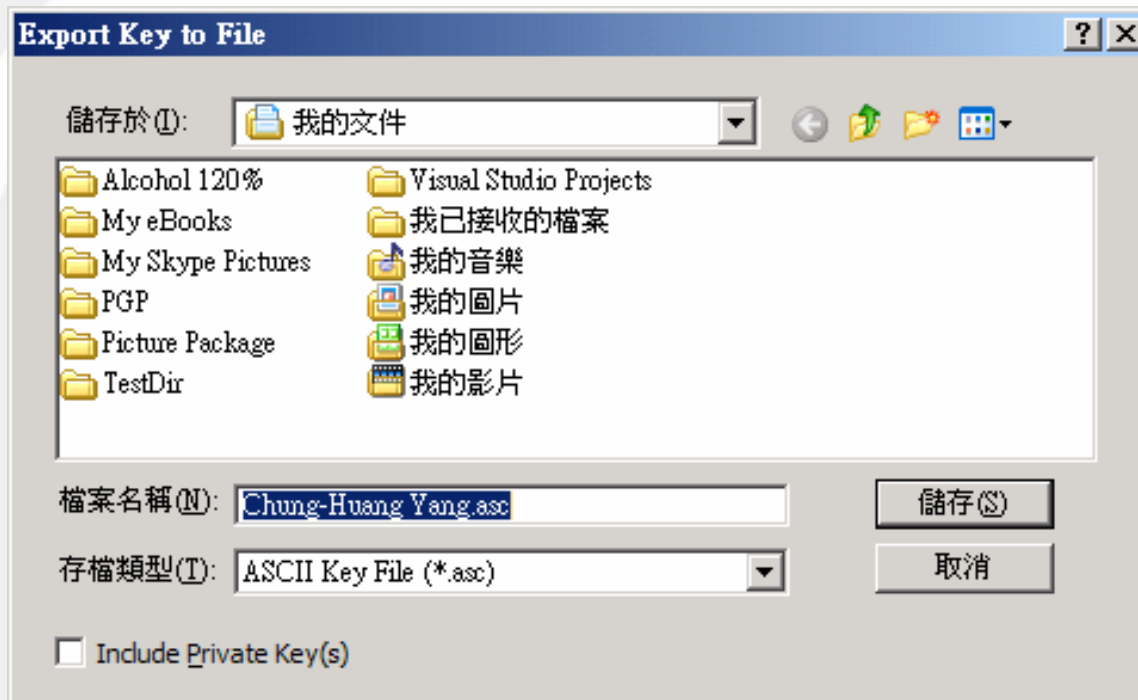
- 金鑰屬性的畫面，內容包括使用者名稱、電子郵件帳號及以下資訊：
 - 照片：畫面左上角鑰匙圖的部分可以置換成自己照片，若檢視別人的金鑰則顯示對方照片
 - ID：以32個bits（4個bytes）表示該金鑰的ID
 - Type：金鑰使用的演算法
 - Size：金鑰的長度
 - Trust：設定對該金鑰的信任程度，如果是自己的金鑰，只能設定None或Implicit（意指絕對信任），對於別人的金鑰則可以設定None、Marginal或Trusted三種信任程度
 - Validity：金鑰的有效性
 - Enabled：設定金鑰是否有用
 - Keyserver：設定金鑰伺服器
 - Created：金鑰的建立日期
 - Expires：金鑰的到期日
 - Group：金鑰的群組，變更需要輸入通行密語
 - Cipher：設定加解密偏好使用的演算法，變更需要輸入通行密語
 - Hash：設定雜湊函數演算法，變更需要輸入通行密語
 - Compression：設定訊息壓縮使用的演算法，變更需要輸入通行密語
 - Fingerprint：檢視金鑰的指紋值
 - Subkeys：檢視子金鑰
 - ADK：檢視額外的加密金鑰（Additional Decryption Key）清單
 - Revokers：檢視撤銷金鑰者的清單



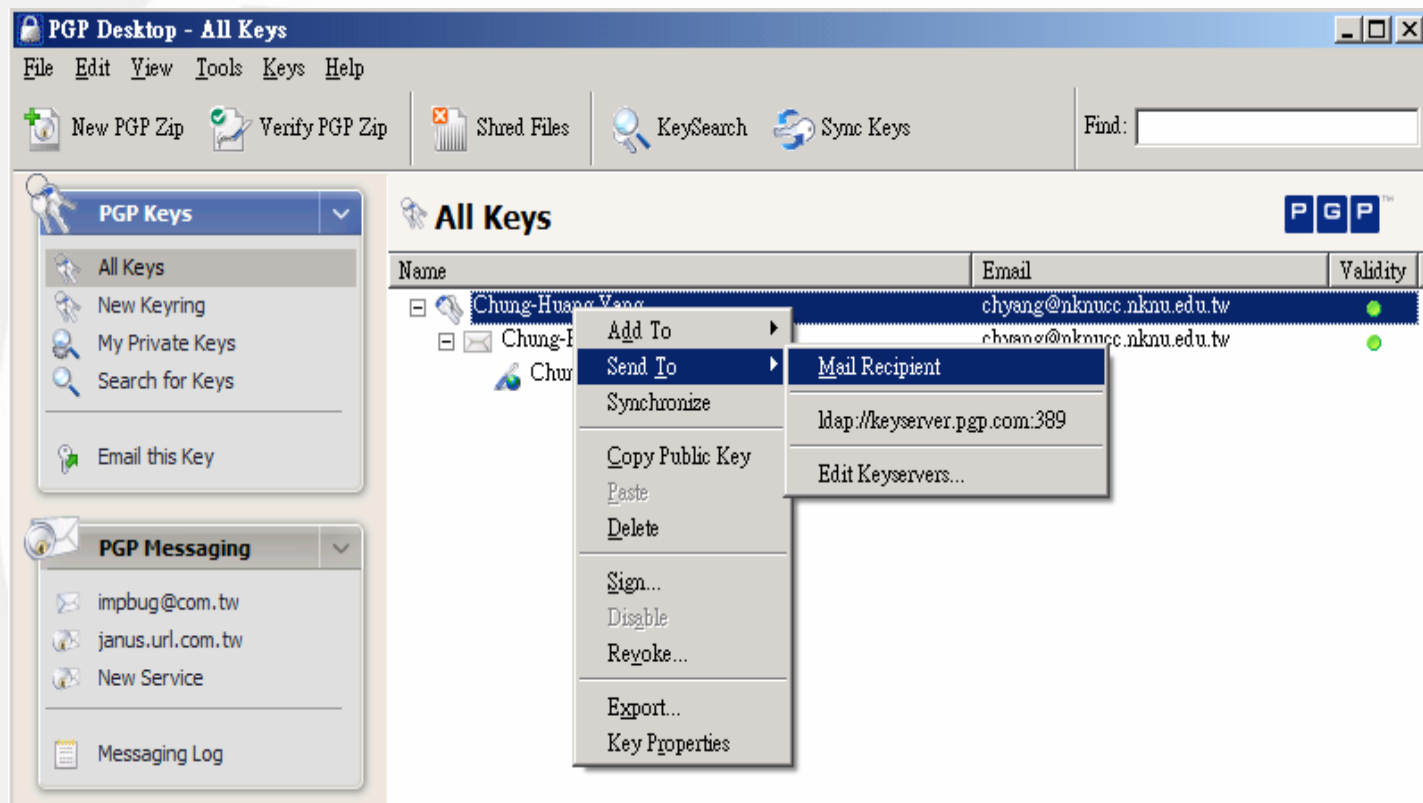
檢視金鑰(其他)

- 此外，在檢視金鑰畫面的最上方，還有三個子功能：
 - Add Email Address**：新增使用者名稱及電子郵件帳號
 - Request Certificate**：為該金鑰要求建立一個CA憑證申請，可設定憑證要包含的額外資訊，如右上圖；而產生後的CA憑證申請內容會暫存在PGP Desktop的剪貼簿中，如右下圖
 - Change Passphrase**（變更通行密語）：必須先輸入原先的通行密語才能進行變更





- 若要將憑證儲存成檔案，請點選金鑰後按滑鼠右鍵選取[**Export...**]功能，便會開啓如上圖的畫面
- 預設檔名可以是使用者名稱再加上.asc副檔名，此檔案可用一般純文字編輯器檢視
- 如果匯出的目的是要自己備份，可以勾選下方[**Include Private Key(s)**]將私鑰一併匯出



- 可直接將檔案以電子郵件方式寄送給對方



準備傳送PGP憑證



- PGP將會開啓預設的電子郵件軟體並附加PGP憑證（公開金鑰）檔，以便使用者直接傳送



新增金鑰伺服器設定

New Server

Server Information

Type: PGP Keyserver LDAP

Address:

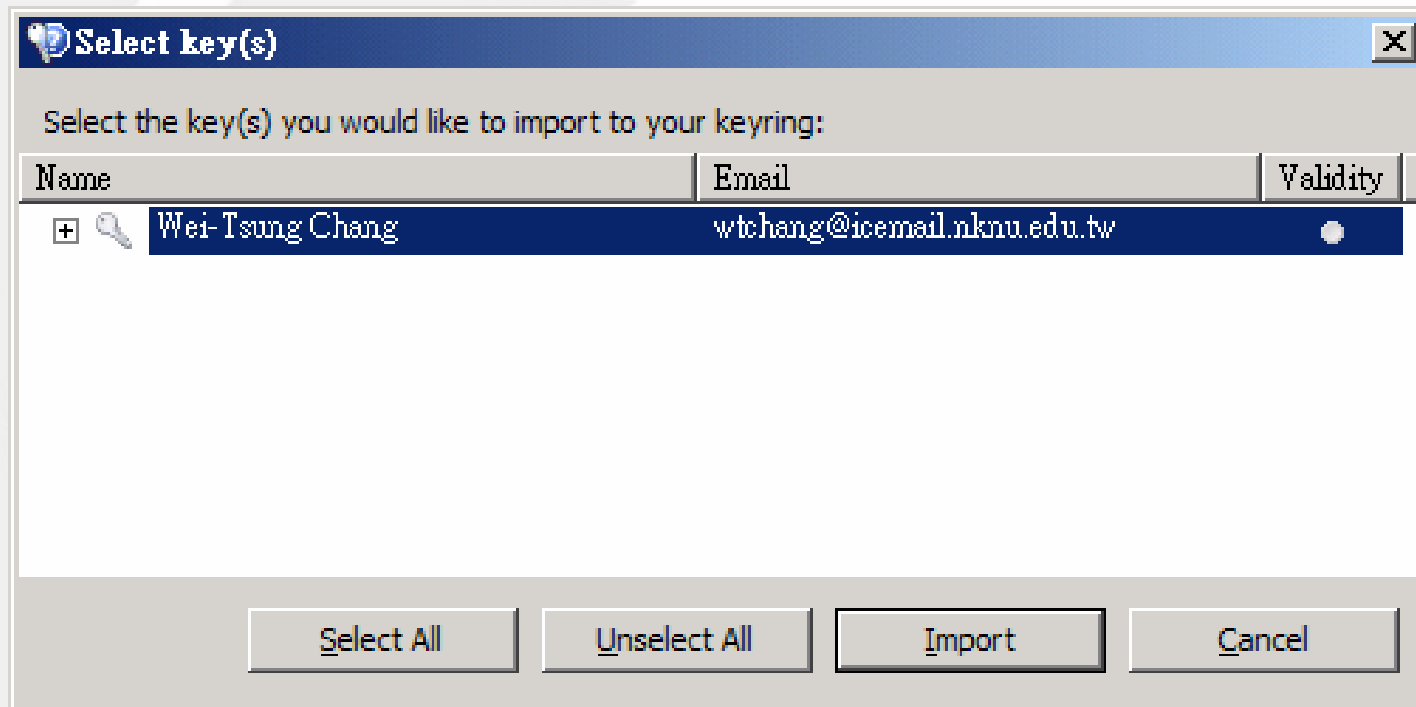
Port:

Base DN:

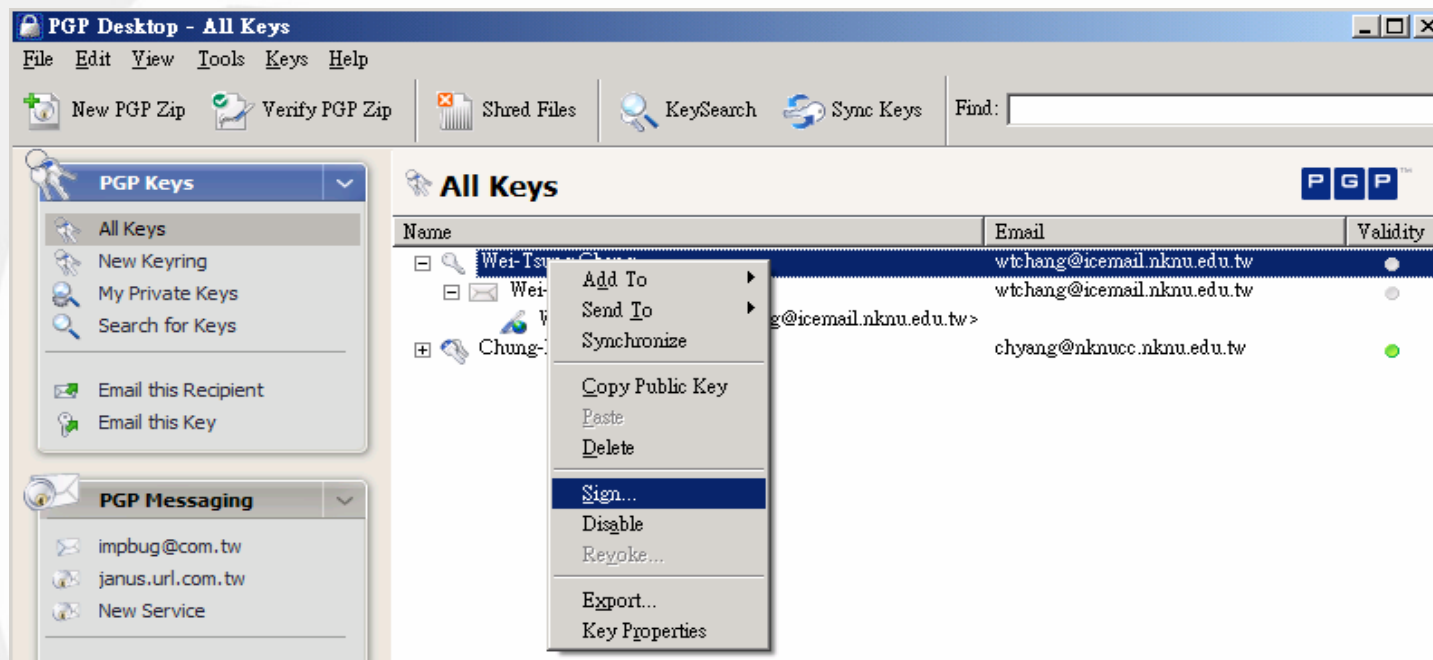
Authentication Certificate: No certificates available

OK Cancel

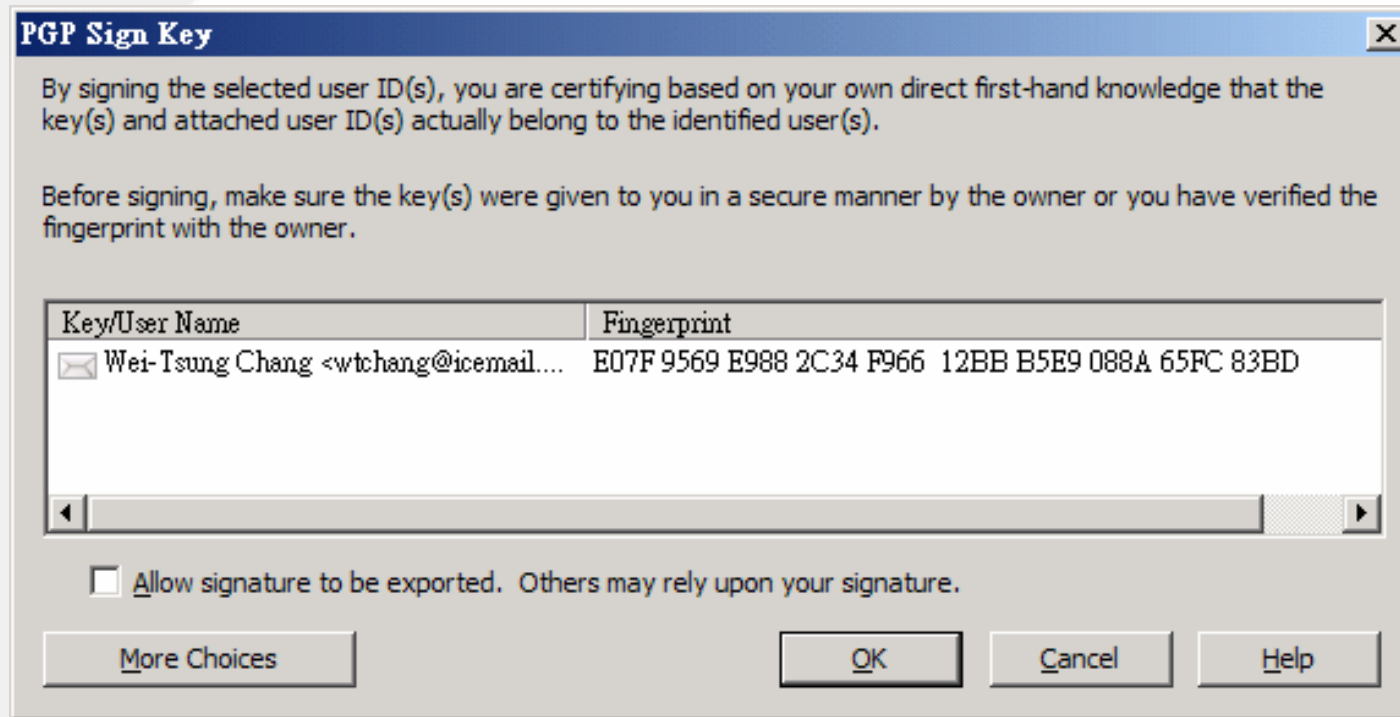
- 或者是傳送至金鑰伺服器，而PGP允許儲存多個金鑰伺服器，以供日後選用，設定畫面如上圖



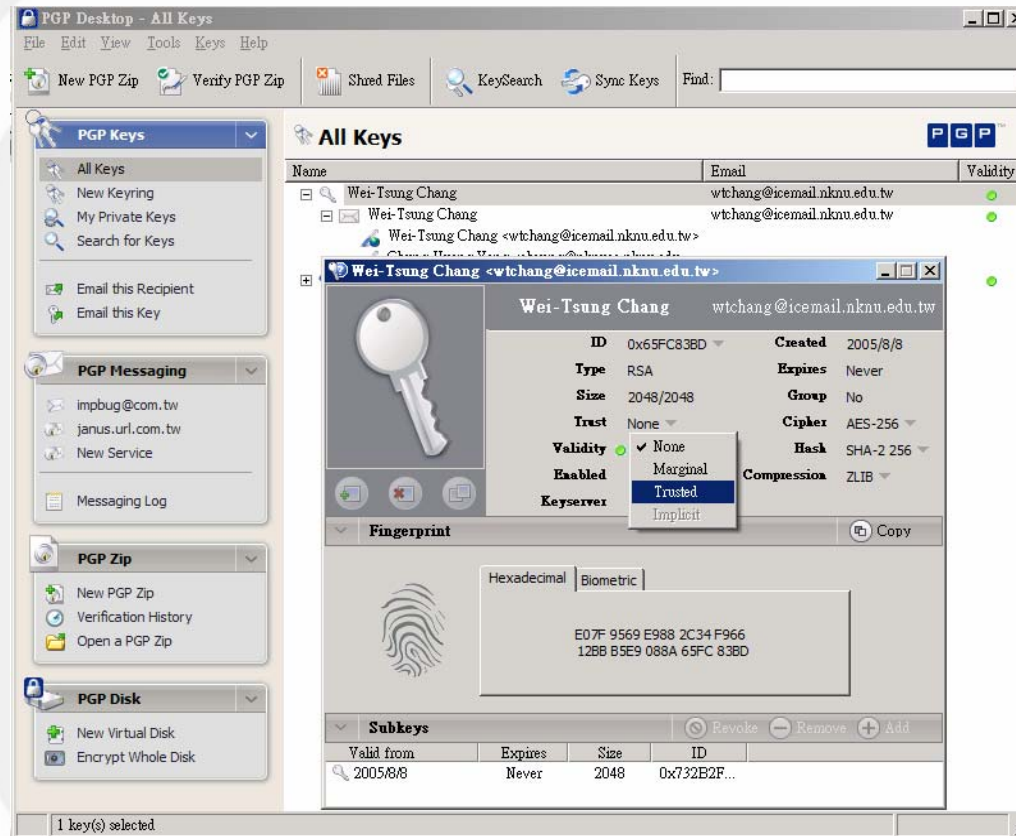
- 當收到對方PGP憑證，可點選主選單的[File]子選單下的[Import...]功能，並選取檔案，如“Wei-Tsung Chang.asc”
- 執行後的畫面如上圖，便可將其憑證匯入自己的鑰匙環中



- 匯入他人PGP憑證後，就是要簽署對方的公開金鑰使其有效，簽署的執行方式如上圖



- 上圖便是執行簽署後的畫面，PGP會顯示該公開金鑰的指紋值
- 使用者可依此資訊確認這公開金鑰確實是通訊對方所有，但簽署時必須輸入通行密語



- 要為對方的公開金鑰設定信任等級，同樣要先檢視其金鑰內容屬性，可直接在[Trust]欄位變更即可

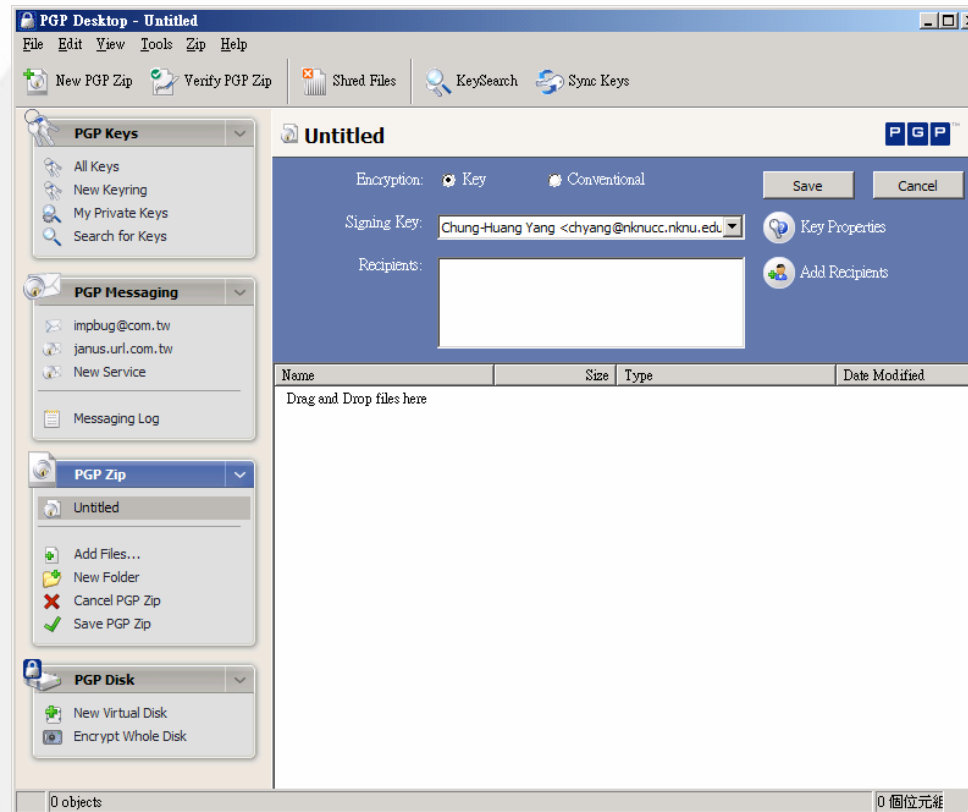


PGP Zip的使用

- PGP Zip的功能，是將檔案的加解密及數位簽章整合在同一操作介面
- 用法與WinZip這類壓縮軟體差不多，可以針對某些檔案或資料夾加密或簽章，並存成.pgp檔
- 由於PGP服務與Windows系統整合，並在開機時自動啓動，因此在系統預設的快捷工具列亦可使用此項功能，使用者可以在檔案總管檢視畫面時，隨時將任何檔案或資料夾做成.pgp檔



PGP Zip的功能畫面



- 首先介紹透過PGP Desktop本身的介面來使用PGP Zip，欲建立PGP Zip檔時，請在主畫面左邊的[PGP Zip]功能表選取[New PGP Zip]，或從工具列點按[New PGP Zip]按鈕執行



PGP Zip的加密方式

- 有兩種選項，分別如下：
- **Key**：使用原先以PGP建立的私密金鑰作加密，這是常用來與他人進行秘密通訊時使用，因此必須選擇接收者（**Recipient**），而接收者可以是多個，其設定法可直接以[**Recipients:**]欄位右邊的[**Add Recipients**]開啓點選即可。如果接收者僅設自己的話，作用如同為個人的檔案實施加密保存
- **Conventional**：傳統用來對個人的檔案以對稱式加密演算法加密保存的方式，並非以原先使用PGP建立的私密金鑰作為對稱式加密的金鑰，則是必須另外輸入一組密碼作為加解密時的金鑰



- 如果要對PGP Zip檔作數位簽章的話，還必須在**[Signing Key:]**欄位選取自己的金鑰
- 在畫面下方標示**[Drag and Drop files here]**的地方，可讓使用者從檔案總管拖曳檔案及資料夾，或是直接在上面以滑鼠右鍵點選快捷工具列的**[Add Files...]**功能選取要加入的檔案及資料夾
- 若選取的資料夾中還有其他的子資料夾，PGP會一起包含進來



PGP Desktop - Untitled

File Edit View Tools Zip Help

New PGP Zip Verify PGP Zip Shred Files KeySearch Sync Keys

PGP Keys

- All Keys
- New Keyring
- My Private Keys
- Search for Keys

PGP Messaging

- imbug@com.tw
- janus.url.com.tw
- New Service
- Messaging Log

PGP Zip

- Untitled
- Add Files...

Untitled

Encryption: ☒ Key ☐ Conventional

Signing Key: Chung-Huang Yang <chyang@nknuc.nknu.edu>

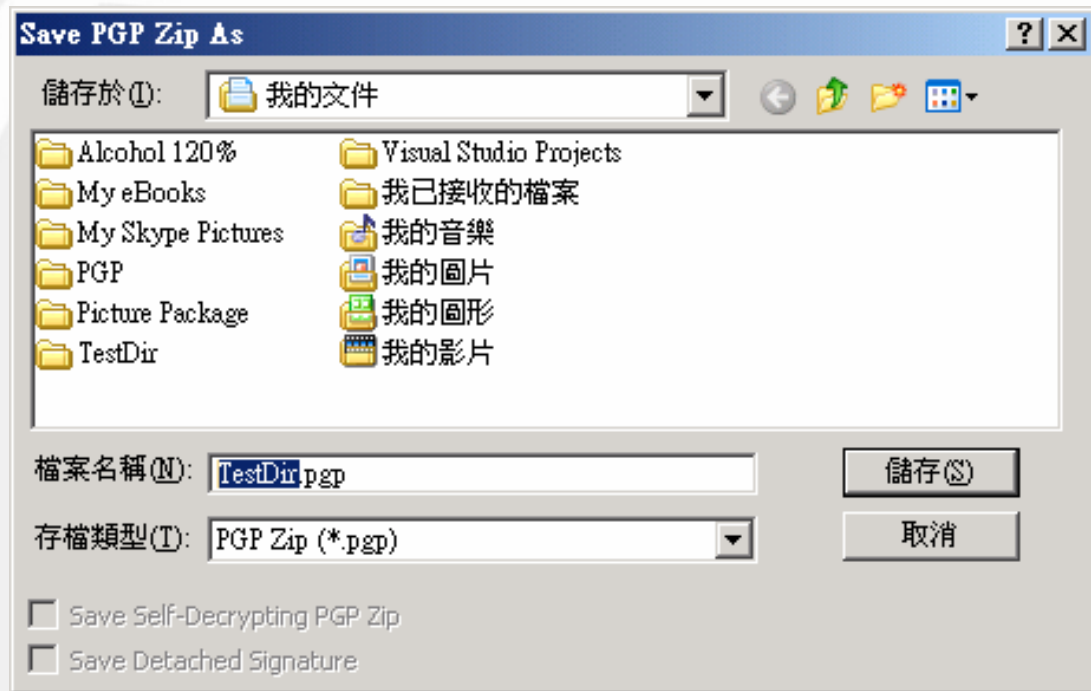
Recipients: Wei-Tsung Chang <wtchang@icemail.nkn...>

Save Cancel

Key Properties

Add Recipients

Name	Size	Type	Date Modified
TestDir		Folder	2005/8/6 下午 04:48
Testfile-1.pdf	383 KB	PDF Document	2005/6/16 上午 08:41
Testfile-2.txt	808 個位元組	文字文件	2005/6/19 下午 08:02
Testfile-3.pdf	24.5 MB	PDF Document	2005/7/28 下午 06:29
Testfile-4.doc	695 KB	Microsoft Word 文件	2005/5/30 上午 08:19
Testfile-5.doc	51.5 KB	Microsoft Word 文件	2005/7/18 下午 07:10
Testfile-6.txt	559 個位元組	文字文件	2005/8/5 下午 09:04
Testfile-7.pps	828 KB	Microsoft PowerPoint 投影片放映	2003/12/3 下午 04:11

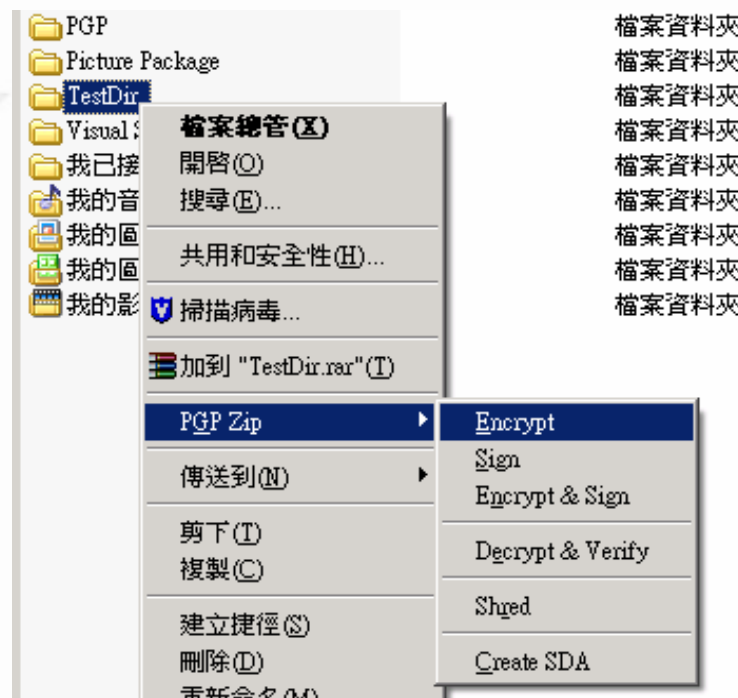


- 使用者亦可在此自行建立新的資料夾，以規劃放置要儲存的檔案，或者是針對某資料夾刪去不要包含的檔案，而使用者設定完畢後，直接按[**Save**]按鈕執行，便會儲存成.pgp檔



開啓PGP Zip快捷工具列

- 請點選任何檔案或資料夾
- 按下滑鼠右鍵開啓系統快捷工具列，以顯示PGP Zip的功能

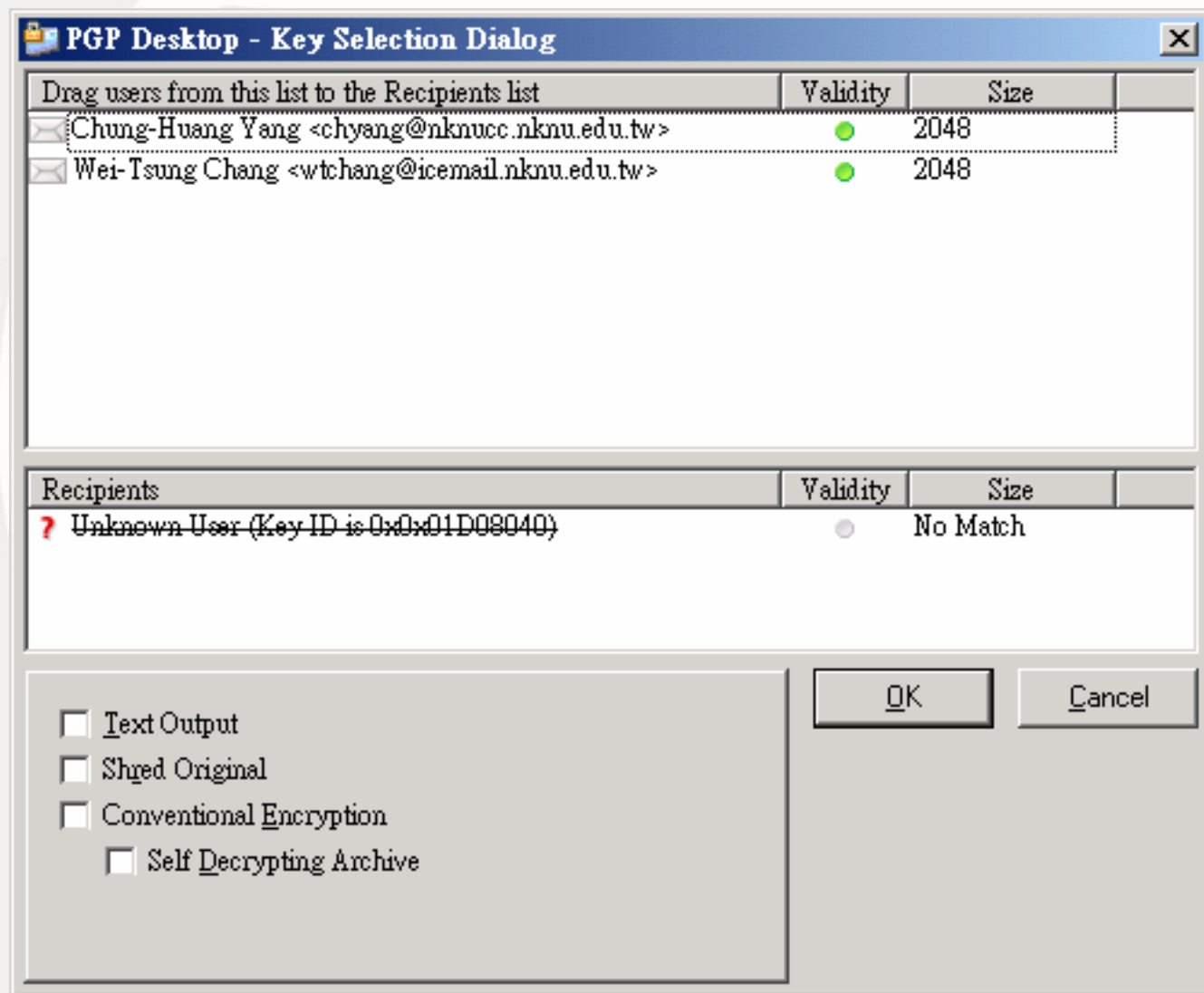


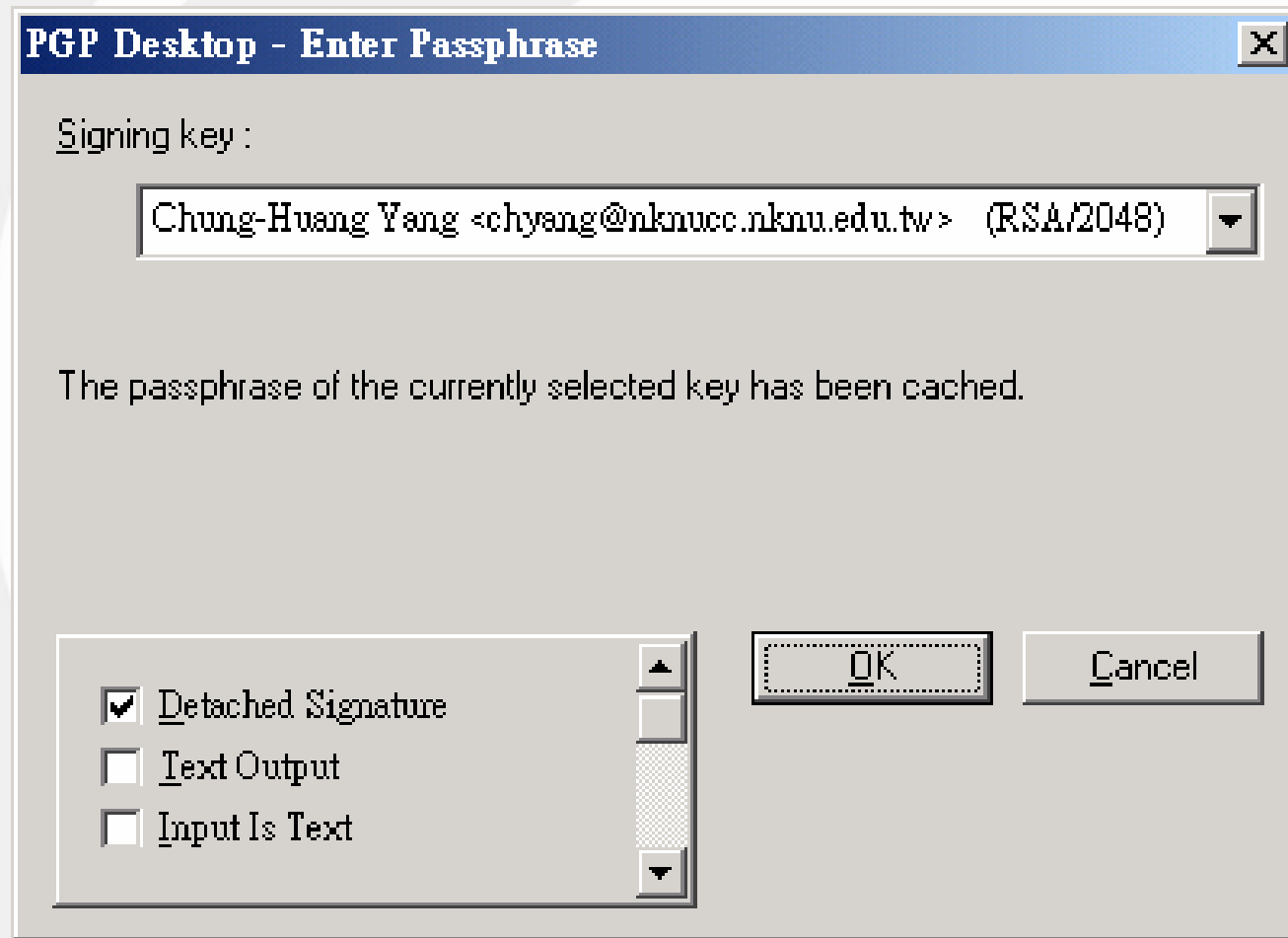


- PGP Zip的快捷工具列可提供以下功能：
- **Encrypt**：僅做加密，同樣會出現接收者清單供使用者挑選。還可選擇其他功能，如：在加密之後粉碎（**Shred Original**）原始檔案，意思就是徹底刪除原始檔案使其完全無法復原；或是建立自解檔（**Self Decrypting Archive**）
- **Sign**：僅做數位簽章，必須要先有用來做簽章的私密金鑰，及輸入通行密語取得私密金鑰。如果選定的檔案為多個，可以選擇針對每個檔案個別做分離式數位簽章檔，預設儲存檔名為原始檔名附加.sig副檔名，而儲存路徑則同原始檔案



- **Encrypt & Sign**：對選定的檔案或資料夾所壓縮而成的PGP Zip檔，同時做數位簽章及加密動作
- **Decrypt & Verify**：對PGP Zip檔進行數位簽章驗證及解密
- **Shred**：粉碎所選定的資料夾或檔案，但不限於PGP Zip檔，一般檔案也可以使用，須注意執行此項功能後，其檔案將無法復原，會使用此功能通常主要是考量到某些較具機密性的檔案，已無保存在該磁碟中的必要，才會做此處理
- **Create SDA**：產生自動解壓縮解密的檔案（**Self Decrypting Archive**），建立之時需要輸入一組密碼（**Passphrase**）







針對所有檔案建立個別的分離式數位簽章

金禾資訊

伴 您 學 習 成 長 的 每 一 天

TestDir

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 資料夾

網址(D) C:\Documents and Settings\Administrator\My Documents\TestDir

資料夾	名稱	大小	類型
桌面 我的文件 Alcohol 120% My eBooks My Skype Pictures PGP Picture Package TestDir Visual Studio Projects 我已接收的檔案 我的音樂 我的圖片 我的圖形 我的影片 我的電腦 System (C:)	Testfile-1.pdf	384 KB	PDF Document
	Testfile-1.pdf.sig	1 KB	PGP Detached Signat...
	Testfile-2.txt	1 KB	文字文件
	Testfile-2.txt.sig	1 KB	PGP Detached Signat...
	Testfile-3.pdf	25,178 KB	PDF Document
	Testfile-3.pdf.sig	1 KB	PGP Detached Signat...
	Testfile-4.doc	695 KB	Microsoft Word 文件
	Testfile-4.doc.sig	1 KB	PGP Detached Signat...
	Testfile-5.doc	52 KB	Microsoft Word 文件
	Testfile-5.doc.sig	1 KB	PGP Detached Signat...
	Testfile-6.txt	1 KB	文字文件
	Testfile-6.txt.sig	1 KB	PGP Detached Signat...
	Testfile-7.pps	828 KB	Microsoft PowerPoin...
	Testfile-7.pps.sig	1 KB	PGP Detached Signat...



PGP Desktop的其他功能

- PGP Desktop還有一些功能，本節未作介紹，請讀者自行測試
 - **PGP Messaging**：結合電子郵件軟體或是即時通訊軟體（如AIM）作安全傳輸
 - **PGP Whole Disk Encryption**：可以針對整個硬碟或磁碟機加密，包含開機磁區
 - **PGP Virtual Disk volumes**：對虛擬磁碟機使用的空間作加密
- 另外由於本章所使用的PGP Desktop為試用版，有些特別的主要功能並不完全支援，因此無法在此作詳細介紹



原始碼重要模組簡介

- **PGP**密碼學應用包含了數種知名的公開金鑰演算法、對稱式加密演算法及雜湊函數演算法，而這些演算法不僅在密碼學領域極為重要，同時更是網路安全應用的要素，透過使用**PGP**，可瞭解這些個別的技術是如何整合，而提供完備的安全服務，以建構安全網路使用環境
- 以下將就**PGP Desktop 9.0**的原始碼分表簡要說明其密碼相關演算法的主要模組，讀者若要配合查閱原始碼檔案，請將本書所附光碟中的**PGP**目錄底下的**Source**子目錄裡面的**PGPDesktop902Source.zip**解出**PGPDesktop902SourceInner.zip**，再將後者解開到自定的目錄，如D:\PGPDesktop902SourceInner即可



公開金鑰演算法相關模組

所在目錄：..\libs2\pgpsdk\priv\crypto\pubkey

檔案名稱	主要功能
pgpAltRSAGlu.c	針對RSA Data Security公司的RSAREF密碼工具的存取介面。
pgpBSRSAGlu.c	針對RSA Data Security公司的BSafe密碼工具的存取介面。
pgpDSAKey.h、pgpDSAKey.c	DSA數位簽章演算法程式。
pgpDSATests.c	DSA數位簽章演算法測試程式。
pgpECKey.h、pgpECKey.c	橢圓曲線演算法。
pgpElGKey.h、pgpElGKey.c	ElGamal加密演算法。
pgpESK.h、pgpESK.c	加密用會談金鑰的處理程式。
pgpFixedKey.h、pgpFixedKey.c	單一/固定的PGP金鑰解密處理程式。
pgpKeyMisc.h、pgpKeyMisc.c	公開金鑰模組的其他輔助處理函數，例如有關PKCS相容性的處理。
pgpKeySpec.h、pgpKeySpec.c	PGP憑證的其他資訊內容（不包含公開金鑰）處理，如PGP的版本資訊、公開金鑰的建立日期、公開金鑰使用的演算法...等。
pgpMakeSig.h、pgpMakeSig.c	從私密金鑰、雜湊訊息或其他資料產生簽章封包。
pgpMSRSAGlu.h、pgpMSRSAGlu.c	針對微軟CryptoAPI的存取介面。
pgpP11Key.h、pgpP11Key.c	PKCS #11的存取介面。
pgpPubKey.h、pgpPubKey.c	PGP公開金鑰及私密金鑰的結構。
pgpPublicKey.c	公開金鑰及私密金鑰的操作，如用以加解密、數位簽章的簽章與驗章...等。
pgpRSAGlu.c	介於大數運算及RSA操作的存取介面。
pgpRSAKey.h、pgpRSAKey.c	RSA演算法。
pgpRSATests.c	RSA演算法測試程式。
pgpSig.h、pgpSig.c	數位簽章的操作，如產生簽章、檢驗簽章及雜湊函數計算...等。
pgpTokenConf.h、pgpTokenConf.c、 pgpTokenLib.h、pgpTokenLib.c	針對Token（如Smart card）設定及存取的相關函數。

所在目錄：..\libs2\pgpsdk\priv\crypto\cipher

檔案名稱	主要功能
pgpAES.h、pgpAESboxes.h、pgpAES.c	AES演算法。
pgpAESTests.c	AES測試程式。
pgpArc4.h、pgpArc4.c	ARC4（Alleged RC4）演算法。
pgpBlowfish.h、pgpBlowfish.c	Blowfish演算法。
pgpCAST5.h、pgpCASTBox5.h、pgpCAST5.c	CAST5演算法。
pgpCBCPriv.h、pgpCBC.c	CBC操作模式處理程式。
pgpCFBPriv.h、pgpCFB.c	CFB操作模式處理程式。
pgpDES3.h、pgpDES3.c、pgpDES3_68K.c	3DES（TripleDES）演算法。
pgpDES3Tests.c,	3DES演算法測試程式。
pgpIDEA.h、pgpIDEA.c	IDEA演算法。
pgpRC2.h、pgpRC2.c	RC2演算法。
pgpSymmetricCipherPriv.h、 pgpSymmetricCipherPriv.c	對稱式加密演算法的選擇處理程式。
pgpTwofishAES.h、pgpTwofishPlatform.h、 pgpTwofishTable.h、pgpTwofish.c	Twofish演算法。

所在目錄：..\libs2\pgpsdk\priv\crypto\hash

檔案名稱	主要功能
pgpChecksum.h、pgpChecksum.h	計算SHA-256的訊息摘要。
pgpHashPriv.h、pgpHash.c	雜湊函數演算法的選擇處理程式。
pgpHMAC.c	HMAC計算程式。
pgpHMACTests.c	HMAC測試程式。
pgpMD2.h、pgpMD2.c	MD2演算法。
pgpMD5.h、pgpMD5.c	MD5演算法。
pgpRIPEMD160.h、pgpRIPEMD160.c	RIPEMD160演算法。
pgpSHA2.h	SHA-2演算法程式標頭檔。
pgpSHA256.c、pgpSHA384_512.c	SHA-2演算法（for 32位元電腦）
pgpSHA384_512_64.c	SHA-2演算法（for 64位元電腦）。
pgpSHATests.c	SHA-2演算法測試程式。



- P. R. Zimmermann, *The Official PGP User's Guide*, The MIT Press, 1995
- PGP Corporation, "An Introduction to Cryptography", \<PGP Desktop Installation Directory>\Documentation\Intro To Crypto.pdf, July 2005
- PGP Corporation, "PGP Desktop 9.0 for Windows User's Guide", \<PGP Desktop Installation Directory>\Documentation\ PGP Desktop User's Guide.pdf, July 2005
- S. Garfinkel, *PGP: Pretty Good Privacy*, O'Reilly & Associates, Inc., 1995
- W. Stallings, *Cryptography and Network Security, 3rd Edition*, Prentice-Hall, Inc., November 2002